Key findings from the 2011 Global State of Information Security Survey®

Respected – but still restrained

In the aftermath of the worst global economic jolt in 30 years, information security confronts a new economic order.

September 2010

CIO Business Technology Leadership

CSO BUSINESS RISK LEADERSHIP

PRICEWATERHOUSECOOPERS

It’s an uncertain world.

As global economic conditions continue to fluctuate, security executives are reluctant to loosen the purse strings – according to the results of the 2011 Global State of Information Security Survey®.

This is in spite of clear evidence that, as information security emerges from the smoke of a brutal year – and a “trial by fire” – it is sporting a new hard-won respect (and maybe a little love) from the business side of the house.

And doing so, in fact, with greater vigor than ever before.

But as the spending restraint continues, some “block and tackle” security capabilities that took a full decade to develop are degrading and, day by day, opening up new windows of risk.

This year, the tension is acute.
Between maturation in the security function and regression.
Between caution in this economy and optimism.
Between preserving cash and protecting the business.

Hanging in the balance is the information security function – thirsty for funds and poised to continue systematically driving into the operating heart of the business.

Agenda

1. Methodology
2. Spending: A subtle but enormously meaningful shift
3. Economic context: The leading impacts and strategies
4. Funding and budgets: A balance between caution and optimism
5. Capabilities and breaches: Trends too large to ignore
6. New areas of focus: Where the emerging opportunities lie
7. Regional trends: A changing of the guard
8. The road ahead: What this means for your business

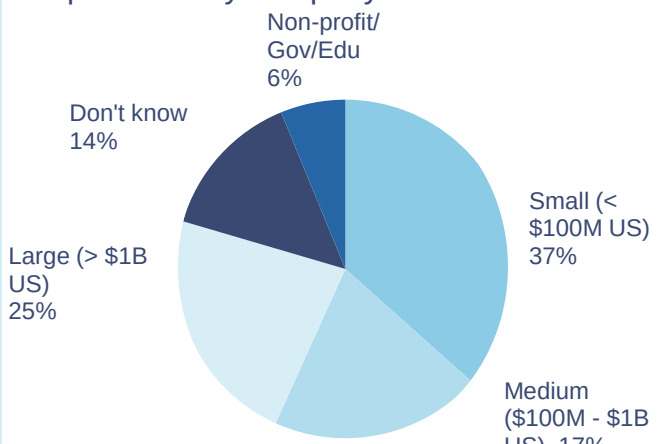
A worldwide study

The 2011 Global State of Information Security Survey®, a worldwide study by PricewaterhouseCoopers, *CIO Magazine* and *CSO Magazine*, was conducted online from February 19, 2010 to March 4, 2010.

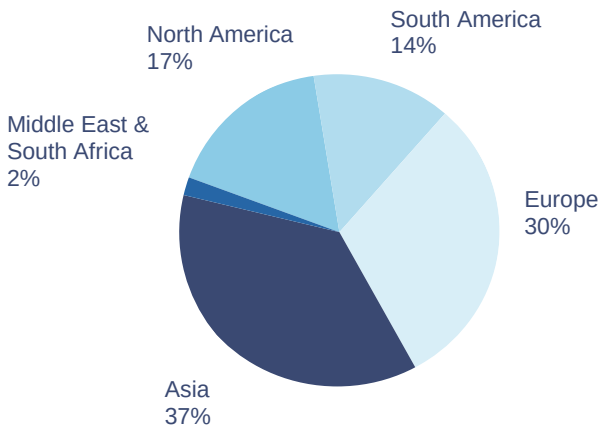
- PwC's 13th year conducting the online survey, 8th with *CIO* and *CSO* magazines
- Readers of *CIO* and *CSO* magazines and clients of PwC from 135 countries
- More than 12,840 responses from CEOs, CFOs, CIOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty percent (30%) from companies with revenue of $500 million+

A global, cross-industry response from business and IT executives, administrators and managers

