THE SECURITY STANDARD™

Securing the Enterprise from a Dangerous Cyberworld

September 19-20, 2011 • Marriott Brooklyn Bridge, New York City

Produced by
CSO

An Exclusive Survey Preview: The Global State of Information Security

Fred Rica

Principal – Advisory Services, PricewaterhouseCoopers

Bob Bragdon

Publisher, *CSO* magazine

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

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 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. Confidence and progress

Section 4. Vulnerability and exposure

Section 5. Windows of improvement

Section 6. Global trends

Section 7. Learn from the leaders

Section 1

Methodology

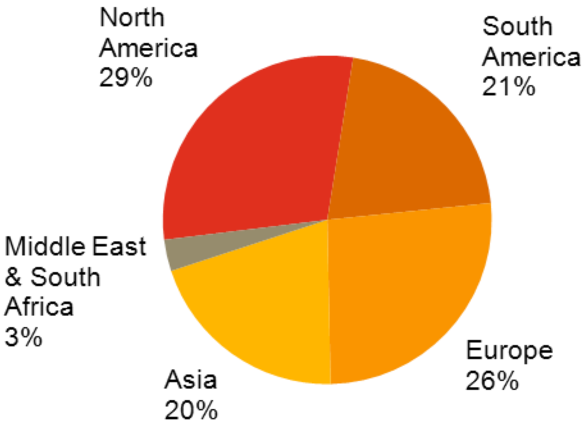
A worldwide study

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.

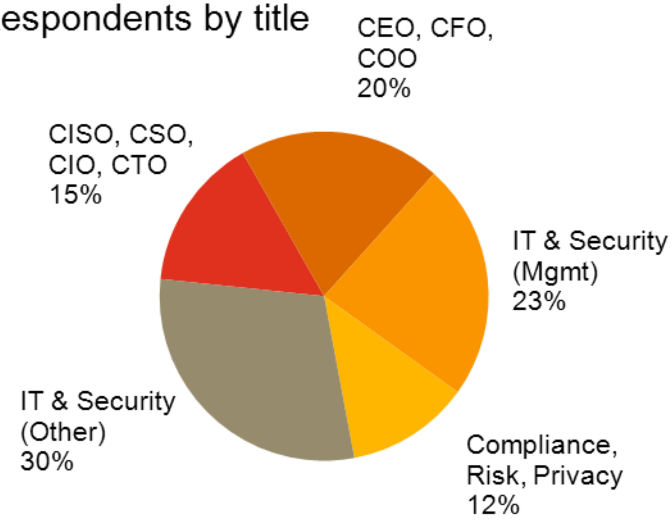
- PwC's 14th year conducting the online survey, 9th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 138 countries
- More than 9,600 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy 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

