Contents

www.pwc.com/security

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 .

Eye of the storm

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

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 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.

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.

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

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.

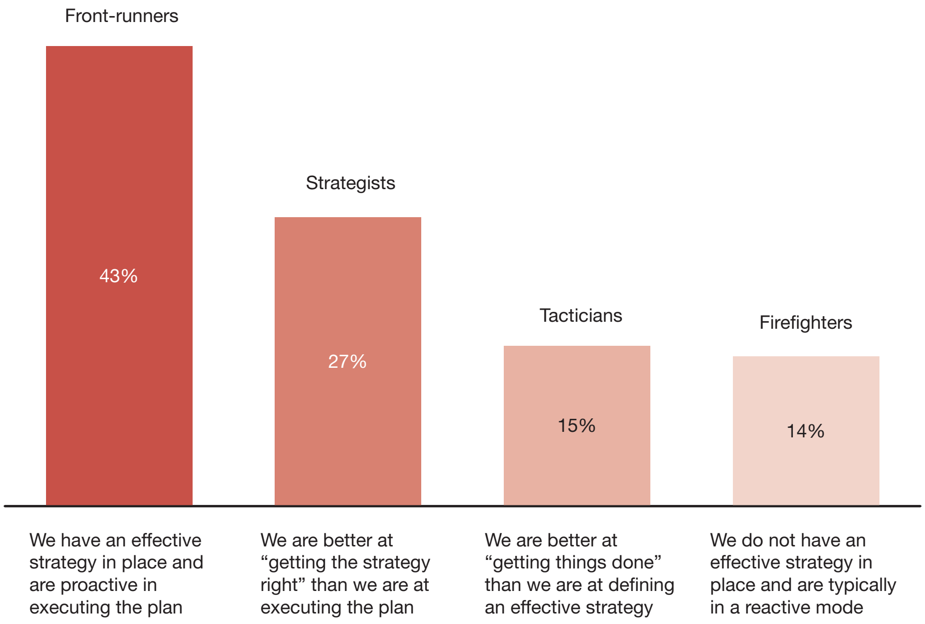
Curious about how this year's more than 9,600 respondents would categorize their organization's approach to protecting information security, we asked the question directly—and then, for analytical purposes, organized respondents as belonging to one of four groups: Front-runners, Strategists, Tacticians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

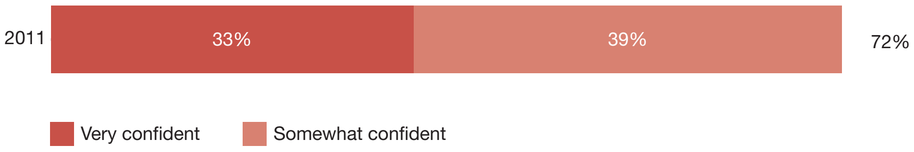
Finding #4. A clear majority of respondents are confident that their organization's information security activities are effective.

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.

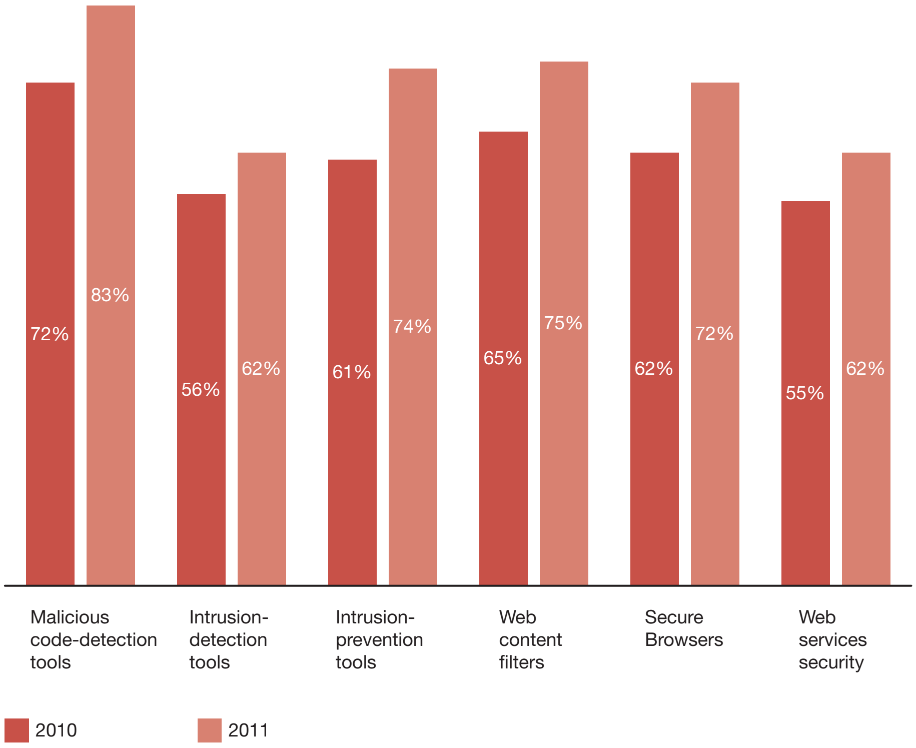
That's a huge gain in perspective—and it appears to be influencing where organizations are placing their bets, at a time when funding to support the function is not as freely available as it was before 2008. Where exactly are these investments being made? In prevention, detection and web-related technologies—three 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%.

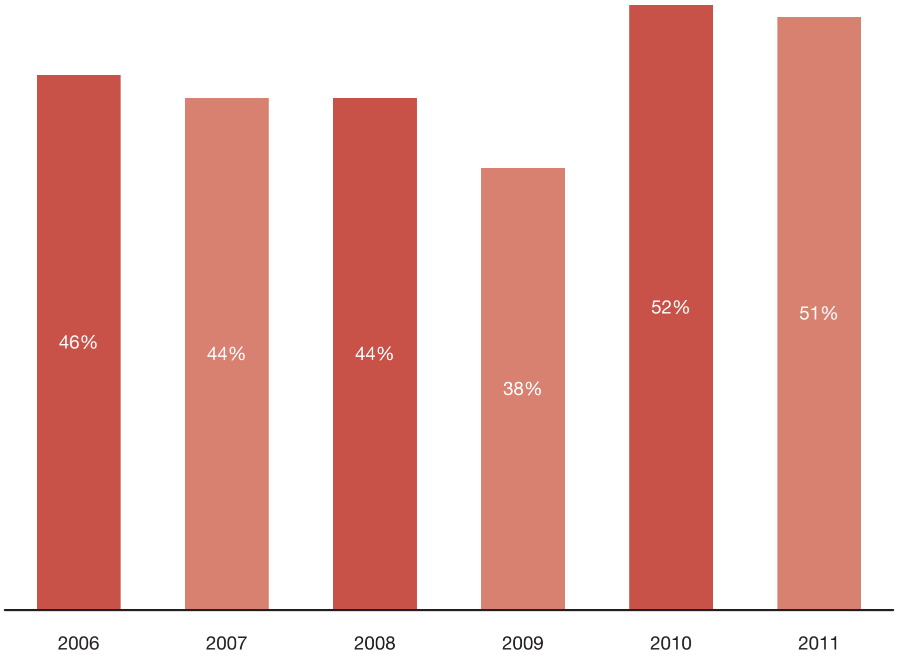
Finding #6. After three years of cutting information security budgets and deferring security-related initiatives, respondents are "bullish" about security spending.

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.

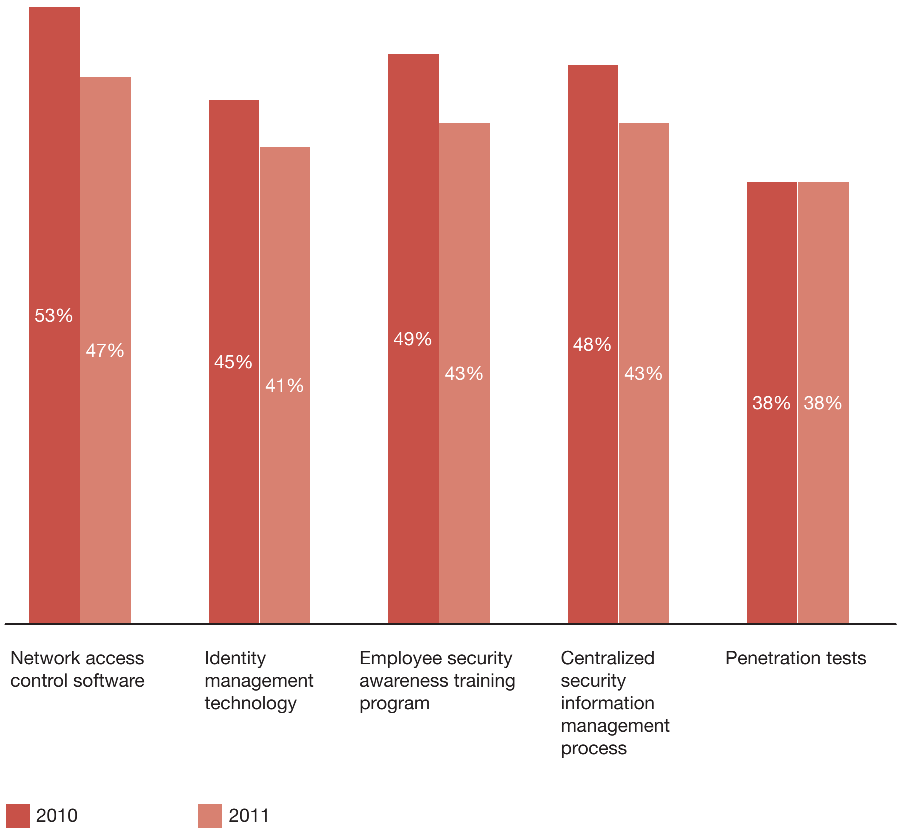
The most sophisticated, adaptive and persistent class of cyber threats is no longer a rare event. In the few short months since this survey was launched on February 10, 2011, for example, leading organizations worldwide have been targeted by Advanced Persistent Threat attacks. These entities include 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



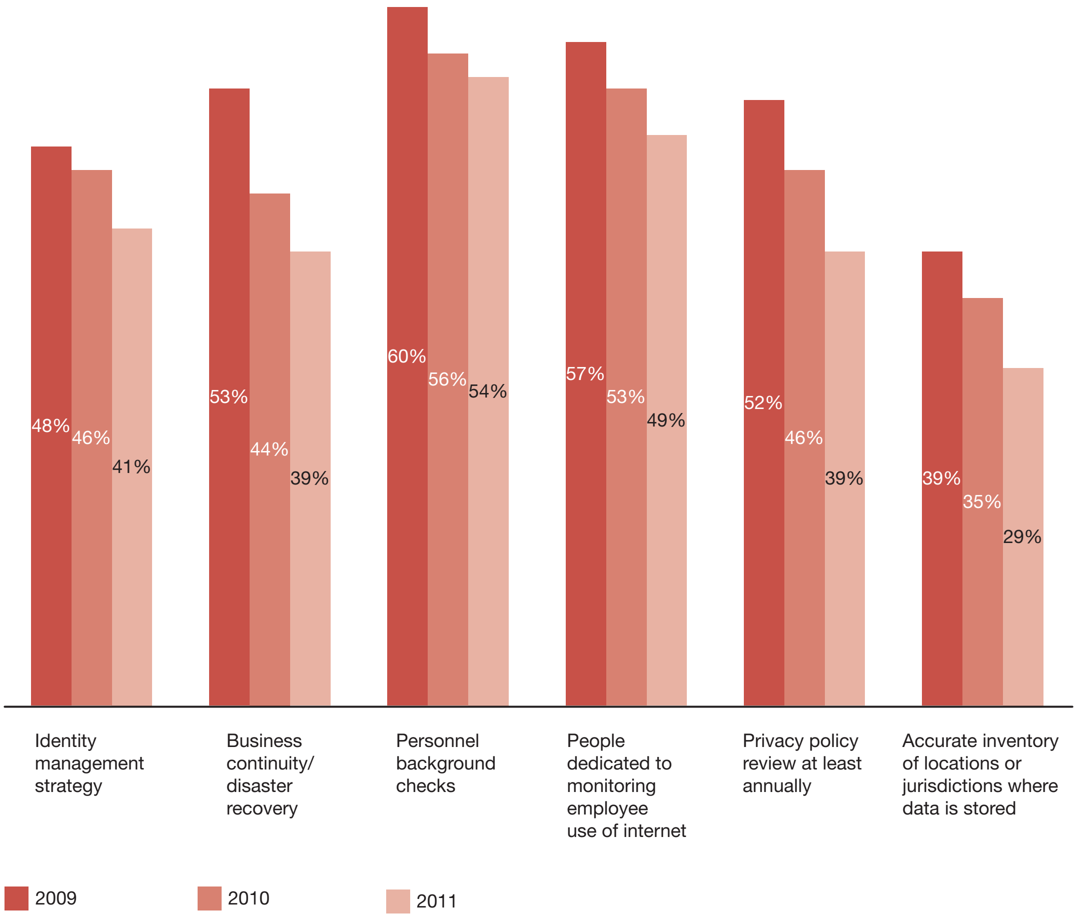
Source: The 2012 Global State of Information Security Survey®
Not all factors shown. Totals do not add up to 100%.

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.

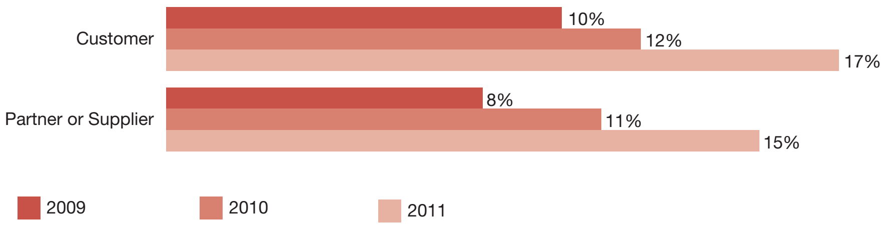
Insider risk has always been a focus for CISOs, CSOs and others charged with "protecting the house." For years, the most commonly suspected source of breaches has been employees, both current and former. And they still are. But less attention is typically paid to other classes of insiders, such as partners 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)

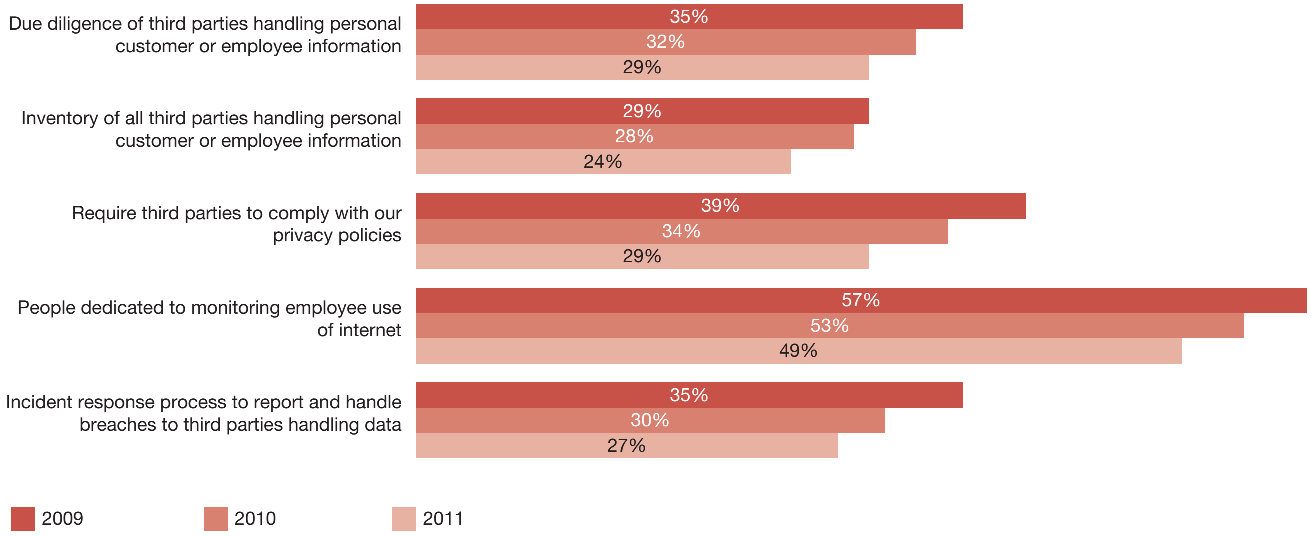
What *should* change quickly—and now with suspicions rising, they may very well over the next 12 months—are the maturity levels for a host of security capabilities that together represent the "front line" in managing third party-related risk. (Figure 12)

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%.

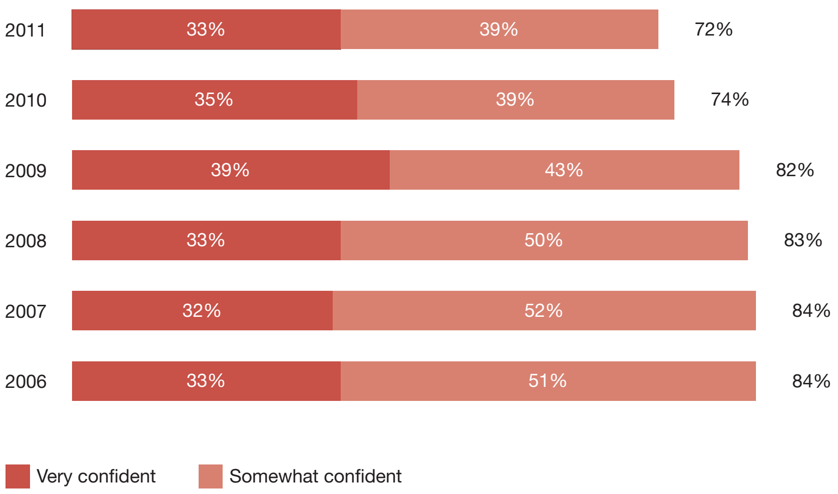
Finding #10. That 72% worldwide confidence rating in security practices may seem high—but it has declined markably since 2006.

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%

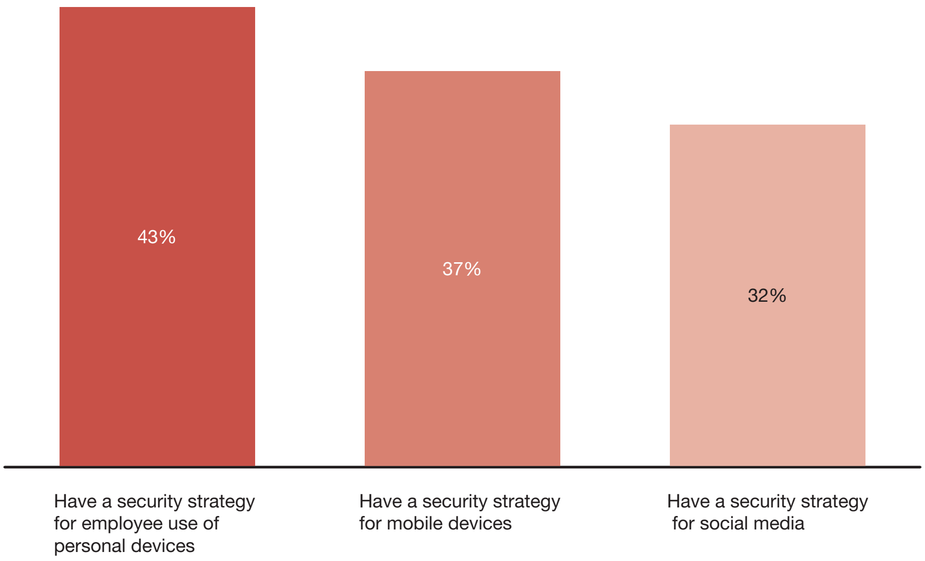
Source: The 2012 Global State of Information Security Survey®
Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

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%.

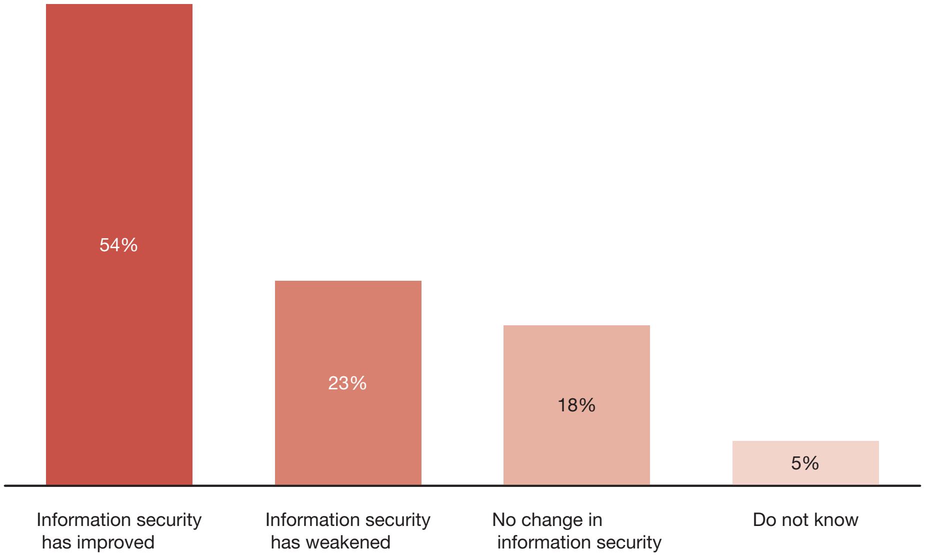
Finding #13. Cloud computing is improving security. But many want better enforcement of provider security policies, among other priorities.

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)

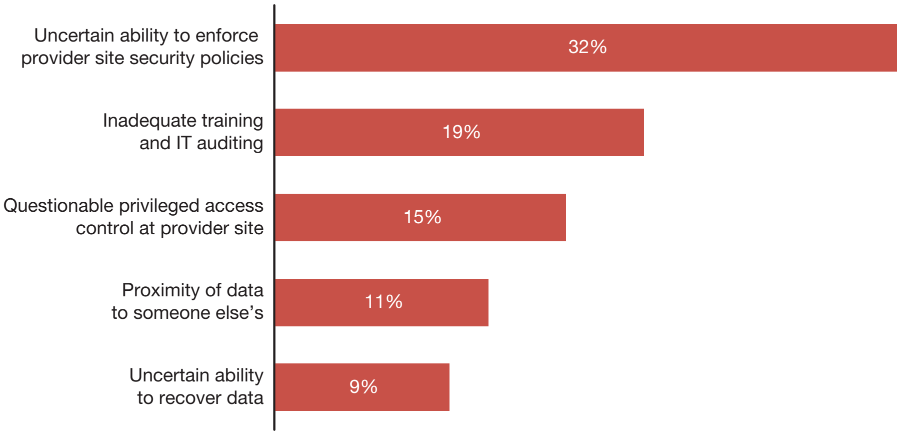
What about the greatest risks to cloud computing strategies? The largest one is perceived to be the uncertain ability to enforce provider security policies. Others include inadequate training and IT auditing, questionable privileged access control at the provider site, the proximity of data to someone 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/giss2012

For more information, please contact:

Gary Loveland
Principal, National Security Leader
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

Or visit: www.pwc.com/giss2012

This document is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. DH-12-0036

www.pwc.com/security

Eye of the storm

As the global economy stalls and information security threats such as cyber crime and Advanced Persistent Threats cloud the horizon, many see sunshine and clear skies overhead

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

September 2011

CIO Business Technology Leadership

CSO Business Risk Leadership

pwc

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*

The economic thunderheads of 2008 may have passed. But across global markets and industries, some clouds 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.

Nonetheless, according to PwC's 2012 Global State of Information Security Survey®, the vast majority of executives across industries are confident in the effectiveness of their information security practices.

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

Yet all is not in order. Security event frequency is up. Risks associated with business partners are on the rise. And the capital and operating expenditures crucial to early prevention and agile response are more likely to be deferred or canceled than at any time since 2008.

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, the reasons to do so quickly and strategically are mounting.

Agenda

Section 1.	Methodology
Section 2.	A world of front-runners
Section 3.	Learn from the leaders
Section 4.	Confidence and progress
Section 5.	Vulnerability and exposure
Section 6.	Windows of improvement
Section 7.	Global trends

Section 1

Methodology

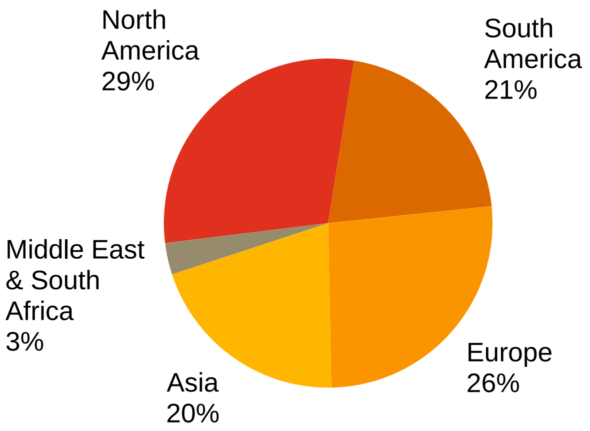
A worldwide study

The 2012 Global State of Information Security Survey$^{®}$, a worldwide study by PwC, CIO Magazine and CSO Magazine, was conducted online from February 10, 2011 to April 18, 2011.

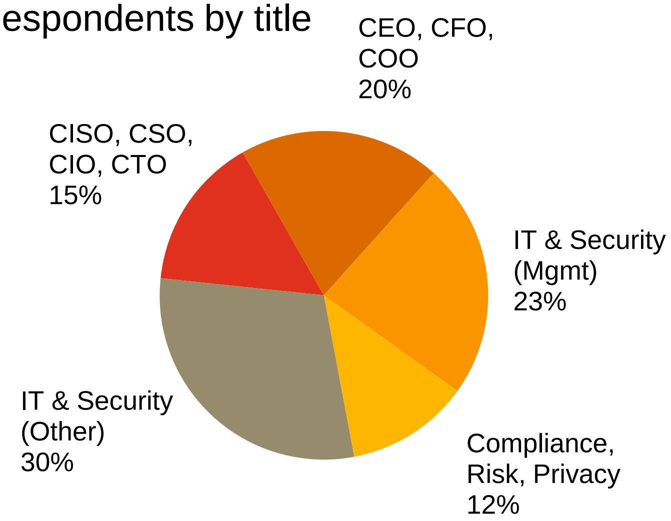
- PwC's 14th year conducting the online survey, 9th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 138 countries
- More than 9,600 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-one percent (31%) of respondents from companies with revenue of $500 million+
- 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%

A global, cross-industry survey of business and IT executives

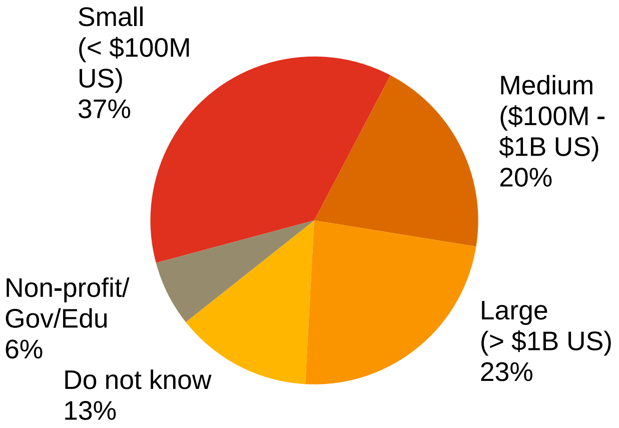
Respondents by region of employment



Respondents by title



Respondents by company revenue size



(Numbers reported may not reconcile exactly with raw data due to rounding)

Survey response levels by industry

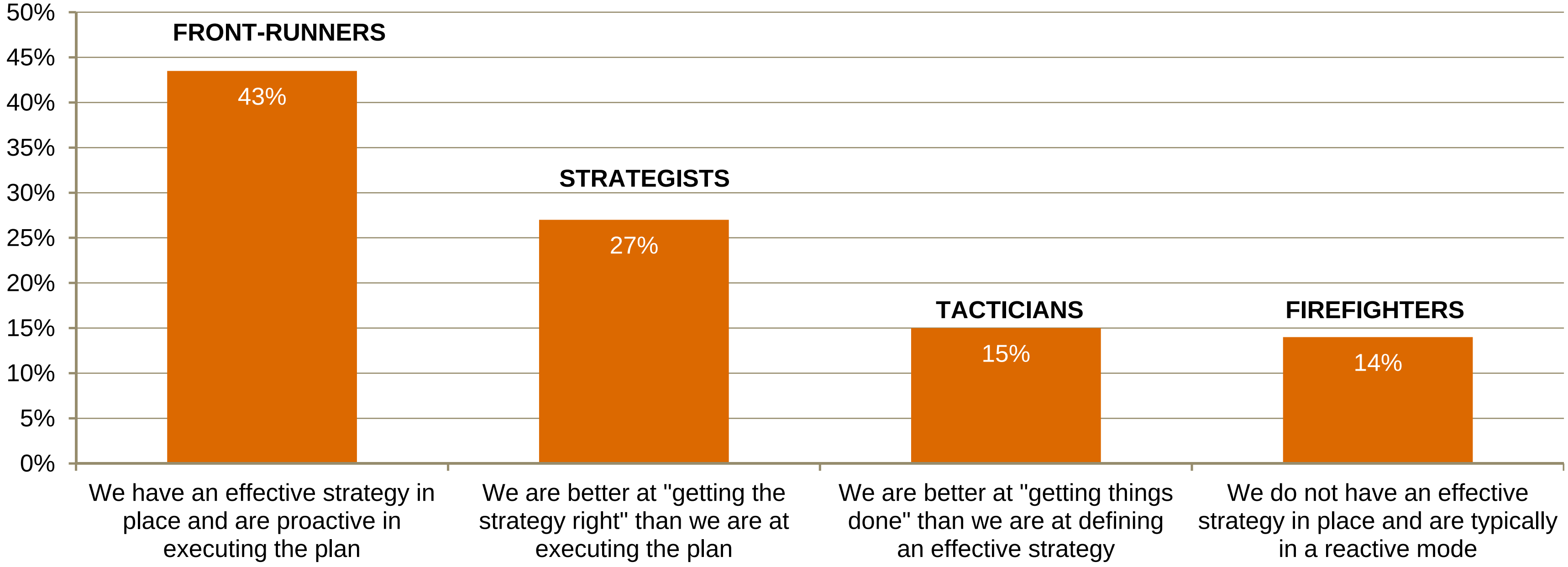
	Number of responses this year
Technology	1,606
Financial Services	1,293
Retail & Consumer	996
Industrial Products	859
Government	717
Telecommunications	647
Health Providers	483
Entertainment & Media	435
Automotive	265
Aerospace & Defense	253
Utilities	184
Energy (Oil & Gas)	143
Pharmaceutical	134

Section 2

A world of front-runners: Respondents categorize their organization

Nearly half (43%) of respondents see their organization as a "front-runner" in information security strategy and execution.

Two of the most crucial drivers of information security effectiveness are having an effective strategy in place and proactively executing it. Nearly half of this year's respondents say their organization meets both criteria. From a statistical perspective, this data bears no resemblance to the bell-shaped curve of the standard normal distribution. Yet it does give us some intriguing insights into perceptions.



Question 26n11: "Which statement best characterizes your organization's approach to protecting information security?" (Numbers reported may not reconcile exactly with raw data due to rounding)

Among “front-runners”, client requirement is the most important justification for information security spending.

All respondents – Front-runners, Strategists, Tacticians, and Firefighters alike – say economic conditions and the need to prepare for business continuity and disaster recovery are key drivers of security spending. How they “justify” security spending varies remarkably, however. Front-runners are far more likely to cite client requirement.

	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%

Question 32: “What business issues or factors are driving your company's information security spending?” Question 26: “Which statement best characterizes your organization’s approach to protecting information security?” (Not all factors shown. Totals do not add up to 100%.)

Front-runners are more committed to protecting data, particularly customer information.

Front-runners are clearly more passionate about protecting all kinds of information – from financial data and intellectual property to company, customer, and employee information. Safeguarding customer data is their top priority.

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

Question 32n11: “What level of importance does your company place on protecting the following types of information? “ (Respondents who answered “Extremely important.” Totals do not add up to 100%.)

All four groups remain reluctant to spend on information security, but Strategists are far more likely to clamp down on funding.

All respondents are actively reducing budgets for security initiatives and deferring security-related initiatives, but Strategists lead the pack. Why? One reason may be that, without a sustained focus on execution, they are simply not seeing the value of results on the ground. Another is that they're confident in their strategy – and simply spending on what matters most.

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

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

Question 12: "Has your company deferred security-related initiatives?" Question 13: "Has your company reduced the cost for any security-related initiatives?" (Not all factors shown. Total does not add up to 100%.)

Section 3

Learn from the leaders

A new working definition of a leader

Who are the leaders? We revisited the data and carved out a smaller bracket of respondents – those who reported that their organization:

- Has an overall information security strategy
- Employs a CISO or equivalent who reports to the “top of the house” (i.e., to the CEO, CFO, COO or legal counsel)
- Has measured and reviewed the effectiveness of security within the past year
- Understands exactly what type of security events have occurred in the past year

The profile of our new group of leaders

SIZE	13% of survey
RESPONDENT TYPE	Business executives, 40%
	IT executives, 60%
REGION	Asia, 39%
	South America, 25%
	Europe, 19%
	North America, 16%

What these leaders are seeing – and doing – differently

These leaders report capability levels that are 15 to 25 percentage points higher than survey averages. This narrows to approximately 10 points in the few areas where many companies have been concentrating investments this year – i.e., prevention, detection and web-related technologies. Where are the greatest gaps? In these areas:

	Leaders	All survey
Number of incidents per year	1,274	2,562
Expect security spending to increase over the next year	76%	51%
Exploitation - Data	45%	26%
Exploitation - Mobile devices	36%	23%
Likely source of events - Employees	38%	32%
Likely source of events - Hackers	50%	35%
Employ a CSO or equivalent	75%	40%
Have an overall information security strategy	100%	63%
Both measured and reviewed security over the past year	100%	54%
Dedicate security personnel to support internal business departments	72%	46%
Confidence in the effectiveness of security	93%	72%

The implication for your business

What does this mean for you? How can you use this information to improve your security, protect your assets and operations, and improve your business?

- Use this information to define a vision for your information security program.
- Ask us for more information on this bracket of leaders in areas critical to your business.
- Then define – and refine – your information security strategy.
- At minimum, focus acutely on (1) leadership, (2) strategy, (3) alignment with the business and (4) customer centricity.

Section 4

Confidence and progress: A decade of maturation

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

More than seven out of ten (72%) of respondents say they feel confident in the effectiveness of their organization's information security capabilities. This level of assurance indicates that information security is viewed as a critical business function rather than a "patchwork of technical guesses" or merely a line item in the CIO's budget. In other words, survey respondents appear to believe that the information security function is doing its job quite well.

	2011
Very confident	**33%**
Somewhat confident	**39%**
Total	**72%**

Question 35: "How confident are you that your organization's information security activities are effective?"

Insights into the frequency, type, and source of security breaches have leaped dramatically over the past 12 months.

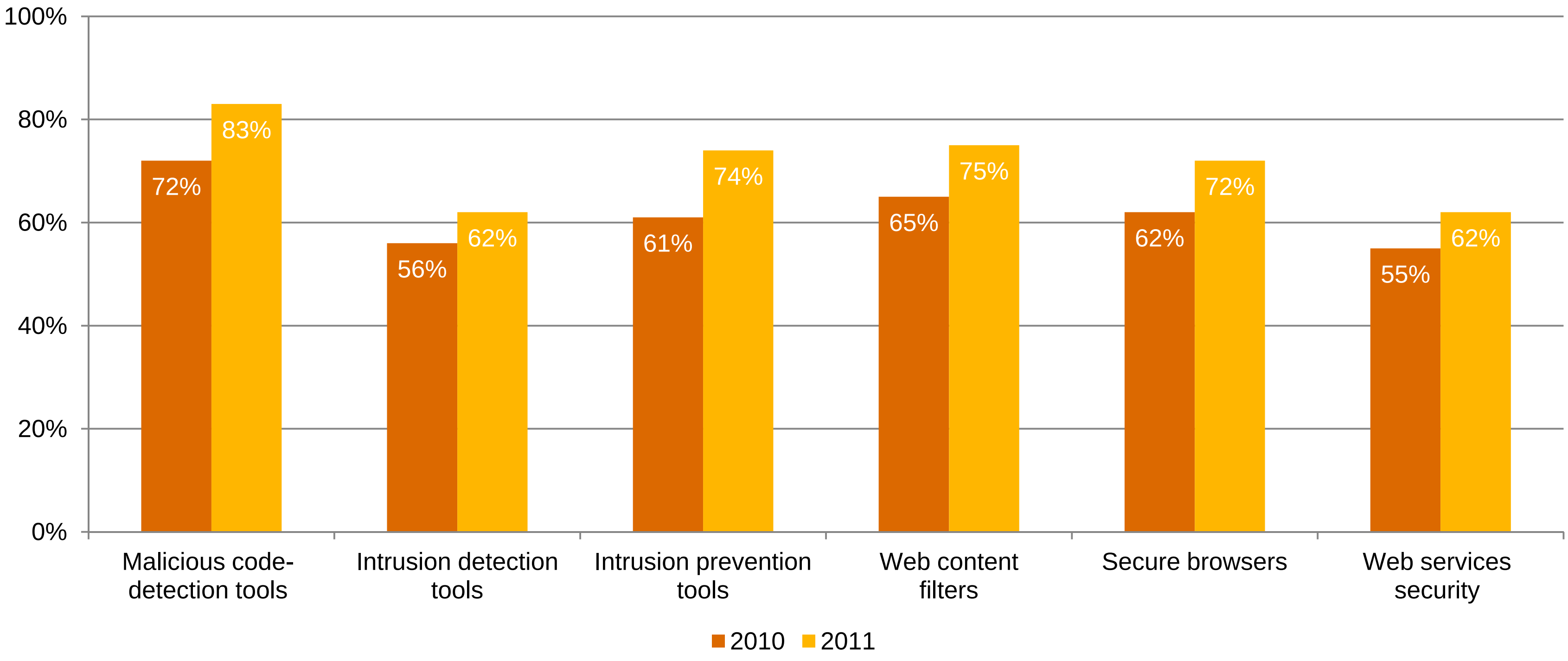
Just a few years ago, almost half of this survey's respondents couldn't answer the most basic questions about the nature of cyber crimes and security-related breaches. Now, approximately 80% or more of respondents can answer specific questions about factors such as security event frequency, type, and source. The gains in the past 12 months are particularly striking.

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%**

Question 19: "Number of security incidents in the past 12 months." Question 20: "What types of security incidents (breach or downtime) occurred?" Question 22: "Estimated likely source of incident." (Totals do not add up to 100%.)

Despite tight budgets, organizations are proactively adopting certain safeguards to bolster data security.

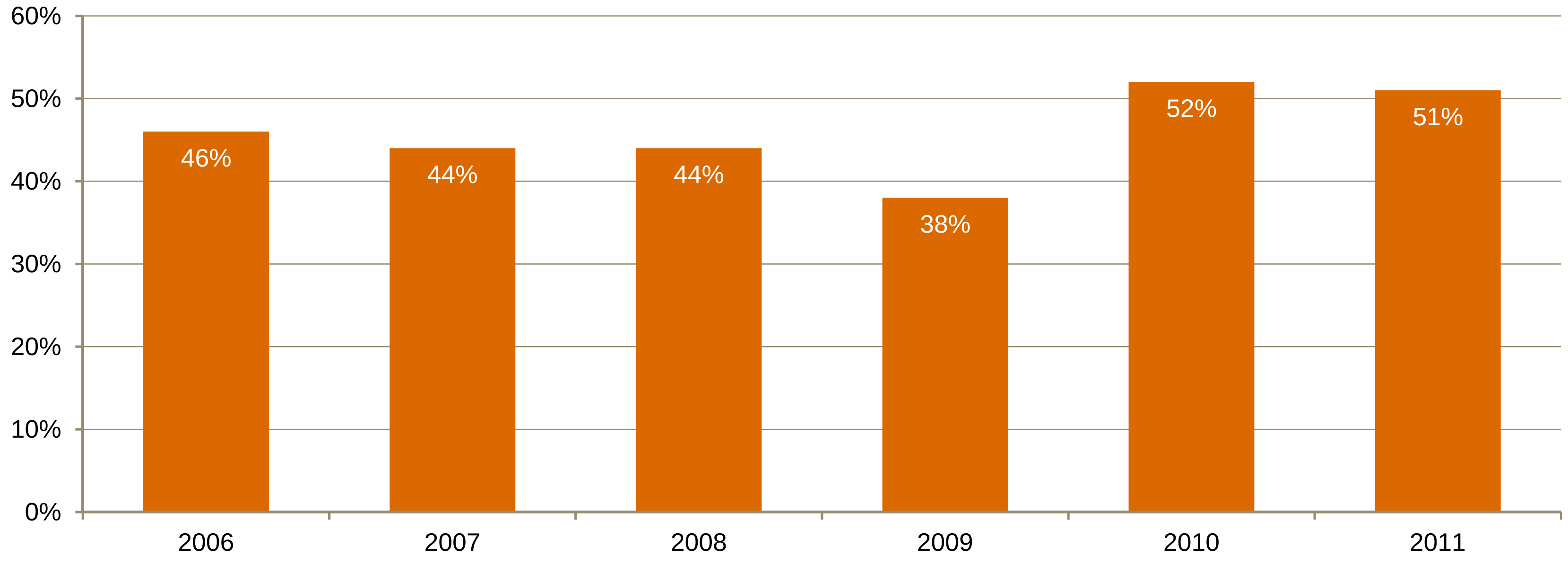
Better insight into security incidents appears to be influencing how organizations invest in security spending. Over the past year, respondents have boosted investments in capabilities related to detection, prevention, and Web-related technologies.



Question 18: “What technology information security safeguards does your organization currently have in place?” (Not all factors shown. Totals do not add up to 100%.)

Is the spending drought ending? A majority of respondents forecast increased security spending over the next 12 months.

Optimism carries the day. More than half (51%) of respondents believe that security spending will increase across industries.



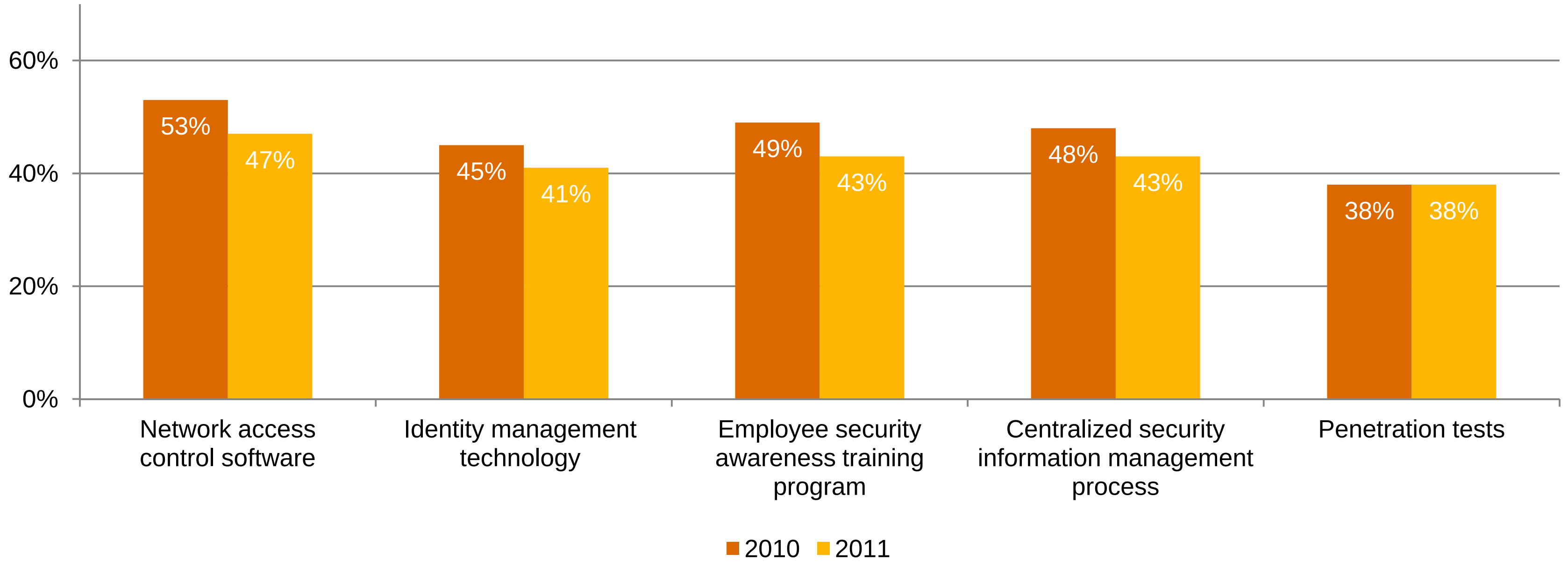
Question 9: “When compared with last year, security spending over the next 12 months will:” (Respondents who answered “Increase up to 10%,” “Increase 11-30%,” or “Increase more than 30%”)

Section 5

Vulnerability and exposure: Capability degradation since 2008

Advanced Persistent Threat is a dangerous – and increasingly common – threat. Yet few organizations are prepared to combat it.

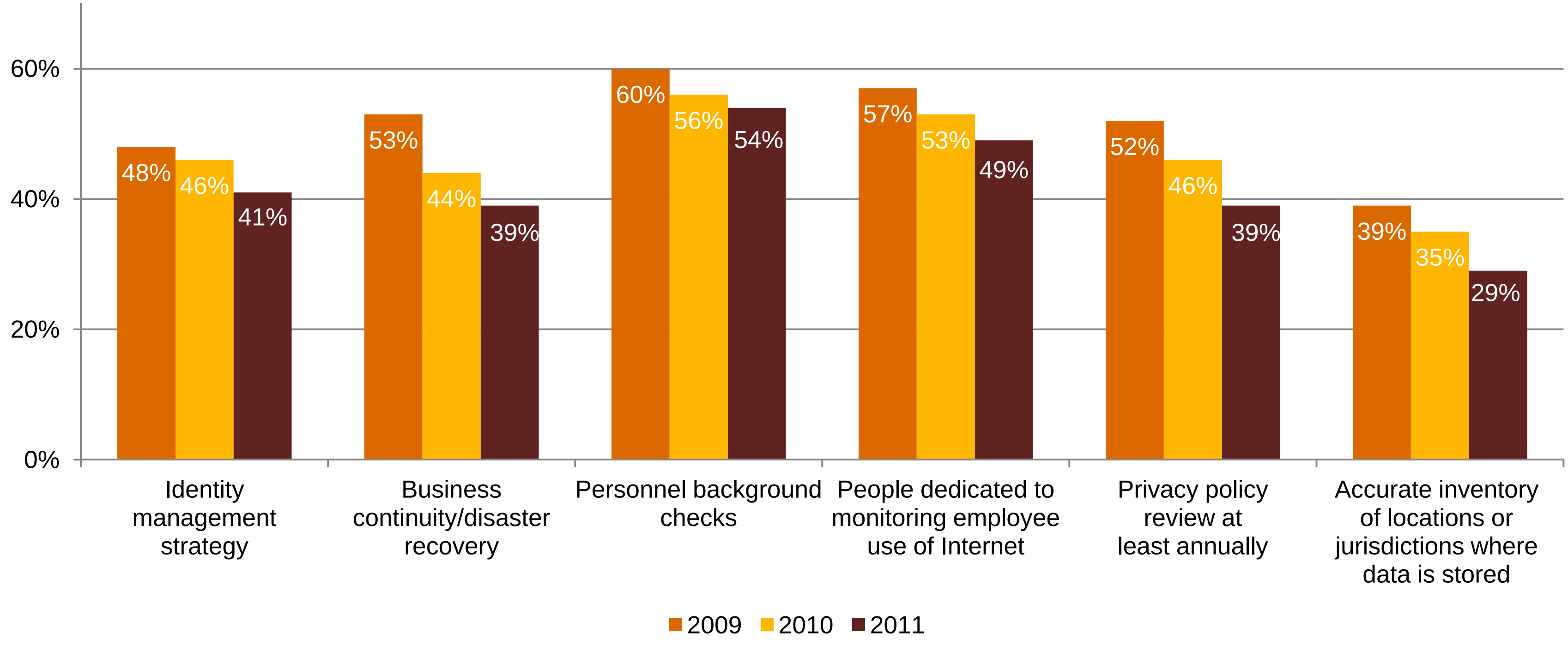
This year, significant percentages of respondents from various industries agree that APT drives their organization's security spending, yet only 16% say their company has a security policy that addresses APT. Worse, implementation of certain tools and processes crucial to combatting this new threat has slowed over the past year.