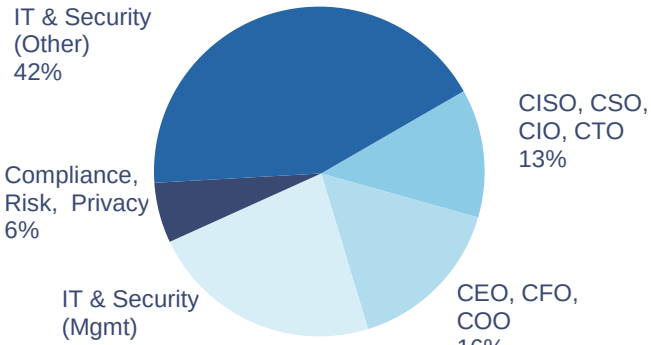
Respondents by company revenue



Respondents by region of employment



Respondents by title



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

List of industry response levels

	Number of responses this year
Technology	1,374
Industrial Products	1,348
Financial Services	1,222
Consulting / Professional Services	1,142
Retail & Consumer	1,062
Public Sector	939
Engineering / Construction	930
Education / Non-profit	839
Health Industries	819
Telecommunications	710
Transportation / Logistics	584
Energy / Utilities / Mining	435
Hospitality / Travel	384
Entertainment & Media	339
Agriculture	226
Aerospace / Defense	188

Agenda

1. Methodology
2. Spending: A subtle but enormously meaningful shift
3. Economic context: The leading impacts and strategies
4. Funding and budgets: A balance between caution and optimism
5. Capabilities and breaches: Trends too large to ignore
6. New areas of focus: Where the emerging opportunities lie
7. Global trends: A changing of the guard
8. The road ahead: What this means for your business

So, which factors are driving spending this year?

Top 3 spending drivers in 2010	2010
1. Economic conditions	49%
2. Business continuity/disaster recovery	40%
3. Company reputation	35%

Question 32: “What business issues or factors are driving your information security spending?” Not all factors shown. Total does not add up to 100%.)

Here's the surprise: Almost every one of these factors are trending at – or very near – *four-year lows*.

In fact, these four-year trend lines reveal fascinating clues about how information security spending is evolving – now and over time.

- First, let's clarify a key issue: Does this mean these factors are less important?
- Absolutely not. They've never been more vital.
- They're just not as vigorous spending drivers as they've been in the past.

Top 5 spending drivers in 2010	2007	2008	2009	2010	Three-year change*
1. Economic conditions	n/a	n/a	39%	49%	n/a
2. Business continuity/disaster recovery	68%	57%	41%	40%	- 41%
3. Company reputation	44%	39%	32%	35%	- 20%
4. Internal policy compliance	51%	46%	38%	34%	- 33%
5. Regulatory compliance	54%	44%	37%	33%	- 39%

Question 32: "What business issues or factors are driving your information security spending?" 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 2007 to 2010.

Three strategic trends in spending are now hard to miss.

Security is on the CFO's "protect" list

As the function matures – and contributes more to the business – it is encountering much **more stable funding curves**. As the survey revealed last year, funding is protected on the "down" cycle. And it is increased as market vigor returns.

But it is still vulnerable to the "flavor of the year"

Because security now sits in the heart of the business, its **spending drivers have been susceptible to the "flavor of the year."** Examples: the economy in 2008, regulatory compliance after SOX, business continuity after the events of 9/11.

The "water drop" effect

Big splash – then diffusion. After peaking as drivers, each of **these factors shifts from an "external game-changer" to an "internal given."** They remain important – but become integrated into the business through, for example: (1) newly automated systems,(2) updated job descriptions, (3) better internal controls.

What's the new "flavor of the year"? Client requirement.

Is this just a "new flavor"? Or is it a more enduring driver?

- Could "client requirement" become the globally acknowledged leading driver of security spending in the next two or three years?
- Is this one sign that – after 15 years – the information security function is taking on a far more customer-facing, business-supporting, strategic value-building role?