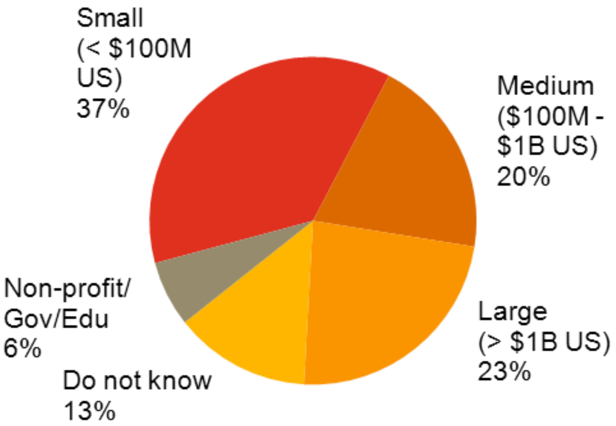
Respondents by region of employment



Respondents by title



Respondents by company revenue size



September 2011

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

Survey response levels by industry

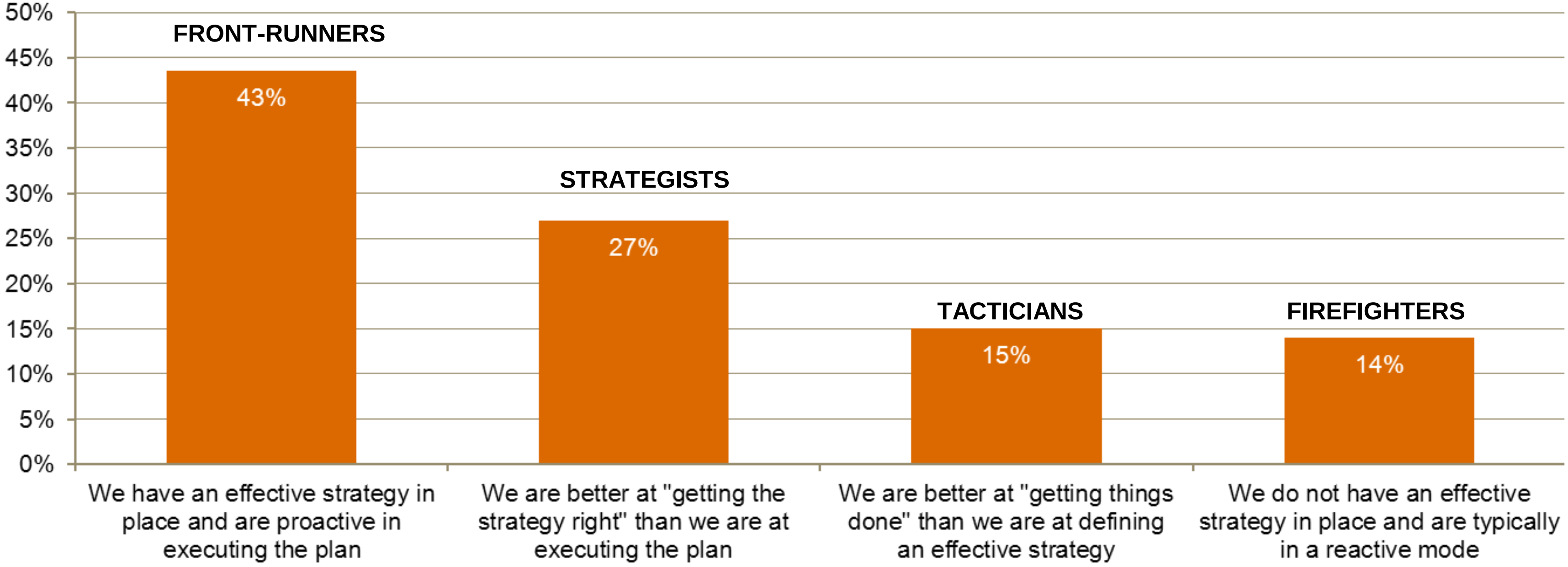
	Number of responses this year
Technology	1,606
Financial Services	1,293
Retail & Consumer	996
Industrial Products	859
Government	717
Telecommunications	647
Health Providers	483
Entertainment & Media	435
Automotive	265
Aerospace & Defense	253
Utilities	184
Energy (Oil & Gas)	143
Pharmaceutical	134

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)

September 2011

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

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.