Question 28: "Which of the following elements, if any, are included in your organization's security policy?" Question 17: "What process information technology security safeguards does your organization currently have in place?" Question 18: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown. Totals do not add up to 100%.)

After three years of budget constraints, degradation in core security capabilities continues.

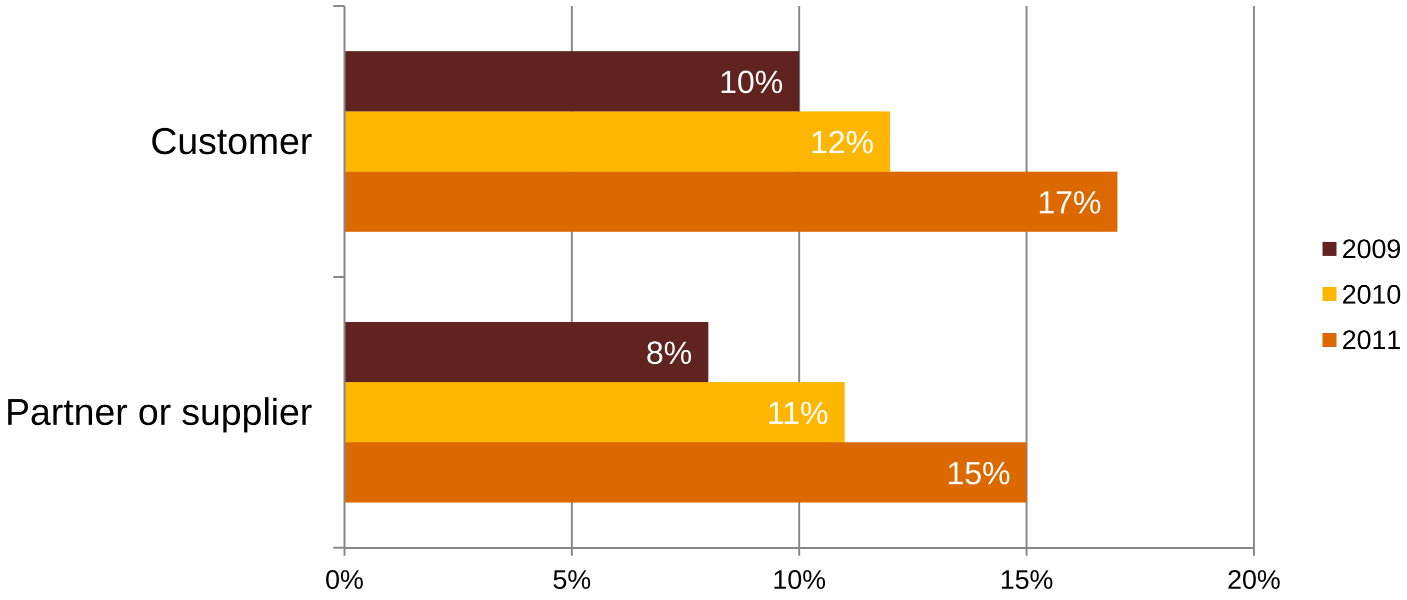
While organizations have invested in capabilities for prevention, detection, and Web-related security initiatives, this year's survey reveals a troubling degradation in core security-related capabilities.



Question 17: "What process information security safeguards does your organization have in place?" Question 16: "What information security safeguards related to people does your organization currently have in place?" Question 15: "Which data privacy safeguards does your organization have in place?" (Not all factors shown. Totals do not add up to 100%.)

Managing security risks associated with customers, partners, and suppliers is becoming an increasingly serious issue.

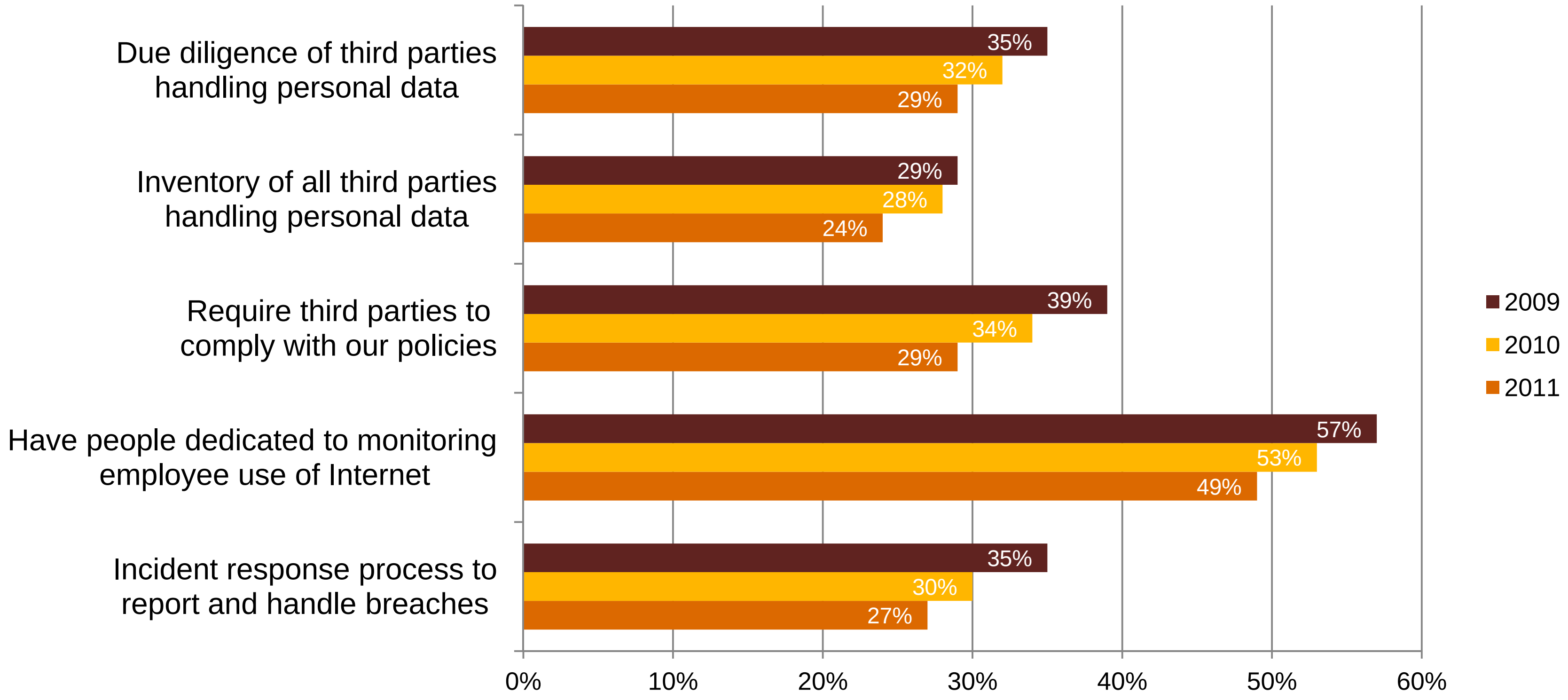
Customers and “insiders” like partners and suppliers traditionally have not been considered likely suspects in data breaches. That’s changing – fast. Over the past 24 months, the number of security incidents attributed to customers, partners, and suppliers has nearly doubled.



Question 22: “Estimated likely source of incident.” (Not all factors shown. Totals do not add up to 100%.)

While risks associated with third parties continue to increase, many companies are less prepared to defend their data.

Over the past two years, organizations have allowed data privacy safeguards to degrade, exposing the enterprise to potential compromise.



Question 15: “Which data privacy safeguards does your organization have in place?” Question 16: “What information security safeguards related to people does your organization currently have in place?”(Not all factors shown. Totals do not add up to 100%.)

And that high confidence rating? It has actually declined 12 points since 2006.

Confidence is always good. But a decline in confidence is telling. The confidence rating among respondents is actually 12 points lower than it was a few years ago. Business and IT personnel – across the world – are less sure that their organization is prepared to address the threats that confront critical information.

	2006	2007	2008	2009	2010	2011	CHANGE
Total	**84%**	84%	83%	82%	74%	**72%**	**- 12 pts**

Question 35: “How confident are you that your organization’s information security activities are effective?” (Respondents who answered “Very confident” or “Somewhat confident” combined)

Section 6

Windows of improvement: Where the best opportunities lie

What are the greatest obstacles to effective information security? A lack of funding and leadership at "the top of the house."

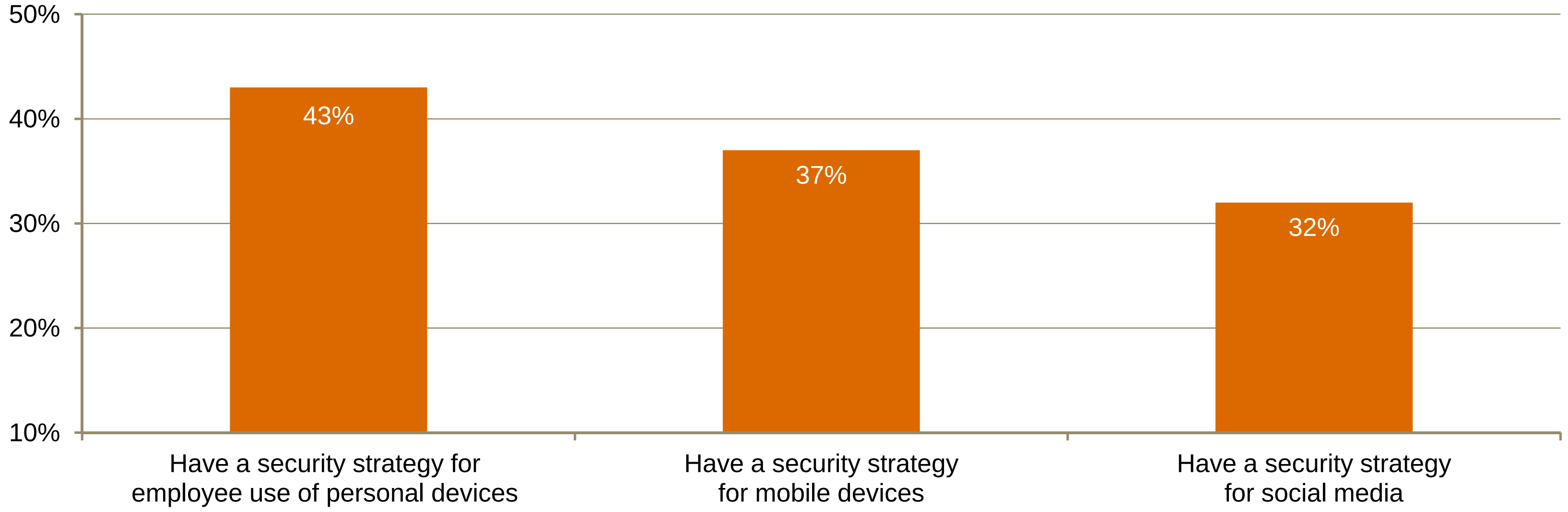
When asked to identify the highest hurdle to improving information security, responses vary by role. CEOs point first to a lack of capital and then themselves – and lastly to the CISO. CFOs cite the CEO. Interestingly, CIOs and CISOs report a lack of vision and an effective security strategy – and rank themselves at the bottom of the list.

	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 an effective information security strategy	18%	25%	25%	30%
Lack of an 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%

Question 27n11: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?" (Total does not add up to 100%.)

Mobile devices and social media: New rules and new risks

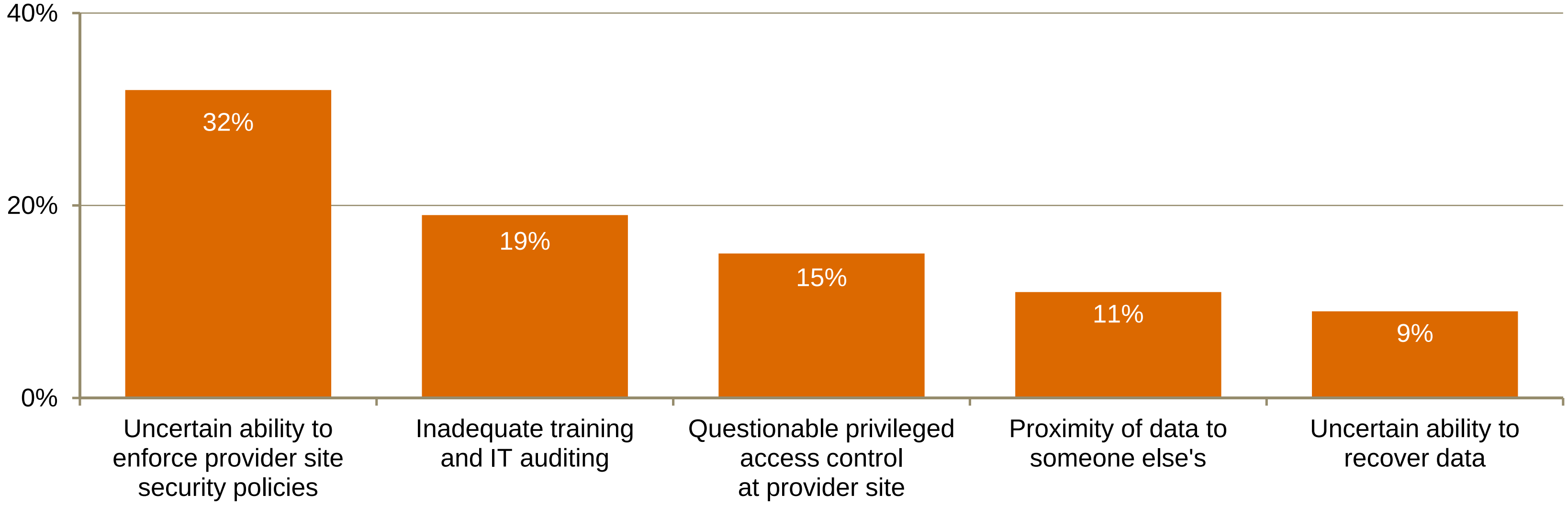
Organizations are beginning to implement strategies to keep pace with employee adoption of mobile devices and social networking, as well as use of personal technology within the enterprise. Yet much remains to be done: Less than half of respondents have implemented safeguards to protect the enterprise from the security hazards that mobile devices and social media can introduce.



Question 17: “What process information security safeguards does your organization currently have in place?” (Not all factors shown. Total does not add up to 100%.)

Cloud computing: Is it improving information security? Yes, but many want better enforcement of provider security policies.

Four out of ten (41%) respondents say their organization uses cloud services – and 54% of those that do say the cloud has improved their information security. The greatest risks associated with cloud computing? An uncertain ability to enforce provider security policies and inadequate training and IT auditing are top concerns.



Question 41: “Does your organization currently use cloud services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or Infrastructure-as-a-Service (IaaS)?” Question 41c: “What impact has cloud computing had on your company’s information security?” Question 41b: “What is the greatest security risk to your cloud computing strategy?” (Not all factors shown. Total does not add up to 100%.)

Section 7

Global trends: Asia races ahead while the world’s information security arsenals age

For several years, Asia has led the world in a commitment to funding information security. The results are dramatic.

Today 76% of respondents in Asia say their organization has implemented an overall security strategy, insights into security incidents have soared, and the importance of the security function is more widely acknowledged than in any other region.

	2009	2011
Security spending will increase over the next 12 months	53%	74%
Increased risk environment has elevated importance of security function	62%	74%
Don't know number of security incidents in the past 12 months	21%	3%
Don't know types of security incidents in the past 12 months	30%	6%
Don't know estimated likely source of security incidents in the past 12 months	32%	17%
Use identity management solutions	49%	62%
Dedicate security personnel to internal business departments	48%	61%
Have malicious code detection tools	70%	81%
Have vulnerability scanning tools	55%	71%
Have established a written privacy policy	59%	70%
Conduct due diligence of third parties handling personal data	33%	43%
Use data loss prevention (DLP) tools	44%	57%

(Not all factors shown.)

North American organizations remain reluctant to invest in security initiatives – and cracks in their defenses are starting to appear.

The reluctance to fund security projects has resulted in erosion of key capabilities, including strategy, identity management, and business continuity/disaster recovery. A few signs of new strengths appear in adoption of detection and prevention tools.

	2009	2011
Security spending will increase over the next 12 months	29%	31%
Have overall security strategy in place	73%	58%
Have business continuity/disaster recovery plans	65%	46%
Conduct due diligence of third parties handling personal data	45%	27%
Have established a written privacy policy	65%	57%
Have network access control software	58%	42%
Have secure remote access (VPN)	67%	49%
Use identity management solutions	47%	33%
Use secure browsers	68%	77%
Have intrusion prevention tools	62%	72%

(Not all factors shown.)

As economic uncertainty lingers and security capabilities decline, Europe pulls the purse strings even tighter.

Increasingly complex regulations, greater risks, and weakened partners and suppliers are impeding security efforts in Europe. Worse, organizations are likely to cut security budgets in the coming year. The good news? Respondents report gains in select capabilities.

	2009	2011
Regulatory environment has become more complex and burdensome	47%	53%
Risks to the company's data have increased due to employee layoffs	34%	42%
Threats to the security of our information assets have increased	32%	38%
Our business partners have been weakened by the economic conditions	33%	51%
Our suppliers have been weakened by the economic conditions	33%	48%
Reduced budgets for security-related capital expenditures	43%	57%
Reduced budgets for security-related operating expenditures	41%	56%
Require third parties to comply with our privacy policies	31%	22%
Use intrusion prevention tools	48%	73%
Have Web content filters	55%	72%
Have malicious code detection tools	66%	80%

(Not all factors shown.)

South America suffers a crisis of confidence and struggles to fund future security initiatives.

Budget deferrals and cut-backs for security initiatives have increased enormously since 2009, while levels for key security capabilities have continued to decline. It’s not surprising that respondents report declining confidence in the effectiveness of security programs.

	2009	2011
Deferred initiatives for security-related capital expenditures	49%	68%
Deferred initiatives for security-related operating expenditures	44%	63%
Reduced budgets for security-related capital expenditures	50%	66%
Reduced budgets for security-related operating expenditures	48%	66%
Are confident that our organization’s information security is effective	89%	71%
Are confident that our partners’ and suppliers’ information security is effective	86%	70%
Conduct personnel background checks	55%	53%
Have centralized security information management process	50%	38%
Have business continuity/disaster recovery plan	43%	30%
Have overall information security strategy	56%	60%
Employ Chief Information Security Officer	45%	53%

(Not all factors shown.)

For more information, please contact:

Gary Loveland
Principal, National Security Leader
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

Or visit www.pwc.com/giss2012 to explore the data for your industry and benchmark yourself.

This document is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

www.pwc.com/security

Eye of the storm

As the global economy stalls and information security threats such as cyber crime and Advanced Persistent Threats cloud the horizon, many see sunshine and clear skies overhead

CIO Business Technology Leadership

CSO BUSINESS RISK LEADERSHIP

Aerospace & Defense

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

September 2011

pwc

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

The economic thunderheads of 2008 may have passed. But across the global aerospace and defense (A&D) industry, some clouds 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.

Nonetheless, according to PwC's 2012 Global State of Information Security Survey®, the vast majority of A&D executives are confident in the effectiveness of their information security practices.

They have an effective strategy in place. They consider their organizations proactive in executing it. And their most senior security leader now typically reports "to the top of the house."

Yet all is not in order. Security event frequency is up. Financial impacts from events are on the rise. And the capital and operating expenditures crucial to early prevention and agile response are more likely to be deferred or canceled than at any time since 2008.

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, the reasons to do so quickly and strategically are mounting.

Agenda

Section 1.	Methodology
Section 2.	Confidence and progress
Section 3.	Signs of vulnerability and exposure
Section 4.	The greatest opportunities for improvement

Section 1

Methodology

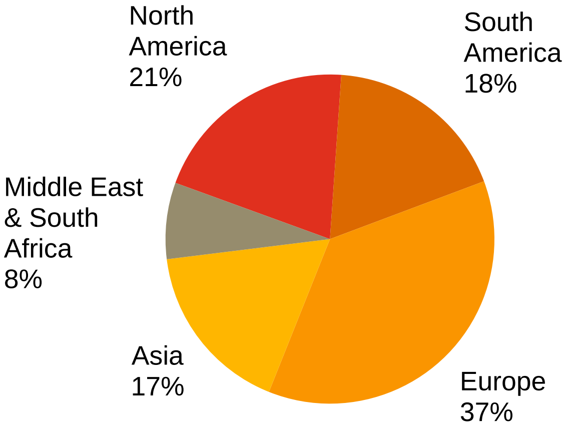
A worldwide study

The 2012 Global State of Information Security Survey®, a worldwide study by PwC, CIO Magazine and CSO Magazine, was conducted online from February 10, 2011 to April 18, 2011.

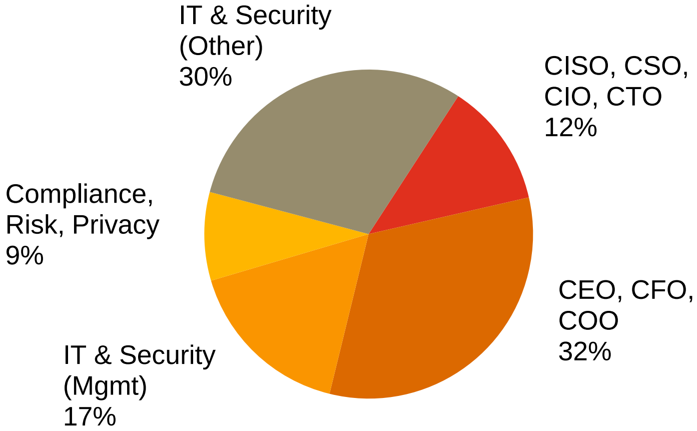
- PwC’s 14th year conducting the online survey, 9th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 138 countries
- More than 9,600 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-one percent (31%) of respondents from companies with revenue of $500 million+
- Survey included 253 respondents from the aerospace and defense (A&D) industry
- The margin of error is less than 1%

Demographics

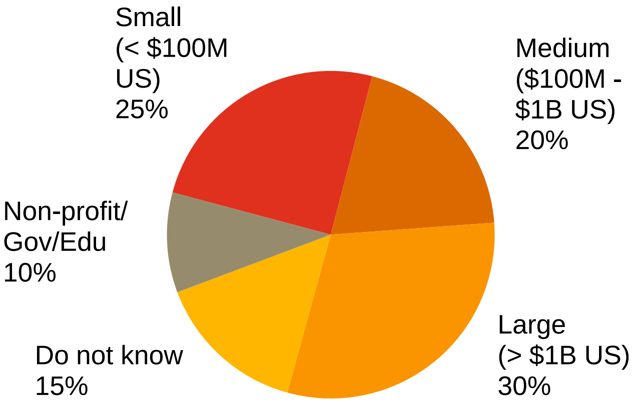
A&D respondents by region of employment



A&D respondents by title



A&D respondents by company revenue size



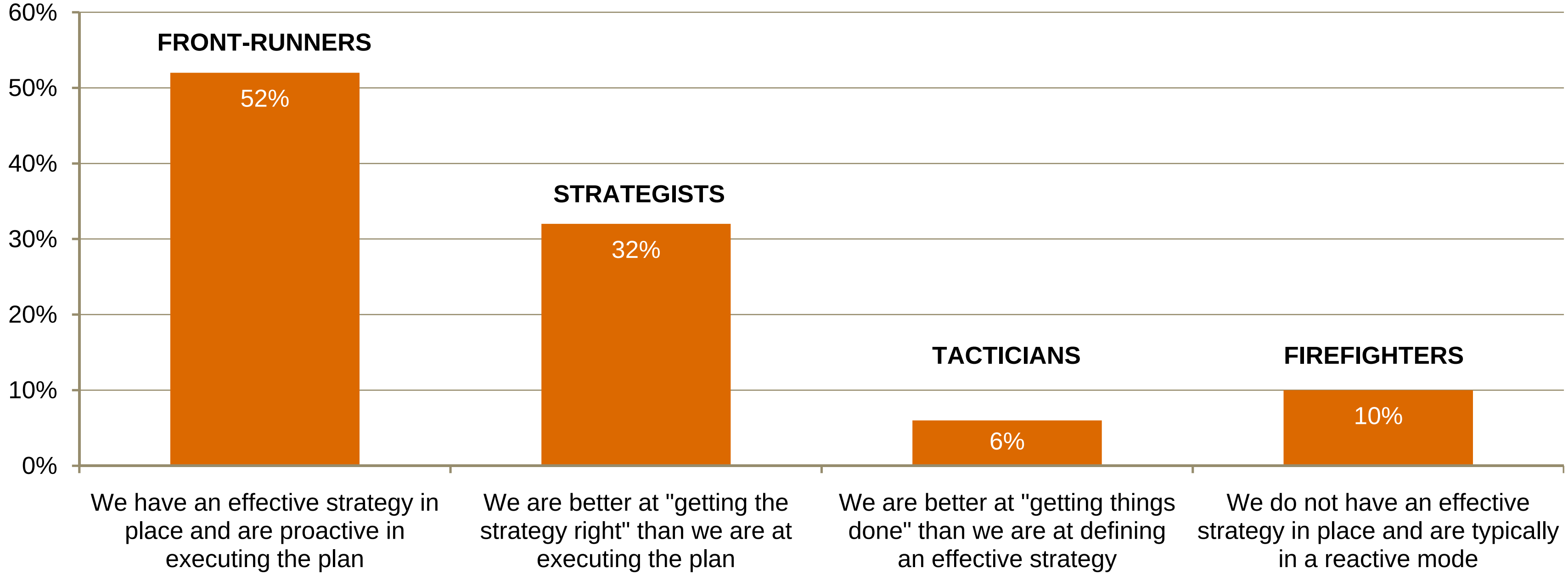
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

Confidence and progress

Most A&D respondents (52%) see their organization as a “front-runner.”

More than half of this year’s A&D respondents say their organization has a strategy in place and is proactive in executing it.



Question 26n11: “Which statement best characterizes your organization’s approach to protecting information security?”

They are also highly confident in their organization’s security.

A clear majority – nearly three out of four (72%) – of A&D respondents are also confident that their organization’s information security activities are effective.

	2011
Very confident	**46%**
Somewhat confident	**26%**
Total	**72%**

Question 35: “How confident are you that your organization’s information security activities are effective?”

The CISO is more likely to report to the "top of the house."

Continuing a long-term trend, A&D companies are increasingly likely to ensure that the Chief Information Security Officer or equivalent executive reports to the most senior business and governance leaders in the organization.

Whom the CISO reports to	2007	2008	2009	2010	2011
Board of Directors	18%	15%	22%	32%	**31%**
Chief Executive Officer	31%	45%	51%	29%	**33%**
Chief Financial Officer	10%	8%	21%	10%	**19%**

Question 16a: "Where/to whom does your CISO or equivalent senior information security officer report?" (Not all factors shown. Totals do not add up to 100%.)

Insights into the frequency, type, and source of security breaches have leaped dramatically over the past 12 months.

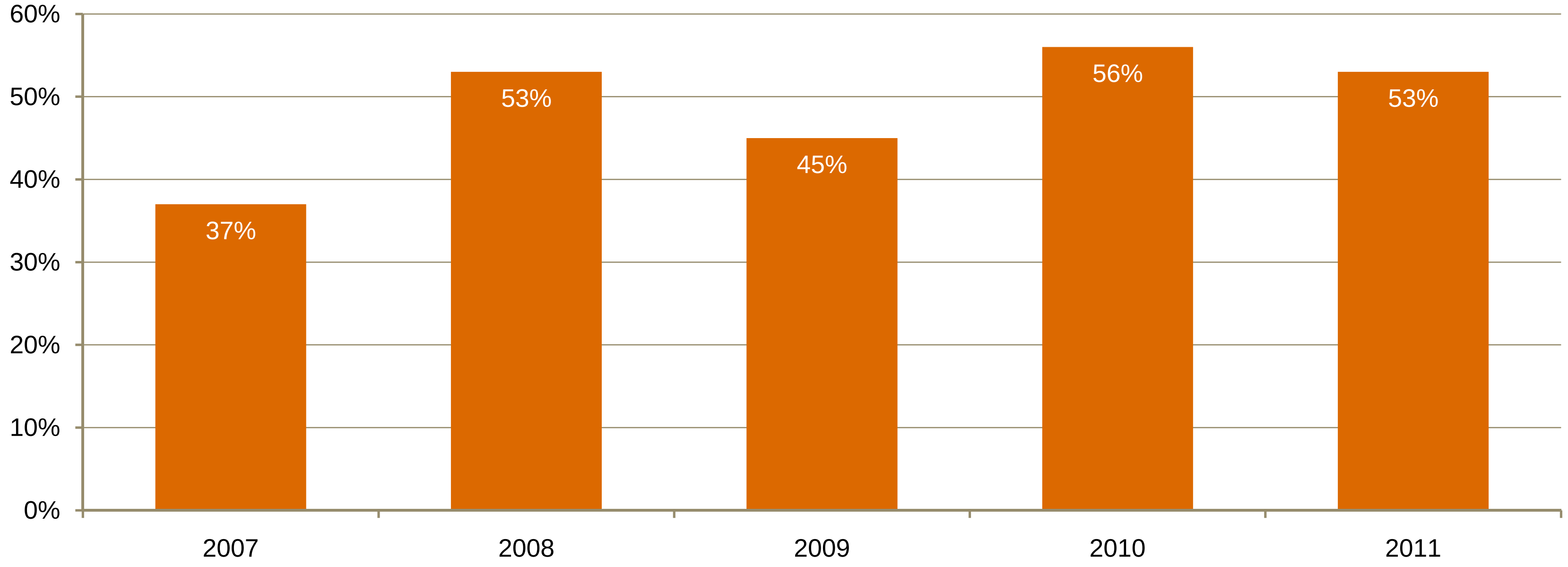
Just a few years ago, half of this survey’s A&D respondents couldn’t answer the most basic questions about the nature of security-related breaches. Now, approximately 80% or more of A&D respondents can answer specific survey questions about factors such as security event frequency, type, and source.

Respondents who answered “Do not know” or “Unknown”	2007	2008	2009	2010	2011
How many incidents occurred in past 12 months?	54%	49%	44%	30%	**12%**
What type of incident occurred?	51%	49%	42%	34%	**21%**
What was the source of the incident?	N/A	37%	31%	29%	**19%**

Question 19: “Number of security incidents in the past 12 months.” Question 20: “What types of security incidents (breach or downtime) occurred?” Question 22: “Estimated likely source of incident.” (Totals do not add up to 100%.)

At the same time, a majority of A&D respondents are "bullish" about security spending over the next 12 months.

Will security spending in the industry increase? Optimism carries the day. More than half of A&D respondents believe that it will.



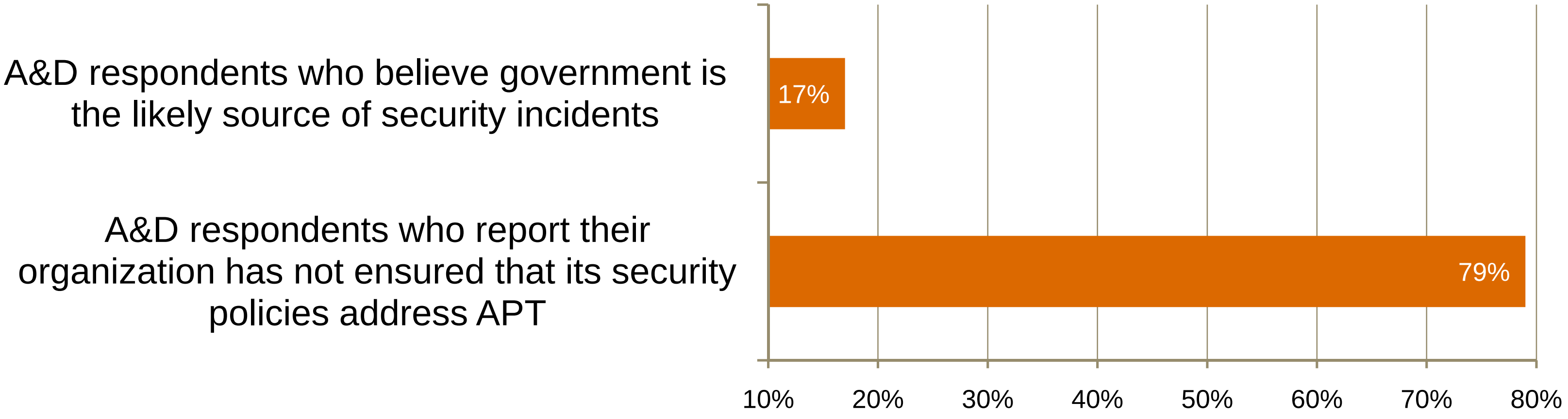
Question 9: "When compared with last year, security spending over the next 12 months will:" (Respondents who answered "Increase up to 10%," "Increase 11-30%," or "Increase more than 30%")

Section 3

Signs of vulnerability and exposure

Advanced Persistent Threats: They can be devastating – but just how concerned are A&D organizations about addressing them?

Interestingly, 17% of A&D respondents report that “government” is the likely source of an incident – though it isn’t clear whether they are referring to their own country’s government or another’s. This figure that is more than triple the cross-industry average. In spite of this, however, nearly 80% also report that their organization’s security policies do not address APT.



Question 22: “Estimated likely source of incident.” Question 28: “Which of the following elements, if any, are included in your organization’s security policy?” (Not all factors shown.)

Other trends in this year's survey are also troubling. Take the increase in security events, for example.

It is tempting to trumpet the fact that more than one out of five A&D respondents (21%) report no security events in the past year. Yet reports of incidents increased this year, especially among respondents indicating 50 or more negative events.

Number of security incidents	2007	2008	2009	2010	2011
No incidents	11%	14%	14%	26%	21%
1 to 9 incidents	24%	22%	29%	33%	40%
10 to 49 incidents	5%	5%	4%	7%	8%
50 or more incidents	6%	10%	9%	4%	19%

Question 19: "Number of security incidents in the past 12 months." (Totals do not add up to 100%.)

At the same time, more A&D organizations are reporting increases in financial losses.

A&D respondents are more than twice as likely as they were in 2008 to report financial losses as a result of these security incidents. Reported levels for other negative impacts also increased.

Business impacts	2008	2009	2010	2011	Three-year change*
Financial losses	8%	12%	12%	17%	**+ 113%**
Brand/reputation compromised	10%	8%	13%	11%	**+ 10%**
Loss of shareholder value	1%	4%	6%	8%	**+ 700%**
Extortion	3%	3%	4%	7%	**+ 133%**

Question 23: "How was your organization impacted by the security incident? Business:" (Not all factors shown. Total does not add up to 100%.)
*This calculation measures the difference between response levels over a three-year period from 2008 to 2011.

Most significant is the fact that security spending deferrals and cut-backs – for both capital and operating projects – have jumped.

For the third year in a row, spending deferrals and cut-backs for security-related initiatives are high. This year's reluctance to spend on security priorities has increased by approximately 20% to 40% over last year's reported levels. In fact, spending appears even more restrained than it was during the two years immediately following 2008.

Has your company **deferred** security initiatives?	2009	2010	2011
Yes, for *capital* expenditures	45%	42%	58%
Yes, for *operating* expenditures	38%	41%	54%

Has your company **reduced the cost** for security initiatives?	2009	2010	2011
Yes, for *capital* expenditures	46%	46%	59%
Yes, for *operating* expenditures	49%	48%	57%

Question 12: "Has your company deferred security-related initiatives?" Question 13: "Has your company reduced the cost for any security-related initiatives?" (Not all factors shown. Total does not add up to 100%.)

This lingering reluctance to maintain security capabilities isn't "just short-term" and "under 10%." It's across the board.

Has your company **deferred** security initiatives?	2009	2010	2011
Yes, for *capital* expenditures	45%	42%	58%
• **By less than 6 months**	25%	22%	30%
• **By 6 to 12 months**	10%	13%	16%
• **By 1 year or more**	10%	7%	12%
Yes, for *operating* expenditures	38%	41%	54%
• **By less than 6 months**	23%	22%	27%
• **By more than 6 months**	7%	12%	17%
• **By 1 year or more**	8%	7%	11%

Has your company **reduced the cost** for security initiatives?	2009	2010	2011
Yes, for *capital* expenditures	46%	46%	59%
• **By under 10%**	16%	21%	19%
• **By 10% to 19%**	17%	14%	18%
• **By 20% or more**	13%	11%	22%
Yes, for *operating* expenditures	49%	48%	57%
• **By under 10%**	19%	20%	23%
• **By 10% to 19%**	14%	16%	14%
• **By 20% or more**	15%	11%	21%

Question 12: "Has your company deferred security-related initiatives?" Question 13: "Has your company reduced the cost for any security-related initiatives?" (Not all factors shown. Total does not add up to 100%. Numbers reported may not reconcile exactly with raw data due to rounding.)

And that high confidence rating? It has actually declined 19 points since 2006.

Confidence is always good. But a decline in confidence is telling. These numbers indicate that A&D business and IT personnel – across the world – are either less sure that their organization is prepared to address the threats that confront its critical information or concerned about the possibility that governments in countries such as the U.S. will significantly increase regulatory requirements related to the treatment of sensitive defense-related data.

	2006	2007	2008	2009	2010	2011	CHANGE
Total	**91%**	86%	87%	81%	69%	**72%**	**- 19 pts**

Question 35: "How confident are you that your organization's information security activities are effective?" (Respondents who answered "Very confident" or "Somewhat confident" combined)

Section 4

The greatest opportunities for improvement

What's holding security back?

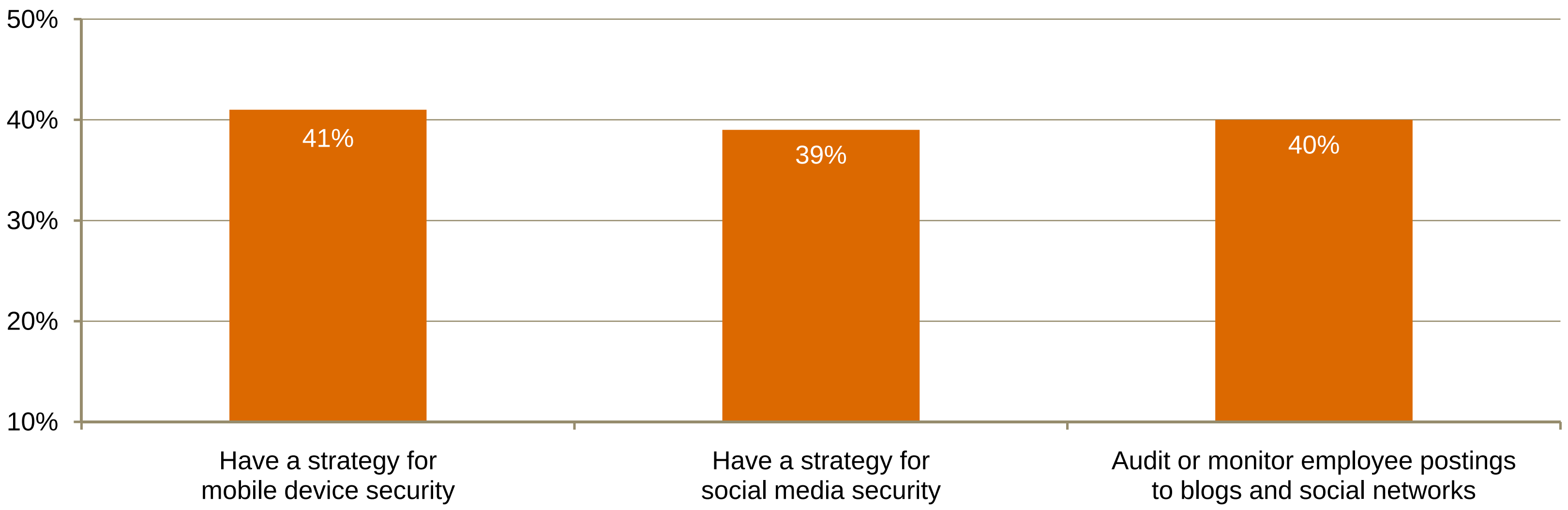
Given the austere spending environment – not just this year, but since 2008 – and a steady regression in the readiness of security capabilities, it's not surprising that A&D respondents consider insufficient capital one of the leading obstacles to the effectiveness of their organization's information security function. It's hard to keep the leading edge of prevention-oriented capabilities razor sharp when budgets are tight. What we didn't expect to find is that A&D respondents consider the single greatest obstacle to be the decision-makers "at the top of the house."

	2011
1. Leadership – CEO, president, board, or equivalent	29%
2. Insufficient capital expenditures	27%
3. Lack of an effective information security strategy	26%
4. Lack of an actionable vision or understanding	25%
5. Absence of shortage of in-house technical expertise	22%
6. Poorly integrated or overly complex information/IT systems	21%
7. Leadership – CIO or equivalent	21%
8. Leadership – CISO, CSO, or equivalent	20%

Question 27n11: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?" (Not all factors shown. Total does not add up to 100%.)

Mobile devices and social media: New rules are in effect this year – but not yet critical mass.

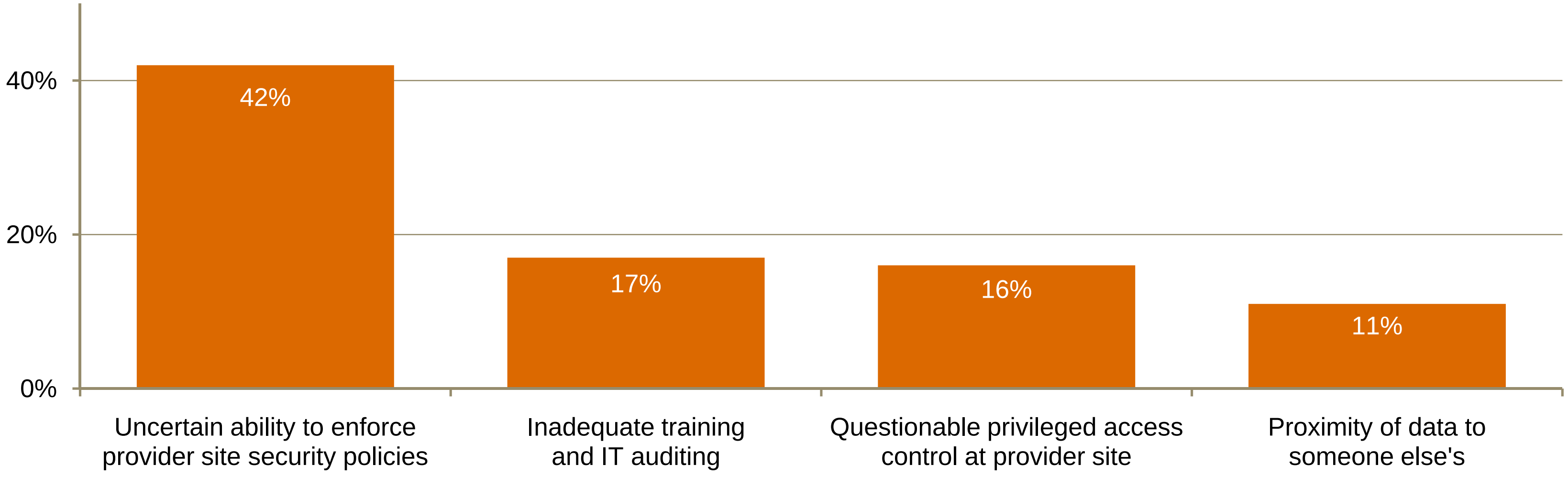
The possibility of having thousands of highly confidential files made public is keeping many – but not all – A&D decision-makers up at night. Some view this risk as just one among other important issues they're focused on.



Question 17: "What process information security safeguards does your organization currently have in place?" (Not all factors shown. Total does not add up to 100%.)

Cloud computing: Is it improving information security? Yes, but many want better enforcement of provider security policies.

This year, about half of all A&D respondents (48%) report that their organization uses cloud services – and 70% of those that do say the cloud has improved their information security. Responses also revealed that, while the leading security risk to cloud computing is enforcing the provider's security policies, A&D respondents are also concerned about inadequate training and IT auditing as well as access control at provider sites.



Question 41: "Does your organization currently use cloud services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or Infrastructure-as-a-Service (IaaS)?" Question 41c: "What impact has cloud computing had on your company's information security?" Question 41b: "What is the greatest security risk to your cloud computing strategy?" (Not all factors shown. Total does not add up to 100%.)

For more information, please contact:

National Security Contacts

Gary Loveland
Principal, National Security Leader
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

Aerospace & Defense Contacts

Fred Rica
Principal
973.236.4052
frederick.j.rica@us.pwc.com

Mike Amadei
Director
703.918.3051
michael.d.amadei@us.pwc.com

Or visit www.pwc.com/giss2012

This document is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

www.pwc.com/security

Eye of the storm

As the global economy stalls and information security threats such as cyber crime and Advanced Persistent Threats cloud the horizon, many see sunshine and clear skies overhead

CIO Business Technology Leadership

CSO BUSINESS RISK LEADERSHIP

Automotive

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

September 2011

pwc

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*

The economic thunderheads of 2008 may have passed. But across the global automotive industry, some clouds 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.

Nonetheless, according to PwC's 2012 Global State of Information Security Survey®, the majority of automotive executives are confident in the effectiveness of their information security practices.

They have an effective strategy in place. They consider their organizations proactive in executing it. And funding expectations are running high.

Yet all is not in order. Security event frequency is up. Third-party risks have begun to increase. And respondents are far more concerned about protecting customer data than they were twelve months ago.

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, the reasons to do so quickly and strategically are mounting.

Agenda

Section 1.	Methodology
Section 2.	Confidence and progress
Section 3.	Signs of vulnerability and exposure
Section 4.	The greatest opportunities for improvement

Section 1

Methodology

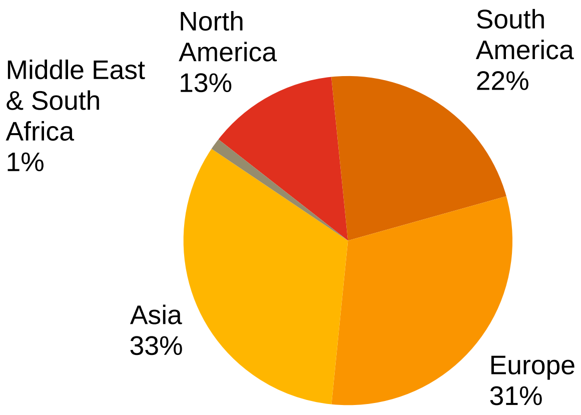
A worldwide study

The 2012 Global State of Information Security Survey®, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 10, 2011 to April 18, 2011.

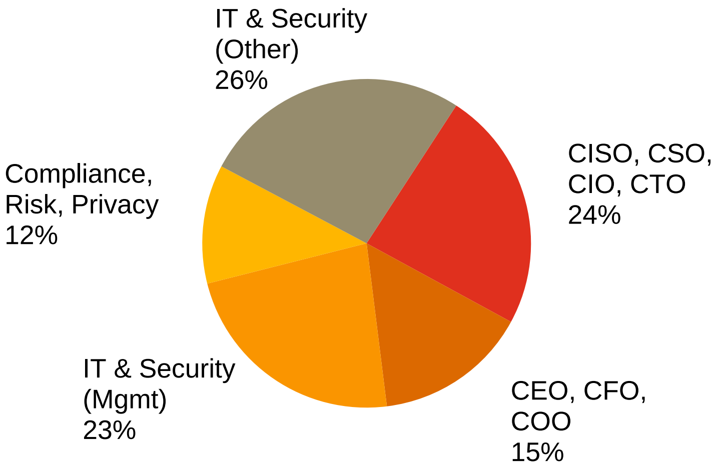
- PwC’s 14th year conducting the online survey, 9th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 138 countries
- More than 9,600 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-one percent (31%) of respondents from companies with revenue of $500 million+
- Survey included 265 respondents from the global automotive industry
- The margin of error is less than 1%

Demographics

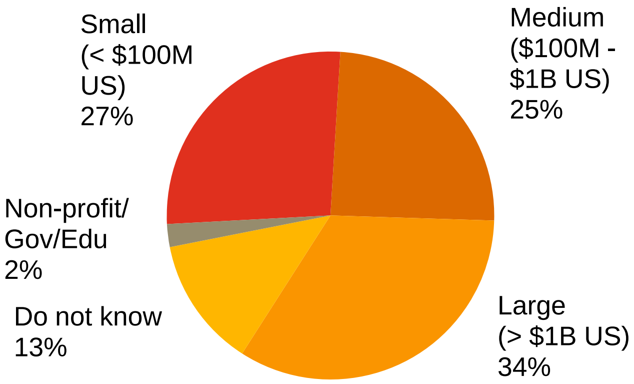
Automotive respondents by region of employment



Automotive respondents by title



Automotive respondents by company revenue size



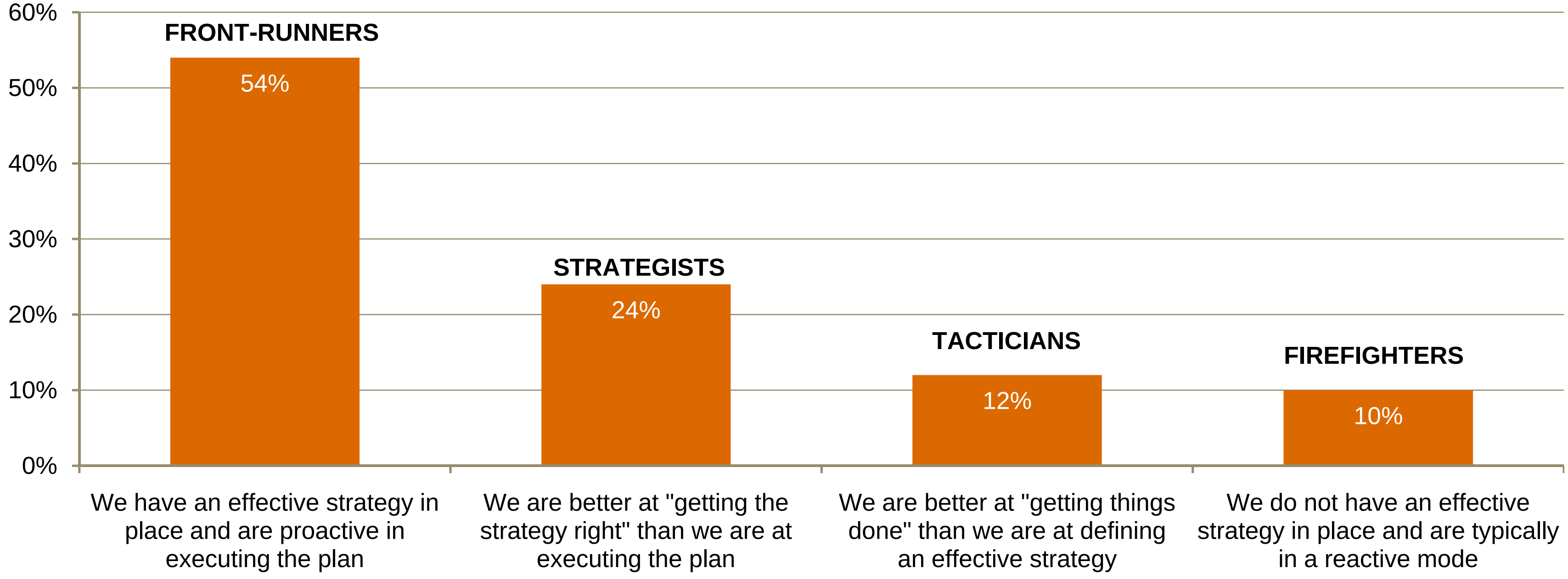
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

Confidence and progress

Most respondents from the automotive industry see their organization as a “front-runner.”

More than half (54%) of this year’s automotive industry respondents say their organization has a strategy in place and is proactive in executing it.



Question 26n11: “Which statement best characterizes your organization’s approach to protecting information security?”

They are also highly confident in their organization’s security.

A clear majority – 83% – of industry respondents are also confident that their organization’s information security initiatives are effective.

	2011
Very confident	**38%**
Somewhat confident	**45%**
Total	**83%**

Question 35: “How confident are you that your organization’s information security activities are effective?”

Insights into the frequency, type, and source of security breaches have leaped dramatically over the past 12 months.

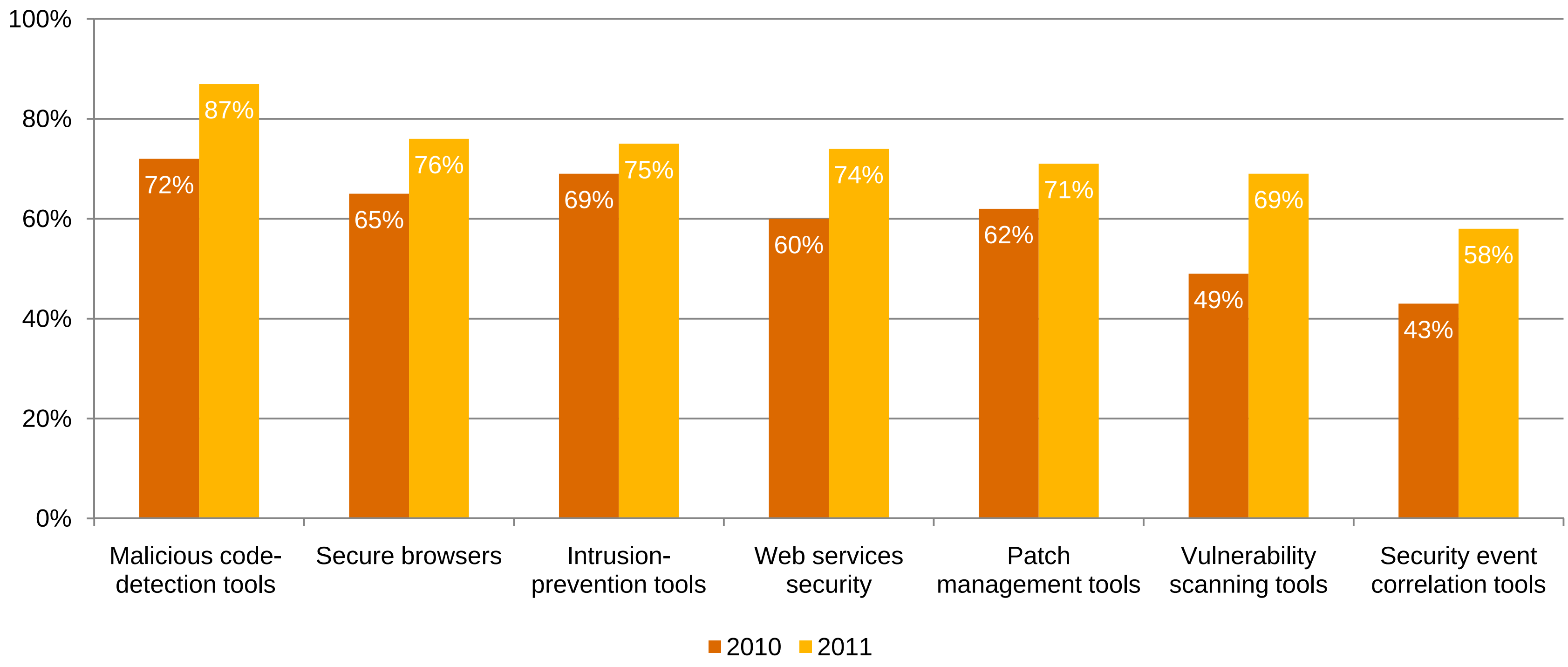
Just a few years ago, as many as 39% of automotive respondents couldn’t answer the most basic questions about the nature of security-related breaches. Now, 88% or more of automotive industry respondents can answer specific survey questions about factors such as security event frequency, type, and source.

Respondents who answered “Do not know” or “Unknown”	2007	2008	2009	2010	2011
How many incidents occurred in past 12 months?	39%	33%	24%	16%	**4%**
What type of incident occurred?	34%	47%	36%	25%	**8%**
What was the source of the incident?	N/A	38%	39%	27%	**12%**

Question 19: “Number of security incidents in the past 12 months.” Question 20: “What types of security incidents (breach or downtime) occurred?” Question 22: “Estimated likely source of incident.” (Totals do not add up to 100%.)

Many automotive companies are proactively adopting safeguards to bolster data security and prevent cyber crime.

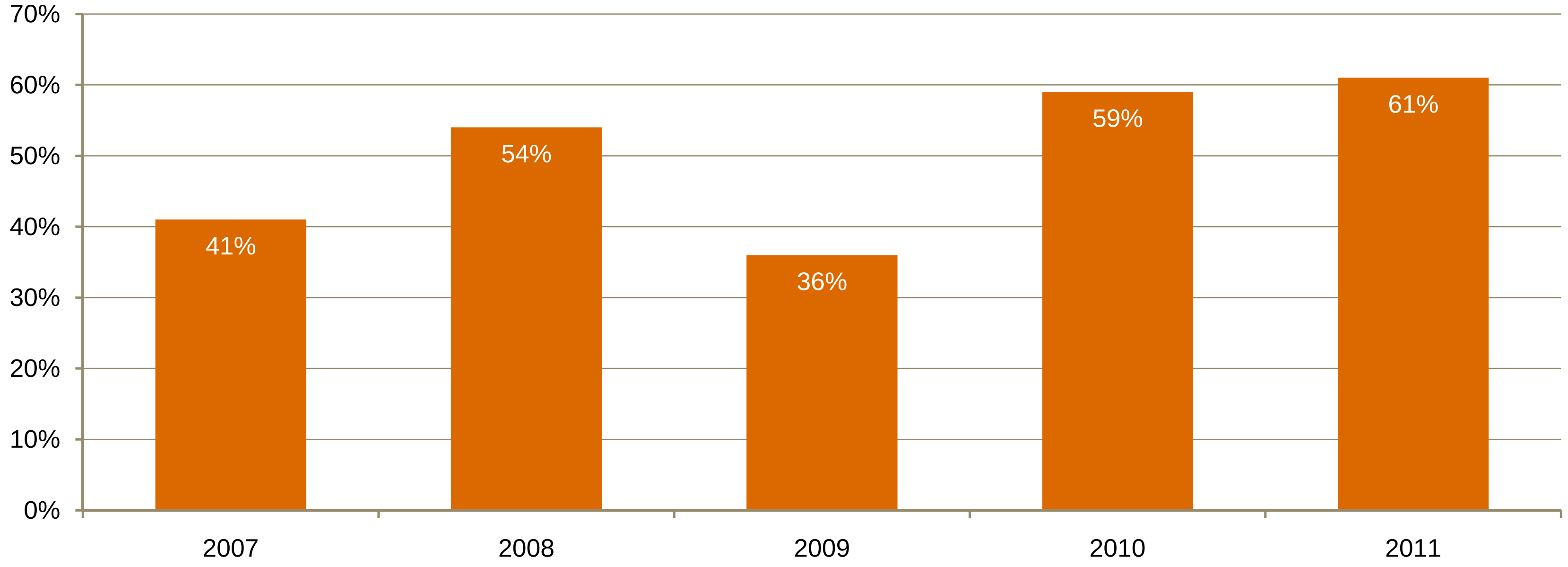
Over the past year, automotive companies have made solid gains in strengthening detection and prevention safeguards to protect information from potential breaches.



Question 18: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown. Totals do not add up to 100%.)

At the same time, most automotive respondents are optimistic about security spending over the next 12 months.

Will security spending in the industry increase? Optimism carries the day. More than half (61%) of automotive industry respondents believe that it will. This level of expectation is the highest it has been in the industry since before the 2008 economic downturn.



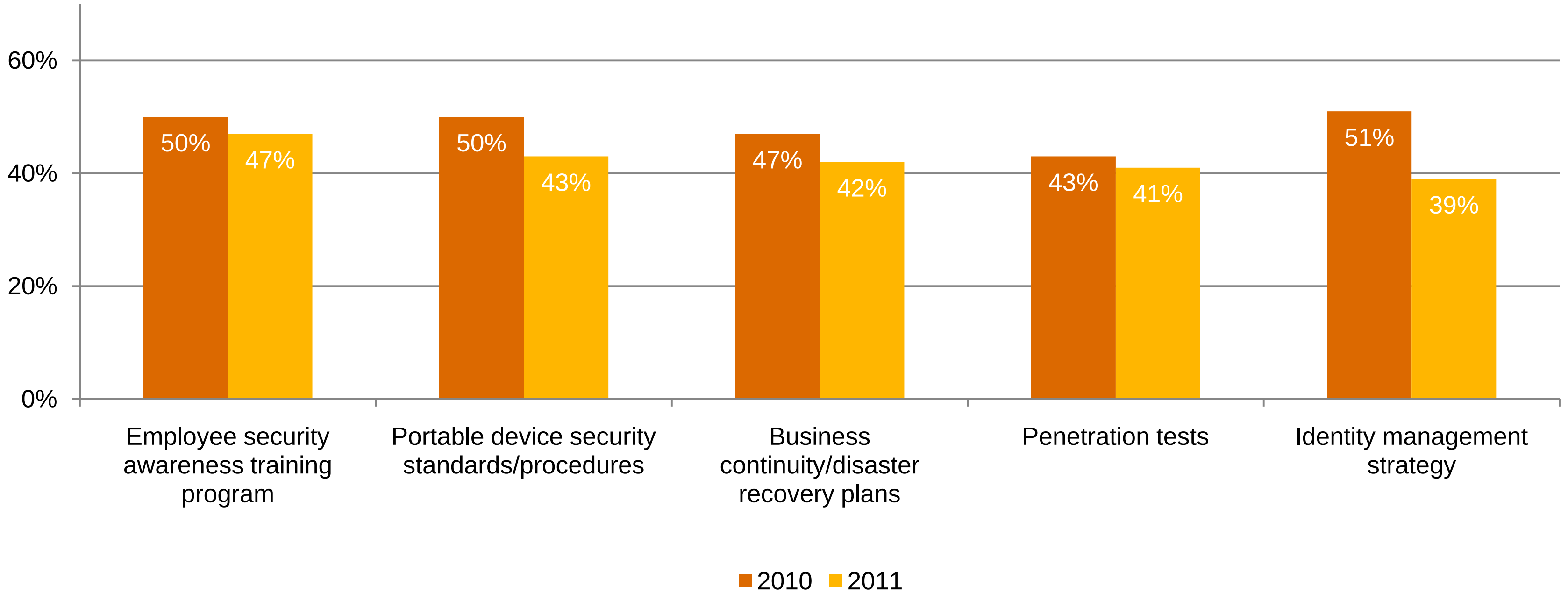
Question 9: “When compared with last year, security spending over the next 12 months will:” (Respondents who answered “Increase up to 10%,” “Increase 11-30%,” or “Increase more than 30%”)

Section 3

Signs of vulnerability and exposure

Advanced Persistent Threats: They can be devastating – but just how prepared are automotive companies to address them?

While 19% of automotive respondents say their organization has a security policy that addresses APT, many lack the tools to combat these new threats.



Question 28" "Which of the following elements, if any, are included in your organization's security policy?" Question 17: "What process information technology security safeguards does your organization currently have in place?" (Not all factors shown. Totals do not add up to 100%.)

Other trends in this year's survey are also troubling. Take the increase in security events, for example.

It is tempting to trumpet the fact that almost one in three (31%) of all automotive industry respondents report no security events in the past year. Yet incidents increased significantly this year among respondents indicating 10 or more negative events.

Number of security incidents	2007	2008	2009	2010	2011
No incidents	16%	26%	17%	27%	31%
1 to 9 incidents	39%	31%	36%	47%	45%
10 to 49 incidents	4%	6%	14%	8%	12%
50 or more incidents	2%	3%	9%	3%	7%

Question 19: "Number of security incidents in the past 12 months." (Totals do not add up to 100%.)

This year's results reveal regression in a key best practice – and a leap in the percentage of CISOs reporting to the CIO.

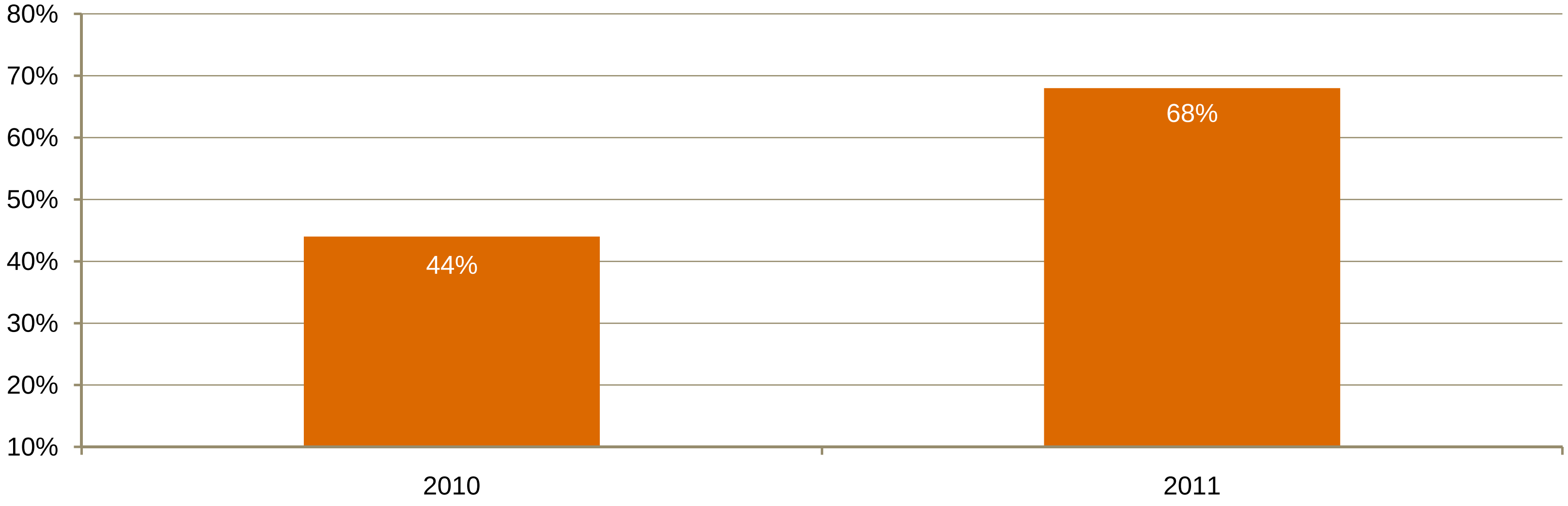
Reversing a multi-year trend, the number of automotive industry respondents who say their Chief Information Security Officer (or equivalent executive) reports to the CIO increased 180% over last year.

Whom the CISO reports to	2007	2008	2009	2010	2011
Board of Directors	24%	28%	24%	33%	**33%**
Chief Executive Officer	35%	28%	41%	44%	**45%**
Chief Financial Officer	6%	6%	11%	19%	**18%**
Chief Information Officer	65%	42%	39%	15%	**42%**

Question 16a: "Where/to whom does your CISO or equivalent senior information security officer report?" (Not all factors shown. Totals do not add up to 100%.)

Concern about protecting customer data has surged this year – though core data protections are often weak or absent.

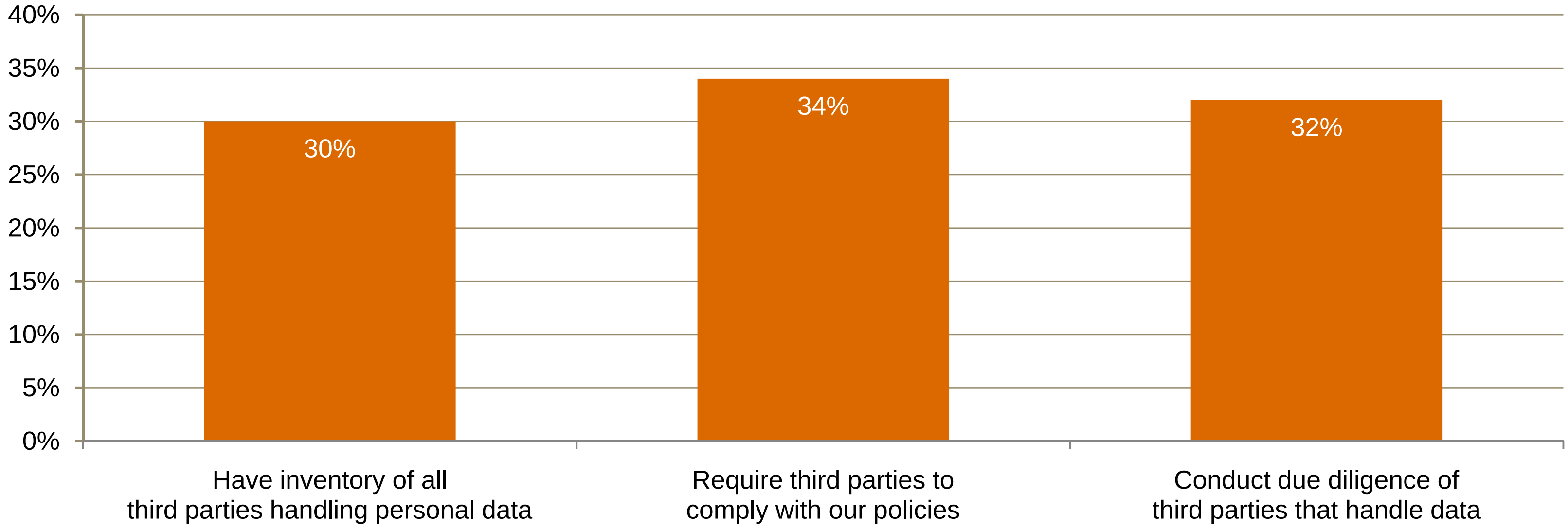
Industry respondents report a tremendous increase (55%) in the level of importance now placed upon protecting customer data – from 44% last year to 68% this year. Yet fewer than half report that their organization keeps an accurate inventory of employee and customer data (40%), has a security policy that addresses data protection, disclosure and destruction (42%) and encrypts backup media (49%).



Question 32n11: “What level of importance does your company place on protecting the following types of information? Customer information” Questions15 and 18 “Which data privacy/technology information security safeguards does your organization have in place?” Question 28: “Which of the following elements, if any, are included in your organization’s security policy?”

Third party risk is on the rise.

Since 2008, the percentage of industry respondents that consider partners or suppliers the likely source of security breaches has more than doubled – from 8% to 19%. Is the industry combating this risk? Not necessarily. Many have not yet established strategies and practices governing service providers and other third parties.



Question 22: “Estimated likely source of incident.” Question 15: “Which data privacy safeguards does your organization have in place?” (Not all factors shown. Total does not add up to 100%.)

Section 4

The greatest opportunities for improvement

What's holding security back?

Given the austere spending environment, it would make sense if industry respondents considered insufficient capital one of the leading obstacles to the effectiveness of their organization's information security function.

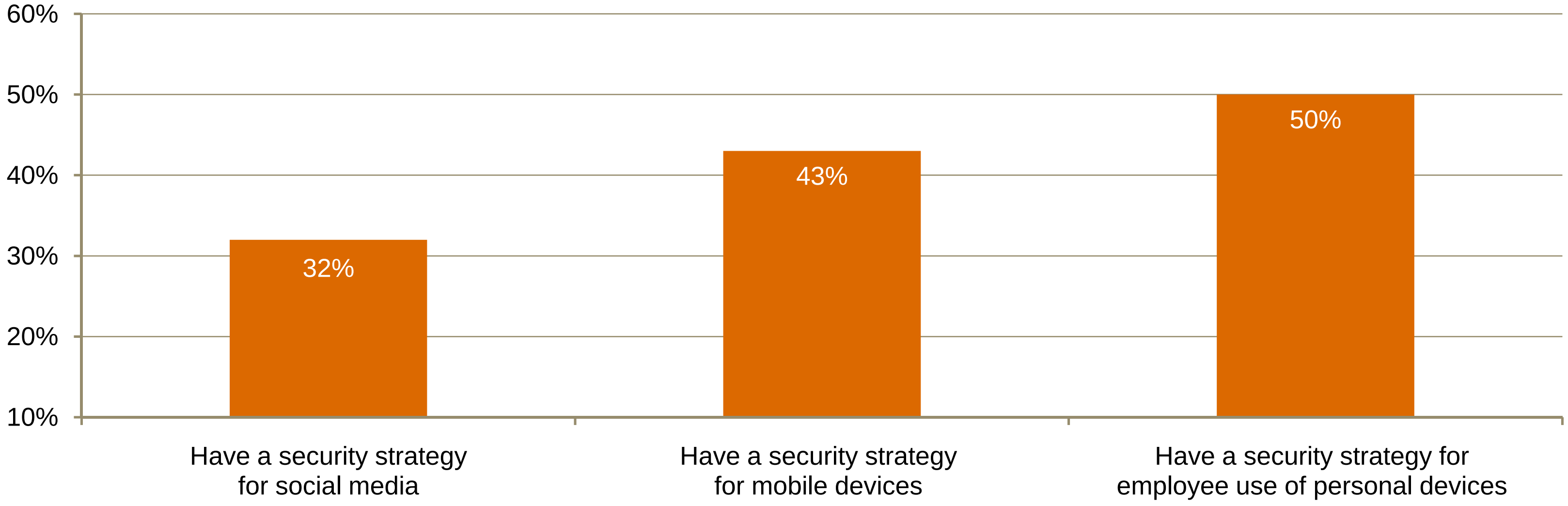
Surprisingly, they don't. More than one out of three point to the lack of an actionable vision, and almost as many reference the absence of an effective information security strategy.

	2011
1. Lack of an actionable vision or understanding	34%
2. Lack of an effective information security strategy	28%
3. Leadership – CEO, President, Board, or equivalent	27%
4. Leadership – CIO or equivalent	27%
5. Insufficient capital expenditures	26%
6. Absence or shortage of in-house technical expertise	23%
7. Insufficient operating expenditures	21%

Question 27n11: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?" (Not all factors shown. Total does not add up to 100%.)

Mobile devices and social media: New rules are in effect this year – but adoption has yet to reach critical mass.

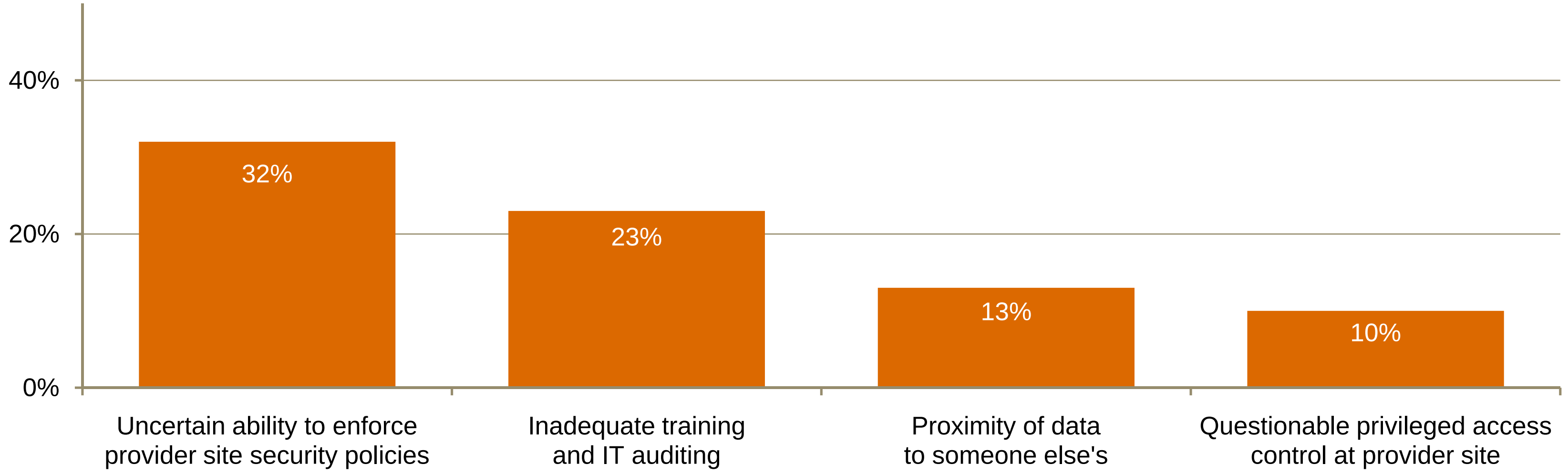
Automotive companies are implementing strategies to keep pace with employee adoption of new technologies – including use of mobile devices and social-networking tools – and are creating rules about how employees can use personal technology within the enterprise.



Question 17: “What process information security safeguards does your organization currently have in place?” (Not all factors shown. Total does not add up to 100%.)

Cloud computing continues to evolve this year, but many respondents want better enforcement of provider security policies.

This year, almost half (49%) of automotive respondents report that their organization uses cloud services. Among those that have adopted cloud solutions, 77% say the technology has improved their security posture. Responses also revealed that while enforcing provider security policies is seen as the principal security challenge, respondents are also concerned about training as well as multi-tenancy issues.



Question 41: “Does your organization currently use cloud services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or Infrastructure-as-a-Service (IaaS)?” Question 41c: “What impact has cloud computing had on your company’s information security?” Question 41b: “What is the greatest security risk to your cloud computing strategy?” (Not all factors shown. Total does not add up to 100%.)

For more information, please contact:

National Security Contacts

Gary Loveland
Principal, National Security Leader
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

Automotive Contacts (North America)

Brian Decker
US Automotive Advisory Leader
313.394.6263
brian.d.decker@us.pwc.com

Michael Compton
Principal
313.394.3535
michael.d.compton@us.pwc.com

Or visit www.pwc.com/giss2012

www.pwc.com/security

Eye of the storm

As the global economy stalls and information security threats such as cyber crime and Advanced Persistent Threats cloud the horizon, many see sunshine and clear skies overhead

CIO Business Technology Leadership

CSO BUSINESS RISK LEADERSHIP

Entertainment & Media

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

September 2011

pwc

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

The economic thunderheads of 2008 may have passed. But across the global entertainment and media (E&M) industry, some clouds 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.

Nonetheless, according to PwC's 2012 Global State of Information Security Survey®, the vast majority of E&M executives are confident in the effectiveness of their information security practices.

They have an effective strategy in place. They consider their organizations proactive in executing it. And funding expectations are running high.

Yet all is not in order. Security event frequency is up. Risks associated with partners and suppliers are on the rise. And more than half of respondents report that their organization cannot yet fully detect unauthorized access.

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, the reasons to do so quickly and strategically are mounting.

Agenda

Section 1.	Methodology
Section 2.	Confidence and progress
Section 3.	Signs of vulnerability and exposure
Section 4.	The greatest opportunities for improvement

Section 1

Methodology

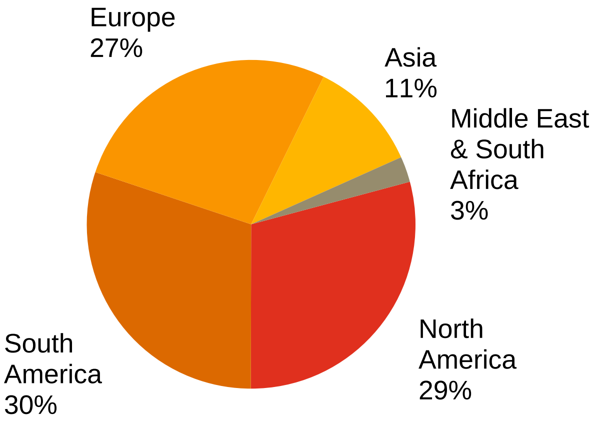
A worldwide study

The 2012 Global State of Information Security Survey®, a worldwide study by PwC, CIO Magazine and CSO Magazine, was conducted online from February 10, 2011 to April 18, 2011.

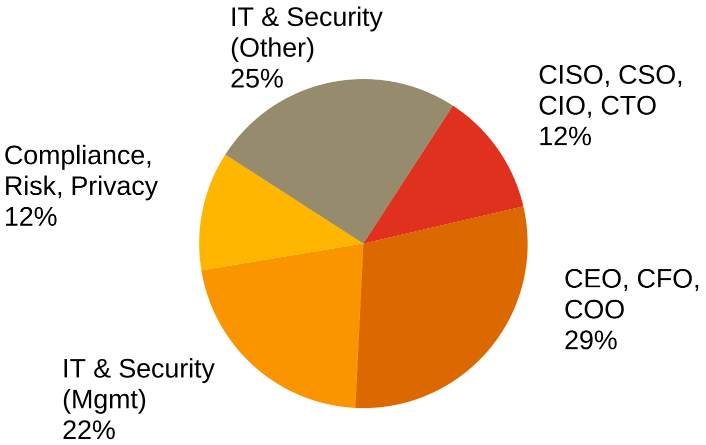
- PwC's 14th year conducting the online survey, 9th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 138 countries
- More than 9,600 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-one percent (31%) of respondents from companies with revenue of $500 million+
- Survey included 435 respondents from the entertainment and media (E&M) industry
- The margin of error is less than 1%

Demographics

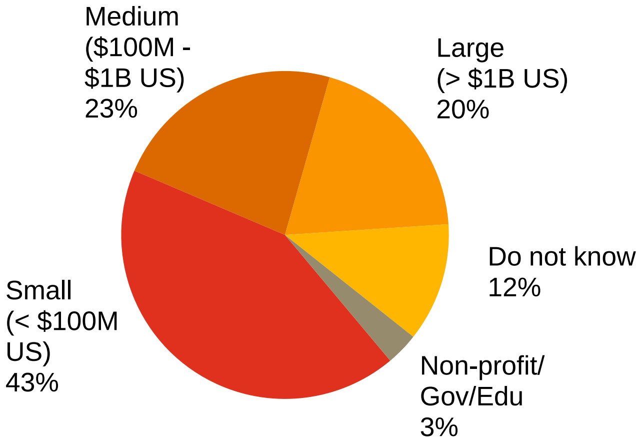
E&M respondents by region of employment



E&M respondents by title



E&M respondents by company revenue size



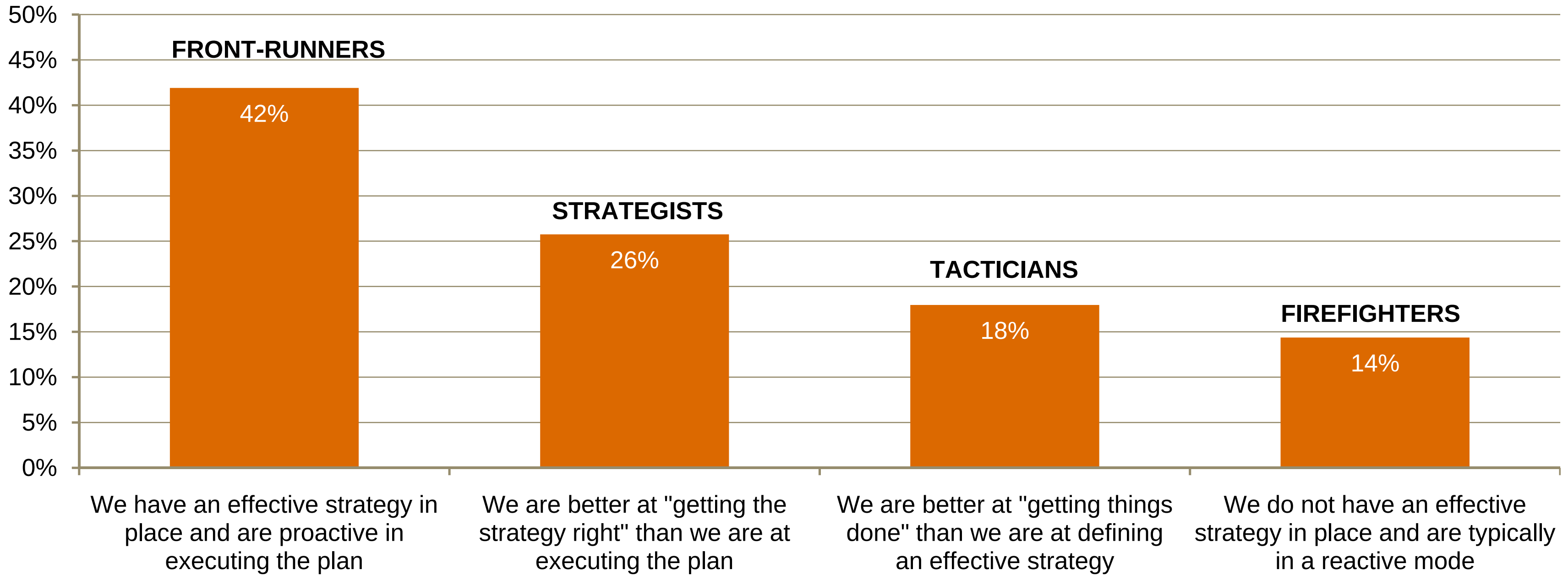
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

Confidence and progress

Most E&M respondents see their organization as a “front-runner.”

Almost half of this year’s E&M respondents (42%) say their organization has a strategy in place and is proactive in executing it.



Question 26n11: “Which statement best characterizes your organization’s approach to protecting information security?”

They are also highly confident in their organization’s security.

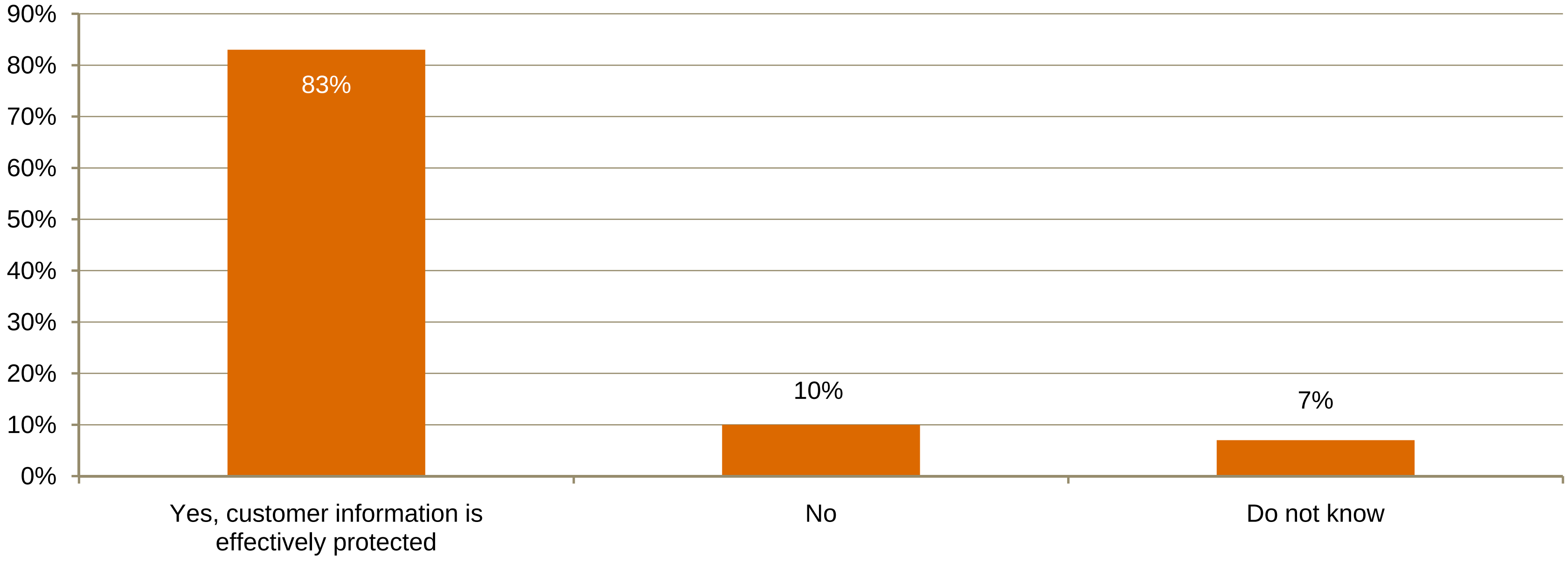
This year, a clear majority – 69% – of E&M respondents are also confident that their organization’s information security activities are effective.

	2011
Very confident	**34%**
Somewhat confident	**35%**
Total	**69%**

Question 35: “How confident are you that your organization’s information security activities are effective?”

Customer information is safe with us – at least in the opinion of most E&M respondents.

Although major data breaches impacting customer data are occurring across industries, E&M respondents do not appear overly concerned. More than three-quarters (83%) report that their organization is effectively protecting customer information.



(Asked only of Entertainment & Media respondents) Question 4a: "Does your organization have effective security to protect customer information?"

Insights into the frequency, type, and source of security breaches have leaped dramatically over the past 12 months.

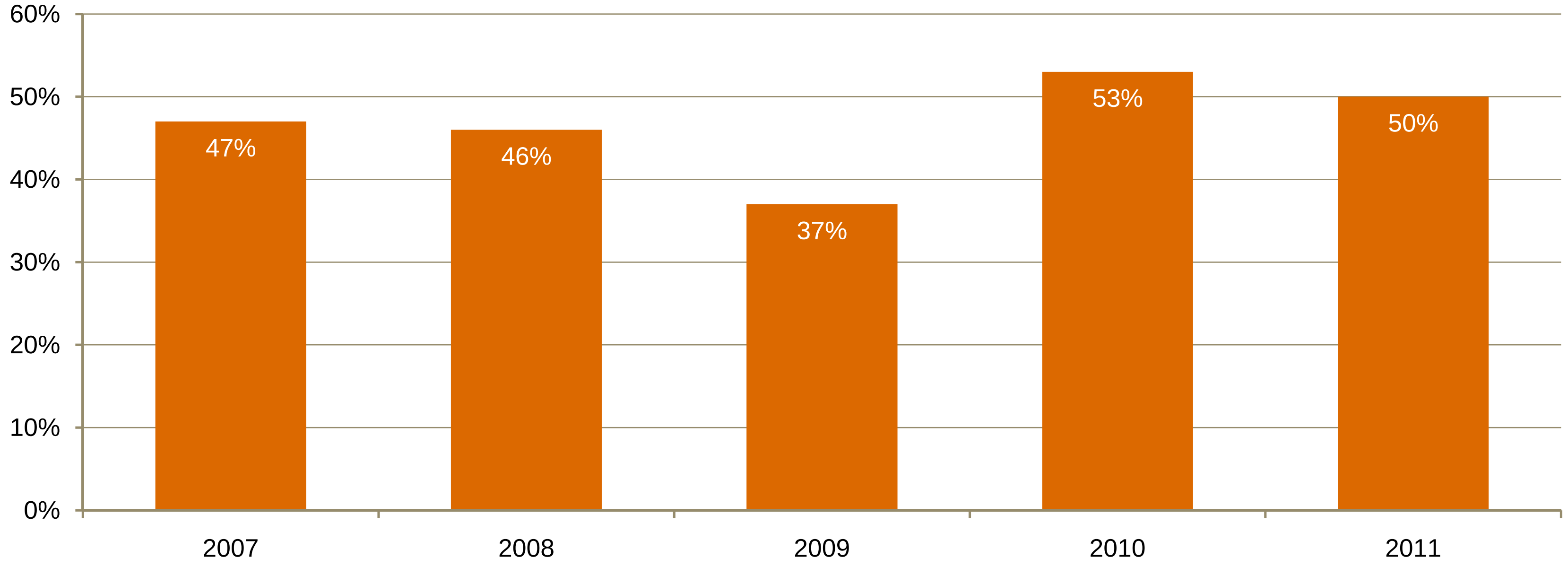
Just a few years ago, a great number of this survey’s E&M respondents couldn’t answer the most basic questions about the nature of security-related breaches. Now, approximately 80% or more of E&M respondents can answer specific survey questions about factors such as security event frequency, type, and source.

Respondents who answered “Do not know” or “Unknown”	2008	2009	2010	2011
How many incidents occurred in past 12 months?	28%	31%	14%	**6%**
What type of incident occurred?	44%	36%	27%	**14%**
What was the source of the incident?	43%	40%	30%	**18%**

Question 19: “Number of security incidents in the past 12 months.” Question 20: “What types of security incidents (breach or downtime) occurred?” Question 22: “Estimated likely source of incident.” (Totals do not add up to 100%.)

At the same time, half of E&M respondents are "bullish" about security spending over the next 12 months.

Will security spending in the industry increase? Optimism carries the day. Half of E&M respondents believe that it will.



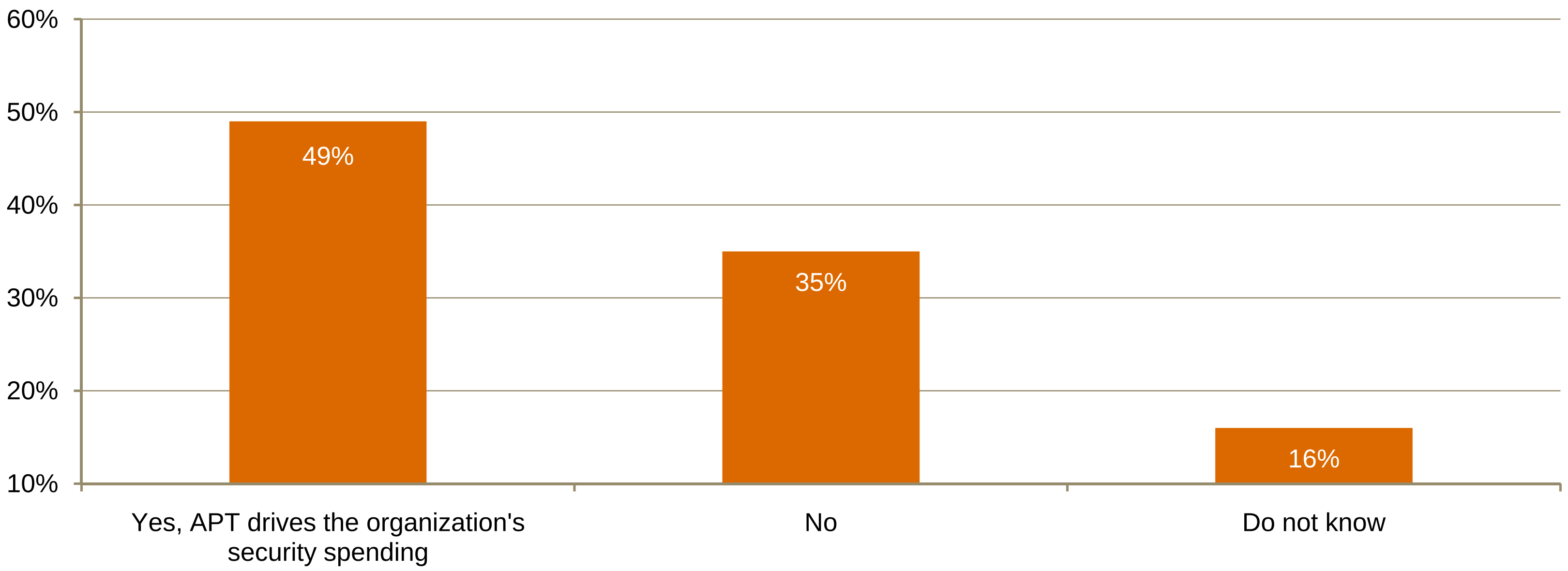
Question 9: "When compared with last year, security spending over the next 12 months will:" (Respondents who answered "Increase up to 10%," "Increase 11-30%," or "Increase more than 30%")

Section 3

Signs of vulnerability and exposure

Advanced Persistent Threats: They can be devastating – but just how concerned are E&M organizations about addressing them?