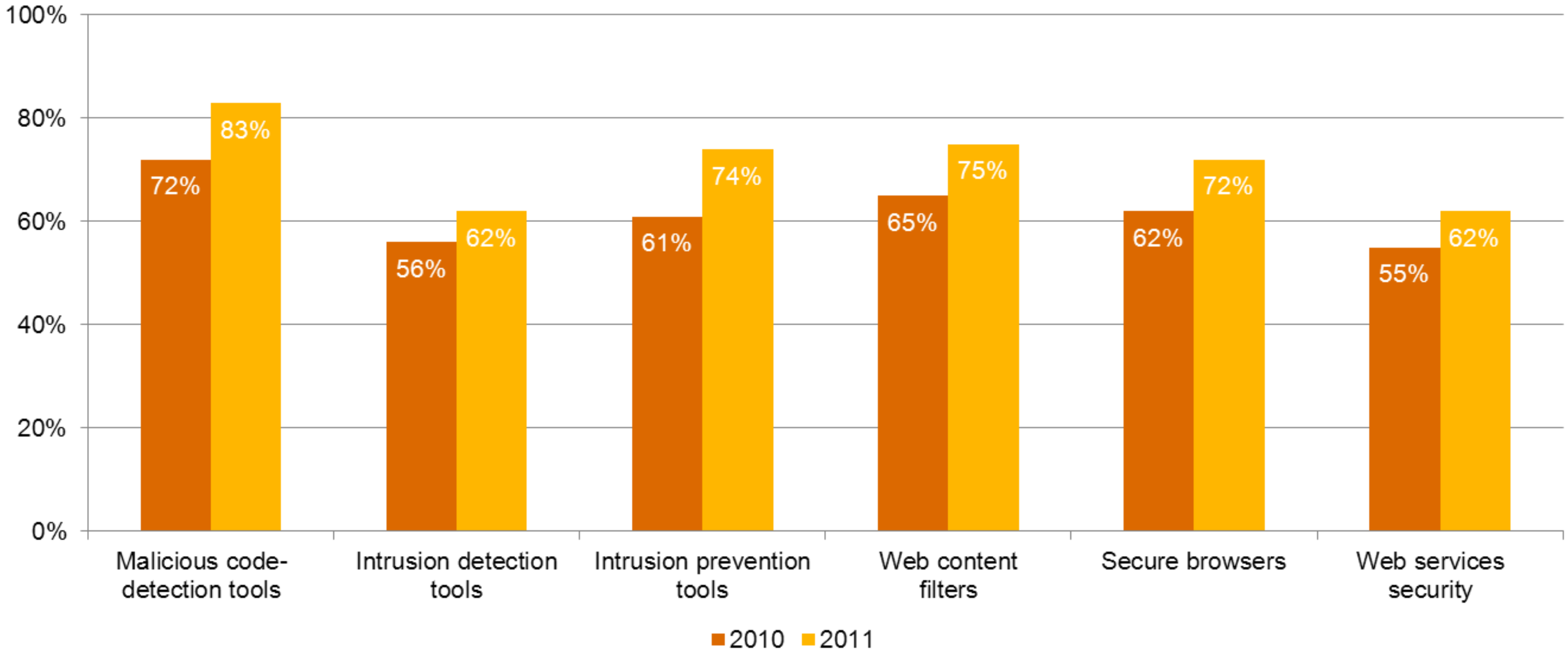
Just a few years ago, almost half of this survey's respondents couldn't answer the most basic questions about the nature of cyber crimes and security-related breaches. Now, approximately 80% or more of respondents can answer specific questions about factors such as security event frequency, type, and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

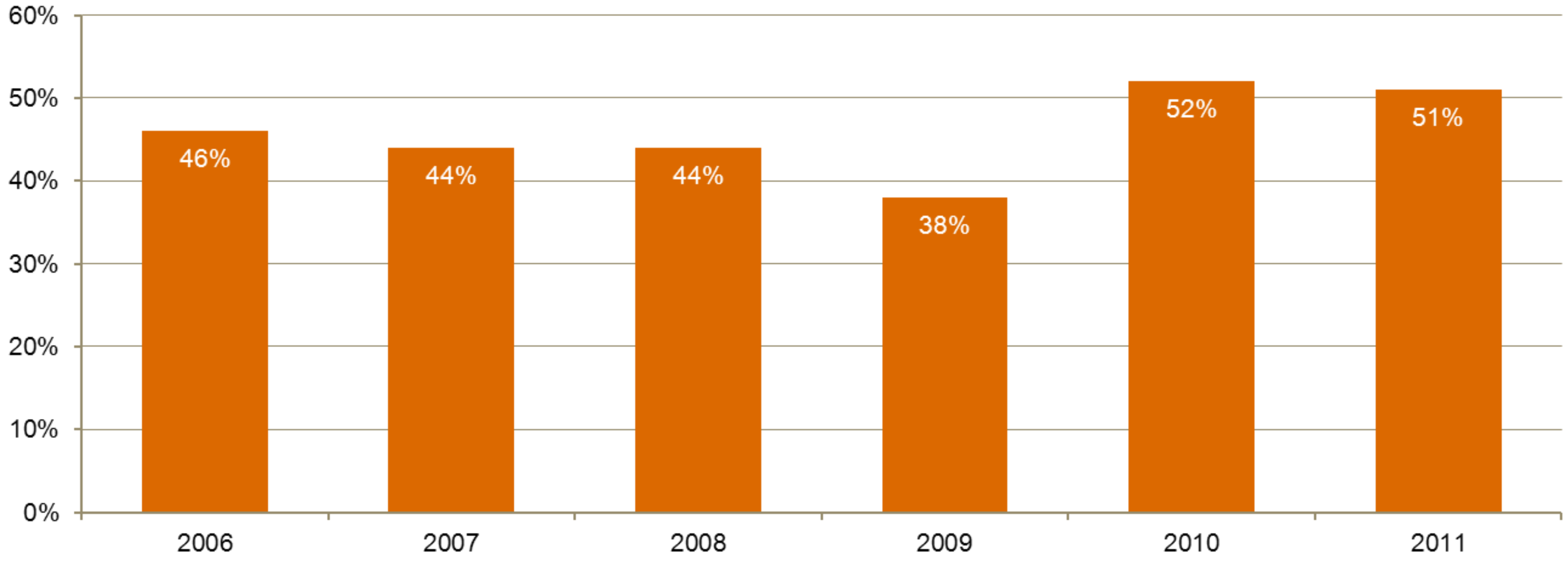
Better insight into security incidents appears to be influencing how organizations invest in security spending. Over the past year, respondents have boosted investments in capabilities related to detection, prevention, and Web-related technologies.



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%")

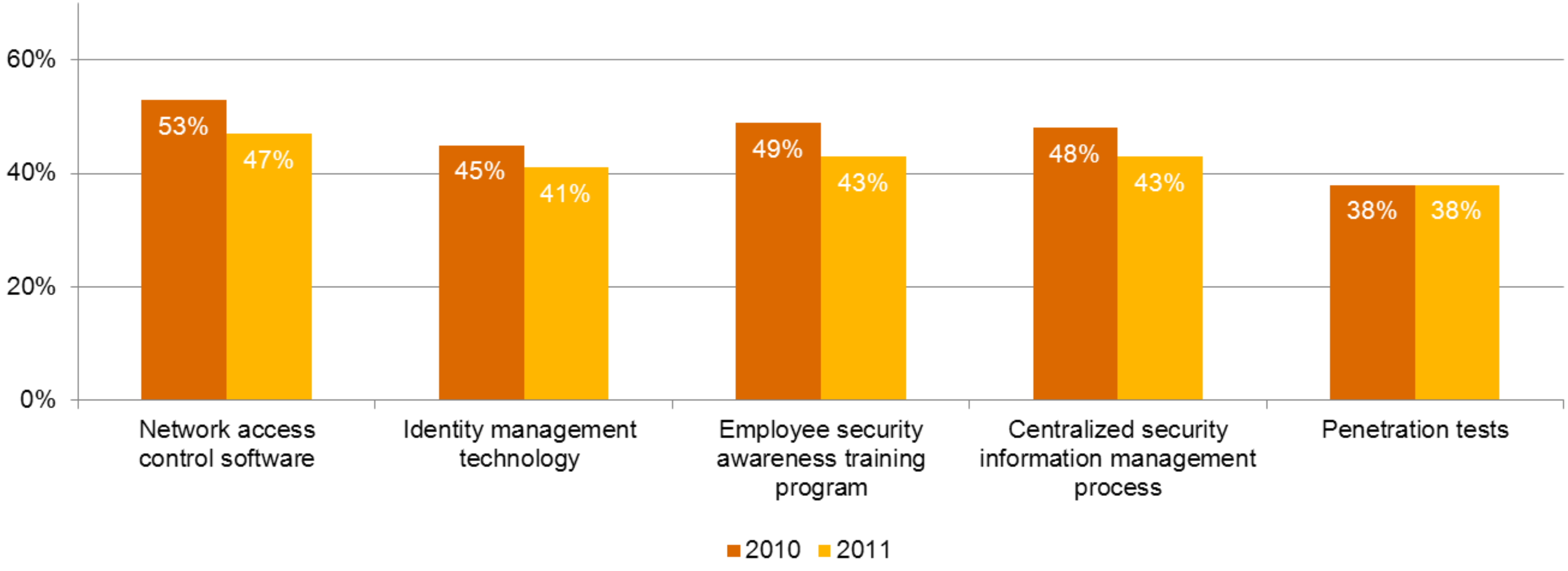
September 2011

Section 4

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.