Nearly half of all E&M respondents (49%) stated that APT was driving their organization’s security spending. That’s a big number – especially given the fact that only 14% report that their organization’s security policies specifically address APT.



Question 6 (E&M): “Does Advanced Persistent Threat drive your organization’s security spending?” Question 28: “Which of the following elements, if any, are included in your organization’s security policy?”

Other trends in this year's survey are also troubling. Take the increase in security events, for example.

It is tempting to trumpet the fact that nearly three out of ten E&M respondents (29%) report no security events in the past year. Yet reports of incidents increased this year among respondents indicating 50 or more negative events.

Number of security incidents	2007	2008	2009	2010	2011
No incidents	24%	31%	19%	32%	**29%**
1 to 9 incidents	29%	34%	33%	40%	**40%**
10 to 49 incidents	6%	4%	11%	11%	**11%**
50 or more incidents	6%	3%	6%	4%	**13%**

Question 19: "Number of security incidents in the past 12 months." (Totals do not add up to 100%.)

The compromise of digital media is now at a dangerously high level. And the source of the risk? Insiders.

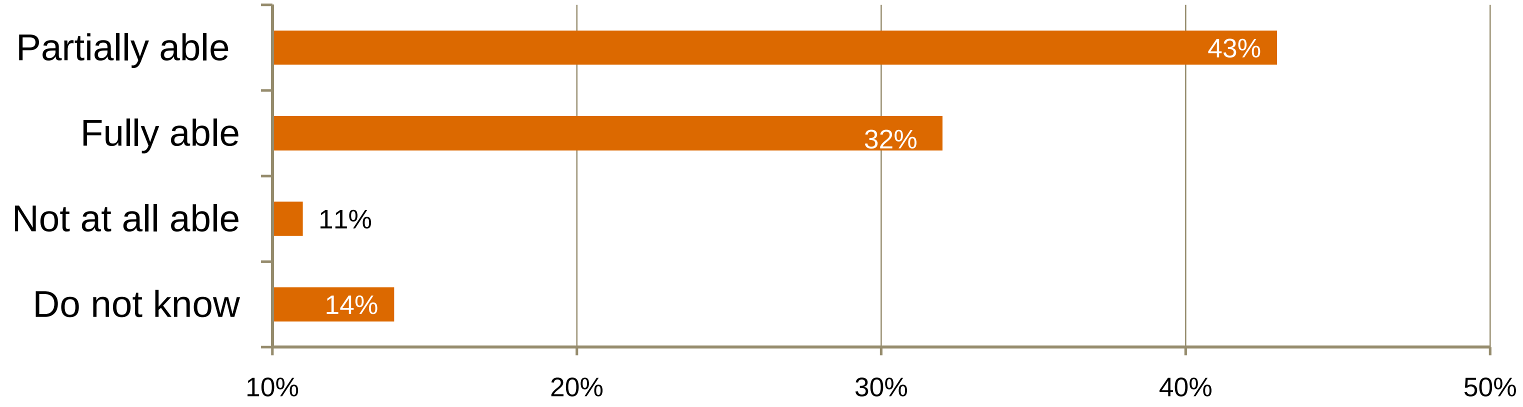
More than one out of three (37%) of E&M respondents report their organization had an incident in which digital media was stolen prior to a major launch. That is a significant number. What was the source of the theft? Insiders – current and former employees as well as partners and suppliers.

Source of incident	2011
Former employee	**38%**
Employee	**27%**
Partner/supplier	**16%**
Outsider/customer	**12%**
Do not know	**7%**

Question 2 (E&M): "In the past year, has your organization had an incident in which digital media has been stolen prior to a major launch window (e.g., theatrical, DVD)?" Question 2a (E&M): "Identify the likely source of that incident.."

Detecting unauthorized access to digital content is a challenge, according to many E&M respondents.

Is the industry prepared to counter threats to digital content? No – at least, not most E&M organizations. Less than one-third (32%) of E&M respondents reported that their organization was fully able to detect unauthorized access to high-value digital content.



Question 3 (E&M): “Is your organization able to detect unauthorized access to high-value digital content (e.g., digital masters)?”

In fact, this year's survey reveals degradation in many of the E&M industry's strategic security and privacy processes.

While the industry is investing in detection, prevention and web-based technologies to harden the perimeter, many core processes that support information security and privacy across E&M operations are showing signs of deterioration. This is true for capabilities that range from security baselines for multiple entities to training and background checks.

	2009	2010	2011
Vulnerability scanning tools	54%	50%	**60%**
Intrusion prevention tools	60%	57%	**71%**
Security baselines for partners, customers, vendors	46%	41%	**32%**
Centralized security information management	49%	40%	**32%**
Employee security awareness training program	48%	38%	**35%**
Conduct personnel background checks	63%	53%	**50%**
Accurate inventory of employees' and customers' personal data	36%	32%	**31%**
Due diligence of third parties handling personal data	33%	29%	**25%**
Employ Chief Privacy Officer	38%	34%	**32%**

Question 15: "What data privacy safeguards does your organization have in place?" Question 16: "What information security safeguards related to people does your organization have in place?" Question 17: "What information security safeguards related to process does your organization have in place?" Question18: "What technology information security safeguards does your organization currently have in place?"

And that high confidence rating? It has actually declined 13 points since 2006.

Confidence is always good. But a decline in confidence is telling. These numbers indicate that E&M business and IT personnel – across the world – are less sure that their organization is prepared to address the threats that confront its critical information.

	2006	2007	2008	2009	2010	2011	CHANGE
Total	**83%**	76%	84%	78%	65%	**70%**	**- 13 pts**

Question 35: "How confident are you that your organization's information security activities are effective?" (Respondents who answered "Very confident" or "Somewhat confident" combined)

Section 4

The greatest opportunities for improvement

What’s holding security back?

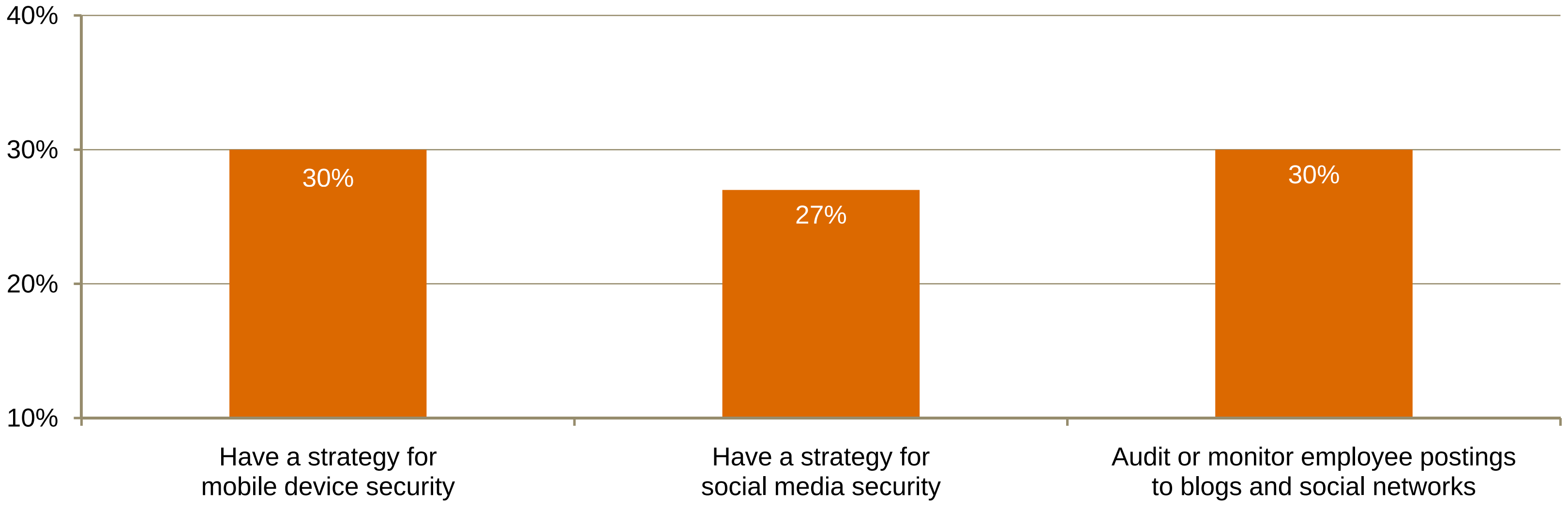
Given the austere spending environment – not just this year, but since 2008 – and a steady regression in the readiness of security capabilities, it’s not surprising that E&M respondents consider insufficient capital one of the leading obstacles to the effectiveness of their organization’s information security function. It’s hard to keep the leading edge of prevention-oriented capabilities razor sharp when budgets are tight. What we didn’t expect to find is that E&M respondents consider the single greatest obstacle to be the decision-makers “at the top of the house.”

	2011
Insufficient capital expenditures	**31%**
Lack of an effective information security strategy	**25%**
Insufficient operating expenditures	**24%**
Leadership – CEO, President, Board or equivalent	**23%**
Absence or shortage of in-house technical expertise	**23%**

Question 27n11: “What are the greatest obstacles to improving the overall strategic effectiveness of your organization’s information security function?” (Not all factors shown. Total does not add up to 100%.)

Mobile devices and social media: New corporate safeguards are in effect this year – but not yet critical mass.

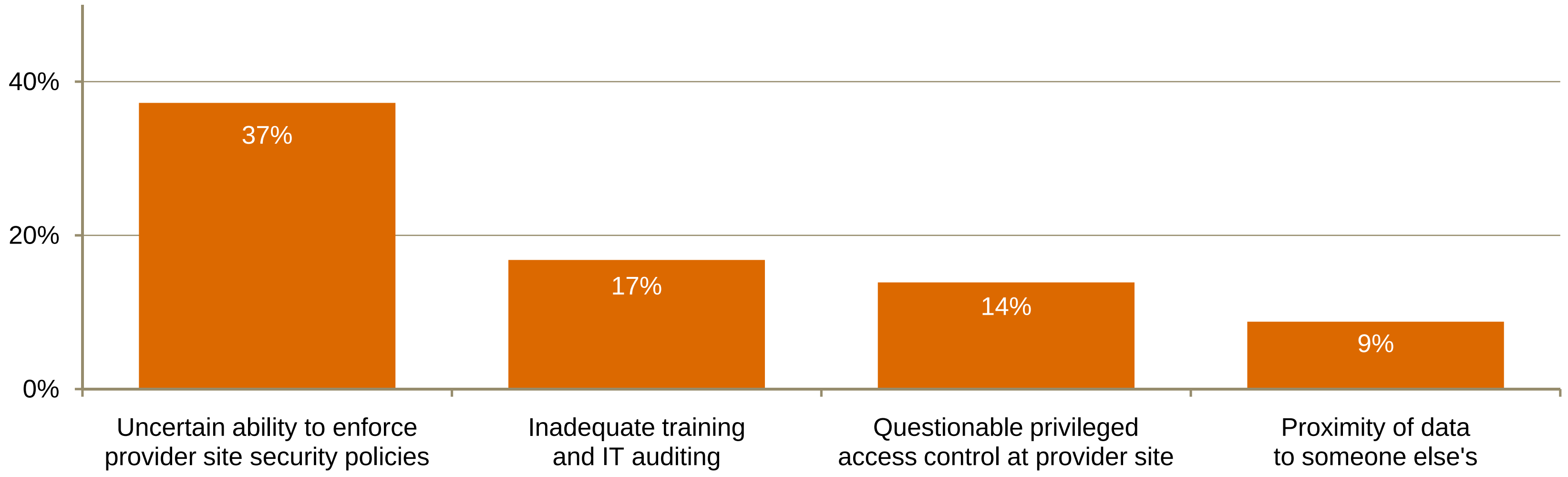
E&M companies are implementing strategies to keep pace with employee adoption of new technologies – particularly the use of mobile devices and social-networking tools – and are creating rules about how employees can use personal technology within the enterprise.



Question 17: “What process information security safeguards does your organization currently have in place?” (Not all factors shown. Total does not add up to 100%.)

Cloud computing: Is it improving information security? Yes, but many want better enforcement of provider security policies.

This year, about half of all E&M respondents (45%) report that their organization uses cloud services – and 47% of those say the cloud has improved their information security. Responses also revealed that while enforcing provider security policies is seen as the principal security challenge, respondents are also concerned about training as well as multi-tenancy issues.



Question 41: “Does your organization currently use cloud services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or Infrastructure-as-a-Service (IaaS)?” Question 41c: “What impact has cloud computing had on your company’s information security?” Question 41b: “What is the greatest security risk to your cloud computing strategy?” (Not all factors shown. Total does not add up to 100%.)

For more information, please contact:

National Security Contacts

Gary Loveland
Principal, National Security Leader
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

Entertainment & Media Contact

Deborah Bothun
Principal, Entertainment & Media Leader
213.217.3302
deborah.k.bothun@us.pwc.com

Or visit www.pwc.com/giss2012

www.pwc.com/security

Eye of the storm

As the global economy stalls and information security threats such as cyber crime and Advanced Persistent Threats cloud the horizon, many see sunshine and clear skies overhead

Financial Services

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

September 2011

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*

The economic thunderheads of 2008 may have passed. But across the global financial services industry, some clouds 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.

Nonetheless, according to PwC’s 2012 Global State of Information Security Survey®, the vast majority of financial services executives are confident in the effectiveness of their information security practices.

They have an effective strategy in place. They consider their organizations proactive in executing it. And the business impacts of security incidents appear to have declined – across the board.

Yet all is not in order. Security event frequency is up. Strategic security processes are beginning to degrade. And the capital and operating expenditures crucial to early prevention and agile response are more like to be deferred or canceled than at any time since 2008.

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, the reasons to do so quickly and strategically are mounting.

Agenda

Section 1. Methodology

Section 2. Confidence and progress

Section 3. Signs of vulnerability and exposure

Section 4. The greatest opportunities for improvement

Section 1

Methodology

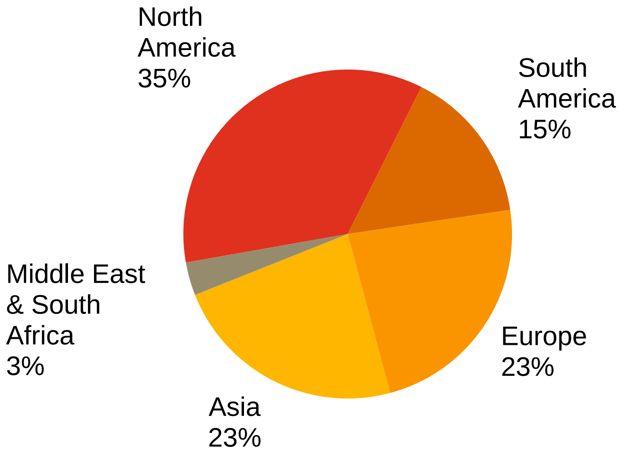
A worldwide study

The 2012 Global State of Information Security Survey®, a worldwide study by PwC, CIO Magazine and CSO Magazine, was conducted online from February 10, 2011 to April 18, 2011.

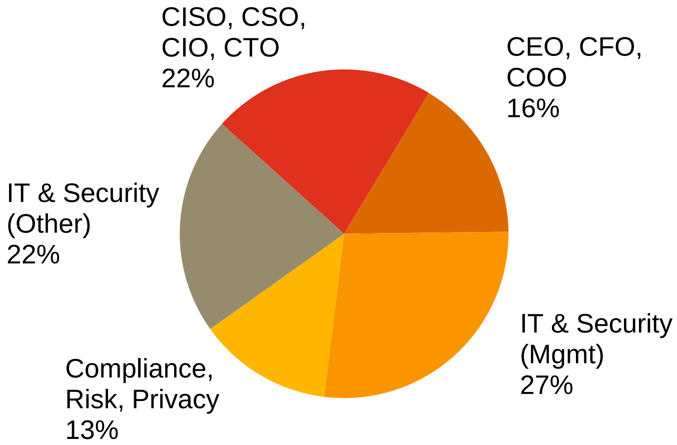
- PwC’s 14th year conducting the online survey, 9th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 138 countries
- More than 9,600 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-one percent (31%) of respondents from companies with revenue of $500 million+
- Survey included 1,293 respondents from the financial services (FS) industry
- The margin of error is less than 1%

Demographics

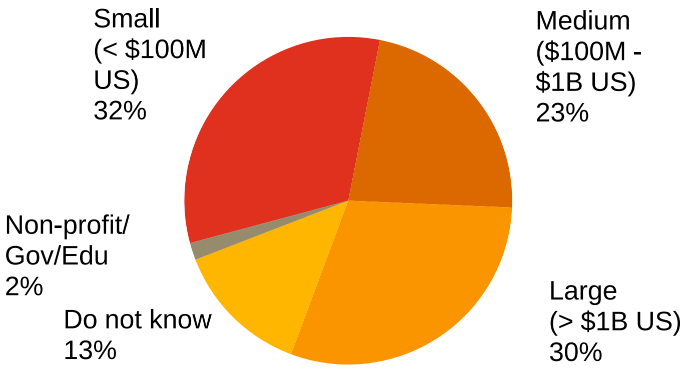
Financial services respondents by region of employment



Financial services respondents by title



Financial services respondents by company revenue size



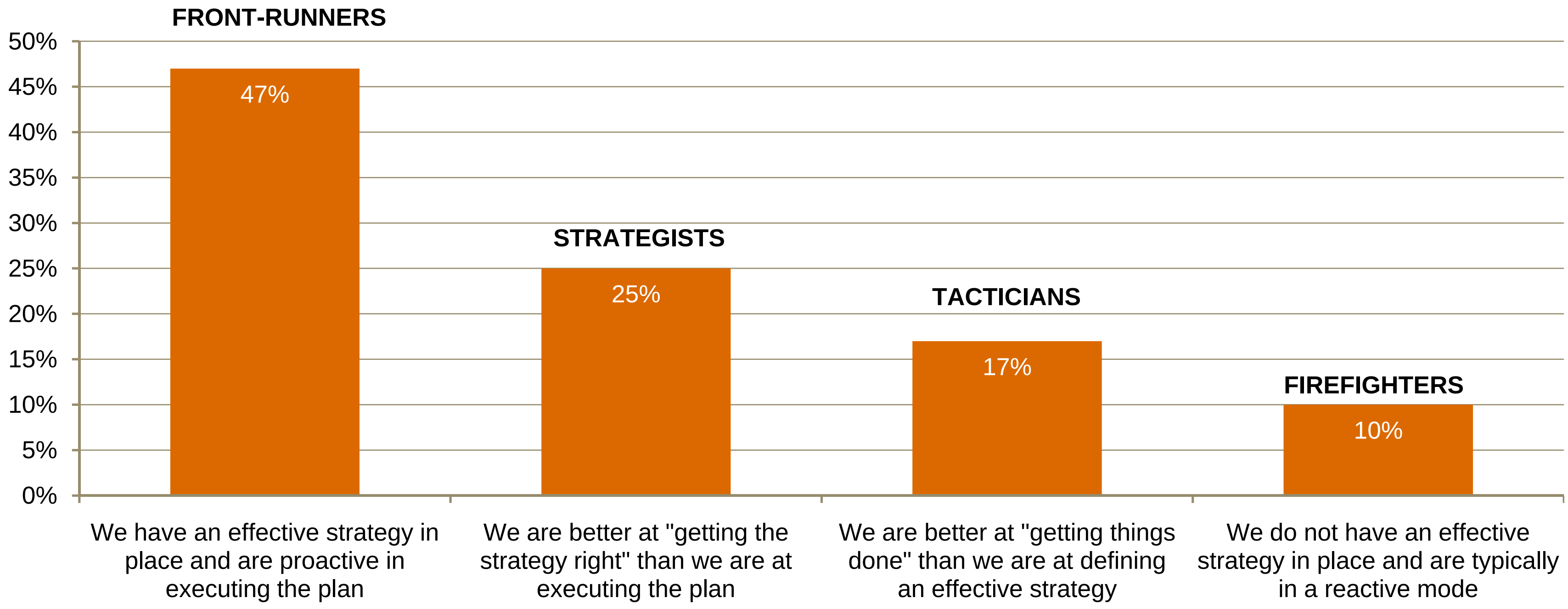
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

Confidence and progress

Many respondents (47%) from the financial services industry see their organization as a "front-runner."

Just less than half of this year's industry respondents say their organization has a strategy in place and is proactive in executing it.



Question 26n11: "Which statement best characterizes your organization's approach to protecting information security?" (Numbers reported may not reconcile exactly with raw data due to rounding)

They are also highly confident in their organization's security.

A clear majority – eight out of ten (80%) – of industry respondents are also confident that their organization's information security activities are effective.

	2011
Very confident	**36%**
Somewhat confident	**44%**
Total	**80%**

Question 35: "How confident are you that your organization's information security activities are effective?"

Insights into the frequency, type, and source of security breaches have leaped dramatically over the past 12 months.

Just a few years ago, nearly half of this survey's financial services respondents couldn't answer the most basic questions about the nature of security-related breaches. Now, approximately 76% or more respondents can answer specific survey questions about factors such as security event frequency, type, and source.

Respondents who answered "Do not know" or "Unknown"	2007	2008	2009	2010	2011
How many incidents occurred in past 12 months?	45%	38%	32%	24%	**8%**
What type of incident occurred?	49%	44%	35%	32%	**13%**
What was the source of the incident?	N/A	45%	37%	32%	**24%**

Question 19: "Number of security incidents in the past 12 months." Question 20: "What types of security incidents (breach or downtime) occurred?" Question 22: "Estimated likely source of incident." (Totals do not add up to 100%.)

When incidents did occur, they were much less likely to impact business than one year ago.

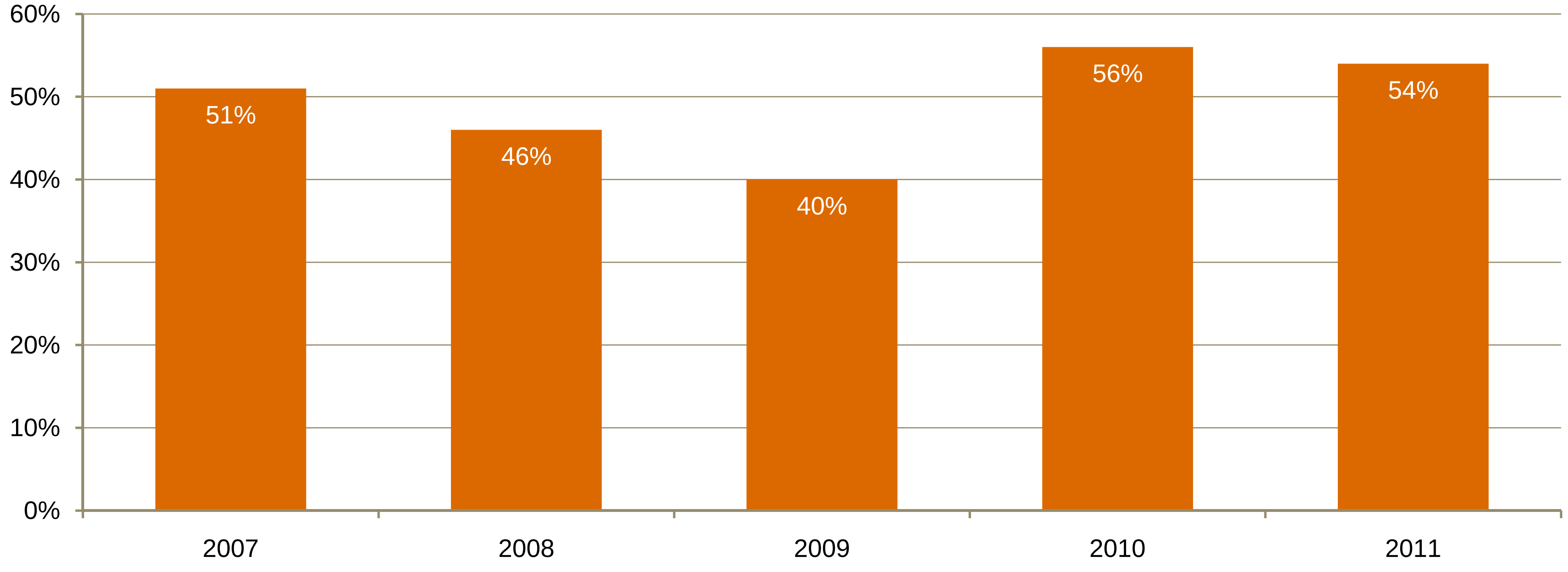
This year, respondents from the financial services industry report lower business impacts – from financial losses and damage to the company's brand and reputation to legal exposure and extortion.

Business impacts	2010	2011	CHANGE
Financial losses	22%	**14%**	**- 36%**
Brand / reputation compromised	15%	**12%**	**- 20%**
Intellectual property theft	13%	**9%**	**- 31%**
Fraud	11%	**6%**	**- 45%**
Loss of shareholder value	7%	**5%**	**- 29%**
Legal exposure / lawsuit	7%	**3%**	**- 57%**
Extortion	5%	**3%**	**- 40%**

Question 23: "How was your organization impacted by the security incident? Business:" (Not all factors shown. Totals do not add up to 100%.)

At the same time, a majority of industry respondents are "bullish" about security spending over the next 12 months.

Will security spending in the industry increase? Optimism carries the day. More than half of all respondents in the financial services industry believe that it will.



Question 9: "When compared with last year, security spending over the next 12 months will:" (Respondents who answered "Increase up to 10%," "Increase 11-30%," or "Increase more than 30%")

Section 3

Signs of vulnerability and exposure

Despite signs of confidence, some trends in this year's survey are troubling. Take the increase in security events, for example.

It is tempting to trumpet the fact that more than one-third of industry respondents (34%) report no security events in the past year. Yet reports of incidents increased this year, especially among respondents indicating 50 or more negative events.

Number of security incidents	2007	2008	2009	2010	2011
No incidents	21%	23%	17%	27%	**34%**
1 to 9 incidents	23%	27%	36%	37%	**38%**
10 to 49 incidents	6%	7%	10%	7%	**10%**
50 or more incidents	4%	5%	4%	5%	**10%**

Question 19: "Number of security incidents in the past 12 months" (Totals do not add up to 100%.)

This year’s data revealed some regression in a best-practice trend – having the CISO report to the “top of the house.”

Reversing a multi-year trend, 31% of industry respondents now say their Chief Information Security Officer or equivalent executive reports not to the Board, the CEO or the CFO, but to the CIO.

Whom the CISO reports to	2008	2009	2010	2011
Board of Directors	21%	27%	28%	**25%**
Chief Executive Officer	30%	36%	34%	**31%**
Chief Financial Officer	7%	12%	17%	**16%**
Chief Information Officer	35%	36%	29%	**31%**

Question 16a: “Where/to whom does your CISO or equivalent senior information security officer report?” (Not all factors shown. Totals do not add up to 100%.)

Most significant is the fact that security spending deferrals and cut-backs – already high – have increased even further.

For the third year in a row, security-related spending deferrals and cut-backs – for both capital and operating expenditures – are high. This year's reluctance to spend on security priorities increased or remained constant for all categories. In fact, spending appears even more restrained than it was during the two years immediately following 2008.

Has your company **deferred** security initiatives?	2009	2010	2011
Yes, for *capital* expenditures	44%	44%	47%
Yes, for *operating* expenditures	40%	41%	44%

Has your company **reduced the cost** for security initiatives?	2009	2010	2011
Yes, for *capital* expenditures	48%	44%	46%
Yes, for *operating* expenditures	47%	43%	44%

Question 12: "Has your company deferred security-related initiatives?" Question 13: "Has your company reduced the cost for any security-related initiatives?" (Not all factors shown. Total does not add up to 100%.)

With spending tight, degradation in many of the industry's security capabilities is starting to appear.

Although financial services firms have been investing in technology related to detection, prevention and web-related security, this year's survey reveals a troubling degradation in core strategic processes.

Current information security standards	2008	2009	2010	2011
Overall information security strategy	75%	74%	76%	**69%**
Business continuity and disaster recovery plans	72%	68%	63%	**57%**
Compliance testing	64%	62%	58%	**57%**
Employee security awareness training program	71%	65%	61%	**54%**
Personnel background checks	69%	68%	65%	**63%**

Question 16: "What information security safeguards related to people does your organization have in place?" Question 17: "What process information security safeguards does your organization currently have in place?" (Not all factors shown. Totals do not add up to 100%.)

And that high confidence rating? It has actually declined 12 points since 2006.

Confidence is always good. But a decline in confidence is telling. These numbers indicate that financial services business and IT personnel – across the world – are less sure that their organization is prepared to address the threats that confront its critical information.

	2006	2007	2008	2009	2010	2011	CHANGE
Total	**92%**	89%	87%	88%	81%	**80%**	**- 12 pts**

Question 35: "How confident are you that your organization's information security activities are effective?" (Respondents who answered "Very confident" or "Somewhat confident" combined)

Section 4

The greatest opportunities for improvement

What's holding security back?

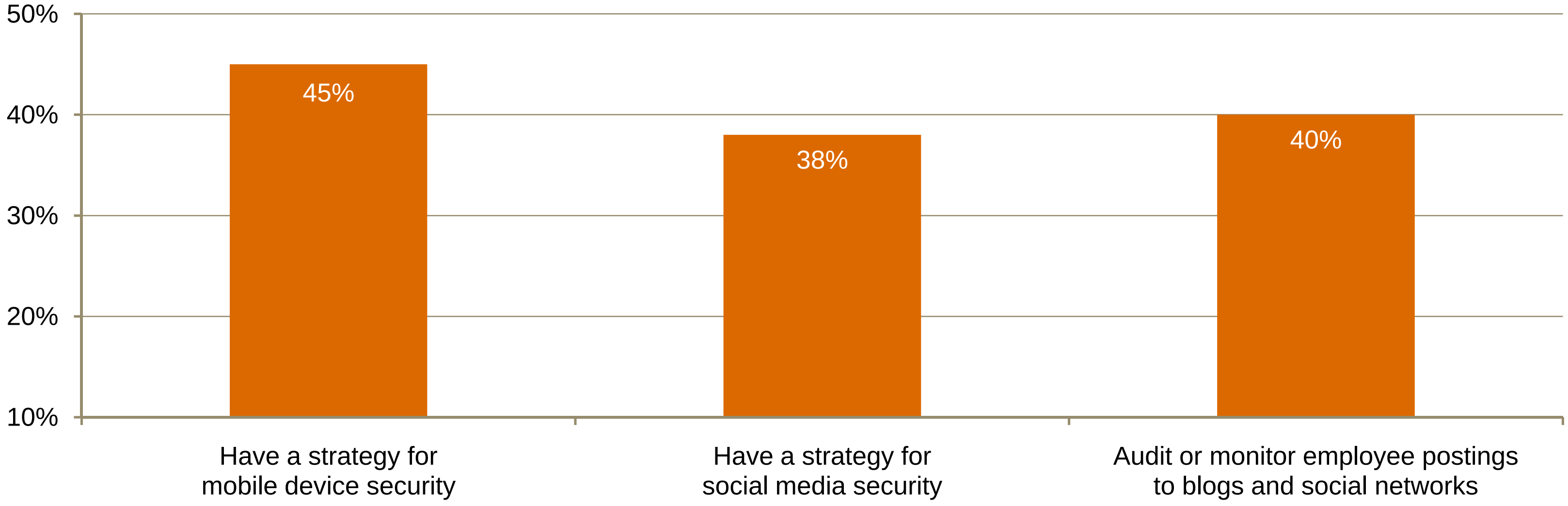
Given the austere spending environment – not just this year, but since 2008 – and a steady regression in the readiness of security capabilities, it's not surprising that financial services respondents consider insufficient capital one of the leading obstacles to the effectiveness of their organization's information security function. It's hard to keep the leading edge of prevention-oriented capabilities razor sharp when budgets are tight. What we didn't expect to find is that industry respondents consider the single greatest obstacle to be the lack of an "actionable vision" for the function.

	2011
1. Lack of an actionable vision or understanding	**28%**
2. Insufficient capital expenditures	**25%**
3. Absence of shortage of in-house technical expertise	**25%**
4. Poorly integrated or overly complex information/IT systems	**25%**
5. Lack of an effective information security strategy	**24%**
6. Leadership – CEO, president, board, or equivalent	**21%**
7. Insufficient operating expenditures	**20%**
8. Leadership – CIO or equivalent	**15%**
9. Leadership – CISO, CSO, or equivalent	**15%**

Question 27n11: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?" (Not all factors shown. Total does not add up to 100%.)

Mobile devices and social media: New rules are in effect this year – but not yet critical mass.

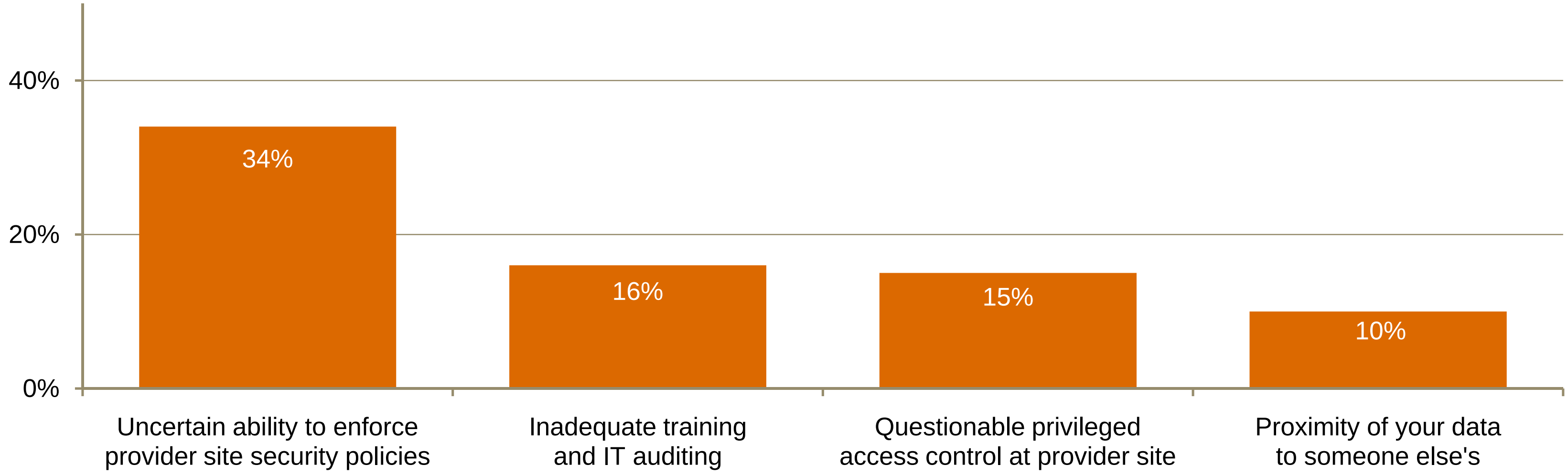
Many financial services companies are implementing strategies to keep pace with employee adoption of new technologies – particularly use of mobile devices and social-networking tools – and are creating rules about how employees can use personal technology within the enterprise. More than half of the industry, however, have not yet begun to put these capabilities into place.



Question 17: "What process information security safeguards does your organization currently have in place?" (Not all factors shown. Total does not add up to 100%.)

Cloud computing: Is it improving information security? Yes, but many want better enforcement of provider security policies.

This year, 40% of all financial services respondents report that their organization uses cloud services – and nearly half (48%) of those say the cloud has improved their information security. Responses also revealed that while enforcing provider security policies is seen as the principal security challenge, respondents are also concerned about training as well as multi-tenancy issues.



Question 41: "Does your organization currently use cloud services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or Infrastructure-as-a-Service (IaaS)?" Question 41c: "What impact has cloud computing had on your company's information security?" Question 41b: "What is the greatest security risk to your cloud computing strategy?" (Not all factors shown. Total does not add up to 100%.)

Increased government involvement: good idea or bad?

More than half of this year's financial services respondents report that their organization formally collaborates with others in the industry, including competitors, to improve security. How about support for government initiatives? On most security-related issues, financial services respondents support increased government action or standards.

Supportive of government implementation of:	2011
1. Government-funded cyber security educational programs	64%
2. Data-encryption minimums for data accessed on mobile devices	62%
3. Intrusion-penetration and identity-threat monitoring standards	62%
4. Government-mandated data encryption for key systems/transactions	59%
5. Government-mandated testing and monitoring of 3rd parties privy to customer information	59%
6. Public reporting on the number of reported threats/violations	53%
7. Government-sponsored insurance fund for information security	50%
8. Mandatory adoption of real-time threat analysis	49%

(Asked only of Financial Services respondents) Question 4: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?" Question 3: "Would you support your national government's implementation of the following?"

For more information, please contact:

National Security Contacts

Gary Loveland
Principal, National Security Leader
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

Financial Services Contacts

Andrew Toner
Principal
646.471.8327
andrew.toner@us.pwc.com

Shawn Connors
Principal
646.471.7278
shawn.joseph.connors@us.pwc.com

Or visit www.pwc.com/giss2012

This document is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

www.pwc.com/security

Eye of the storm

As the global economy stalls and information security threats such as cyber crime and Advanced Persistent Threats cloud the horizon, many see sunshine and clear skies overhead

CIO Business Technology Leadership

CSO BUSINESS RISK LEADERSHIP

Industrial Products

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

September 2011

pwc

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

The economic thunderheads of 2008 may have passed. But across the global industrial products industry, some clouds 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.

Nonetheless, according to PwC's 2012 Global State of Information Security Survey®, the majority of industrial products executives are confident in the effectiveness of their information security practices.

They have an effective strategy in place. They consider their organizations proactive in executing it. And the business impacts of security incidents appear to have declined – across the board.

Yet all is not in order. Security event frequency is up. Data privacy safeguards have begun to degrade over the past year. And third-party risk is starting to climb again.

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, the reasons to do so quickly and strategically are mounting.

Agenda

Section 1. Methodology

Section 2. Confidence and progress

Section 3. Signs of vulnerability and exposure

Section 4. The greatest opportunities for improvement

Section 1

Methodology

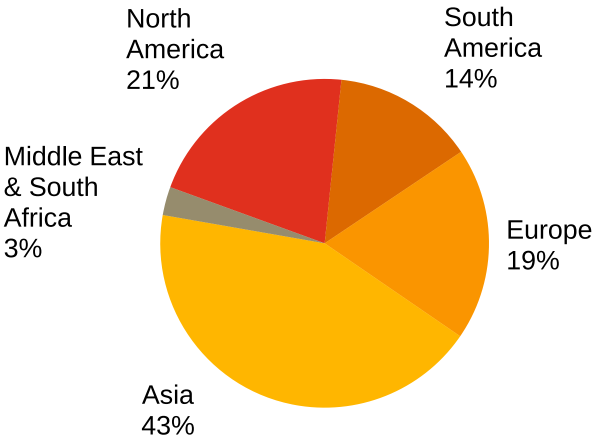
A worldwide study

The 2012 Global State of Information Security Survey®, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 10, 2011 to April 18, 2011.

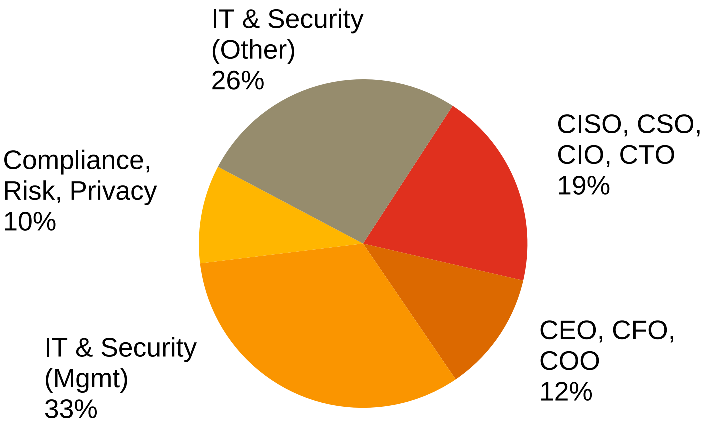
- PwC's 14th year conducting the online survey, 9th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 138 countries
- More than 9,600 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-one percent (31%) of respondents from companies with revenue of $500 million+
- Survey included 859 respondents from the industrial products industry
- The margin of error is less than 1%

Demographics

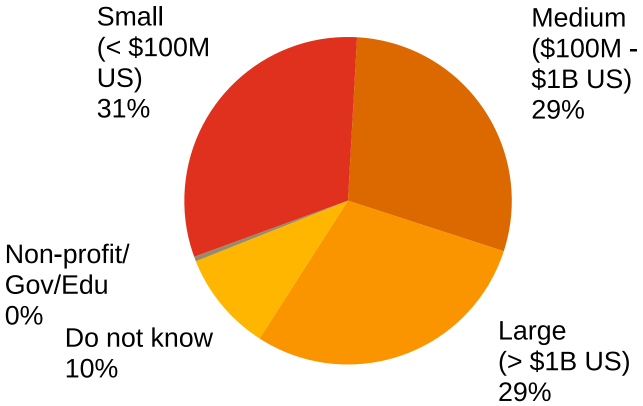
Industrial products respondents by region of employment



Industrial products respondents by title



Industrial products respondents by company revenue size



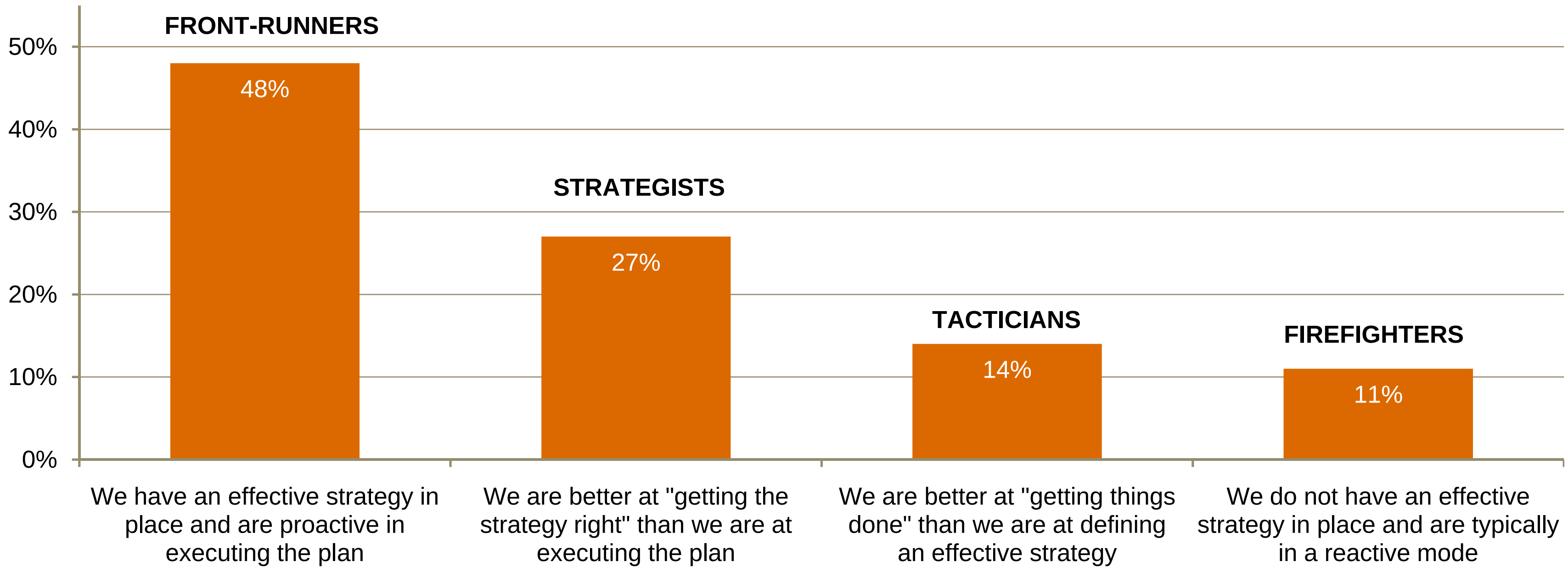
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

Confidence and progress

Many industry respondents see their organization as a "front-runner."

Almost half (48%) of this year's industrial product respondents say their organization has a strategy in place and is proactive in executing it.



Question 26n11: "Which statement best characterizes your organization's approach to protecting information security?"

They are also highly confident in their organization's security.

A very clear majority – 81% – of industry respondents are also confident that their organization's information security initiatives are effective.

	2011
Very confident	**37%**
Somewhat confident	**44%**
Total	**81%**

Question 35: "How confident are you that your organization's information security activities are effective?"

Insights into the frequency, type, and source of security breaches have leaped dramatically over the past 12 months.

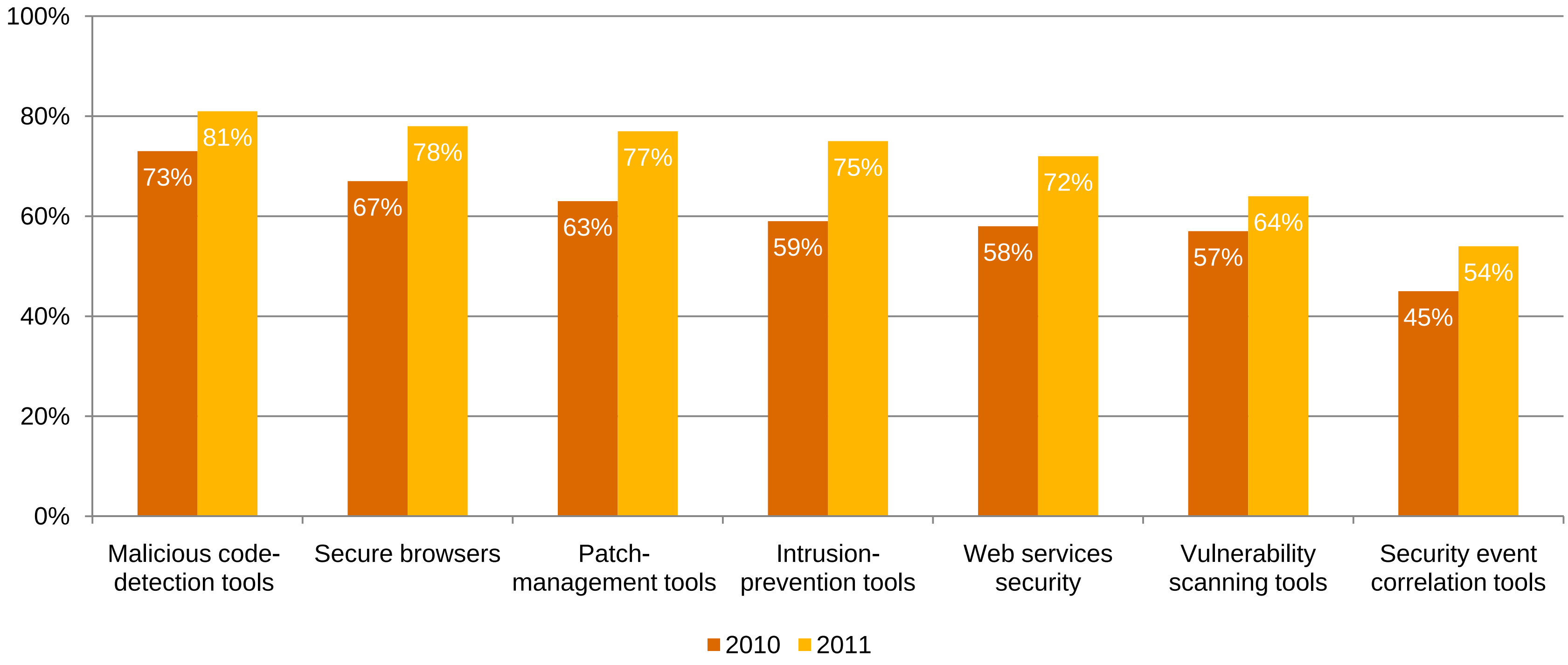
Just a few years ago, as many as 42% of this survey's industrial products respondents couldn't answer the most basic questions about the nature of security-related breaches. Now, 81% or can answer specific survey questions about factors such as security event frequency, type, and source.