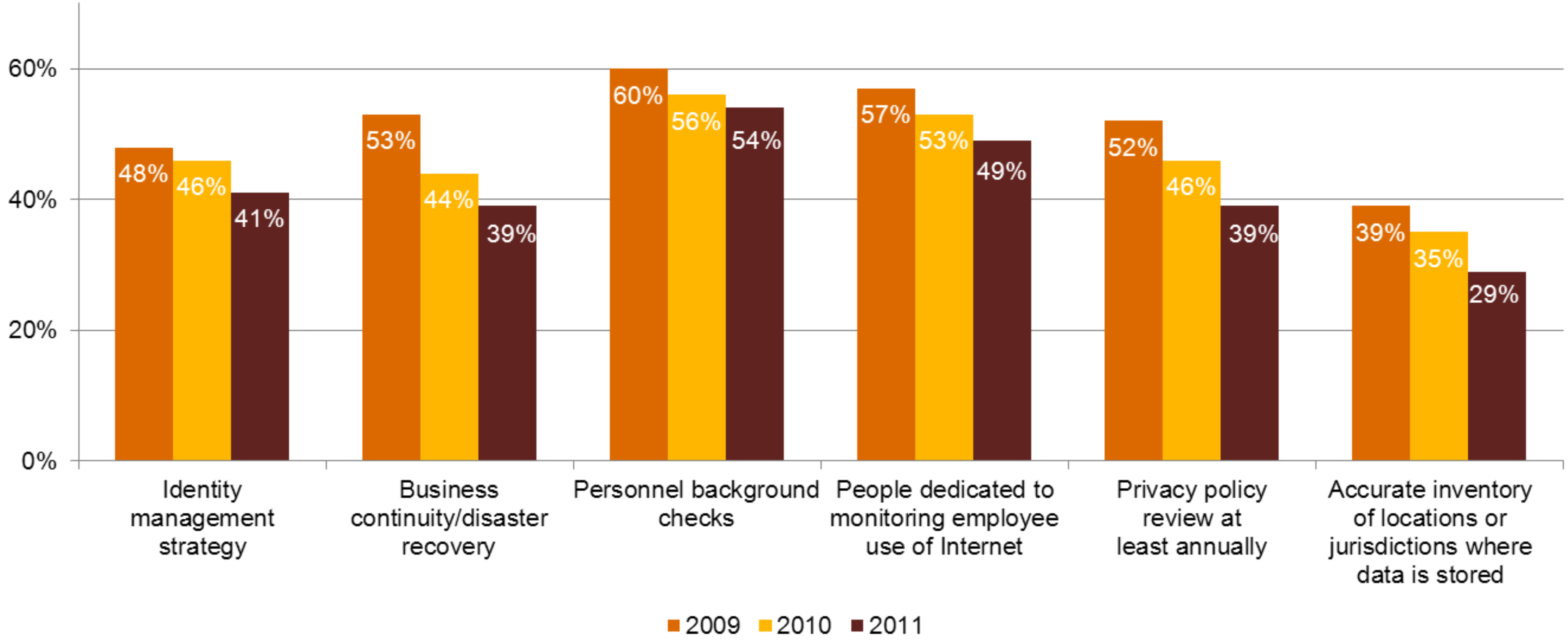
This year, significant percentages of respondents from various industries agree that APT drives their organization's security spending, yet only 16% say their company has a security policy that addresses APT. Worse, implementation of certain tools and processes crucial to combatting this new threat has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

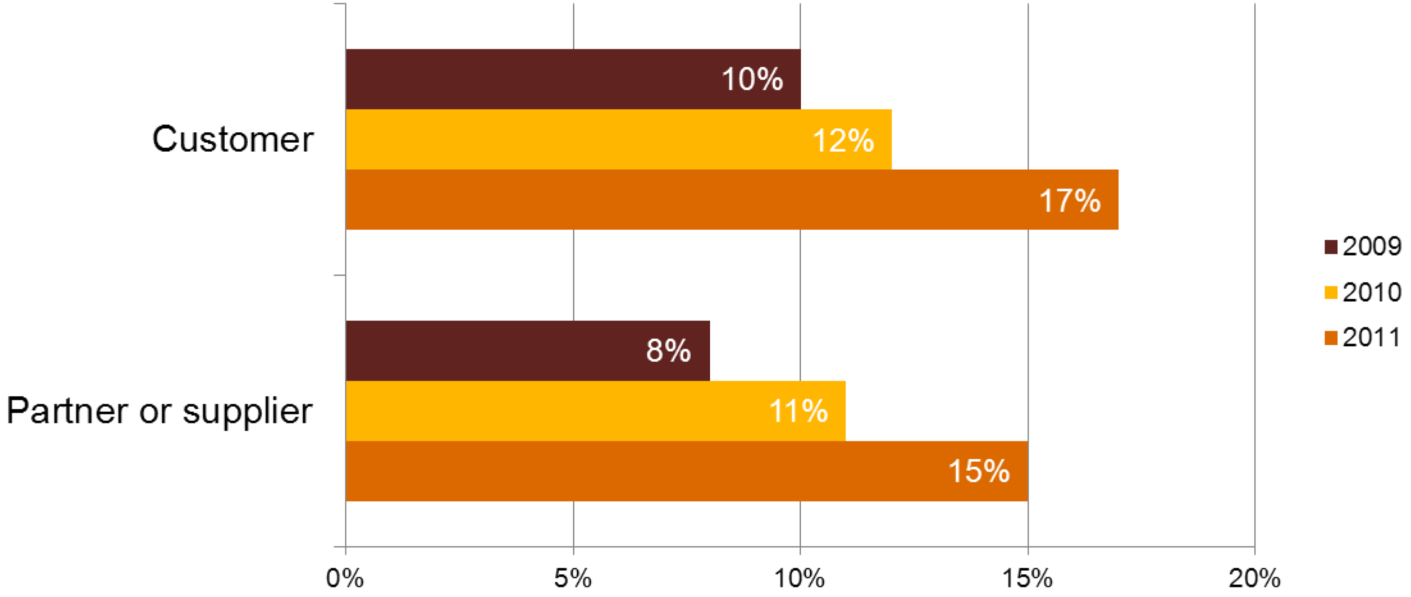
While organizations have invested in capabilities for prevention, detection, and Web-related security initiatives, this year's survey reveals a troubling degradation in core security-related capabilities.



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.