Respondents who answered "Do not know" or "Unknown"	2007	2008	2009	2010	2011
How many incidents occurred in past 12 months?	28%	26%	23%	15%	**7%**
What type of incident occurred?	42%	38%	29%	24%	**11%**
What was the source of the incident?	N/A	40%	33%	28%	**19%**

Question 19: "Number of security incidents in the past 12 months." Question 20: "What types of security incidents (breach or downtime) occurred?" Question 22: "Estimated likely source of incident." (Totals do not add up to 100%.)

Despite tight budgets, industrial products firms are proactively adopting safeguards to bolster data security.

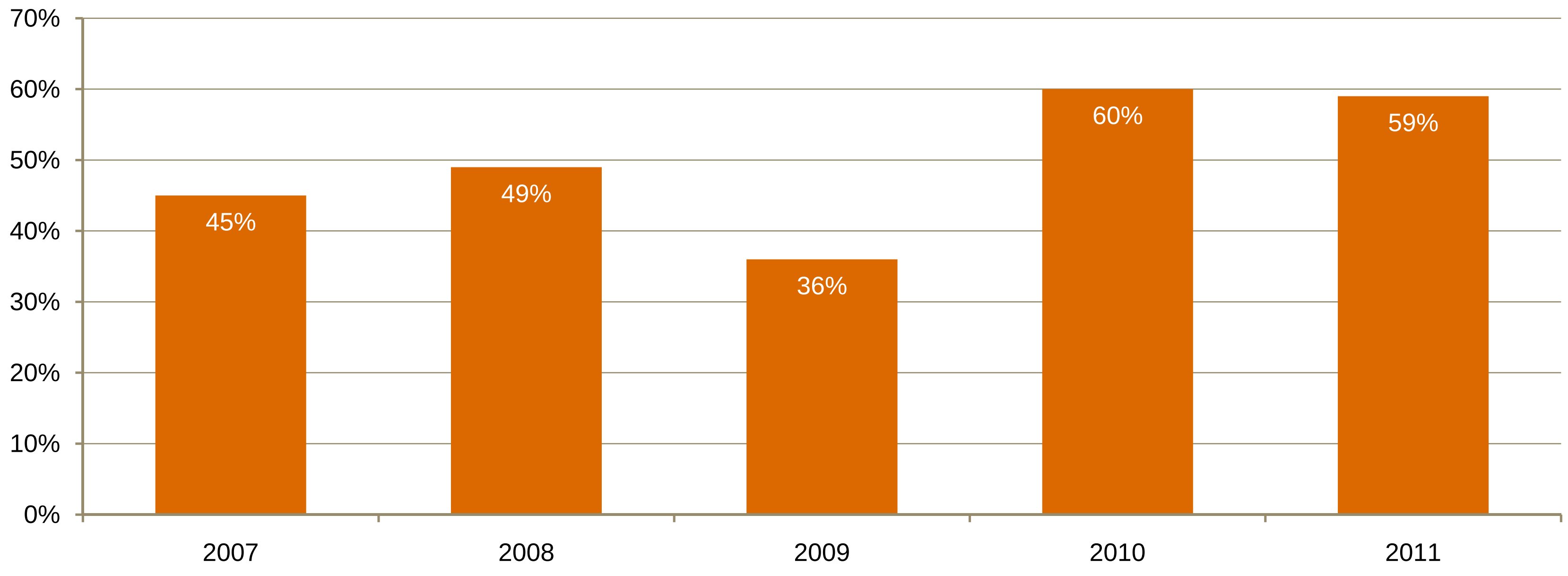
Over the past year, industry respondents have made solid gains in strengthening detection and prevention safeguards to protect information from potential breaches and cyber crime.



Question 18: “What technology information security safeguards does your organization currently have in place?” (Not all factors shown. Totals do not add up to 100%.)

At the same time, a majority of industrial products respondents are "bullish" about security spending over the next 12 months.

Will security spending in the industry increase? Optimism carries the day. More than half (59%) of industrial products respondents believe that it will.



Question 9: "When compared with last year, security spending over the next 12 months will:" (Respondents who answered "Increase up to 10%," "Increase 11-30%," or "Increase more than 30%")

Most significant is the fact that security spending deferrals and cut-backs are beginning to ease.

Security-related spending deferrals and cut-backs – for both capital and operating expenditures – now show real signs of easing this year. Respondents report that their organizations are loosening the security spending purse strings by as much 9% over last year.

Has your company **deferred** security initiatives?	2009	2010	2011
Yes, for *capital* expenditures	47%	45%	46%
Yes, for *operating* expenditures	43%	44%	40%

Has your company **reduced the cost** for security initiatives?	2009	2010	2011
Yes, for *capital* expenditures	47%	47%	43%
Yes, for *operating* expenditures	47%	45%	43%

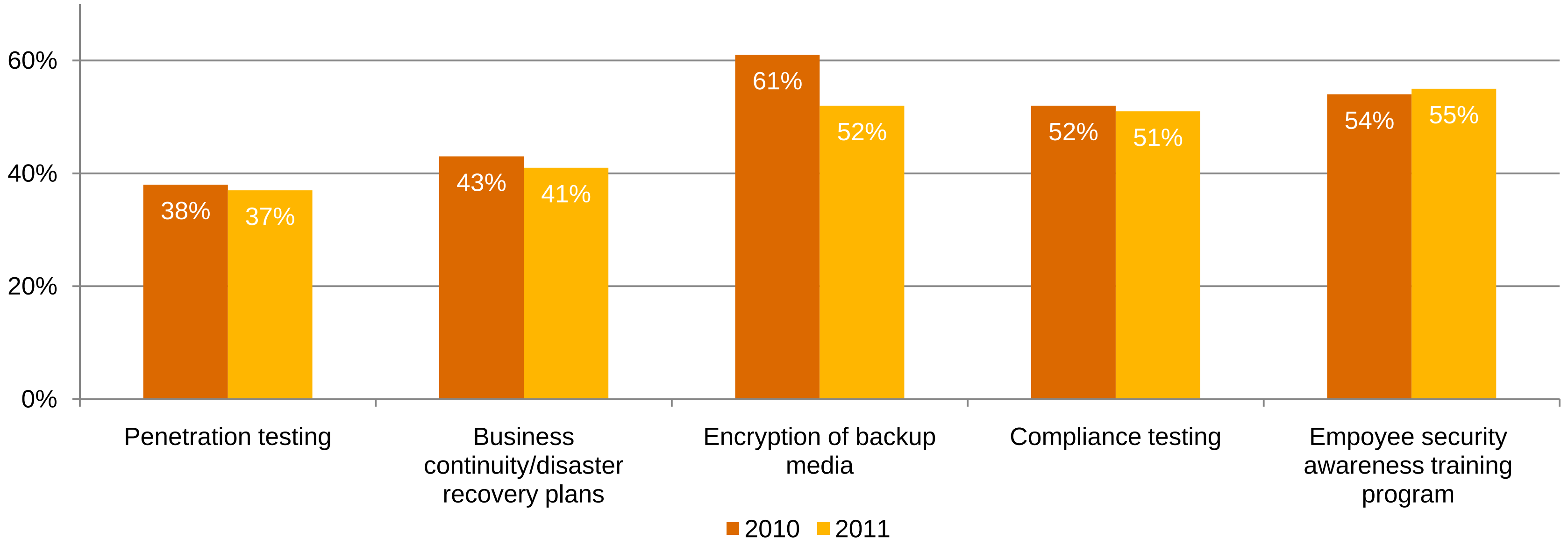
Question 12: “Has your company deferred security-related initiatives?” Question 13: “Has your company reduced the cost for any security-related initiatives?” (Not all factors shown. Total does not add up to 100%.)

Section 3

Signs of vulnerability and exposure

Advanced Persistent Threats: They can be devastating – but just how prepared are industrial products companies to address them?

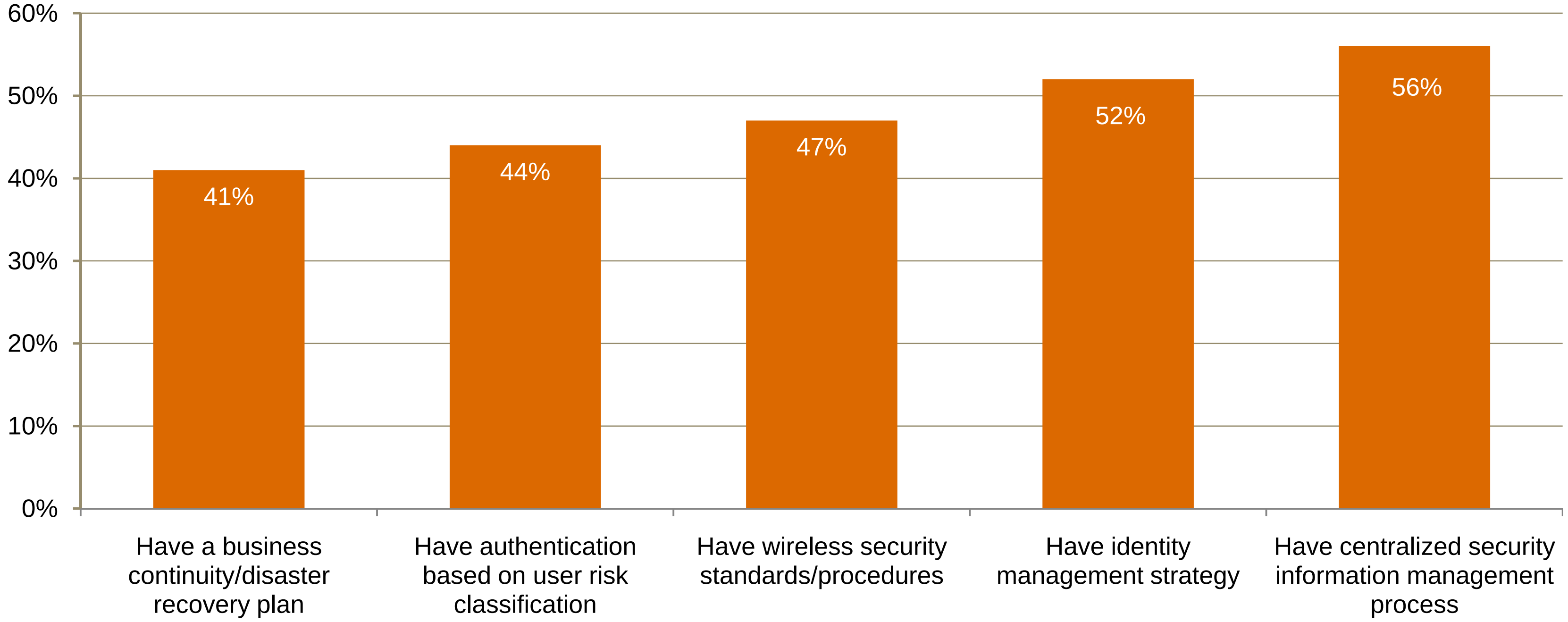
While 64% of industrial products respondents say Advanced Persistent Threat drives their organization's security spending, only 19% say their company has a security policy that addresses APT. At the same time, implementation of certain tools and processes crucial to combatting this new threat has slowed or stalled over the past year.



Question 4 (Industrial Products): "Does Advanced Persistent Threat drive your organization's security spending?" Question 28: "Which of the following elements, if any, are included in your organization's security policy?" Question 17: "What process information technology security safeguards does your organization currently have in place?" Question 18: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown. Totals do not add up to 100%.)

Industry respondents are also concerned about threats to critical controls systems. Yet many lack key strategies and standards.

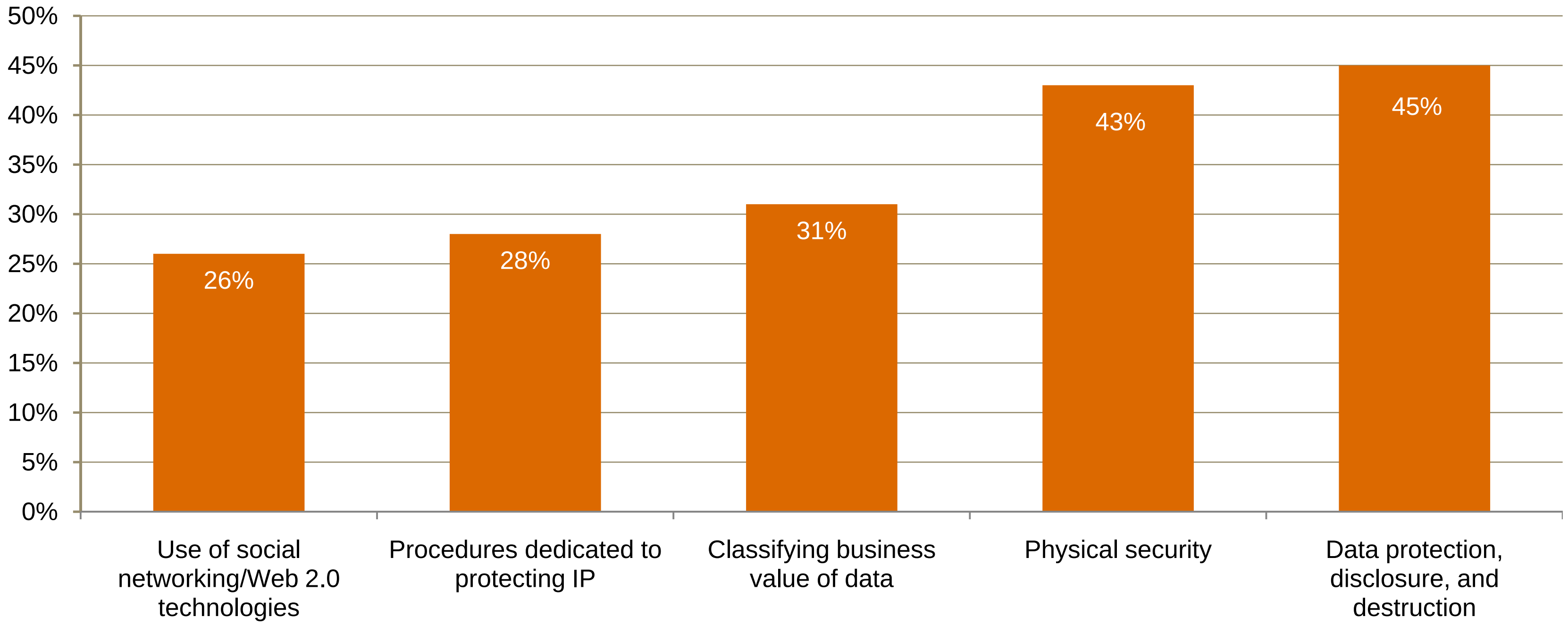
A clear majority (69%) of industrial products respondents say they have a security plan in place to mitigate breaches of manufacturing systems controls. At the same time, many have not implemented critical security safeguards essential to protecting control systems.



Question 1 (Industrial Products): “Does your organization have a security plan in place to mitigate a breach of your manufacturing systems controls?” Question 17: “What process information security safeguards does your organization currently have in place?” (Not all factors shown. Totals do not add up to 100%.)

While safeguarding intellectual property is a high priority for industrial products companies, core policy implementation lags.

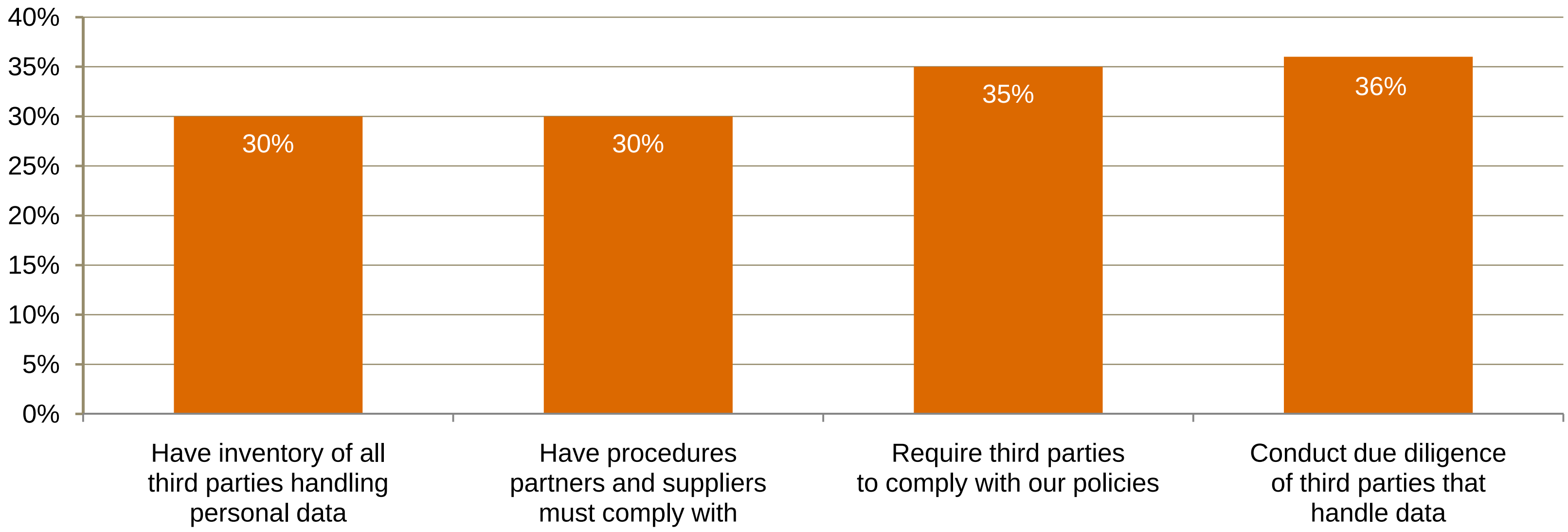
This year, 74% of industry respondents report that their organizations has a plan in place to protect intellectual property. In spite of this, most organizations have not established many security policies crucial to protecting proprietary and other sensitive information.



Question 2 (Industrial Products): “Does your organization have a security plan in place to protect intellectual property?” Question 28: “Which of the following elements, if any, are included in your organization's security policy?” (Not all factors shown. Totals do not add up to 100%.)

Third party risk is on the rise.

Since 2009, the percentage of industrial products respondents that consider partners or suppliers the likely source of security breaches has more than doubled – from 7% to 17%. Is the industry combating this risk? Nearly two-thirds (64%) of industry respondents say their organization has a security plan for outsourcing arrangements. But many have not yet established strategies and practices governing service providers and other third parties.



Question 22: "Estimated likely source of incident?" Question 3 (Industrial Products): "Does your organization have a security plan for outsourcing arrangements?" Question 15: "Which data privacy safeguards does your organization have in place?" Q28. Which of the following elements, if any, are included in your organization's security policy? (Not all factors shown. Total does not add up to 100%.)

Section 4

The greatest opportunities for improvement

What's holding security back?

Given the austere spending environment, it would make sense if industrial products respondents considered insufficient capital one of the leading obstacles to the effectiveness of their organization's information security function.

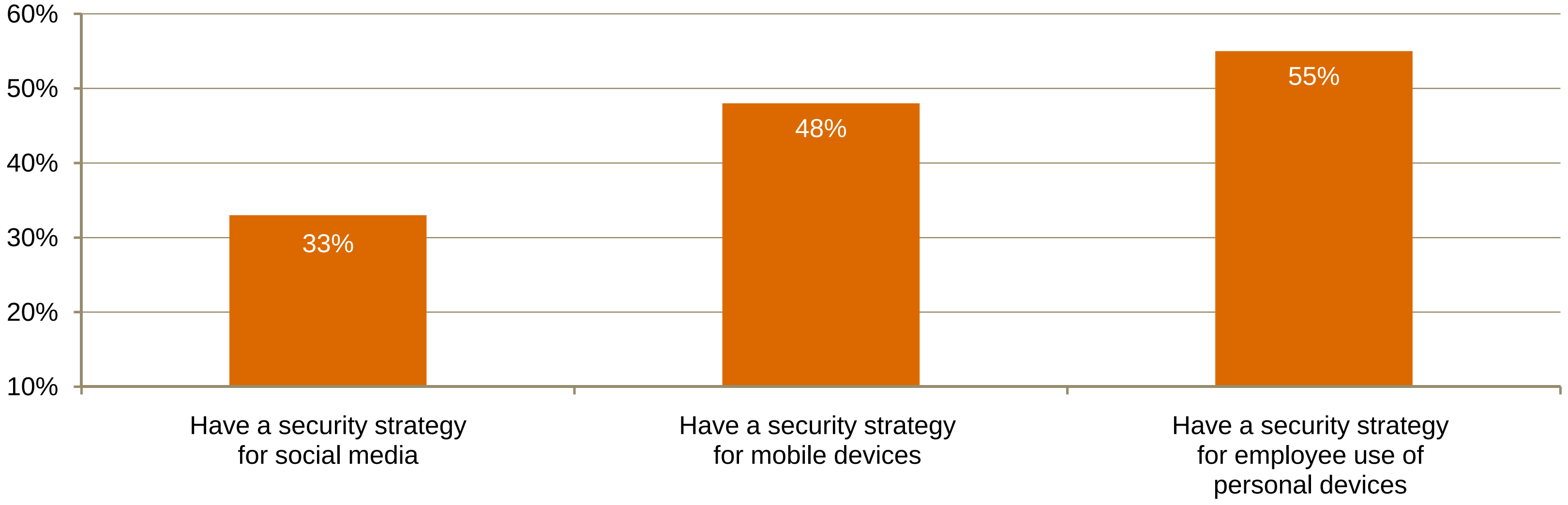
Surprisingly, they don't. One out of three point to the lack of an actionable vision, and almost as many reference the absence of an effective information security strategy.

	2011
1. Lack of an actionable vision or understanding	33%
2. Lack of an effective information security strategy	29%
3. Insufficient capital expenditures	27%
4. Poorly integrated or overly complex IT systems	23%
5. Leadership – CEO, President, Board, or equivalent	23%
6. Insufficient operating expenditures	20%
7. Absence or shortage of in-house technical expertise	20%

Question 27n11: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?" (Not all factors shown. Total does not add up to 100%.)

Mobile devices and social media: New rules are in effect this year – but not yet critical mass.

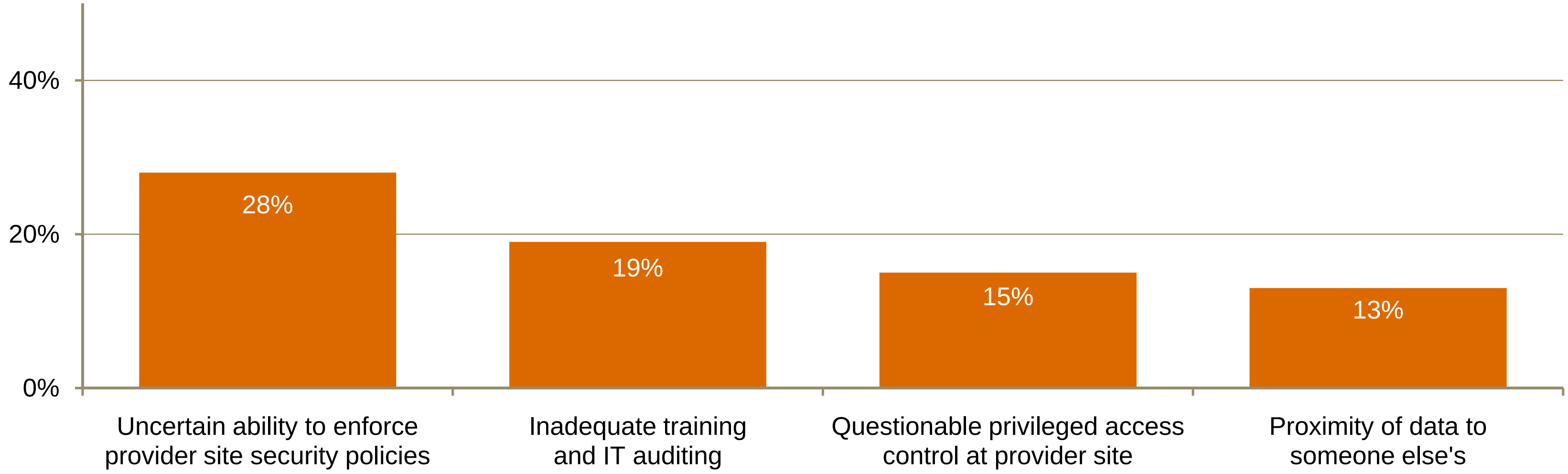
Industrial products firms are implementing strategies to keep pace with employee adoption of new technologies – including use of mobile devices and social-networking tools – and are creating rules about how employees can use personal technology within the enterprise.



Question 17: "What process information security safeguards does your organization currently have in place?" (Not all factors shown. Total does not add up to 100%.)

Cloud computing is mainstream this year, but many respondents want better enforcement of provider security policies.

This year, half (50%) of industrial products respondents report that their organization uses cloud services. Among those that do, 64% say the technology has improved their security posture. Responses also revealed that while enforcing provider security policies is seen as the principal security challenge this year, respondents are also concerned about training as well as multi-tenancy issues.



Question 41: “Does your organization currently use cloud services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or Infrastructure-as-a-Service (IaaS)?” Question 41c: “What impact has cloud computing had on your company’s information security?” Question 41b: “What is the greatest security risk to your cloud computing strategy?” (Not all factors shown. Total does not add up to 100%.)

For more information, please contact:

National Security Contacts

Gary Loveland
Principal, National Security Leader
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

Industrial Products Contacts

Karen Vitale
Partner
973.236.5347
vitalek@us.pwc.com

Fred Rica
Principal
973.236.4052
frederick.j.rica@us.pwc.com

Or visit www.pwc.com/giss2012

www.pwc.com/security

Eye of the storm

As the global economy stalls and information security threats such as cyber crime and Advanced Persistent Threats cloud the horizon, many see sunshine and clear skies overhead

CIO Business Technology Leadership

CSO BUSINESS RISK LEADERSHIP

Oil & Gas

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

September 2011

pwc

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*

The economic thunderheads of 2008 may have passed. But across the global oil and gas (O&G) industry, some clouds 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.

Nonetheless, according to PwC's 2012 Global State of Information Security Survey®, the vast majority of O&G executives are confident in the effectiveness of their information security practices.

They have an effective strategy in place. They consider their organizations proactive in executing it. Funding expectations are running high. And their most senior security leader now typically reports "to the top of the house."

Yet all is not in order. Security event frequency is up. Incidents are exploiting assets and devices across the board. Core policies are deficient. And the risks associated with partners and suppliers are increasing.

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, the reasons to do so quickly and strategically are mounting.

Agenda

Section 1.	Methodology
Section 2.	Confidence and progress
Section 3.	Signs of vulnerability and exposure
Section 4.	The greatest opportunities for improvement

Section 1

Methodology

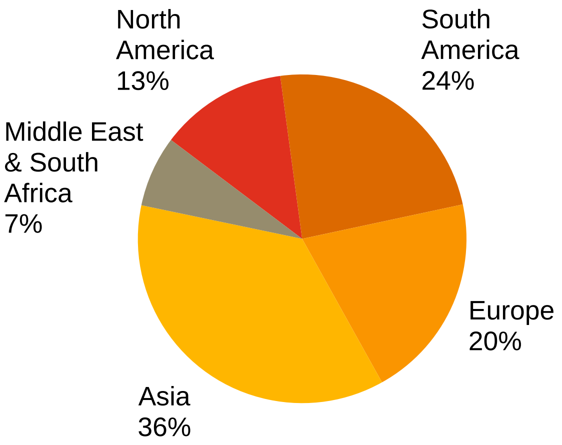
A worldwide study

The 2012 Global State of Information Security Survey®, a worldwide study by PwC, CIO Magazine and CSO Magazine, was conducted online from February 10, 2011 to April 18, 2011.

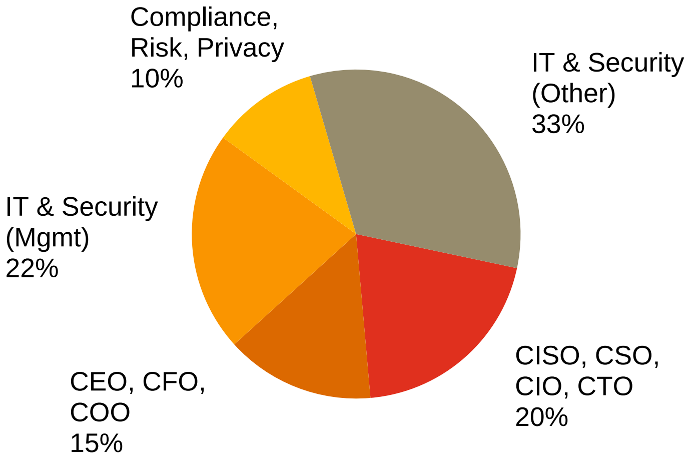
- PwC’s 14th year conducting the online survey, 9th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 138 countries
- More than 9,600 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-one percent (31%) of respondents from companies with revenue of $500 million+
- Survey included 143 respondents from the oil and gas (O&G) industry
- The margin of error is less than 1%

Demographics

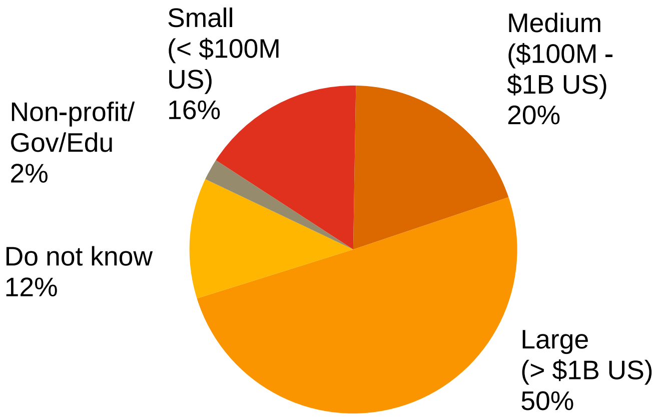
Oil & Gas respondents by region of employment



Oil & Gas respondents by title



Oil & Gas respondents by company revenue size



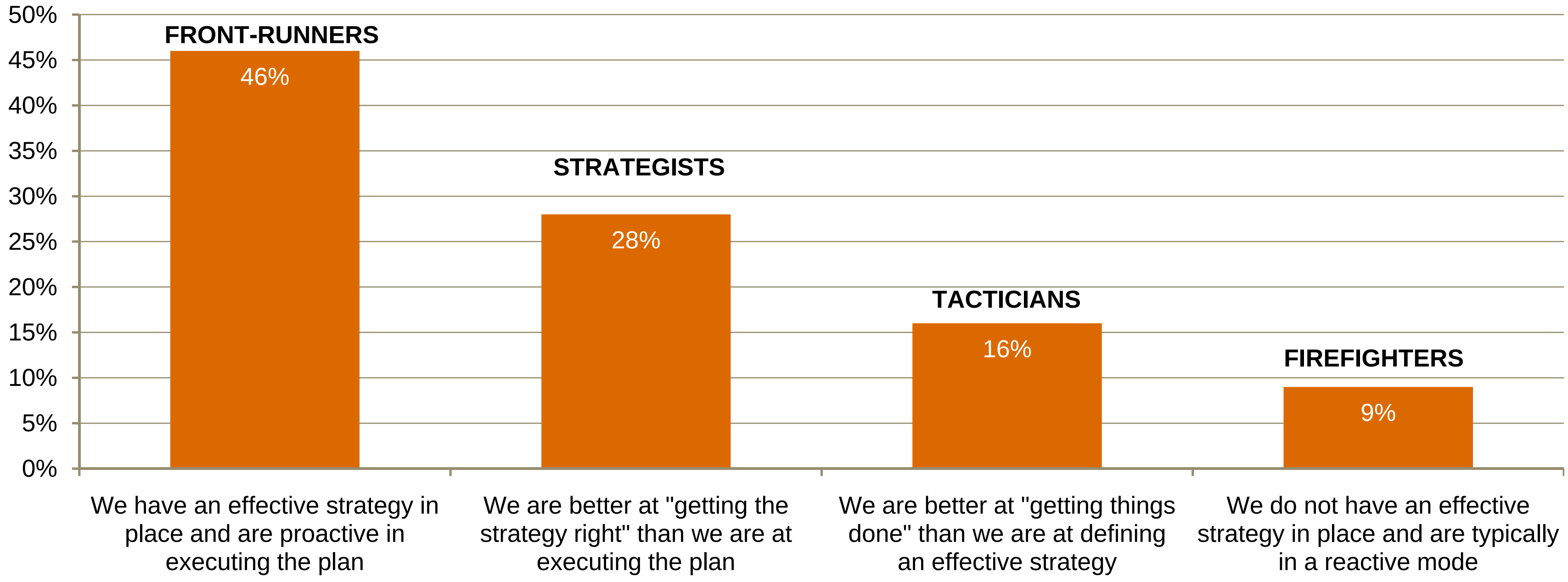
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

Confidence and progress

Most O&G respondents see their organization as a "front-runner."

Almost half of this year's O&G respondents (46%) say their organization has a strategy in place and is proactive in executing it.



Question 26n11: "Which statement best characterizes your organization's approach to protecting information security?" (Numbers reported may not reconcile exactly with raw data due to rounding)

They are also highly confident in their organization's security.

A clear majority – more than three out of four (77%) – of O&G respondents are also confident that their organization's information security activities are effective.

	2011
Very confident	**37%**
Somewhat confident	**40%**
Total	**77%**

Question 35: "How confident are you that your organization's information security activities are effective?"

The CISO is more likely to report to the "top of the house."

Continuing a long-term trend, O&G companies are increasingly likely to ensure that the Chief Information Security Officer or equivalent executive reports to the most senior business and governance leaders and legal advisors in the organization.

Whom the CISO reports to	2007	2008	2009	2010	2011
Board of Directors	26%	20%	24%	20%	**25%**
Chief Executive Officer	7%	30%	26%	23%	**33%**
Chief Financial Officer	0%	5%	11%	9%	**11%**
Legal Counsel	4%	10%	8%	3%	**11%**

Question 16a: "Where/to whom does your CISO or equivalent senior information security officer report?" (Not all factors shown. Totals do not add up to 100%.)

Insights into the frequency, type, and source of security breaches have leaped dramatically over the past 12 months.

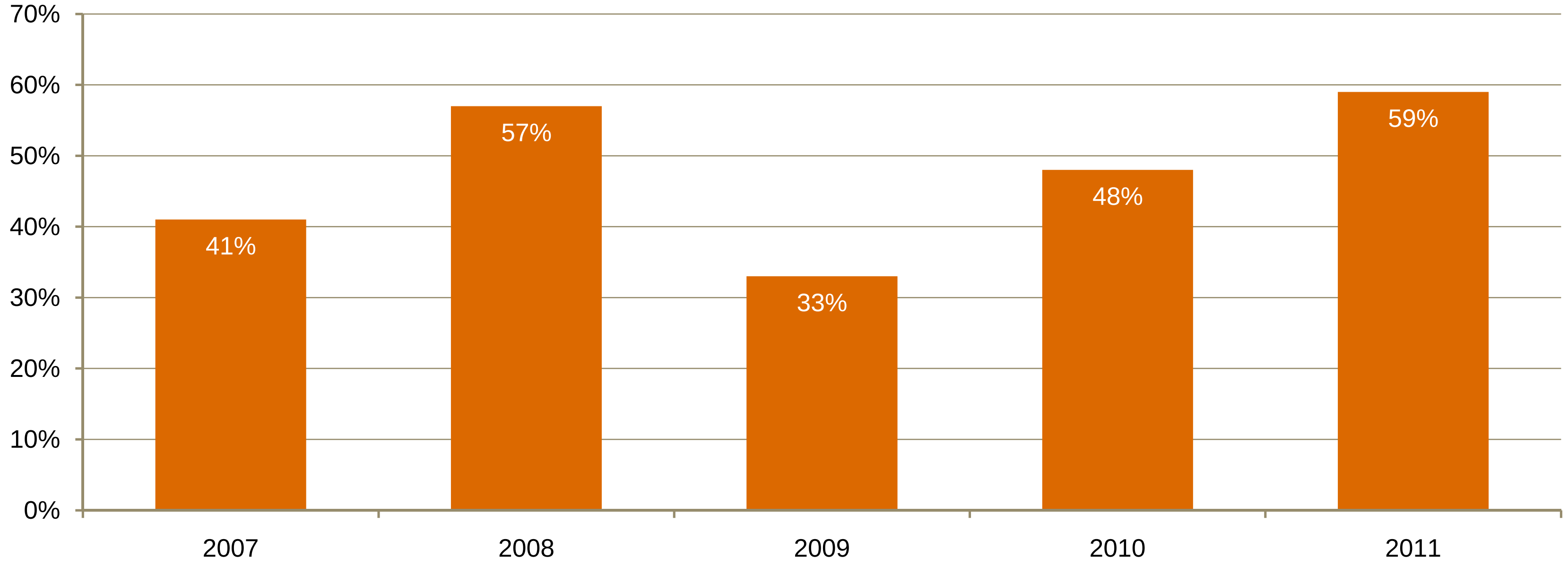
Just a few years ago, nearly half of this survey's O&G respondents couldn't answer the most basic questions about the nature of security-related breaches. Now, approximately 80% or more of O&G respondents can answer specific survey questions about factors such as security event frequency, type, and source.

Respondents who answered "Do not know" or "Unknown"	2007	2008	2009	2010	2011
How many incidents occurred in past 12 months?	45%	45%	29%	25%	**9%**
What type of incident occurred?	37%	48%	26%	33%	**10%**
What was the source of the incident?	NA	48%	26%	32%	**21%**

Question 19: "Number of security incidents in the past 12 months." Question 20: "What types of security incidents (breach or downtime) occurred?" Question 22: "Estimated likely source of incident." (Totals do not add up to 100%.)

At the same time, a majority of O&G respondents are "bullish" about security spending over the next 12 months.

Will security spending in the industry increase? Optimism carries the day. Almost six out of every 10 O&G respondents believe that it will – a higher number than at any time since before 2007.



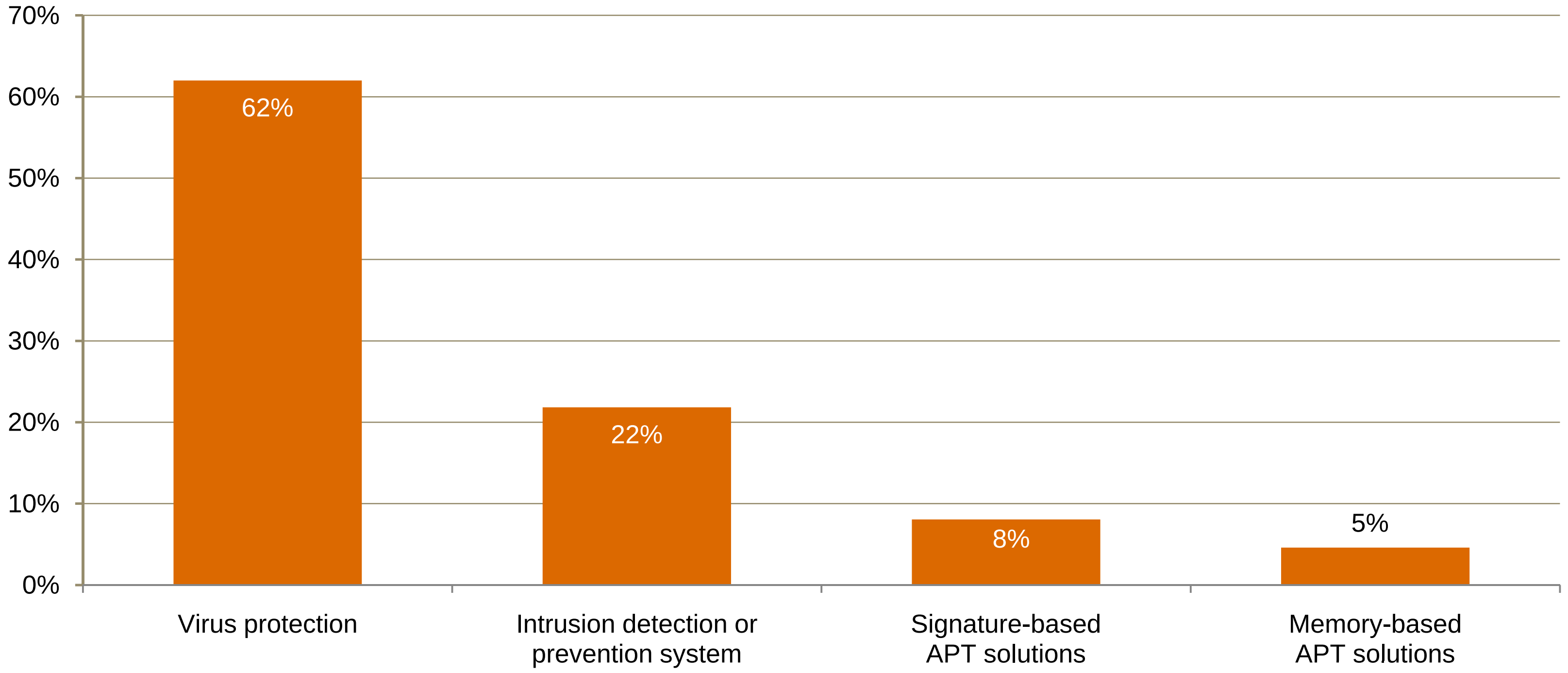
Question 9: "When compared with last year, security spending over the next 12 months will:" (Respondents who answered "Increase up to 10%," "Increase 11-30%," or "Increase more than 30%")

Section 3

Signs of vulnerability and exposure

Advanced Persistent Threats: They can be devastating – but just how concerned are O&G organizations about addressing them?

While more than half (52%) of O&G respondents stated that APT was driving their organization's security spending, very few reported having key capabilities in place to manage this new threat – such as virus protection, intrusion detection systems and either signature-based or memory-based APT solutions.



Question 1: "Does Advanced Persistent Threat drive your organization's security spending?" Question 2: "What technologies does your organization use to combat Advanced Persistent Threat?" (Not all factors shown. Total does not add up to 100%.)

Other trends in this year's survey are also troubling. Take the increase in security events, for example.

It is tempting to trumpet the fact that one out of four O&G respondents (25%) report no security events in the past year. Yet reports of incidents increased this year, especially among respondents indicating 50 or more negative events.

Number of security incidents	2007	2008	2009	2010	2011
No incidents	19%	15%	16%	26%	**25%**
1 to 9 incidents	21%	27%	42%	36%	**40%**
10 to 49 incidents	9%	9%	9%	9%	**12%**
50 or more incidents	5%	4%	4%	4%	**14%**

Question 19: "Number of security incidents in the past 12 months." (Totals do not add up to 100%.)

Exploitation is up across the board – for all layers of security vulnerable to attack.

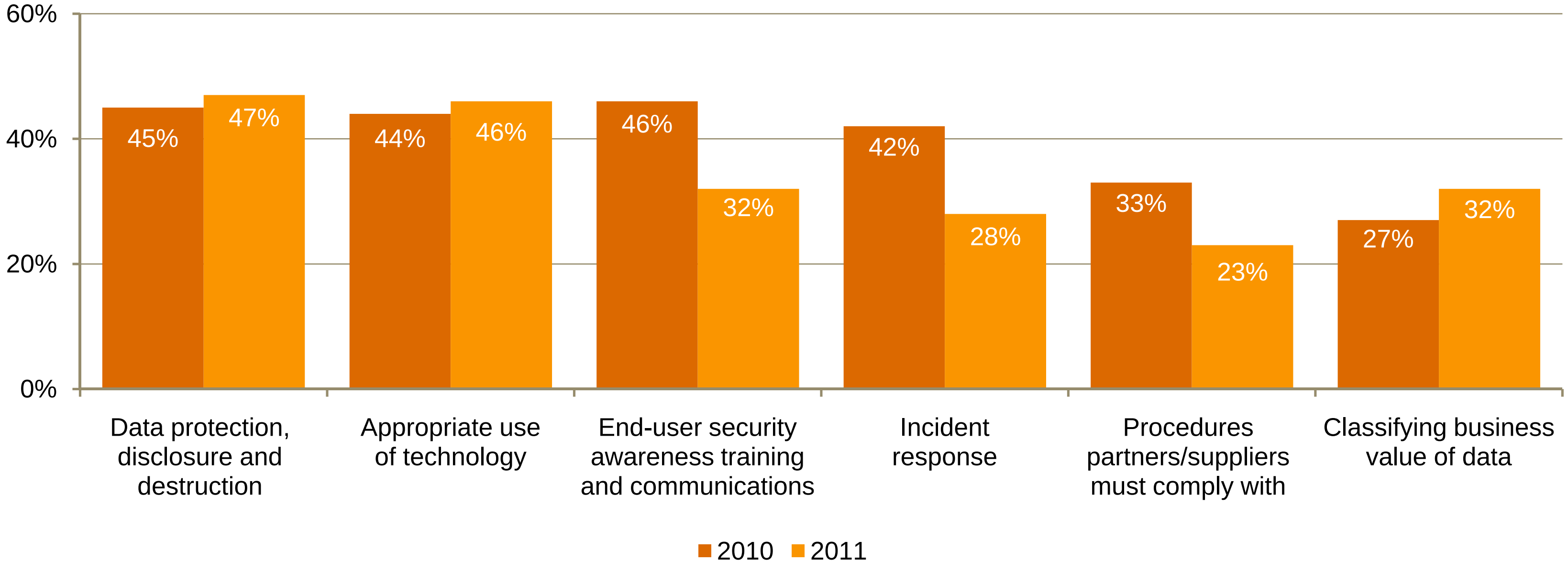
For the second consecutive year, reported levels of data exploitation increased in the O&G industry. Exploitation of applications registered the greatest year-over-year increase, rising to 53% over last year.

Cause of breach or downtime	2008	2009	2010	2011	One-year change*
Data exploited	8%	28%	33%	41%	**+ 24%**
System exploited	15%	30%	31%	37%	**+ 19%**
Network exploited	23%	35%	28%	30%	**+ 7%**
Application exploited	17%	17%	17%	26%	**+ 53%**
Human exploited	19%	19%	18%	25%	**+ 39%**
Mobile device exploited	8%	19%	17%	23%	**+ 35%**

Question 20: “What types of security incidents (breach or downtime) occurred?” (Not all factors shown. Totals do not add up to 100%.) *This calculation measures the difference between response levels over a one-year period from 2010 to 2011.

Deficiencies in basic policy documentation expose the enterprise to many different kinds of compromise.

Despite advances in other areas, protocols governing critical processes are omitted from many O&G organizations' security policies. In fact, more than half the O&G respondents this year report that their organization does not have critical policies in place addressing areas such as data protection, use of technology, security awareness training, and incident response, among many other important domains.



Question 28: "Which of the following elements, if any, are included in your organization's security policy?" (Not all factors shown. Totals do not add up to 100%.)

Third party risks are rising.

Not surprisingly, hackers are suspected as the source of most security incidents. And employees (both current and former) – as one facet of the “insider threat” – remain a significant risk. At the same time, however, third party-risks are increasing at a higher rate than any other category.

Estimated likely source of incident	2008	2009	2010	2011	Three-year change*
Employee	35%	46%	34%	27%	**- 23%**
Former employee	19%	28%	25%	24%	**+ 26%**
Customer	4%	9%	12%	14%	**+ 250%**
Partner / supplier	4%	15%	12%	23%	**+ 475%**
Hacker	23%	35%	39%	47%	**+ 104%**

Question 22: “Estimated likely source of incident. (Check all that apply)” (Not all factors shown. Total does not add up to 100%.) *This calculation measures the difference between response levels over a three-year period from 2008 to 2011.

Section 4

The greatest opportunities for improvement

What's holding security back?

Given the austere spending environment – not just this year, but since 2008 – and a steady regression in the readiness of security capabilities, it would make sense if O&G respondents considered insufficient capital one of the leading obstacles to the effectiveness of their organization's information security function.

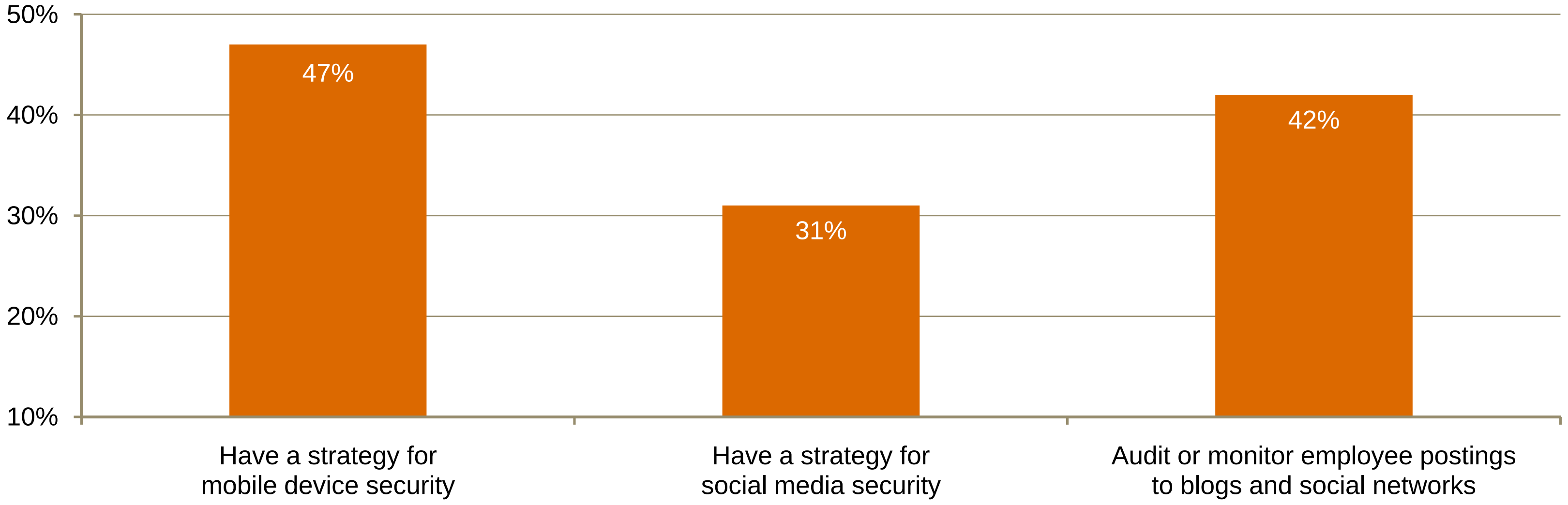
Surprisingly, they don't. Instead almost four out of ten point to the lack of an effective information security strategy and the absence of an actionable "vision."

	2011
1. Lack of an effective information security strategy	38%
2. Lack of an actionable vision or understanding	37%
3. Leadership – CEO, President, Board or equivalent	26%
4. Poorly integrated or overly complex information/IT systems	23%
5. Leadership – CISO, CSO or equivalent	21%
6. Absence or shortage of in-house technical expertise	19%
7. Insufficient capital expenditures	17%
8. Leadership – CIO or equivalent	15%

Question 27n11: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?" (Not all factors shown. Total does not add up to 100%.)

Mobile devices and social media: New rules are in effect this year for many in the industry – though not yet the majority.

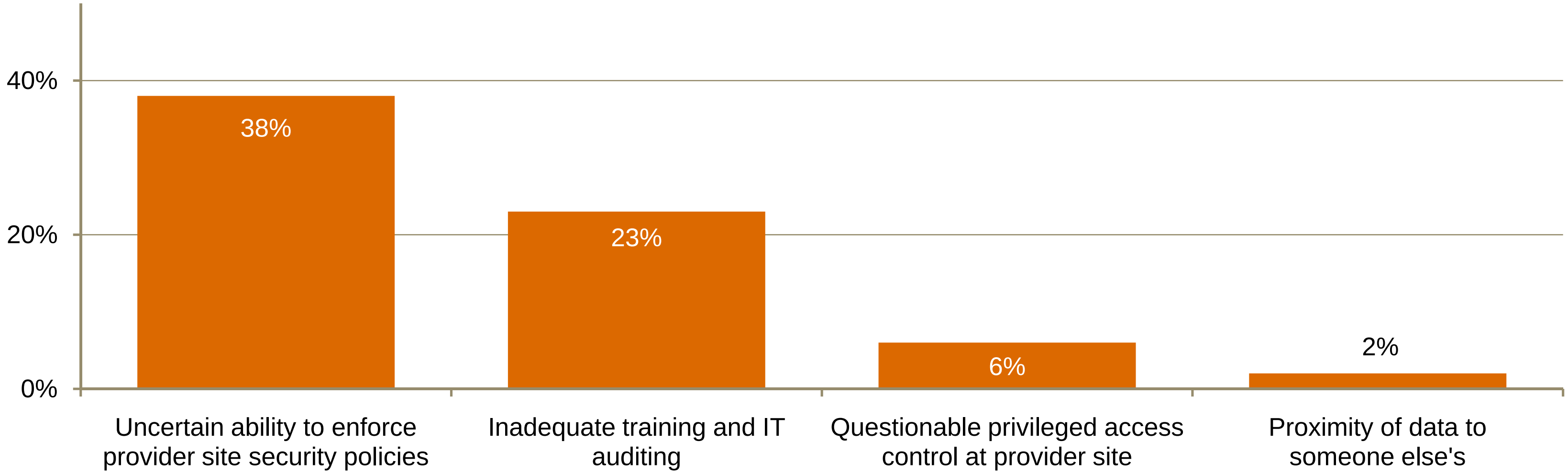
The possibility of having thousands of highly confidential files made public is keeping many – but not all – O&G decision-makers up at night. Some view this risk as just one among other important issues they're focused on.



Question 17: "What process information security safeguards does your organization currently have in place?" (Not all factors shown. Total does not add up to 100%.)

Cloud computing: Is it improving information security? Yes, but many want better enforcement of provider security policies.

This year, nearly half of all O&G respondents (48%) report that their organization uses cloud services – and 72% of those that do say the cloud has improved their information security. Responses also revealed that while the leading security risk to cloud computing is an uncertain ability to enforce provider security policies, respondents are also concerned about inadequate training and IT auditing.



Question 41: “Does your organization currently use cloud services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or Infrastructure-as-a-Service (IaaS)?” Question 41c: “What impact has cloud computing had on your company’s information security?” Question 41b: “What is the greatest security risk to your cloud computing strategy?” (Not all factors shown. Total does not add up to 100%.)

For more information, please contact:

National Security Contacts

Gary Loveland
Principal, National Security Leader
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

Oil & Gas Contacts

Brad Bauch
Principal
713.356.4536
brad.bauch@us.pwc.com

Less Stoltenberg
Director
713.356.4469
less.j.stoltenberg@us.pwc.com

Or visit www.pwc.com/giss2012

www.pwc.com/security

Eye of the storm

As the global economy stalls and information security threats such as cyber crime and Advanced Persistent Threats cloud the horizon, many see sunshine and clear skies overhead

CIO Business Technology Leadership

CSO Business Risk Leadership

Public Sector

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

September 2011

pwc

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*

The economic thunderheads of 2008 may have passed. But across the operations of public entities worldwide, some clouds still linger over budgets, resource levels and the ability to protect the private information of constituents.

Nonetheless, according to PwC's 2012 Global State of Information Security Survey®, the majority of public sector administrators are confident in the effectiveness of their information security practices.

They have an effective strategy in place. They consider their organizations proactive in executing it. And they are diligently implementing technology safeguards to counter cyber crime and bolster security.

Yet all is not in order. Security event frequency is up. Strategic security processes are starting to degrade. And the capital and operating expenditures crucial to early prevention and agile response are more likely to be deferred or canceled than at any time since 2008.

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, the reasons to do so quickly and strategically are mounting.

Agenda

Section 1.	Methodology
Section 2.	Confidence and progress
Section 3.	Signs of vulnerability and exposure
Section 4.	The greatest opportunities for improvement

Section 1

Methodology

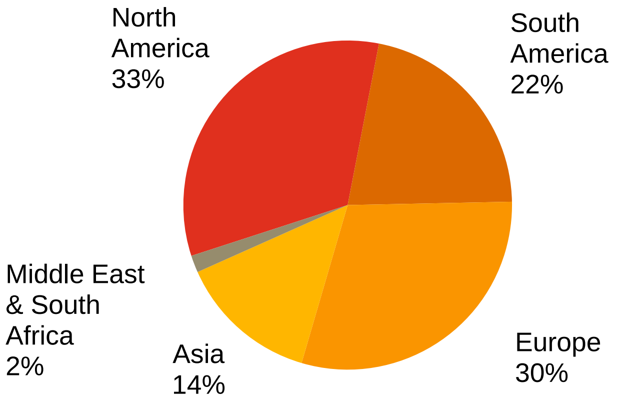
A worldwide study

The 2012 Global State of Information Security Survey®, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 10, 2011 to April 18, 2011.

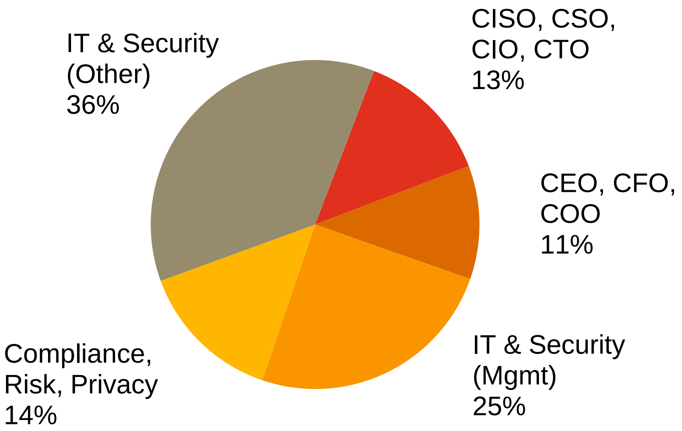
- PwC’s 14th year conducting the online survey, 9th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 138 countries
- More than 9,600 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-one percent (31%) of respondents from companies with revenue of $500 million+
- Survey included 717 respondents from the public sector
- The margin of error is less than 1%

Demographics

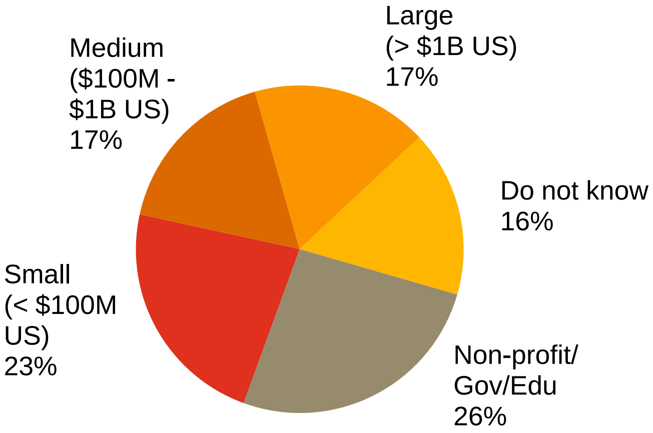
Public sector respondents by region of employment



Public sector respondents by title



Public sector respondents by company revenue size



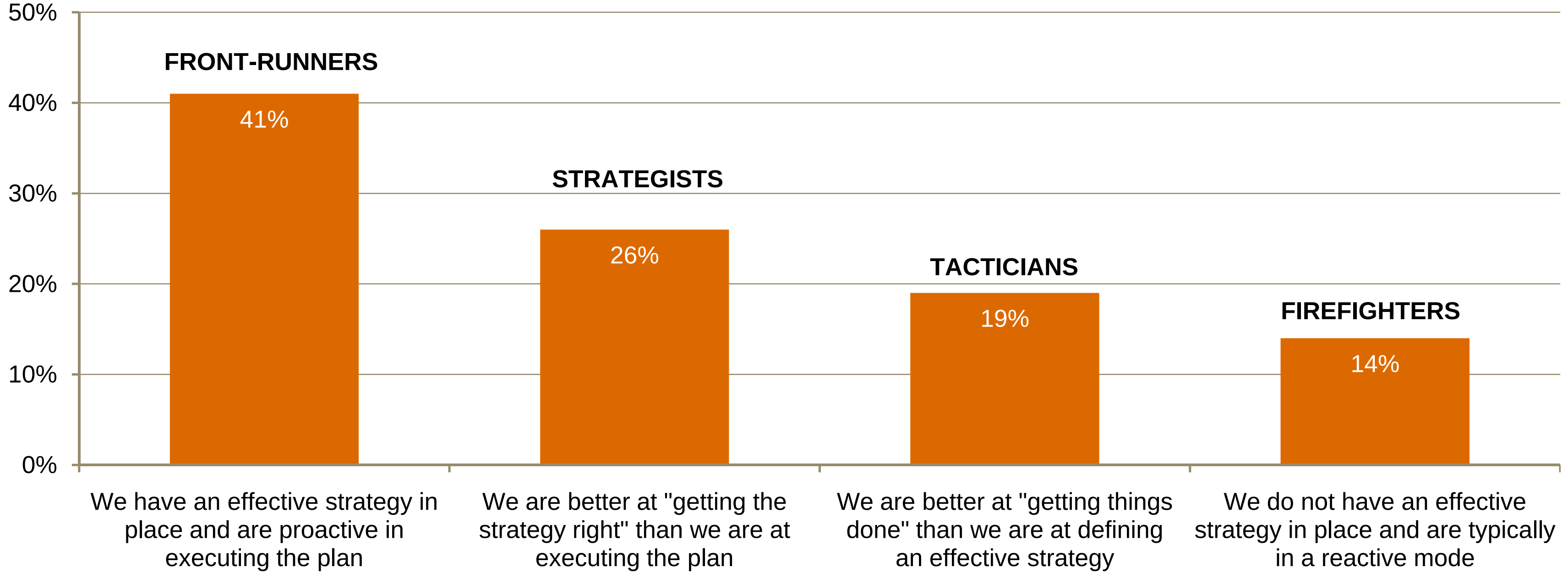
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

Confidence and progress

Many respondents from public sector entities view their organization as a “front-runner.”

Among this year’s public sector respondents, 41% say their organization has an effective strategy in place and is proactive in executing it.



Question 26n11: “Which statement best characterizes your organization’s approach to protecting information security?”

They are also highly confident in their organization’s security.

A majority – 64% – of public sector respondents are also confident that their organization’s information security initiatives are effective.

	2011
Very confident	**26%**
Somewhat confident	**38%**
Total	**64%**

Question 35: “How confident are you that your organization’s information security activities are effective?”

Insights into the frequency, type, and source of security breaches have leaped dramatically over the past 12 months.

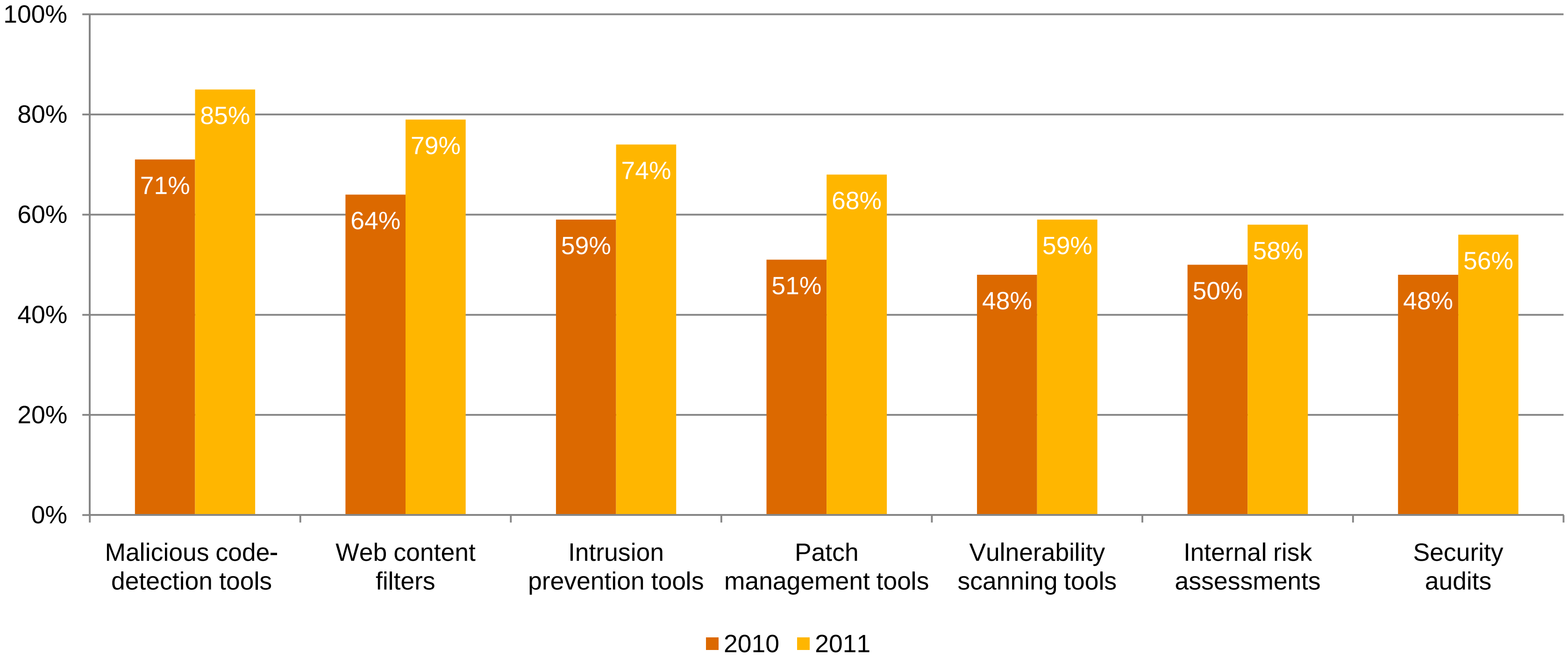
Just a few years ago, as many as half of public sector respondents couldn't answer the most basic questions about the nature of security-related breaches. Now, 73% or more of public sector respondents can answer specific survey questions about factors such as security event frequency, type, and source.

Respondents who answered "Do not know" or "Unknown"	2007	2008	2009	2010	2011
How many incidents occurred in past 12 months?	48%	47%	50%	40%	**15%**
What type of incident occurred?	49%	48%	51%	46%	**15%**
What was the source of the incident?	N/A	49%	51%	47%	**27%**

Question 19: "Number of security incidents in the past 12 months." Question 20: "What types of security incidents (breach or downtime) occurred?" Question 22: "Estimated likely source of incident." (Totals do not add up to 100%.)

Despite tight budgets, public sector entities are proactively adopting safeguards to bolster data security and prevent cyber crime.

Over the past year, the public sector has made solid gains in strengthening detection and prevention safeguards to protect information from potential breaches.



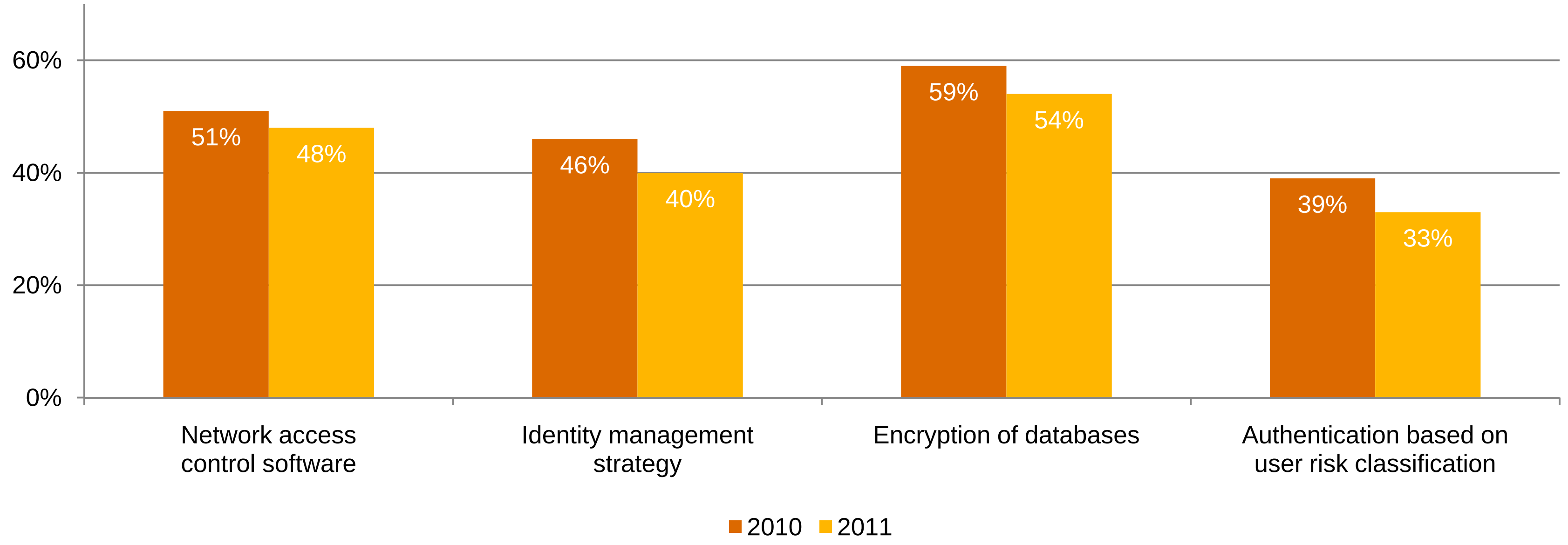
Question 17: “What process information security safeguards does your organization currently have in place?” Question 18: “What technology information security safeguards does your organization currently have in place?” (Not all factors shown. Totals do not add up to 100%.)

Section 3

Signs of vulnerability and exposure

Advanced Persistent Threats: They can be devastating – but just how prepared are public sector entities to address them?

Among public sector respondents, 14% report they have a security policy that addresses APT. In fact, many lack the tools to fight APT – and, among those that do, maintenance of these capabilities has tapered off over the past year.



Question 28: "Which of the following elements, if any, are included in your organization's security policy?" Question 17: "What process information technology security safeguards does your organization currently have in place?" Question 18: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown. Totals do not add up to 100%.)

Other trends in this year’s survey are also troubling. Take the increase in security events, for example.

It is tempting to trumpet the fact that 28% of public sector respondents report no security events in the past year. Yet reports of incidents increased this year – across the board.

Number of security incidents	2007	2008	2009	2010	2011
No incidents	17%	18%	16%	22%	28%
1 to 9 incidents	23%	23%	23%	27%	33%
10 to 49 incidents	6%	8%	8%	5%	11%
50 or more incidents	5%	4%	4%	6%	13%

Question 19: “Number of security incidents in the past 12 months.” (Totals do not add up to 100%.)

This year's survey reveals degradation in many of the public sector's strategic security processes.

Although public sector entities have been investing in technology related to detection, prevention, and web-related security, this year's survey reveals a deterioration in core security policies.

	2009	2010	2011
Overall information security strategy	66%	65%	**60%**
Business continuity / disaster recovery plans	54%	43%	**36%**
Portable device security standards	49%	43%	**39%**
Employee security awareness training	55%	49%	**44%**
Centralized security information management system	55%	50%	**43%**

Question 17: "What process information security safeguards does your organization have in place?"

Most significant is the fact that security spending deferrals and cut-backs have increased significantly over last year.

For the third year in a row, security-related spending deferrals and cut-backs – for both capital and operating expenditures – have jumped. This year's reluctance to spend on security priorities increased across all categories and by as much as 33%. In fact, spending appears even more restrained than it was during the two years immediately following 2008.

Has your company **deferred** security initiatives?	2009	2010	2011
Yes, for *capital* expenditures	33%	40%	**53%**
Yes, for *operating* expenditures	29%	38%	**48%**

Has your company **reduced the cost** for security initiatives?	2009	2010	2011
Yes, for *capital* expenditures	37%	40%	**53%**
Yes, for *operating* expenditures	35%	40%	**52%**

Question 12: "Has your company deferred security-related initiatives?" Question 13: "Has your company reduced the cost for any security-related initiatives?" (Not all factors shown. Total does not add up to 100%.)

And that high confidence rating? It has actually declined 20 points since 2007.

Confidence is always good. But a decline in confidence is telling. These numbers indicate that public sector administrators, directors and staff – across the world – are less sure that their organization is prepared to address the threats that confront its critical information.

	2007	2008	2009	2010	2011	CHANGE
Total	**84%**	84%	75%	70%	**64%**	**- 20 pts**

Question 35: "How confident are you that your organization's information security activities are effective?" (Respondents who answered "Very confident" or "Somewhat confident" combined)

Section 4

The greatest opportunities for improvement

What’s holding security back?

Given the austere spending environment, it’s not surprising that public sector respondents consider insufficient capital the primary obstacle to the effectiveness of their organization’s information security function. After all, it’s hard to keep the leading edge of prevention-oriented capabilities razor sharp when budgets are tight. What we didn’t expect to find is that administrators consider the next greatest obstacles to be the lack of an effective information security strategy and the organization’s leadership itself.

	2011
1. Insufficient capital expenditures	**28%**
2. Lack of an effective information security strategy	**25%**
3. Leadership – CEO, President, Board or equivalent	**25%**
4. Lack of actionable vision or understanding	**23%**
5. Absence or shortage of in-house technical expertise	**22%**
6. Insufficient operating expenditures	**21%**
7. Poorly integrated or overly complex information/IT systems	**20%**

Question 27n11: “What are the greatest obstacles to improving the overall strategic effectiveness of your organization’s information security function?” (Not all factors shown. Total does not add up to 100%.)

What are the top information security priorities in the public sector this coming year?

Public sector respondents plan to shine the spotlight brightest in two key areas: continuous monitoring as well as regulation and compliance.

	2011
1. Continuous monitoring	**38%**
2. Regulation and compliance	**24%**
3. Department to protect government IT systems from cyber attack	**12%**
4. Cloud computing security	**10%**
5. Portable device security	**6%**
6. Combating Advanced Persistent Threat	**6%**

(Asked only of Public Sector respondents) Question 1: "What is your organization's top security priority for the next 12 months?" (Not all factors shown. Total does not add up to 100%.)

While only 12% of respondents report that establishing a department to protect government IT is the highest priority in the coming year, almost half still say they plan to do it.

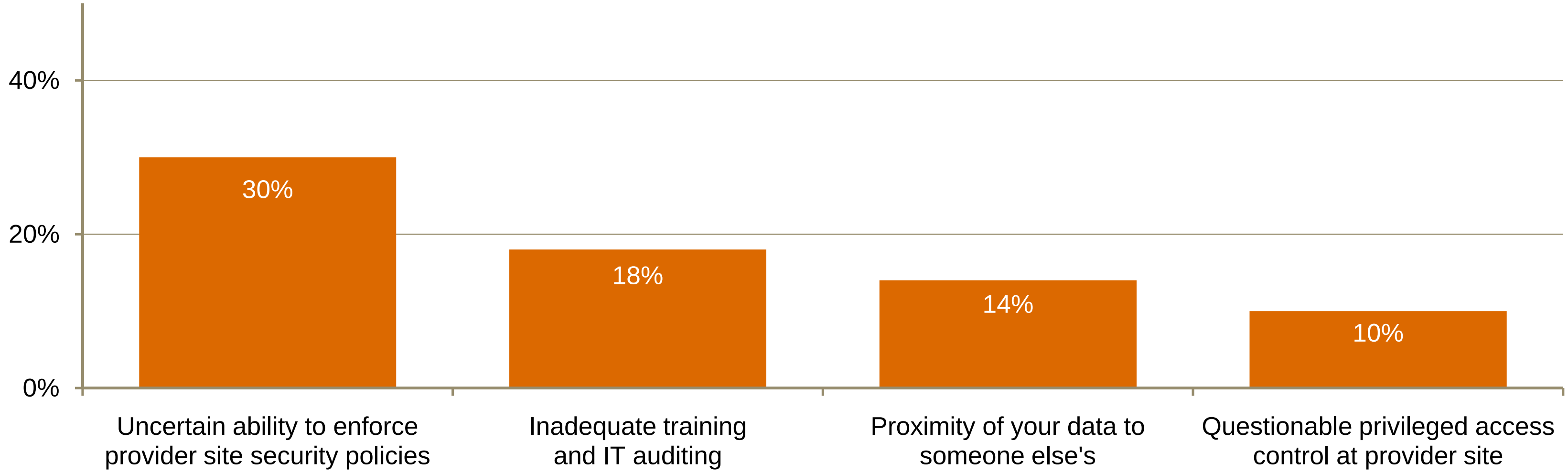
Public sector respondents report that terrorists and hackers account for 39% of all security incidents, so it's not surprising that many intend to establish a department to protect government IT systems from cyber attacks. Those that do plan a cyber crime department say its top executive will report to the CIO (61%) or the CSO (36%).

Plan to establish a department to protect government IT systems from cyber attacks	2011
Yes	45%
No	30%
Do not know	25%

Question 22: "Estimated likely source of incident. (Check all that apply)" Question 2 (Public Sector): "Does your organization plan to establish a department to protect government IT systems from cyber attacks?" Question 2a (Public Sector): "The department will report to: (CIO, CSO or Other)."

Cloud computing: Is it improving information security? Yes, but many want better enforcement of provider security policies.

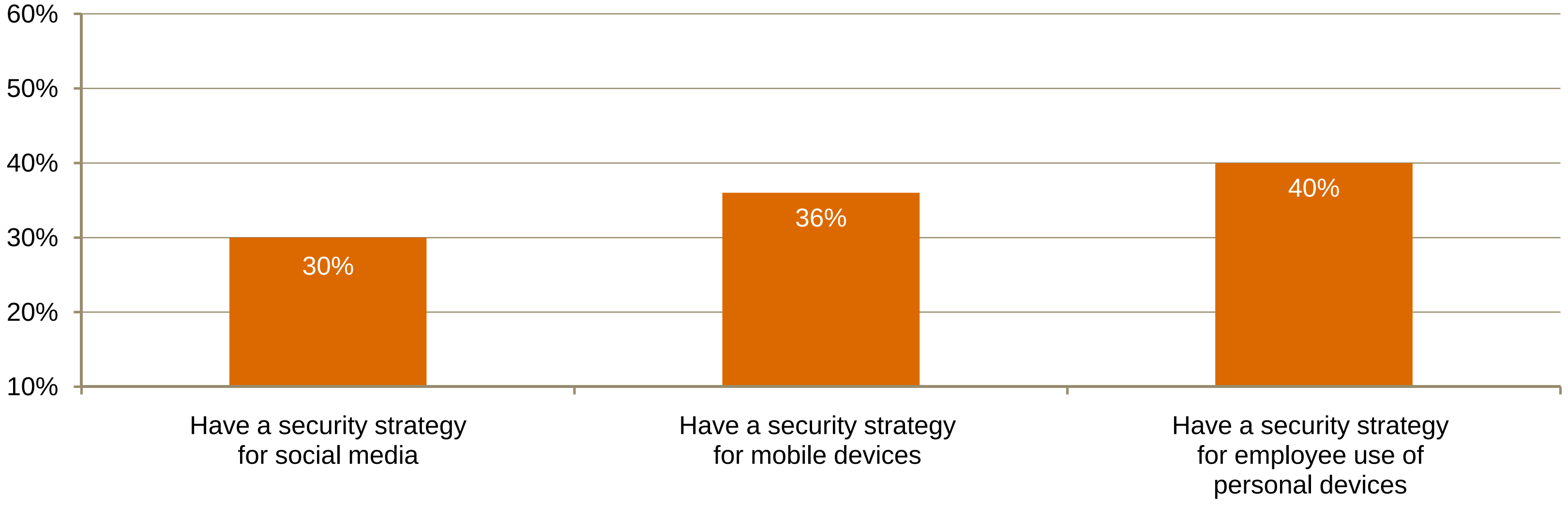
This year, 32% of public sector respondents report that their organization uses cloud services. Among those that have adopted cloud solutions, 51% say the technology has improved their security posture. Responses also revealed that while enforcing provider security policies is seen as the principal security challenge, respondents are also concerned about training as well as multi-tenancy issues.



Question 41: “Does your organization currently use cloud services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or Infrastructure-as-a-Service (IaaS)?” Question 41c: “What impact has cloud computing had on your company’s information security?” Question 41b: “What is the greatest security risk to your cloud computing strategy?” (Not all factors shown. Total does not add up to 100%.)

Mobile devices and social media: New rules are in effect this year – but not yet critical mass.

Public sector entities are also implementing strategies to keep pace with employee adoption of new technologies – including use of mobile devices and social-networking tools – and are creating rules about how employees can use personal technology within the enterprise.



Question 17: "What process information security safeguards does your organization currently have in place?" (Not all factors shown. Total does not add up to 100%.)

For more information, please contact:

National Security Contacts

Gary Loveland
Principal, National Security Leader
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

Public Sector Contacts

Scott McIntyre
Principal
703.918.1352
scott.mcintyre@us.pwc.com

John Hunt
Principal
703.918.3767
john.d.hunt@us.pwc.com

Or visit www.pwc.com/giss2012

This document is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

www.pwc.com/security

Eye of the storm

As the global economy stalls and information security threats such as cyber crime and Advanced Persistent Threats cloud the horizon, many see sunshine and clear skies overhead

CIO Business Technology Leadership

CSO BUSINESS RISK LEADERSHIP

Retail & Consumer

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

September 2011

pwc

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*

The economic thunderheads of 2008 may have passed. But across the global retail and consumer (R&C) industry, some clouds 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.

Nonetheless, according to PwC's 2012 Global State of Information Security Survey®, the vast majority of R&C executives are confident in the effectiveness of their information security practices.

They have an effective strategy in place. They consider their organizations proactive in executing it. And over the past year, the business impacts of security incidents have declined – nearly across the board.

Yet all is not in order. Security event frequency is up. Strategic security processes are beginning to degrade. And the capital and operating expenditures crucial to early prevention and agile response are more like to be deferred or canceled than at any time since 2008.

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, the reasons to do so quickly and strategically are mounting.

Agenda

Section 1. Methodology

Section 2. Confidence and progress

Section 3. Signs of vulnerability and exposure

Section 4. The greatest opportunities for improvement

Section 1

Methodology

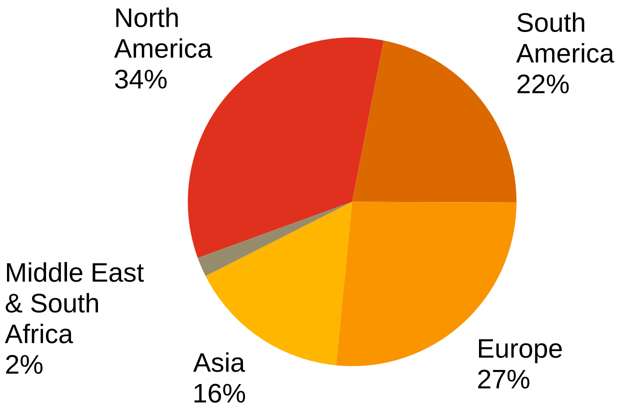
A worldwide study

The 2012 Global State of Information Security Survey®, a worldwide study by PwC, CIO Magazine and CSO Magazine, was conducted online from February 10, 2011 to April 18, 2011.

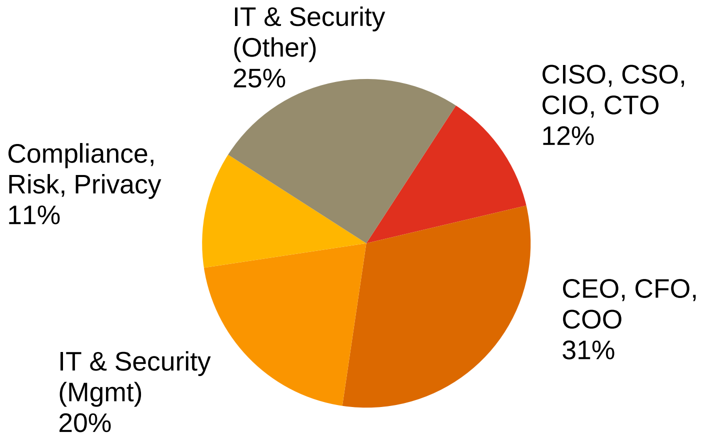
- PwC's 14th year conducting the online survey, 9th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 138 countries
- More than 9,600 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-one percent (31%) of respondents from companies with revenue of $500 million+
- Survey included 996 respondents from the R&C industry
- The margin of error is less than 1%

Demographics

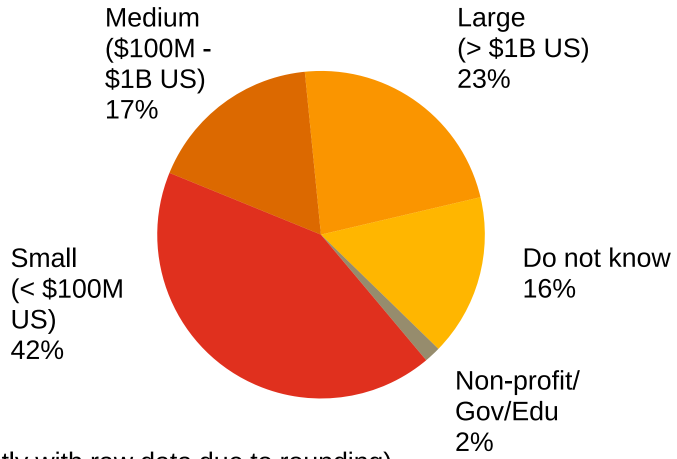
R&C respondents by region of employment



R&C respondents by title



R&C respondents by company revenue size



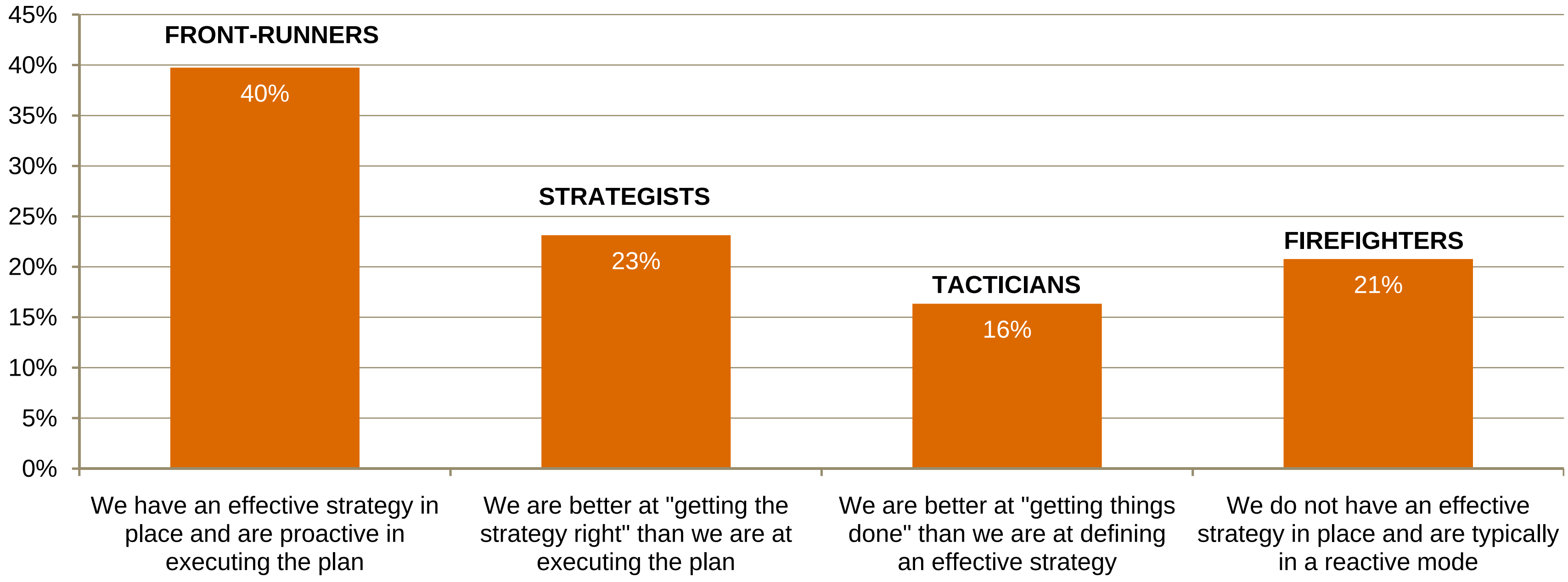
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

Confidence and progress

Many R&C respondents see their organization as a “front-runner” in information security.

Forty percent (40%) of this year’s R&C respondents say their organization has an information security strategy in place and is proactive in executing it.



Question 26n11: “Which statement best characterizes your organization’s approach to protecting information security?”

They are also highly confident in their organization's security.

A clear majority – nearly three quarters (72%) – of industry respondents are also confident that their organization's information security activities are effective.

	2011
Very confident	**35%**
Somewhat confident	**37%**
Total	**72%**

Question 35: "How confident are you that your organization's information security activities are effective?"

Insights into the frequency, type, and source of security breaches have leaped dramatically over the past 12 months.

Just a few years ago, nearly half of this survey's R&C respondents couldn't answer the most basic questions about the nature of security-related breaches. Now, 75% or more respondents can answer specific survey questions about factors such as security event frequency, type, and source.

Respondents who answered "Do not know" or "Unknown"	2008	2009	2010	2011
How many incidents occurred in past 12 months?	28%	34%	23%	**9%**
What type of incident occurred?	44%	48%	34%	**15%**
What was the source of the incident?	41%	42%	36%	**25%**

Question 19: "Number of security incidents in the past 12 months." Question 20: "What types of security incidents (breach or downtime) occurred?" Question 22: "Estimated likely source of incident." (Totals do not add up to 100%.)

When incidents did occur, they were much less likely to impact the business than they were one year ago.

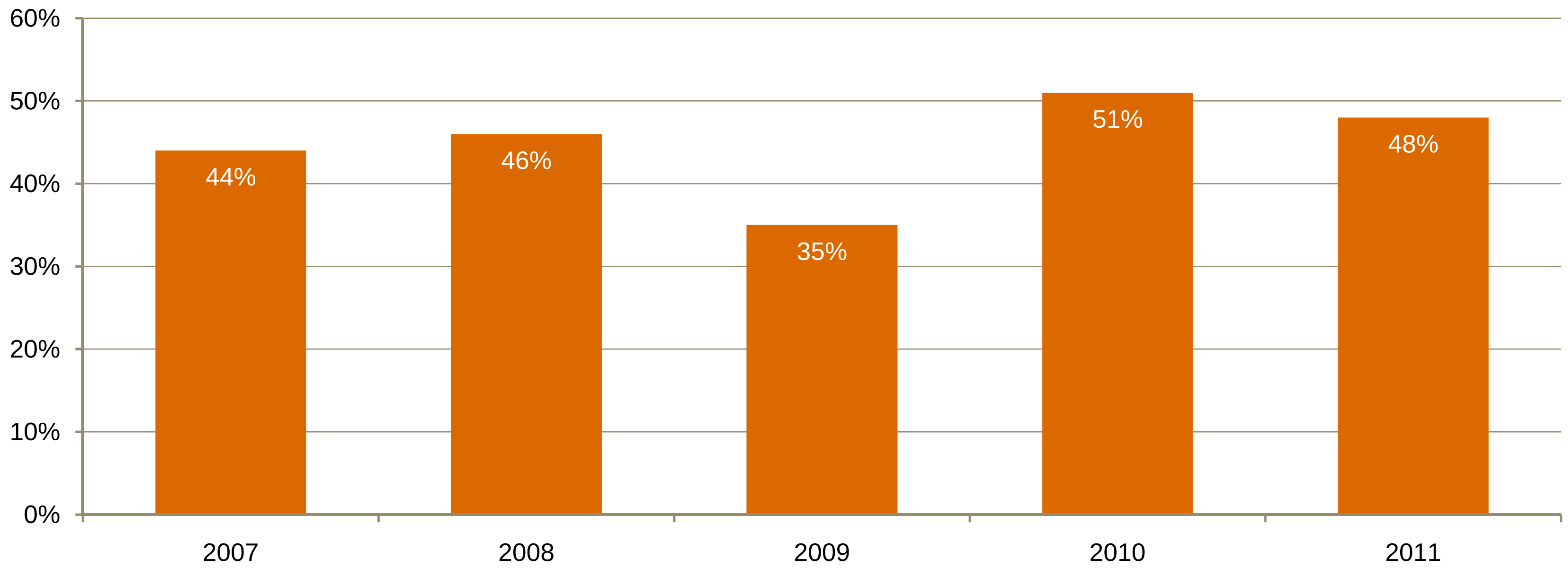
This year, R&C respondents report generally lower impacts to the business – from financial losses and damage to the company's brand to fraud and legal exposure.

Business impacts	2010	2011	CHANGE
Financial losses	21%	16%	**- 24%**
Intellectual property theft	15%	12%	**- 20%**
Brand / reputation compromised	13%	9%	**- 31%**
Fraud	9%	7%	**- 22%**
Legal exposure / lawsuit	6%	3%	**- 50%**

Question 23: "How was your organization impacted by the security incident? Business:" (Not all factors shown. Totals do not add up to 100%.)

At the same time, a majority of industry respondents are “bullish” about security spending over the next 12 months.

Will security spending in the industry increase? Optimism carries the day. Despite a small reduction over last year, almost half of all R&C respondents believe that it will.



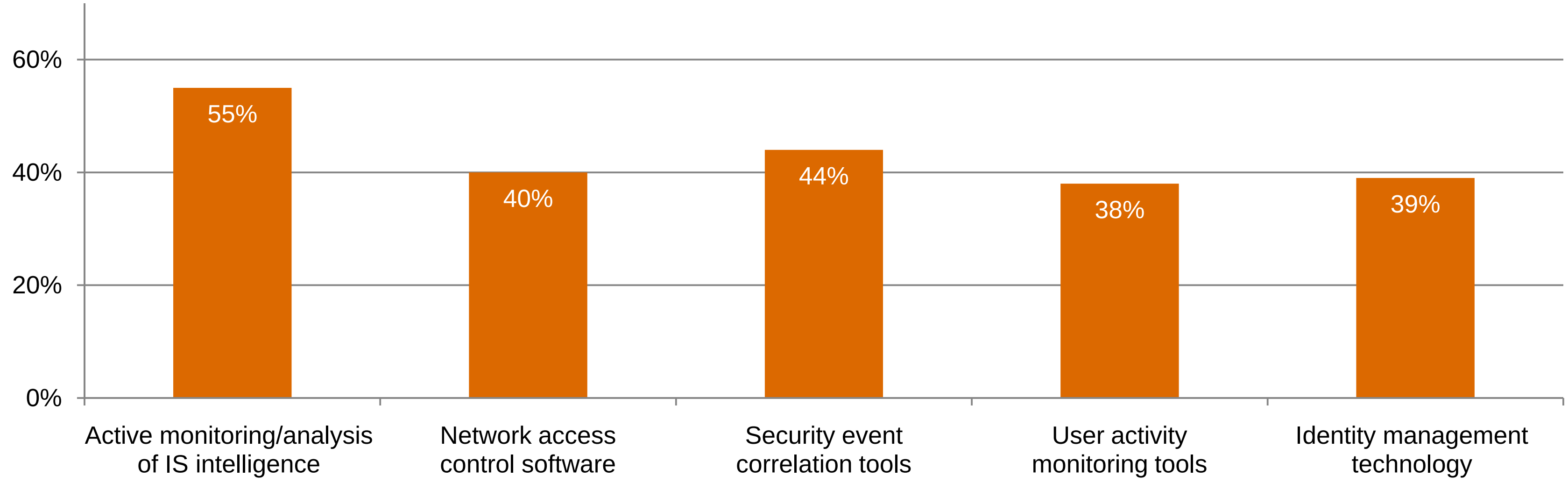
Question 9: “When compared with last year, security spending over the next 12 months will:” (Respondents who answered “Increase up to 10%,” “Increase 11-30%,” or “Increase more than 30%”)

Section 3

Signs of vulnerability and exposure

Advanced Persistent Threats: They can be devastating – but just how prepared are R&C organizations to address them?