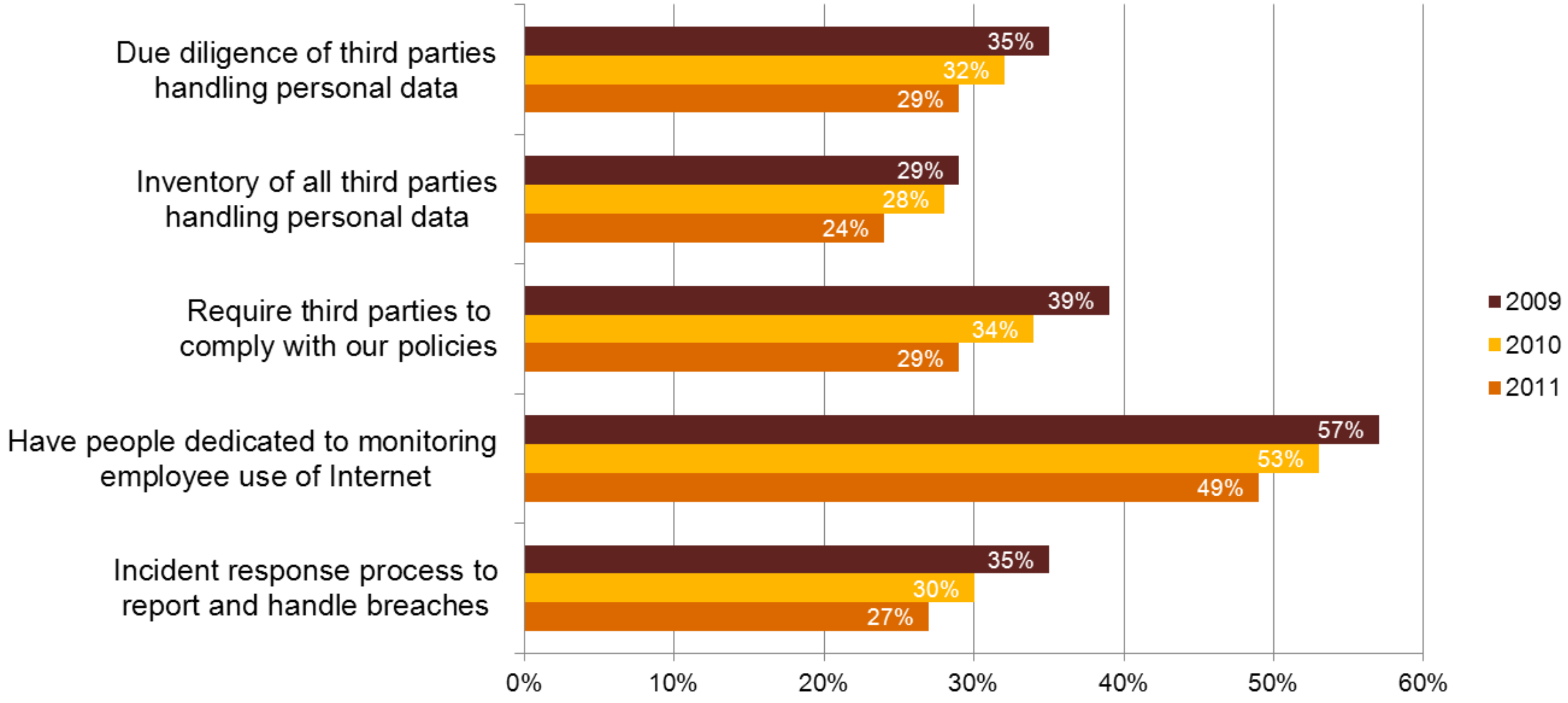
Customers and “insiders” like partners and suppliers traditionally have not been considered likely suspects in data breaches. That’s changing – fast. Over the past 24 months, the number of security incidents attributed to customers, partners, and suppliers has nearly doubled.



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 5

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.”

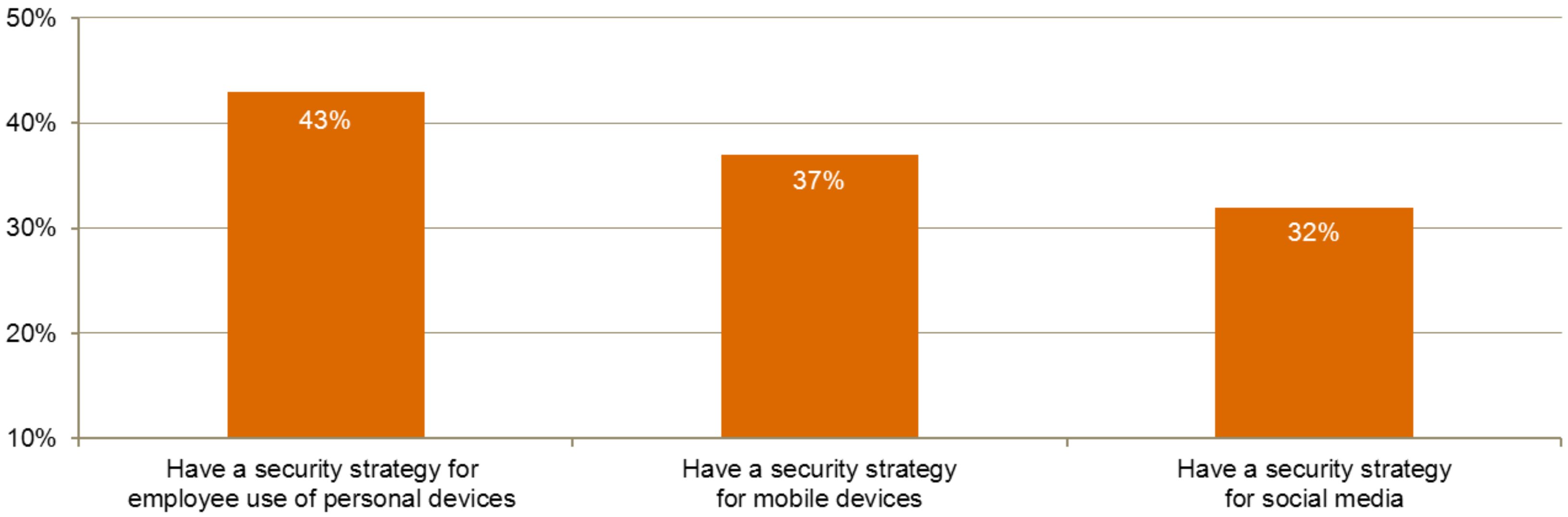
When asked to identify the highest hurdle to improving information security, responses vary by role. CEOs point first to a lack of capital and then themselves – and lastly to the CISO. CFOs cite the CEO. Interestingly, CIOs and CISOs report a lack of vision and an effective security strategy – and rank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