Nearly half of all R&C respondents told us this year that concerns over APT “drives their organization’s security spending.” In spite of this, a majority of R&C respondents (86%) reveal that their organization’s security policy does not address APT. In addition, many industry firms lack the capabilities and tools to combat this new threat.



Question 1 (Retail & Consumer): “Does Advanced Persistent Threat drive your organization’s security spending?” Question 28: “Which of the following elements, if any, are included in your organization’s security policy?” Question 18: “What technology information security safeguards does your organization currently have in place?” (Not all factors shown. Totals do not add up to 100%.)

Other trends in this year's survey are also troubling. Take the increase in security events, for example.

It is tempting to trumpet the fact that one-third of industry respondents (33%) report no security events in the past year. Yet reports of incidents increased this year, across the board.

Number of security incidents	2007	2008	2009	2010	2011
No incidents	25%	34%	24%	31%	**33%**
1 to 9 incidents	34%	28%	33%	37%	**43%**
10 to 49 incidents	7%	9%	6%	6%	**8%**
50 or more incidents	3%	2%	4%	3%	**8%**

Question 19: "Number of security incidents in the past 12 months." (Totals do not add up to 100%.)

This year's data revealed some regression in a best-practice trend: having the CISO report to the "top of the house."

Reversing a multi-year trend, 25% of industry respondents now say their Chief Information Security Officer or equivalent executive reports not to the Board, the CEO or the CFO, but to the CIO.

Whom the CISO reports to	2008	2009	2010	2011
Board of Directors	20%	31%	35%	**33%**
Chief Executive Officer	33%	37%	34%	**31%**
Chief Financial Officer	15%	14%	16%	**16%**
Chief Information Officer	35%	30%	19%	**25%**

Question 16a: "Where/to whom does your CISO or equivalent senior information security officer report?" (Not all factors shown. Totals do not add up to 100%.)

Most significant is the fact that security spending deferrals and cut backs – already high – have increased even further.

For the third year in a row, security-related spending deferrals and cut-backs – for both capital and operating expenditures – are high. This year's reluctance to spend on security priorities increased or remained constant for all categories. In fact, spending appears even more restrained than it was during the two years immediately following 2008.

Has your company **deferred** security initiatives?	2009	2010	2011
Yes, for *capital* expenditures	41%	43%	**48%**
Yes, for *operating* expenditures	37%	40%	**46%**

Has your company **reduced the cost** for security initiatives?	2009	2010	2011
Yes, for *capital* expenditures	47%	43%	**46%**
Yes, for *operating* expenditures	44%	44%	**48%**

Question 12: "Has your company deferred security-related initiatives?" Question 13: "Has your company reduced the cost for any security-related initiatives?" (Not all factors shown. Totals do not add up to 100%.)

With spending tight, degradation across many of the industry's security capabilities continues.

Although R&C industry firms have been investing in technology related to detection, prevention and web-related security, this year's survey reveals a troubling degradation in core strategic processes.

	2008	2009	2010	2011
Employ Chief Privacy Officer	16%	24%	33%	**24%**
Accurate inventory of employees' and customers' personal data	35%	40%	37%	**30%**
Due diligence of third parties that handle personal data	22%	35%	29%	**25%**
People dedicated to monitoring employee use of the Internet	47%	52%	53%	**48%**
Have employee security awareness program	48%	48%	48%	**37%**

Question 15: "Which data privacy safeguards does your organization have in place?" Question 16: "What information security safeguards related to people does your organization have in place?" Question 17: "What process information security safeguards does your organization currently have in place?"

And that high confidence rating? It has actually declined 13 points since 2007.

Confidence is always good. But a decline in confidence is telling. These numbers indicate that R&C business and IT personnel – across the world – are less sure that their organization is prepared to address the threats that confront its critical information.

	2007	2008	2009	2010	2011	CHANGE
Total	**85%**	83%	80%	76%	**72%**	**- 13 pts**

Question 35: “How confident are you that your organization’s information security activities are effective?” (Respondents who answered “Very confident” or “Somewhat confident” combined)

Section 4

The greatest opportunities for improvement

What’s holding security back?

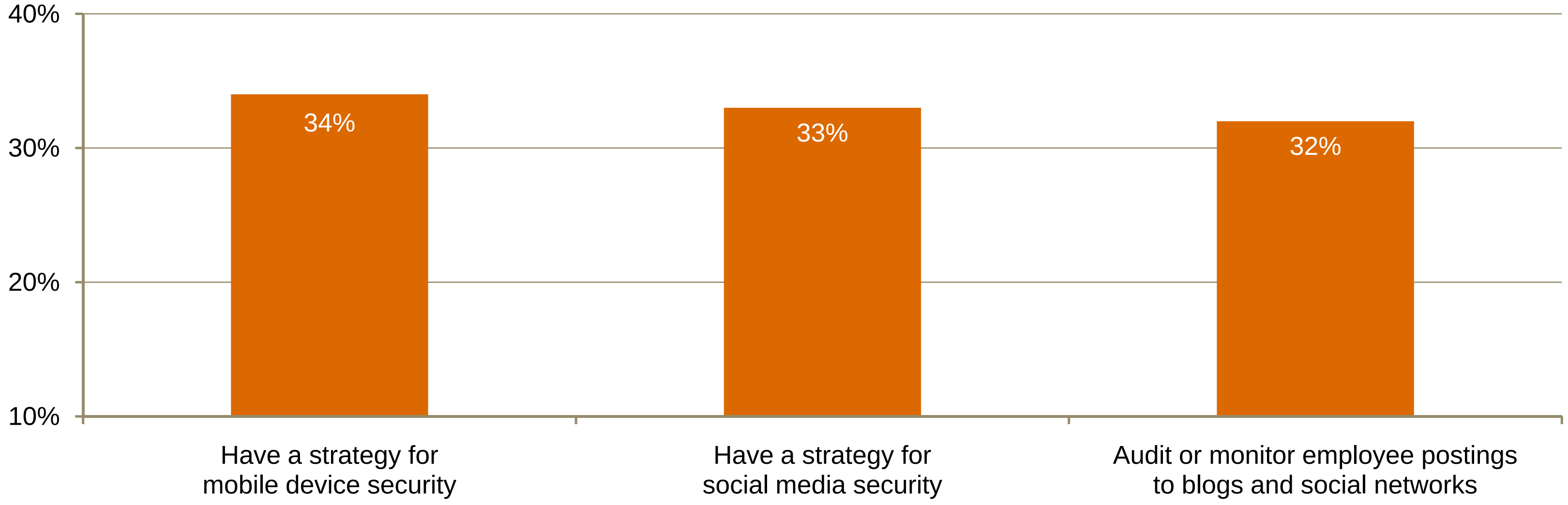
Given the austere spending environment – not just this year, but since 2008 – and a steady regression in the readiness of security capabilities, it’s not surprising that R&C respondents consider insufficient capital and operating expenditures the leading obstacle to the effectiveness of their organization’s information security function. What we didn’t expect to find is that industry respondents consider the next greatest obstacles to be the lack of an “actionable vision” for the security function and the leadership team of the company itself.

	2011
1. Insufficient capital expenditures	**29%**
2. Insufficient operating expenditures	**24%**
3. Lack of an actionable vision or understanding	**24%**
4. Leadership – CEO, president, board, or equivalent	**23%**
5. Lack of an effective information security strategy	**23%**
6. Absence of shortage of in-house technical expertise	**21%**
7. Poorly integrated or overly complex information/IT systems	**16%**
8. Leadership – CISO, CSO, or equivalent	**16%**
9. Leadership – CIO or equivalent	**15%**

Question 27n11: “What are the greatest obstacles to improving the overall strategic effectiveness of your organization’s information security function?” (Total does not add up to 100%.)

Mobile devices and social media: New rules are in effect this year – but not yet critical mass.

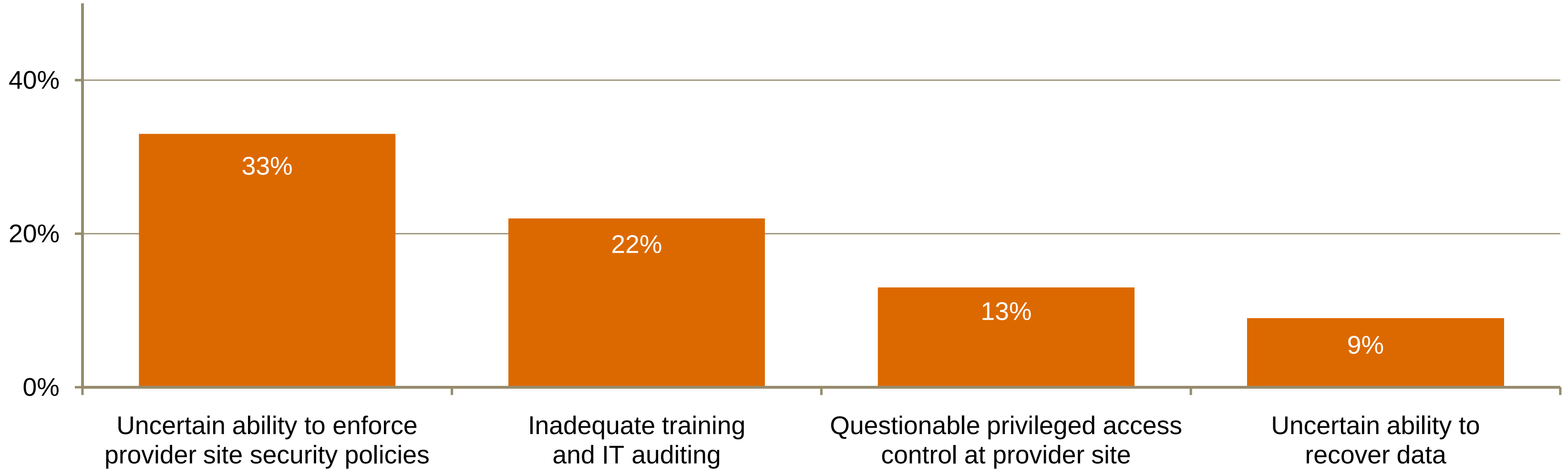
Many R&C companies are implementing strategies to keep pace with employee adoption of new technologies – particularly the use of personal electronic devices and social-networking tools. They're also implementing controls to govern how employees can use personal technology within the enterprise. More than half of the industry, however, has not yet begun to put these capabilities into place.



Question 17: "What process information security safeguards does your organization currently have in place?" (Not all factors shown. Total does not add up to 100%.)

Cloud computing: Is it improving information security? Yes, but many want better enforcement of provider security policies.

This year, 35% of all retail and consumer respondents report that their organization uses cloud services – and over half (54%) of those say the cloud has improved their information security. Responses also revealed that the leading security risk to cloud computing is enforcing the provider's security policies. Beyond the questions asked in the survey, we see another crucial issue challenging many of our R&C clients: monitoring – and the need to confirm that service providers are adhering to the client's policies and standards.



Question 41: "Does your organization currently use cloud services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or Infrastructure-as-a-Service (IaaS)?" Question 41c: "What impact has cloud computing had on your company's information security?" Question 41b: "What is the greatest security risk to your cloud computing strategy?" (Not all factors shown. Total does not add up to 100%.)

For more information, please contact:

National Security Contacts

Gary Loveland
Principal, National Security Leader
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

Retail & Consumer Contacts

Lisa Dugal
Principal, National R&C Leader
646.471.6916
lisa.feigen.dugal@us.pwc.com

Pieter Penning
Director
678.419.1094
peter.penning@us.pwc.com

Paul Ritters
Director
612.596.6356
paul.j.ritters@us.pwc.com

Or visit www.pwc.com/giss2012

This document is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

www.pwc.com/security

Eye of the storm

As the global economy stalls and information security threats such as cyber crime and Advanced Persistent Threats cloud the horizon, many see sunshine and clear skies overhead

Technology

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

September 2011

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*

The economic thunderheads of 2008 may have passed. But across the technology industry, some clouds 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.

Nonetheless, according to PwC's 2012 Global State of Information Security Survey®, the majority of technology industry executives are confident in the effectiveness of their information security practices.

They have an effective strategy in place. They consider their organizations proactive in executing it. And funding expectations are running high.

Yet all is not in order. Security event frequency is up. Strategic security processes are beginning to degrade. And the capital and operating expenditures crucial to early prevention and agile response are more likely to be deferred or canceled than at any time since 2008.

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, the reasons to do so quickly and strategically are mounting.

Agenda

Section 1.	Methodology
Section 2.	Confidence and progress
Section 3.	Signs of vulnerability and exposure
Section 4.	The greatest opportunities for improvement

Section 1

Methodology

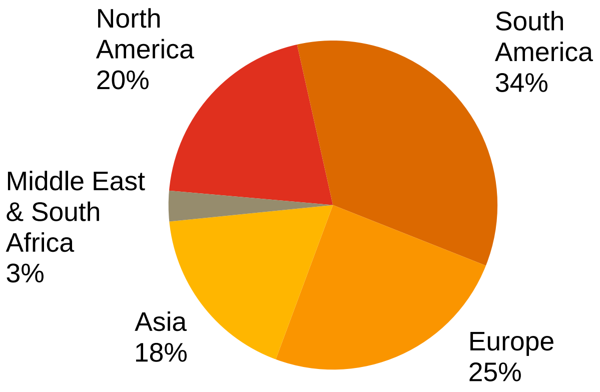
A worldwide study

The 2012 Global State of Information Security Survey®, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 10, 2011 to April 18, 2011.

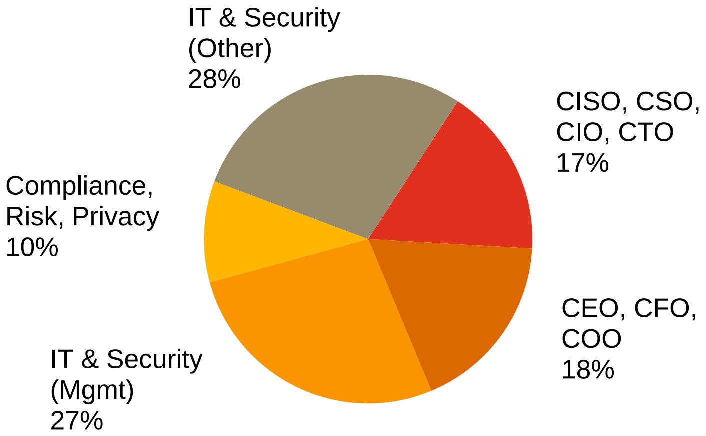
- PwC's 14th year conducting the online survey, 9th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 138 countries
- More than 9,600 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-one percent (31%) of respondents from companies with revenue of $500 million+
- Survey included 1,606 respondents from the technology industry
- The margin of error is less than 1%

Demographics

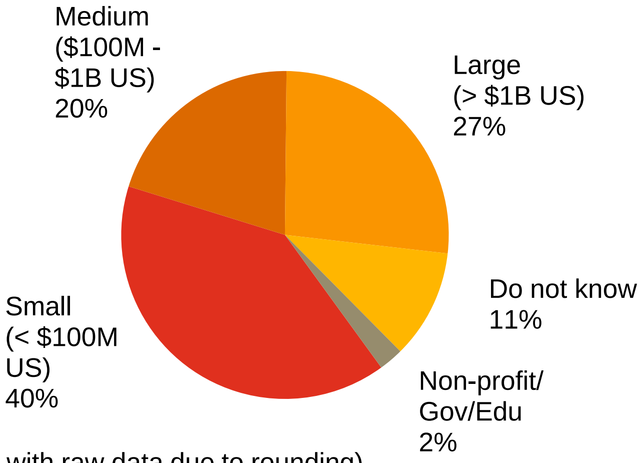
Technology respondents by region of employment



Technology respondents by title



Technology respondents by company revenue size



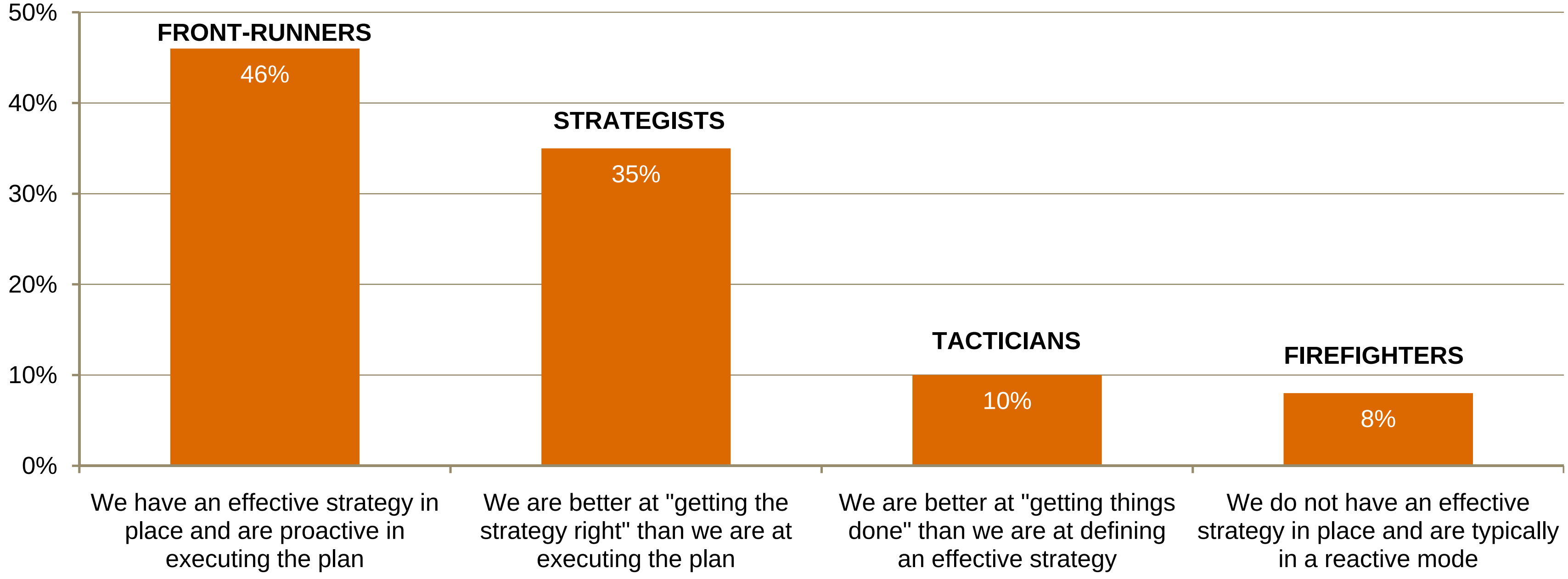
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

Confidence and progress

Almost half of all technology respondents view their organization as a "front-runner" in information security.

Almost half of this year's technology respondents (46%) say their organization has a strategy in place and is proactive in executing it.



Question 26n11: "Which statement best characterizes your organization's approach to protecting information security?" Numbers reported may not reconcile exactly with raw data due to rounding)

They are also highly confident in their organization’s security.

A clear majority – nearly three out of four (72%) – of technology respondents are also confident that their organization’s information security initiatives are effective.

	2011
Very confident	**37%**
Somewhat confident	**35%**
Total	**72%**

Question 35: “How confident are you that your organization’s information security activities are effective?”

Insights into the frequency, type, and source of security breaches have leaped dramatically over the past 12 months.

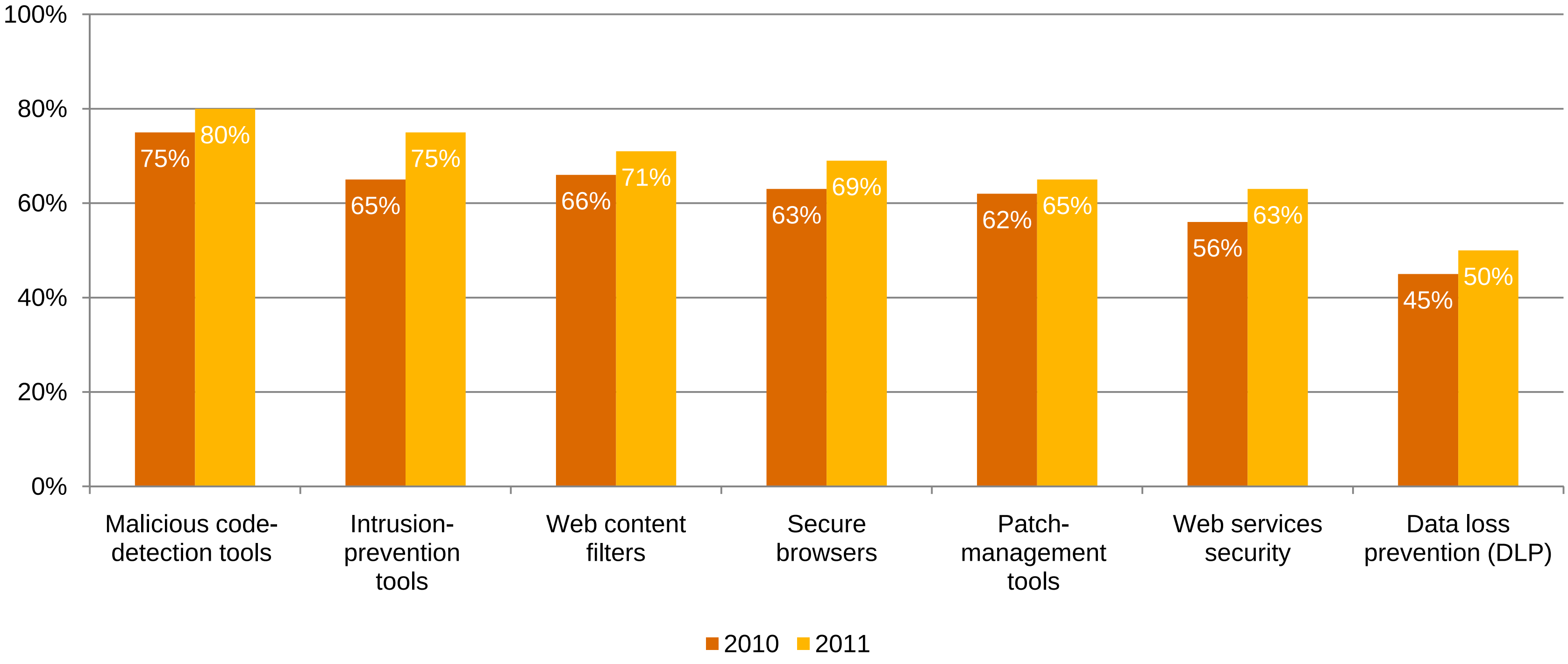
Just a few years ago, as many as 46% of technology respondents couldn't answer the most basic questions about the nature of security-related breaches. Now, 84% or more of them can answer specific survey questions about factors such as security event frequency, type, and source.

Respondents who answered "Do not know" or "Unknown"	2007	2008	2009	2010	2011
How many incidents occurred in past 12 months?	42%	34%	26%	18%	**5%**
What type of incident occurred?	46%	43%	33%	27%	**10%**
What was the source of the incident?	N/A	42%	34%	30%	**16%**

Question 19: "Number of security incidents in the past 12 months." Question 20: "What types of security incidents (breach or downtime) occurred?" Question 22: "Estimated likely source of incident." (Totals do not add up to 100%.)

Despite tight budgets, technology firms are proactively adopting safeguards to protect data and prevent cyber crime.

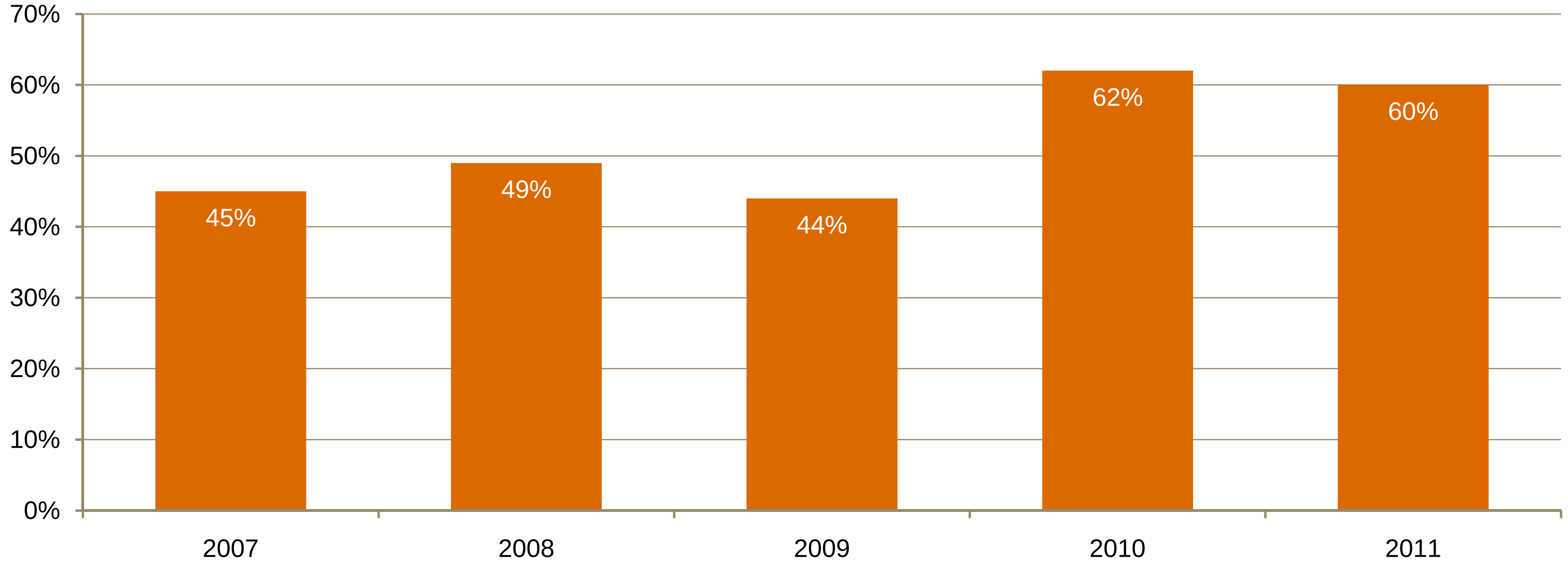
Over the past year, technology companies have made solid gains in strengthening detection and prevention safeguards to protect data from potential breaches.



Question 18: “What technology information security safeguards does your organization currently have in place?” (Not all factors shown. Totals do not add up to 100%.)

At the same time, a majority of technology respondents are "bullish" about security spending over the next 12 months.

Will security spending in the industry increase? Optimism carries the day. Six out of ten (60%) technology industry respondents believe that it will.



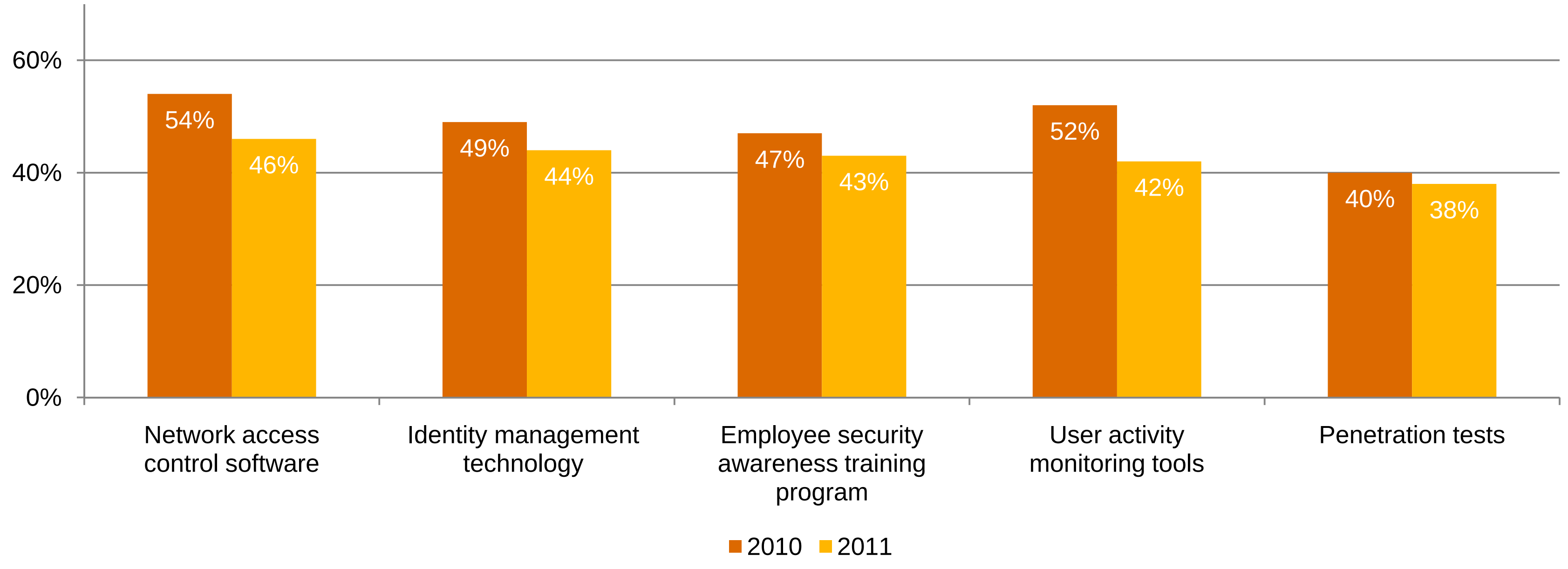
Question 9: "When compared with last year, security spending over the next 12 months will:" (Respondents who answered "Increase up to 10%," "Increase 11-30%," or "Increase more than 30%")

Section 3

Signs of vulnerability and exposure

Advanced Persistent Threats: They can be devastating – but just how prepared are technology entities to address them?

Sixty percent (60%) of technology respondents report that Advanced Persistent Threat drives their organization’s security spending. Yet implementation of certain tools and processes crucial to combatting this new threat has slowed over the past year.



Question 4 (Technology): “Does Advanced Persistent Threat drive your organization’s security spending?” Question 17: “What process information technology security safeguards does your organization currently have in place?” Question 18: “What technology information security safeguards does your organization currently have in place?” (Not all factors shown. Totals do not add up to 100%.)

Other trends in this year’s survey are also troubling. Take the increase in security events, for example.

It is tempting to trumpet the fact that more than almost one out of four (23%) technology industry respondents report no security events in the past year. Yet reports of incidents increased this year, especially among respondents indicating 10 or more negative events.

Number of security incidents	2007	2008	2009	2010	2011
No incidents	20%	23%	17%	24%	**23%**
1 to 9 incidents	27%	30%	40%	43%	**42%**
10 to 49 incidents	7%	7%	11%	8%	**12%**
50 or more incidents	4%	5%	7%	7%	**19%**

Question 19: “Number of security incidents in the past 12 months.” (Totals do not add up to 100%.)

Most significant is the fact that security spending deferrals and cut-backs – already high – have increased even further.

For the third year in a row, security-related spending deferrals and cut-backs – for both capital and operating expenditures – have increased. This year's reluctance to spend on security priorities has jumped by as much as 20% over last year's reported levels. In fact, spending appears even more restrained than it was during the two years immediately following 2008.

Has your company **deferred** security initiatives?	2009	2010	2011
Yes, for *capital* expenditures	47%	53%	**61%**
Yes, for *operating* expenditures	45%	49%	**59%**

Has your company **reduced the cost** for security initiatives?	2009	2010	2011
Yes, for *capital* expenditures	51%	54%	**63%**
Yes, for *operating* expenditures	49%	54%	**62%**

Question 12: "Has your company deferred security-related initiatives?" Question 13: "Has your company reduced the cost for any security-related initiatives?" (Not all factors shown. Total does not add up to 100%.)

With spending tight, degradation in many of the industry's security capabilities is starting to appear.

Although technology firms have been investing in technology related to detection, prevention and web-related security, this year's survey reveals a troubling degradation in core strategic processes.

	2009	2010	2011
Overall information security strategy	70%	67%	**65%**
People dedicated to monitoring employee Internet use	62%	56%	**50%**
Accurate inventory of employee/customer personal data	45%	40%	**34%**
Employee security awareness training program	54%	47%	**43%**
Personnel background checks	59%	57%	**54%**

Question 17: "What process information security safeguards does your organization currently have in place?" Question 16: "What information security safeguards related to people does your organization have in place?" Question 15: "Which data privacy safeguards does your organization have in place?" (Not all factors shown. Totals do not add up to 100%.)

And that high confidence rating? It has actually declined 16 points since 2006.

Confidence is always good. But a decline in confidence is telling. These numbers indicate that the technology industry's business and IT personnel – across the world – are less sure that their organization is prepared to address the threats that confront its critical information.

	2006	2007	2008	2009	2010	2011	CHANGE
Total	**87%**	84%	86%	84%	78%	**71%**	**- 16 pts**

Question 35: "How confident are you that your organization's information security activities are effective?" (Respondents who answered "Very confident" and "Somewhat confident" combined)

Section 4

The greatest opportunities for improvement

What's holding security back?

Given the austere spending environment – not just this year, but since 2008 – we weren't surprised to see that respondents reported insufficient capital expenditures as the third most cited obstacle to the effectiveness of their organization's information security function. It's hard to keep the leading edge of prevention-oriented capabilities razor sharp when budgets are tight. What we didn't expect to find is that technology respondents consider the single greatest obstacle to be the lack of an actionable vision for the function, followed closely by the lack of an effective strategy.

	2011
1. Lack of an actionable vision or understanding	29%
2. Lack of an effective information security strategy	29%
3. Insufficient capital expenditures	25%
4. Leadership – CISO, CSO, or equivalent	25%
5. Leadership – CEO, President, Board, or equivalent	25%
6. Leadership – CIO or equivalent	24%
7. Insufficient operating expenses	19%

Question 27n11: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?" (Not all factors shown. Total does not add up to 100%.)

Mobile devices and social media: New rules are in effect this year – but not yet critical mass.

Some technology firms are implementing strategies to keep pace with employee adoption of new technologies – including use of mobile devices and social-networking tools. These companies are creating rules about how employees can use personal technology within the enterprise. In fact, 41% of technology respondents this year report that their organization plans to increase current social media usage and access.

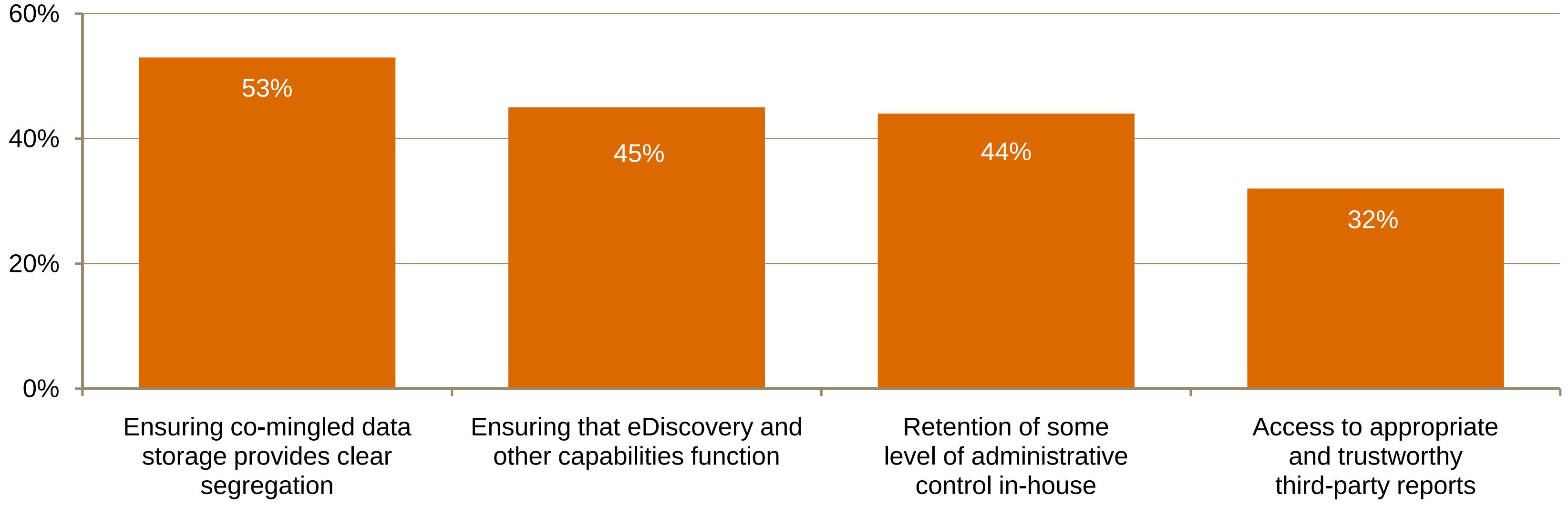
Yes, we have a:	2011
Mobile device security strategy	**36%**
Social media security strategy	**33%**
Security strategy for employee use of personal devices	**43%**

Regarding social media, we plan to:	2011
Increase use of social media tools/access	**41%**
Maintain current level of tool usage/access	**36%**
Decrease use of social media tools/access	**14%**

Question 17: “What process information security safeguards does your organization currently have in place?” Question 2 (Technology): “Regarding social media, does your organization plan to:” (Not all factors shown. Totals do not add up to 100%.)

Cloud computing is mainstream this year, but many respondents want better enforcement of provider security policies.

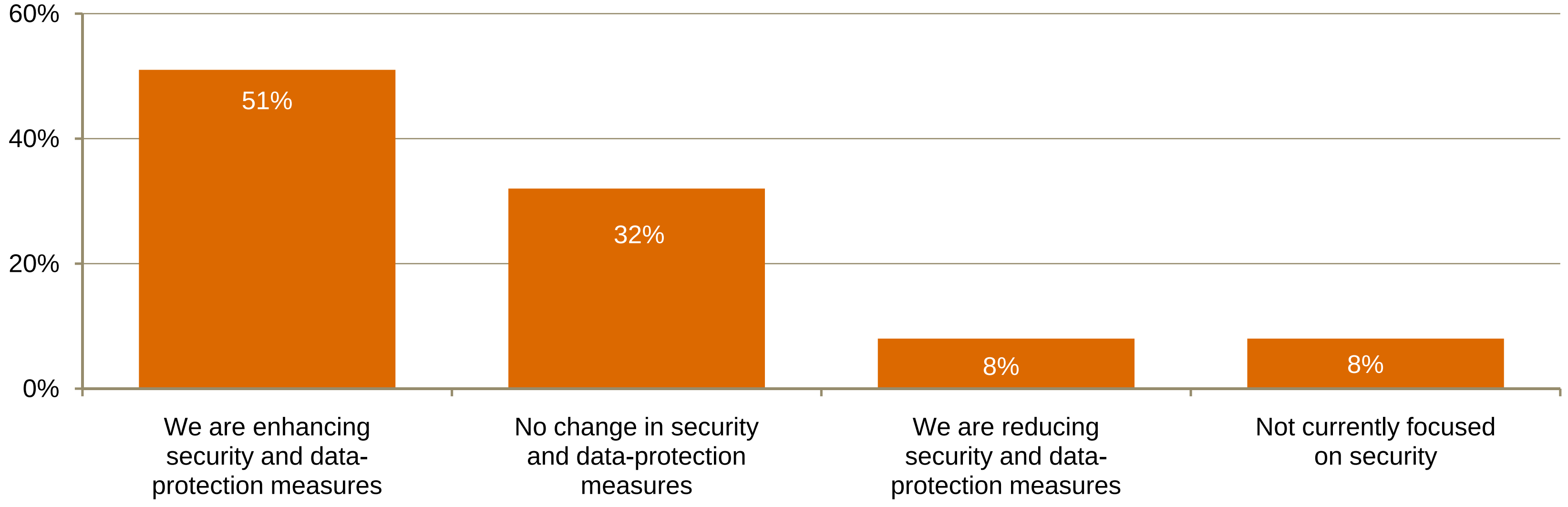
This year, more than half (54%) of technology respondents report that their organization uses cloud services. Responses revealed that, among the most pressing cloud-related security considerations this year, segregation of co-mingled data is viewed as the principal challenge.



Question 41: “Does your organization currently use cloud services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or Infrastructure-as-a-Service (IaaS)?” Question 3 (Technology): ”If your organization is a consumer of cloud computing services, what security considerations are most pressing?” (Not all factors shown. Total does not add up to 100%.)

Is cloud computing improving information security? Yes, but most organizations continue to invest in additional security measures.

Among technology organizations that use cloud computing, more than half (52%) say cloud technology has improved their security posture. Yet most technology respondents acknowledge that appropriate security requires ongoing advances in data protection.



Question 41c: “What impact has cloud computing had on your company’s information security?” Question 1 (Technology): ”Technology firms are investing in cloud computing technology within the enterprise. Which statement best describes your organization?” (Numbers reported may not reconcile exactly with raw data due to rounding)

For more information, please contact:

National Security Contacts

Gary Loveland
Principal, National Security Leader
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

Technology Contacts

Thomas Archer
Partner
408.817.3836
thomas.archer@us.pwc.com

Sohail Siddiqi
Principal
408.817.5844
sohail.siddiqi@us.pwc.com

Or visit www.pwc.com/giss2012

This document is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

www.pwc.com/security

Eye of the storm

As the global economy stalls and information security threats such as cyber crime and Advanced Persistent Threats cloud the horizon, many see sunshine and clear skies overhead

CIO Business Technology Leadership

CSO BUSINESS RISK LEADERSHIP

Telecommunications

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

September 2011

pwc

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

The economic thunderheads of 2008 may have passed. But across the global telecommunications industry, some clouds 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.

Nonetheless, according to PwC’s 2012 Global State of Information Security Survey®, the vast majority of telecom executives are confident in the effectiveness of their information security practices.

They have an effective strategy in place. They consider their organizations proactive in executing it. And they are diligently implementing technology safeguards to counter cyber crime and bolster security.

Yet all is not in order. Security event frequency is up. Incidents are exploiting assets and devices across the board. And the capital and operating expenditures crucial to early prevention and agile response are more likely to be deferred or canceled than at any time since 2008.

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, the reasons to do so quickly and strategically are mounting.

Agenda

Section 1. Methodology

Section 2. Confidence and progress

Section 3. Signs of vulnerability and exposure

Section 4. The greatest opportunities for improvement

Section 1

Methodology

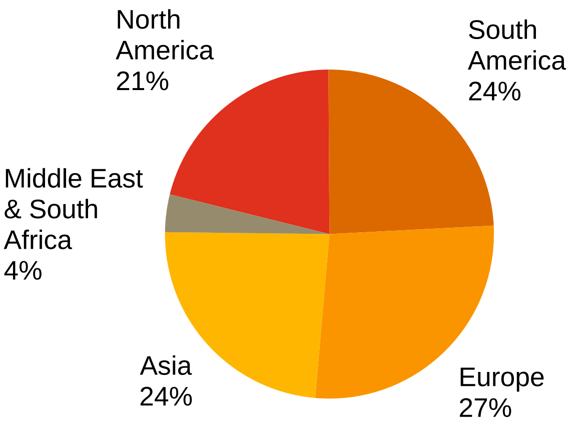
A worldwide study

The 2012 Global State of Information Security Survey®, a worldwide study by PwC, CIO Magazine and CSO Magazine, was conducted online from February 10, 2011 to April 18, 2011.

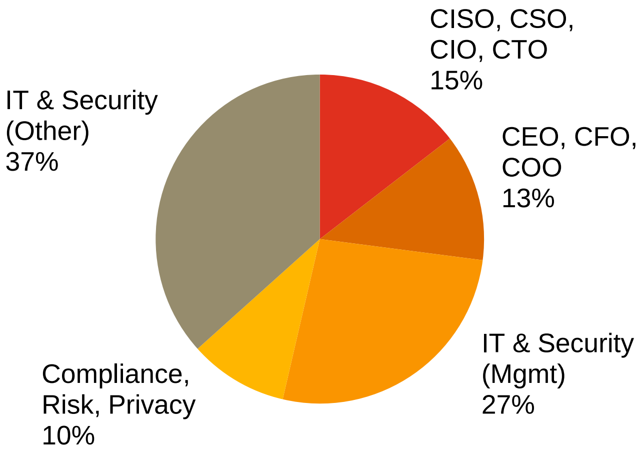
- PwC's 14th year conducting the online survey, 9th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 138 countries
- More than 9,600 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-one percent (31%) of respondents from companies with revenue of $500 million+
- Survey included 647 respondents from the telecommunications industry
- The margin of error is less than 1%

Demographics

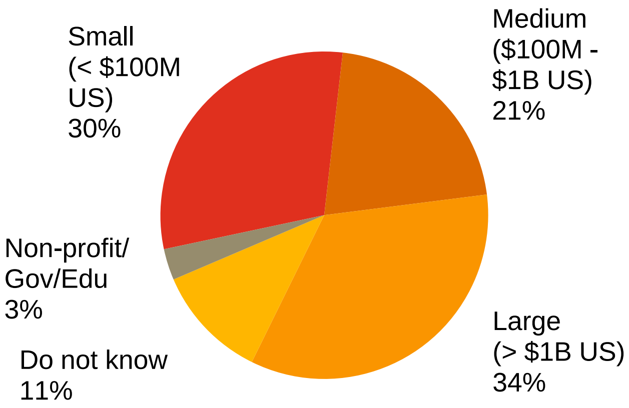
Telecom respondents by region of employment



Telecom respondents by title



Telecom respondents by company revenue size



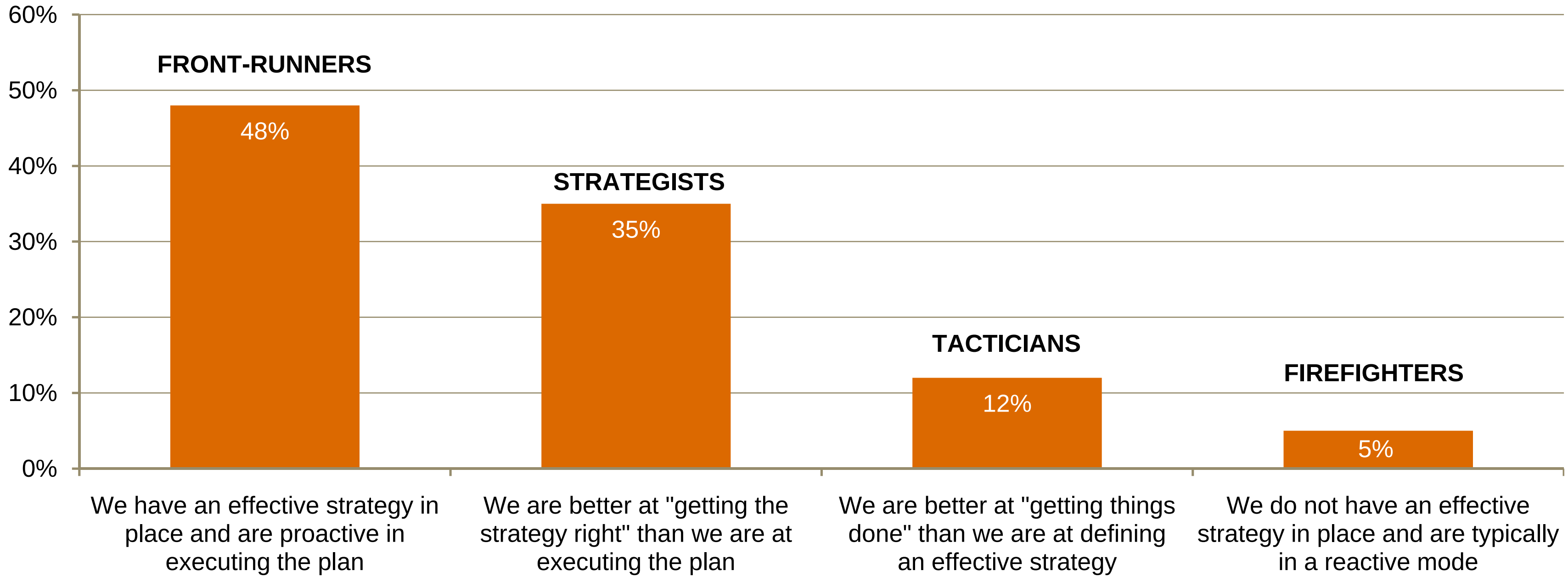
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

Confidence and progress

Many telecom respondents see their organization as a “front-runner.”