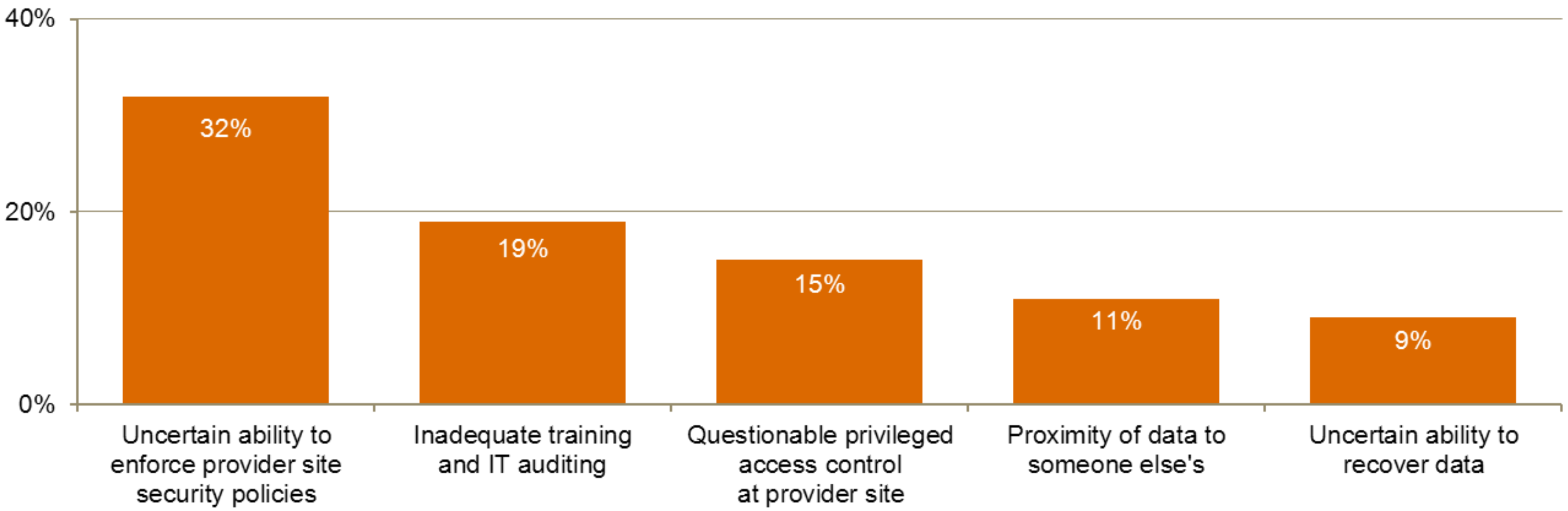
Organizations are beginning to implement strategies to keep pace with employee adoption of mobile devices and social networking, as well as use of personal technology within the enterprise. Yet much remains to be done: Less than half of respondents have implemented safeguards to protect the enterprise 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 6

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.)

Section 7

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%

SELECT INDUSTRIES

• Technology	15%
• Industrial Manufacturing	13%
• Financial Services	10%
• Engineering & Construction	9%
• Telecommunications	8%
• Consumer Products & Retail	8%
• Health	4%
• Government	4%
• Energy & Utilities	4%
• Aerospace & Defense	2%

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.

For more information, please contact:

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

Fred Rica
Principal – Advisory Services,
PricewaterhouseCoopers
frederick.j.rica@us.pwc.com

Or visit www.pwc.com/giss2012