Almost half (48%) of telecom respondents say their organization has a strategy in place and is proactive in executing it.



Question 26n11: “Which statement best characterizes your organization’s approach to protecting information security?”

They are also highly confident in their organization’s security.

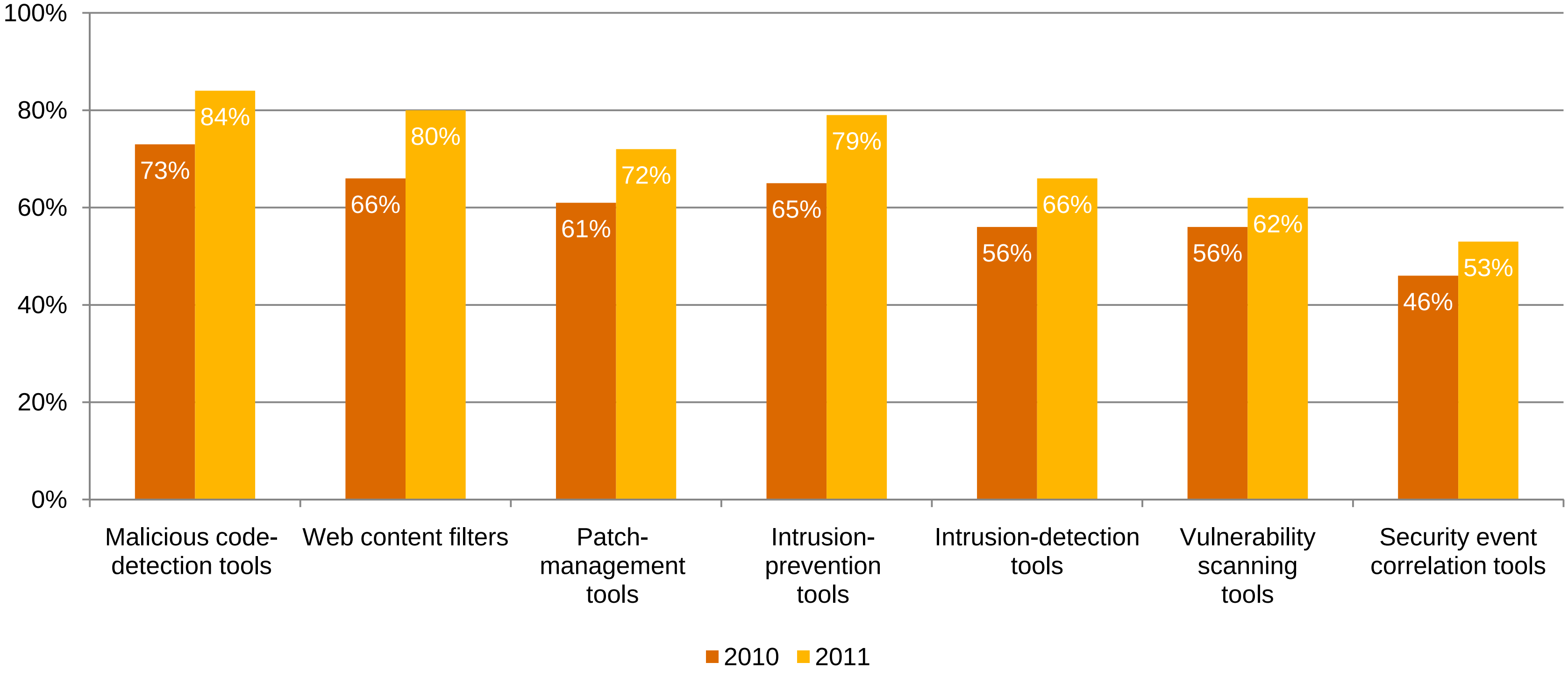
A clear majority – three out of four (75%) – of telecom respondents are also confident that their organization’s information security activities are effective.

	2011
Very confident	36%
Somewhat confident	39%
Total	75%

Question 35: “How confident are you that your organization’s information security activities are effective?”

Despite tight budgets, telecom companies are proactively adopting technology safeguards to bolster data security.

Over the past year, telecoms have made solid gains in strengthening technology safeguards to protect data from potential breaches and cyber crime.



Question 18: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown. Totals do not add up to 100%.)

Insights into the frequency, type, and source of security breaches have leaped dramatically over the past 12 months.

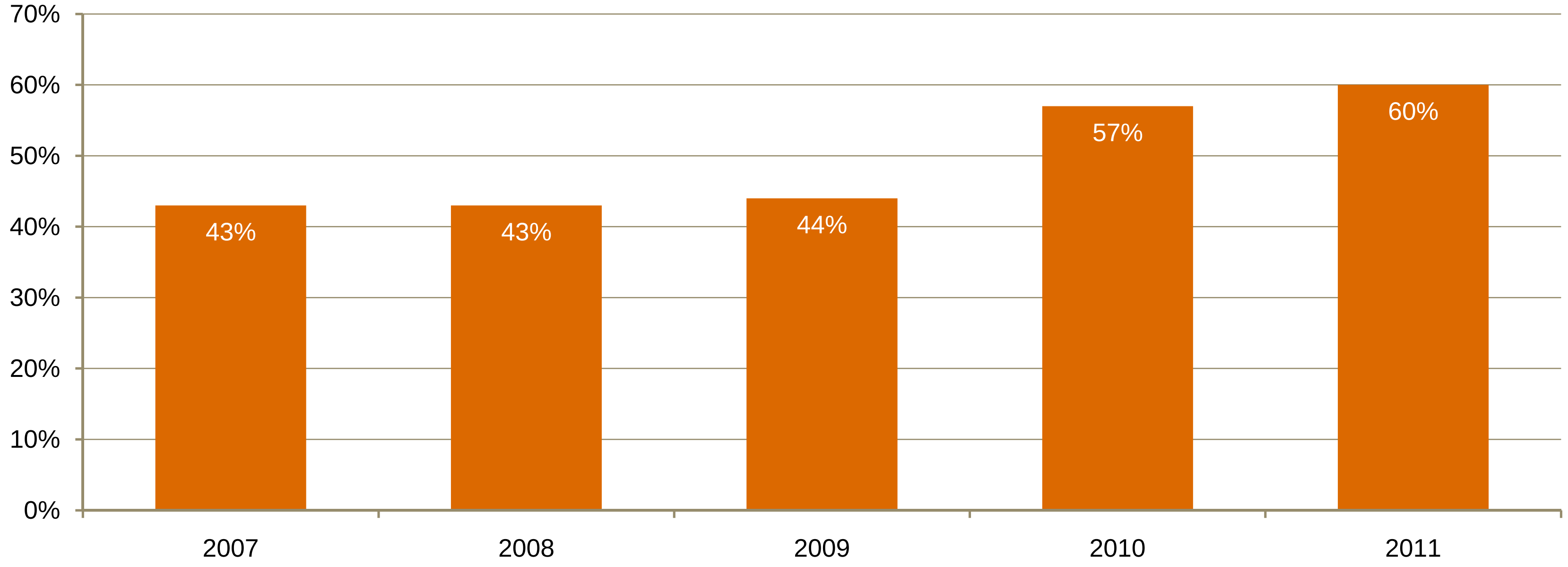
Just a few years ago, almost half of this survey’s telecom respondents couldn’t answer the most basic questions about the nature of security-related breaches. Now, approximately 80% or more of respondents can provide specific information about security event frequency, type, and source. They also report that financial losses due to security breaches are down 28% this year compared to last.

Respondents who answered “Do not know” or “Unknown”	2007	2008	2009	2010	2011
How many incidents occurred in past 12 months?	47%	42%	27%	24%	**8%**
What type of incident occurred?	48%	41%	32%	29%	**11%**
What was the source of the incident?	N/A	38%	35%	33%	**21%**

Question 19: “Number of security incidents in the past 12 months.” Question 20: “What types of security incidents (breach or downtime) occurred?” Question 22: “Estimated likely source of incident.” Question 23: “How was your organization impacted by the security incident: Business?” (Totals do not add up to 100%.)

At the same time, a majority of telecom respondents are "bullish" about security spending over the next 12 months.

Will security spending in the industry increase? Optimism carries the day. Sixty percent of telecom respondents believe that it will.



Question 9: "When compared with last year, security spending over the next 12 months will:" (Respondents who answered "Increase up to 10%," "Increase 11-30%," or "Increase more than 30%")

Section 3

Signs of vulnerability and exposure

Despite signs of confidence, some trends in this year's survey are troubling. Take the increase in security events, for example.

It is tempting to trumpet the fact that 18% of telecom respondents report no security events in the past year. But reports of incidents increased across the board in 2011, particularly among respondents indicating 50 or more negative events.

Number of security incidents	2007	2008	2009	2010	2011
No incidents	15%	12%	19%	22%	**18%**
1 to 9 incidents	25%	31%	39%	39%	**45%**
10 to 49 incidents	8%	8%	7%	9%	**13%**
50 or more incidents	5%	7%	7%	6%	**15%**

Question 19: "Number of security incidents in the past 12 months." (Totals do not add up to 100%.)

Exploitation is up across the board for almost all layers of security vulnerable to attack.

For the second consecutive year, reported levels of exploitation increased in the telecom industry. Exploitation of systems registered the greatest year-over-year jump, rising 36% over last year.

Cause of breach or downtime	2008	2009	2010	2011	One-year change*
Network exploited	23%	22%	31%	35%	**+ 13%**
System exploited	18%	22%	25%	34%	**+ 36%**
Data exploited	18%	26%	32%	31%	**- 3%**
Mobile device exploited	15%	19%	21%	28%	**+ 33%**
Human exploited	20%	16%	17%	23%	**+ 35%**
Application exploited	21%	19%	19%	21%	**+ 11%**

Question 20: “What types of security incidents (breach or downtime) occurred?” (Not all factors shown. Totals do not add up to 100%.) *This calculation measures the difference between response levels over a one-year period from 2010 to 2011.

The likely source of these breaches? Respondents report notable increases for hackers, partners, customers and contractors.

While it's not entirely surprising that hackers were the suspected source of most security incidents, telecom respondents are also more likely to suspect almost every other potential source.

Estimated likely source of incident	2008	2009	2010	2011	One-year change*
Hacker	36%	29%	36%	**44%**	**+ 22%**
Employee	38%	33%	30%	**29%**	**- 3%**
Former employee	22%	25%	27%	**28%**	**+ 4%**
Partner/supplier	12%	11%	14%	**19%**	**+ 36%**
Customer	11%	14%	14%	**17%**	**+ 21%**
Service provider or contractor	10%	14%	11%	**14%**	**+ 27%**

Question 22: "Estimated likely source of incident. (Check all that apply)" (Not all factors shown. Total does not add up to 100%.) *This calculation measures the difference between response levels over a one-year period from 2010 to 2011.

Most significant is the fact that security spending deferrals and cut-backs – for both capital and operating projects – have jumped.

For the third year in a row, spending deferrals and cut-backs for security-related initiatives are high. In fact, this year's reluctance to spend on security priorities has increased by 14% to 22% since 2009.

Has your company **deferred** security initiatives?	2009	2010	2011
Yes, for *capital* expenditures	49%	49%	**56%**
Yes, for *operating* expenditures	45%	48%	**55%**

Has your company **reduced the cost** for security initiatives?	2009	2010	2011
Yes, for *capital* expenditures	51%	51%	**58%**
Yes, for *operating* expenditures	51%	51%	**58%**

Question 12: "Has your company deferred security-related initiatives?" Question 13: "Has your company reduced the cost for any security-related initiatives?" (Not all factors shown. Total does not add up to 100%.)

And that high confidence rating? It has actually declined 12 points since 2009.

Confidence is always good. But a decline in confidence is telling. These numbers indicate that telecom business and IT personnel – across the world – are less sure that their organization is prepared to address the threats that confront its critical information.

	2009	2010	2011	CHANGE
Very confident	43%	37%	**36%**	- 7 pts
Somewhat confident	44%	36%	**39%**	- 5 pts
Total	87%	73%	**75%**	- 12 pts

Question 35: "How confident are you that your organization's information security activities are effective?"

Section 4

The greatest opportunities for improvement

What's holding security back?

Given the austere spending environment – not just this year, but since 2008 – and a steady regression in the readiness of security capabilities, it makes sense that telecom respondents considered insufficient capital one of the leading obstacles to the effectiveness of their organization's information security function.

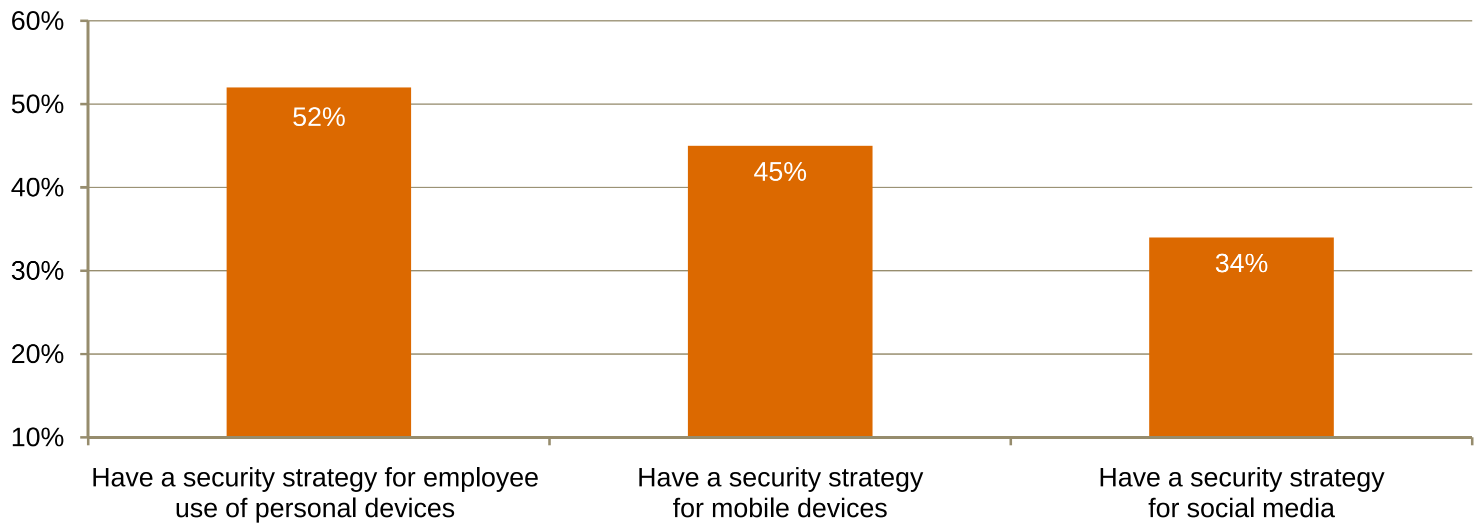
At the same time, nearly one in three point to the lack of an actionable "vision," and almost as many reference the absence of an effective information security strategy and leadership from top executives.

	2011
1. Lack of an actionable vision or understanding	**30%**
2. Insufficient capital expenditures	**28%**
3. Lack of an effective information security strategy	**27%**
4. Leadership – CEO, President, Board, or equivalent	**25%**
5. Leadership – CISO, CSO, or equivalent	**24%**
6. Poorly integrated or overly complex IT	**22%**
7. Leadership – CIO or equivalent	**21%**
8. Insufficient operating expenditures	**21%**

Question 27n11: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?" (Not all factors shown. Total does not add up to 100%.)

Personal technology, mobile devices and social media: New rules are in effect this year – but not yet critical mass.

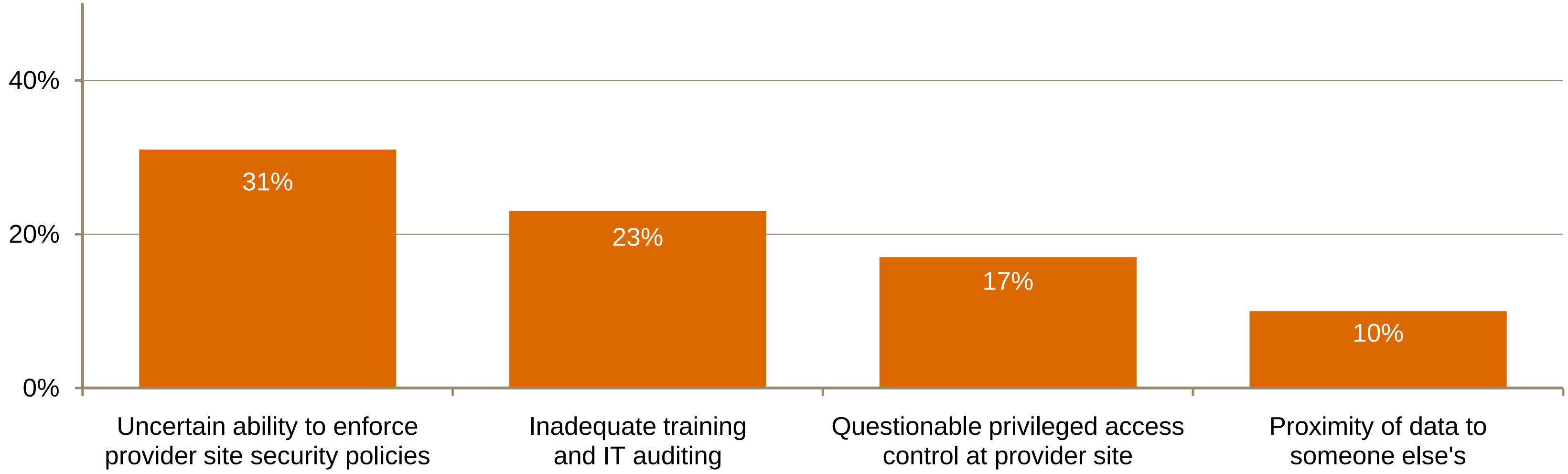
Telecom companies are implementing strategies to keep pace with employee adoption of new technologies. While they are particularly proactive in creating rules for employee use of personal technology within the enterprise, more than half have yet to establish security strategies for mobile devices and social media.



Question 17: "What process information security safeguards does your organization currently have in place?" (Not all factors shown. Total does not add up to 100%.)

Cloud computing: Is it improving information security? Yes, but many want better enforcement of provider security policies.

This year, more than half (55%) of telecom respondents report that their organization uses cloud services – and 51% of those that do say the cloud has improved their information security. Responses also revealed that while the leading security risk to cloud computing is an uncertain ability to enforce provider security policies, respondents are also concerned about training as well as multi-tenancy issues.



Question 41: “Does your organization currently use cloud services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or Infrastructure-as-a-Service (IaaS)?” Question 41c: “What impact has cloud computing had on your company’s information security?” Question 41b: “What is the greatest security risk to your cloud computing strategy?” (Not all factors shown. Total does not add up to 100%.)

For more information, please contact:

National Security Contacts

Gary Loveland
Principal, National Security Leader
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

Telecommunications Contacts

Deborah Bothun
Principal, Client Service
213.217.3302
deborah.k.bothun@us.pwc.com

Joseph Tagliaferro
Director
973.236.4226
joseph.tagliaferro@us.pwc.com

Or visit www.pwc.com/giss2012

This document is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

www.pwc.com/security

Eye of the storm

As the global economy stalls and information security threats such as cyber crime and Advanced Persistent Threats cloud the horizon, many see sunshine and clear skies overhead

CIO Business Technology Leadership

CSO BUSINESS RISK LEADERSHIP

Utilities

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

September 2011

pwc

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

The economic thunderheads of 2008 may have passed. But across the global utilities industry, some clouds 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.

Nonetheless, according to PwC's 2012 Global State of Information Security Survey®, the vast majority of utilities executives are confident in the effectiveness of their information security practices.

They have an effective strategy in place. They consider their organizations proactive in executing it. And they are diligently implementing technology safeguards to counter cyber crime and bolster security.

Yet all is not in order. Security event frequency is up. Financial impacts from events are on the rise. And the capital and operating expenditures crucial to early prevention and agile response are more likely to be deferred or canceled than at any time since 2008.

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, the reasons to do so quickly and strategically are mounting.

Agenda

Section 1. Methodology

Section 2. Confidence and progress

Section 3. Signs of vulnerability and exposure

Section 4. The greatest opportunities for improvement

Section 1

Methodology

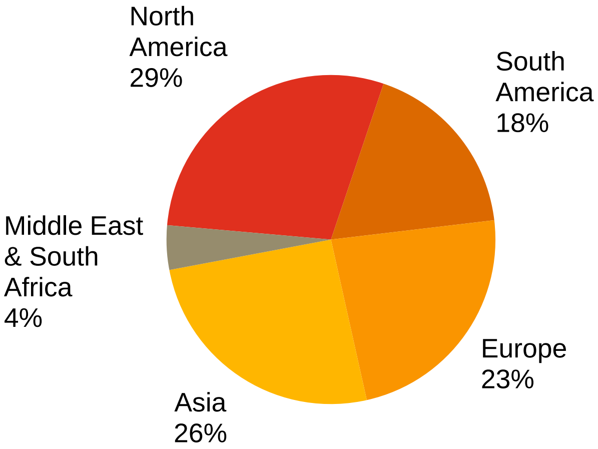
A worldwide study

The 2012 Global State of Information Security Survey®, a worldwide study by PwC, CIO Magazine and CSO Magazine, was conducted online from February 10, 2011 to April 18, 2011.

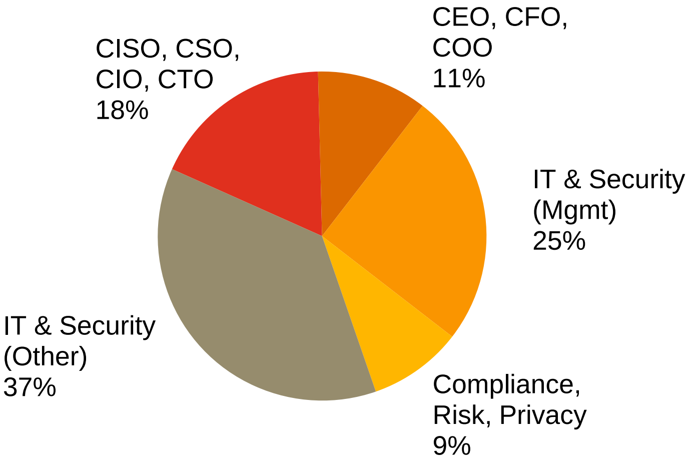
- PwC's 14th year conducting the online survey, 9th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 138 countries
- More than 9,600 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-one percent (31%) of respondents from companies with revenue of $500 million+
- Survey included 184 respondents from the utilities industry
- The margin of error is less than 1%

Demographics

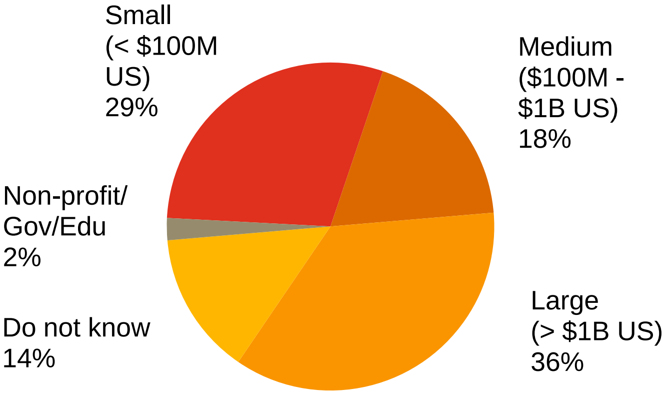
Utilities respondents by region of employment



Utilities respondents by title



Utilities respondents by company revenue size



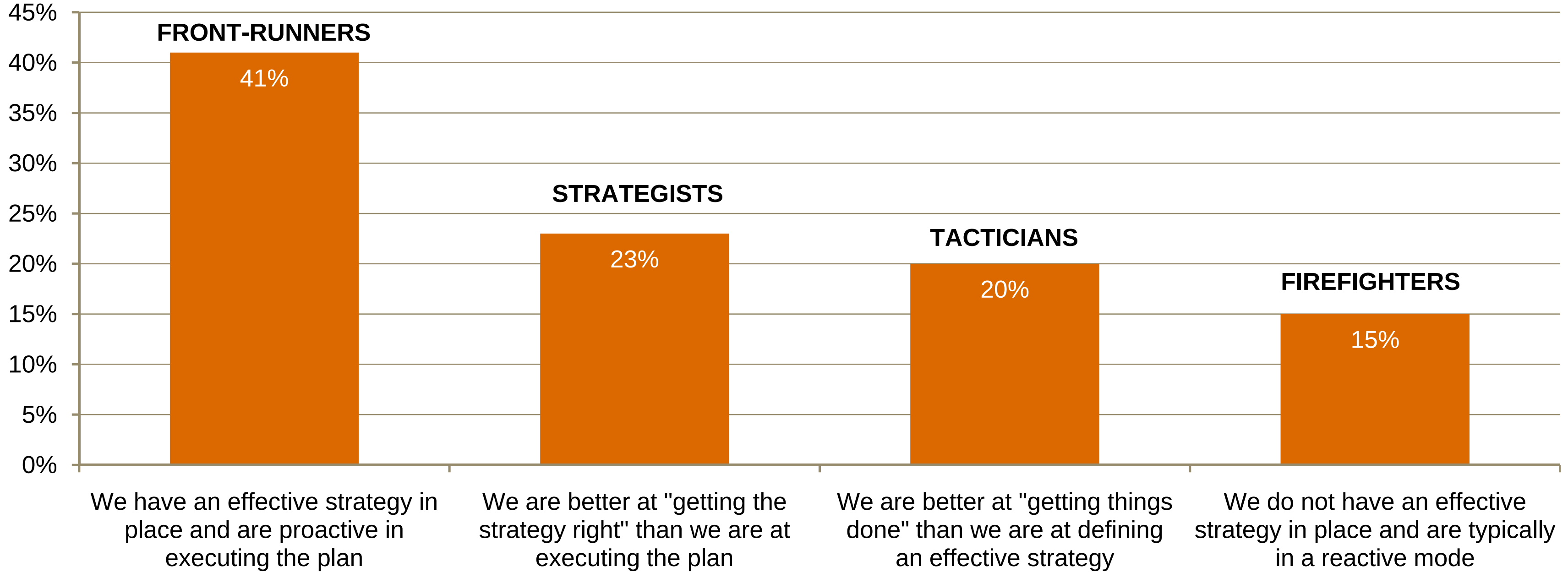
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

Confidence and progress

Many utilities respondents see their organization as a "front-runner."

More than 40% of utilities respondents say their organization has a strategy in place and is proactive in executing it.



Question 26n11: "Which statement best characterizes your organization's approach to protecting information security?" (Numbers reported may not reconcile exactly with raw data due to rounding)

They are also highly confident in their organization’s security.

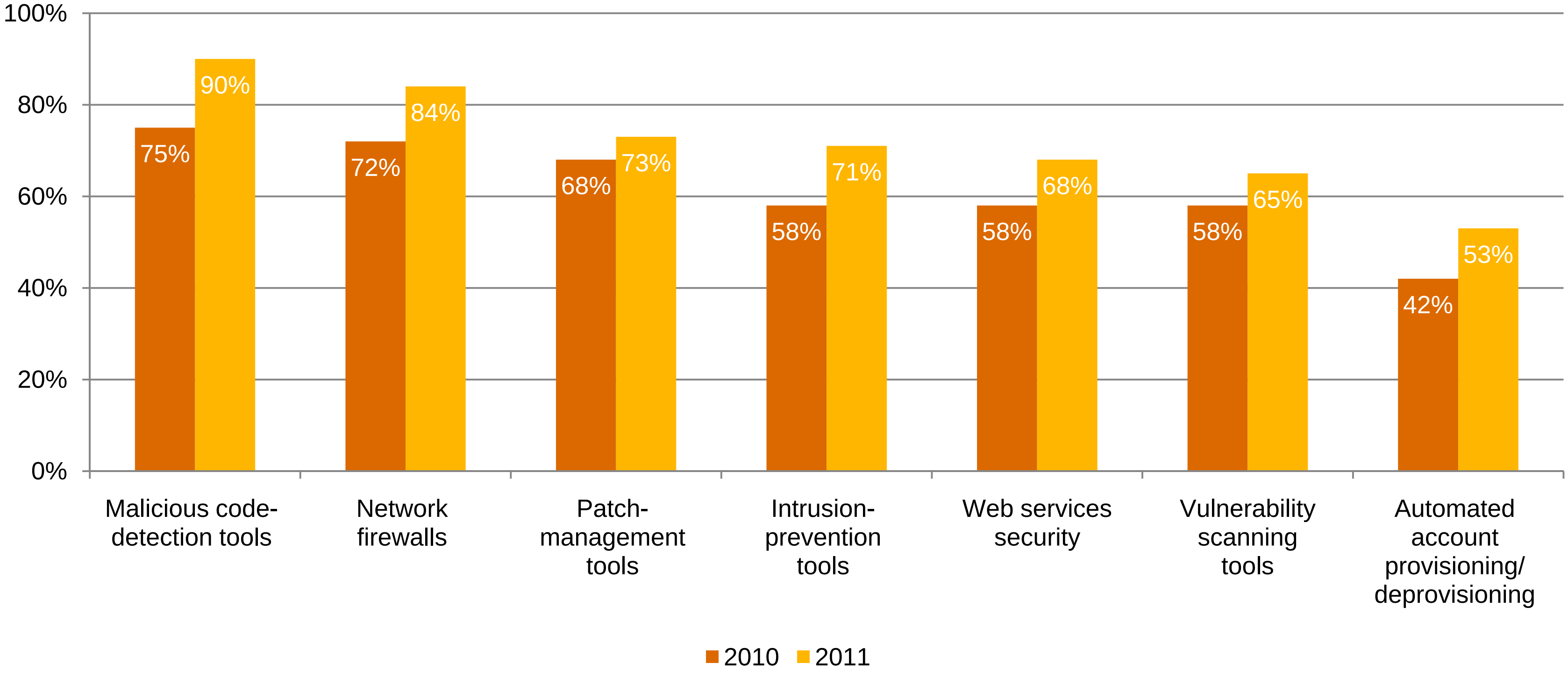
A clear majority – three out of four (75%) – of utilities respondents are also confident their organization’s information security activities are effective.

	2011
Very confident	**32%**
Somewhat confident	**43%**
Total	**75%**

Question 35: “How confident are you that your organization’s information security activities are effective?”

Despite tight budgets, utilities are proactively adopting technology safeguards to bolster data security.

Over the past year, utilities have made solid gains in strengthening technology safeguards to protect data from potential breaches and cyber crime.



Question 18: What technology information security safeguards does your organization currently have in place? (Not all factors shown. Totals do not add up to 100%.)

Insights into the frequency and type of security breaches have leaped dramatically over the past 12 months.

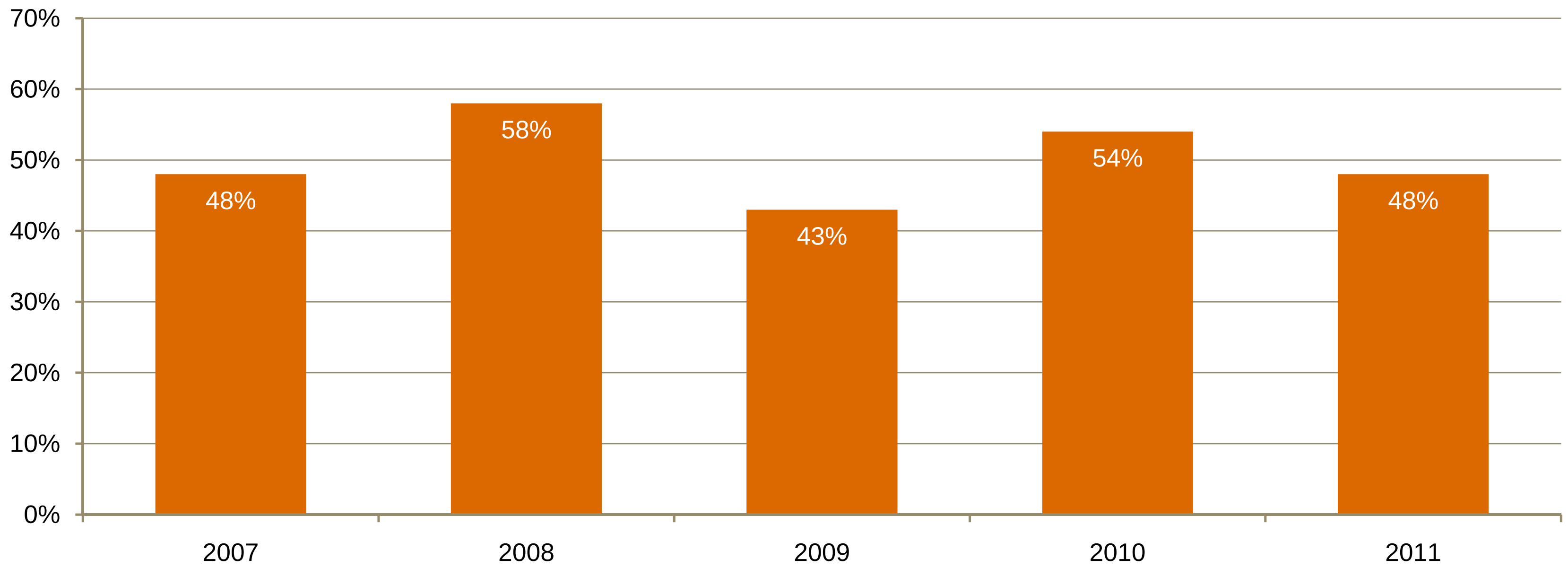
Just a few years ago, almost half of this survey's utilities respondents couldn't answer the most basic questions about the nature of security-related breaches. Now, 80% or more of respondents can answer specific questions about security event frequency and type, with somewhat less insight into the source of security incidents.

Respondents who answered "Do not know" or "Unknown"	2007	2008	2009	2010	2011
How many incidents occurred in past 12 months?	47%	35%	41%	22%	**14%**
What type of incident occurred?	46%	40%	43%	32%	**16%**
What was the source of the incident?	N/A	40%	43%	31%	**34%**

Question 19: "Number of security incidents in the past 12 months." Question 20: "What types of security incidents (breach or downtime) occurred?" Question 22: "Estimated likely source of incident." (Totals do not add up to 100%.)

A majority of utilities respondents are "bullish" about security spending over the next 12 months.

Will security spending in the industry increase? Utility company respondents are somewhat less optimistic this year, although almost half (48%) believe their organization will boost security spending.



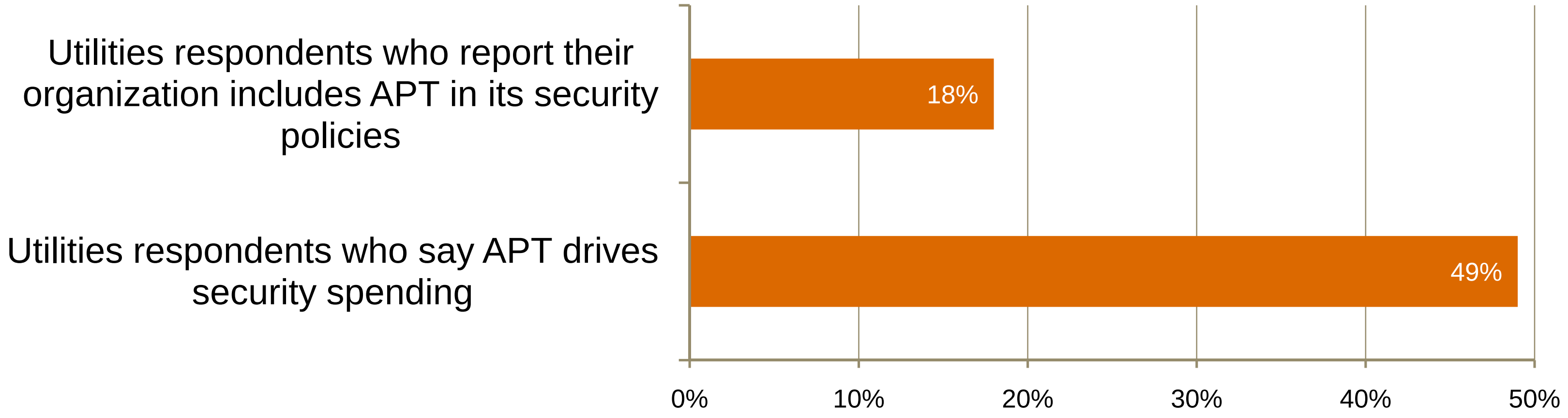
Question 9: "When compared with last year, security spending over the next 12 months will:" (Respondents who answered "Increase up to 10%," "Increase 11-30%," or "Increase more than 30%")

Section 3

Signs of vulnerability and exposure

Advanced Persistent Threats: They can be devastating – but just how concerned are utilities organizations about addressing them?

While 49% of utilities respondents say APT drives security spending, more than 80% report that their organization does not ensure that its security policies address APT. Utilities are countering the threat principally through virus protection (51%) and either intrusion detection/prevention solutions (27%).



Question 28: "Which of the following elements, if any, are included in your organization's security policy?" Question 1 (Utilities): "Does Advanced Persistent Threat drive your organization's security spending?" Question 2 (Utilities): "What technologies does your organization use to combat Advanced Persistent Threat?"

Other trends in this year's survey are also troubling. Take the increase in security events, for example.

It is tempting to trumpet the fact that almost one in three utilities respondents (31%) report no security events in the past year. Yet reports of incidents increased this year among respondents indicating 10 or more negative events.

Number of security incidents	2007	2008	2009	2010	2011
No incidents	19%	15%	15%	29%	**31%**
1 to 9 incidents	25%	35%	34%	42%	**37%**
10 to 49 incidents	7%	11%	7%	2%	**8%**
50 or more incidents	2%	3%	2%	4%	**11%**

Question 19: "Number of security incidents in the past 12 months." (Totals do not add up to 100%.)

This year’s data revealed a striking reversal in a best-practice trend – having the CISO report to the “top of the house.”

Reversing a multi-year trend, 42% of utility industry respondents now say their Chief Information Security Officer or equivalent executive reports not to the Board, the CEO or the CFO but to the CIO.

Whom the CISO reports to	2008	2009	2010	2011
Board of Directors	18%	26%	25%	**19%**
Chief Executive Officer	9%	26%	40%	**15%**
Chief Financial Officer	5%	12%	16%	**8%**
Chief Information Officer	50%	40%	24%	**42%**

Question 16a: “Where/to whom does your CISO or equivalent senior information security officer report?” (Not all responses shown. Totals do not add up to 100%.)

Utility industry respondents reported a notable increase in security incidents attributed to insiders.

Over the past 12 months, the number of security incidents attributed to insiders – including employees, former employees, partners, and suppliers – has increased by as much as 67%.

Source of incident	2008	2009	2010	2011	One-year change*
Employee	35%	34%	30%	**41%**	**+ 37%**
Former employee	18%	22%	18%	**21%**	**+ 17%**
Partner/supplier	14%	11%	12%	**20%**	**+ 67%**

Question 22: “Estimated likely source of incident . (Check all that apply)” (Not all factors shown. Total does not add up to 100%.) *This calculation measures the difference between response levels over a one-year period from 2010 to 2011.

Security spending deferrals and cut-backs – for both capital and operating projects – remain high.

For the third year in a row, spending deferrals and cut-backs for security-related initiatives remain high. This is so for both capital and operating expenditures.

Has your company **deferred** security initiatives?	2009	2010	2011
Yes, for *capital* expenditures	43%	48%	**48%**
Yes, for *operating* expenditures	35%	41%	**44%**

Has your company **reduced the cost** for security initiatives?	2009	2010	2011
Yes, for *capital* expenditures	38%	43%	**46%**
Yes, for *operating* expenditures	39%	44%	**44%**

Question 12: “Has your company deferred security-related initiatives?” Question 13: “Has your company reduced the cost for any security-related initiatives?” (Not all factors shown. Total does not add up to 100%.)

And that high confidence rating? It has actually declined 13 points since 2006.

Confidence is always good, but a decline in confidence is telling. These numbers indicate that utilities business and IT personnel – across the world – are less sure that their organization is prepared to address the threats that confront their organization.

	2006	2007	2008	2009	2010	2011	CHANGE
Total	**88%**	84%	86%	83%	81%	**75%**	**- 13 pts**

Question 35: "How confident are you that your organization's information security activities are effective?" (Respondents who answered "Very confident" or "Somewhat confident" combined)

Section 4

The greatest opportunities for improvement

What's holding security back?

Given the austere spending environment, it would make sense if utilities respondents considered insufficient capital one of the leading obstacles to the effectiveness of their organization's information security function.

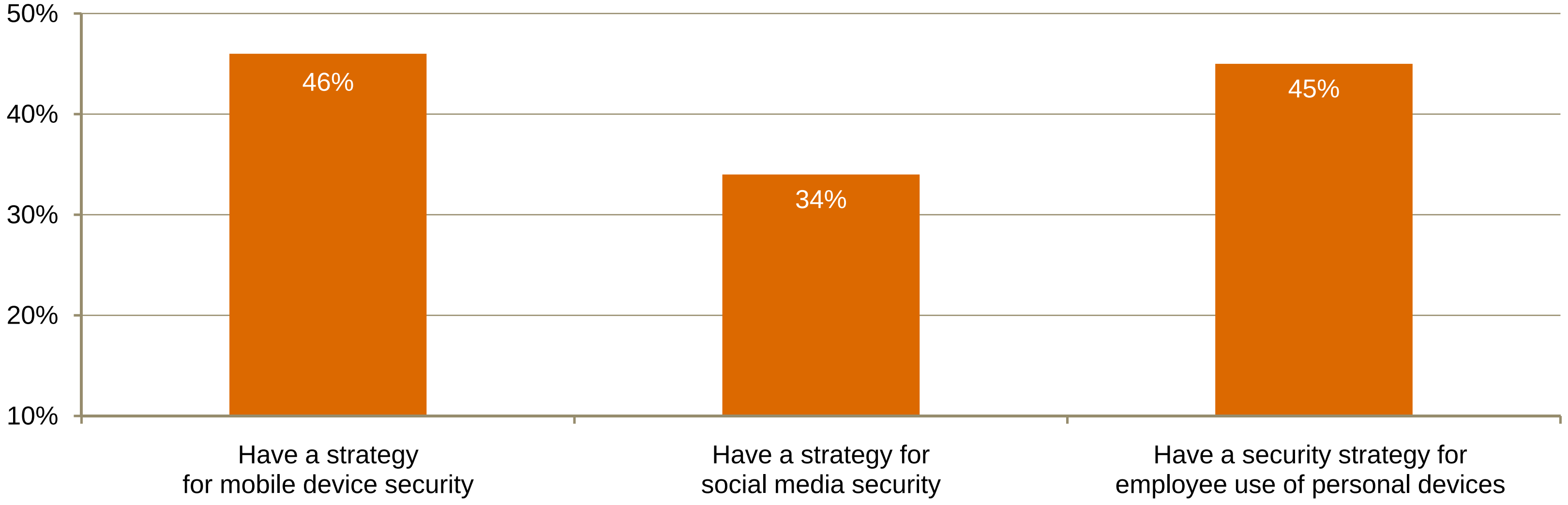
Surprisingly, they don't. More than one out of three point to the lack of an actionable vision, and almost as many reference the absence of effective information security strategy and in-house technical expertise.

	2011
1. Lack of an actionable vision or understanding	**36%**
2. Absence or shortage of in-house technical expertise	**26%**
3. Lack of an effective information security strategy	**26%**
4. Leadership – CEO, president, board, or equivalent	**23%**
5. Insufficient capital expenditures	**23%**
6. Poorly integrated or overly complex IT	**21%**
7. Insufficient operating expenditures	**20%**
8. Leadership – CIO or equivalent	**18%**

Question 27n11: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?" (Not all factors shown. Total does not add up to 100%.)

Mobile devices and social media: New rules are in effect this year for many in the industry – though not yet the majority.

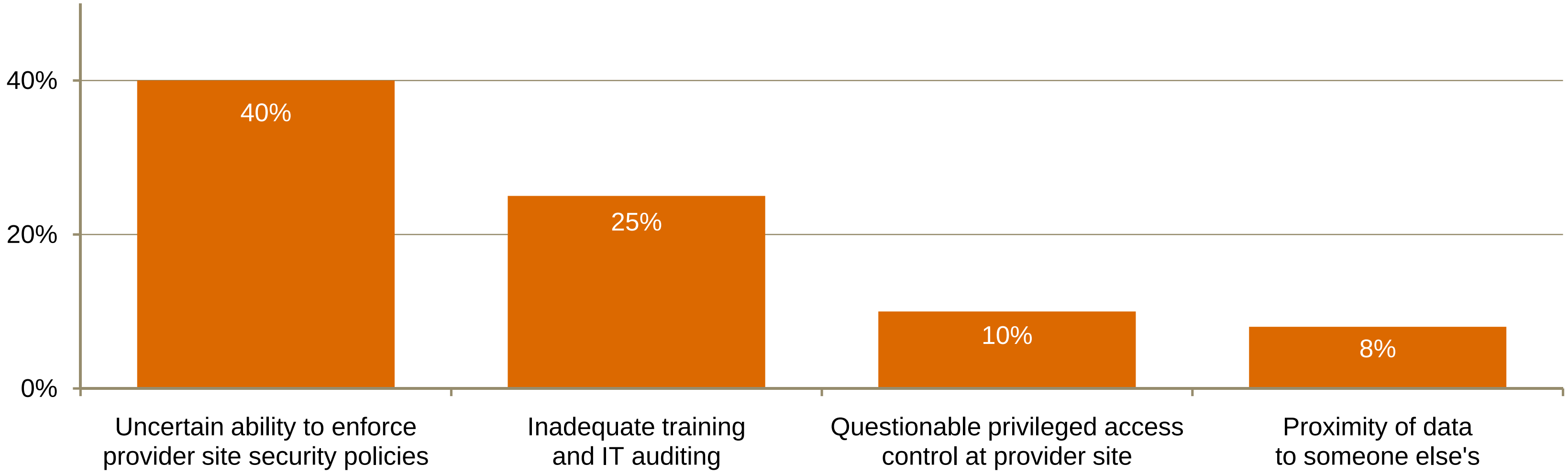
Utilities are implementing strategies to keep pace with employee adoption of new technologies – particularly use of mobile devices and social-networking tools – and are creating rules about how employees can use personal technology within the enterprise.



Question 17: “What process information security safeguards does your organization currently have in place?” (Not all factors shown. Total does not add up to 100%.)

Cloud computing: Is it improving information security? Yes, but many want better enforcement of provider security policies.

This year, 44% of utilities respondents report that their organization uses cloud services – and 40% of those that do say the cloud has improved their information security. Responses also revealed that while the leading security risk to cloud computing is an uncertain ability to enforce provider security policies, respondents are also concerned about training as well as multi-tenancy issues.



Question 41: “Does your organization currently use cloud services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or Infrastructure-as-a-Service (IaaS)?” Question 41c: “What impact has cloud computing had on your company’s information security?” Question 41b: “What is the greatest security risk to your cloud computing strategy?” (Not all factors shown. Total does not add up to 100%.)

For more information, please contact:

National Security Contacts

Gary Loveland
Principal, National Security Leader
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

Utilities Contacts

Brad Bauch
Principal
713.356.4536
brad.bauch@us.pwc.com

Jon Stanford
Director
971.544.4325
jonathan.k.stanford@us.pwc.com

Or visit www.pwc.com/giss2012

This document is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.