Top spending "justifications" in 2010	2007	2008	2009	2010	Three-year change*
1. Legal and regulatory requirement	58%	47%	43%	43%	- 26%
2. Client requirement	34%	31%	34%	41%	+ 21%
3. Professional judgment	45%	46%	40%	40%	- 11%
4. Potential liability/exposure	49%	40%	37%	38%	- 22%
5. Common industry practice	42%	37%	34%	38%	- 10%
6. Risk reduction score	36%	31%	31%	30%	- 17%
7. Potential revenue impact	30%	27%	26%	27%	- 10%

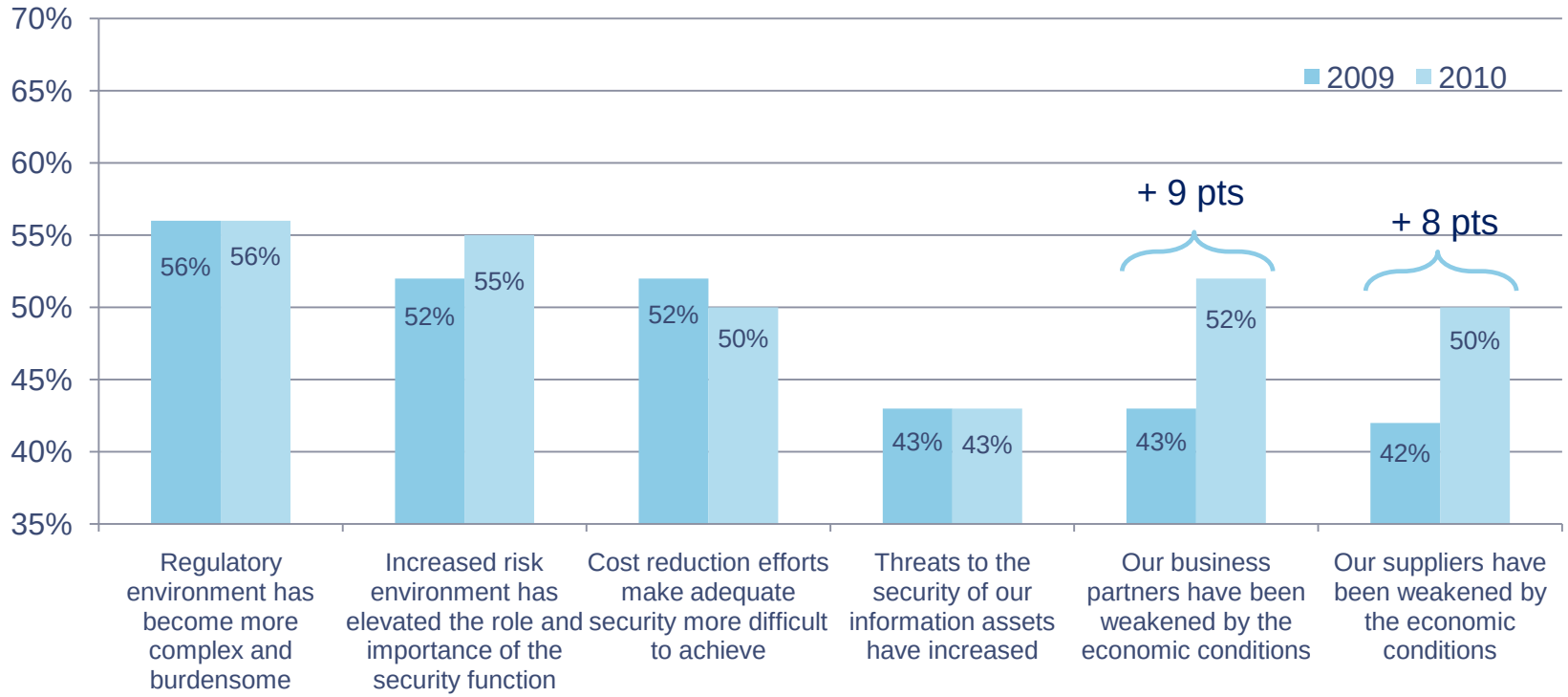
Question 33: "How is information security spending justified in your company?" (Not all factors shown. Total does not add up to 100%.)

* This calculation measures the difference between response levels over a three-year period from 2007 to 2010.

Agenda

1. Methodology
2. Spending: A subtle but enormously meaningful shift
3. Economic context: The leading impacts and strategies
4. Funding and budgets: A balance between caution and optimism
5. Capabilities and breaches: Trends too big to ignore
6. New areas of focus: Where the emerging opportunities lie
7. Regional trends: A changing of the guard
8. The road ahead: What this means for your business

While the impacts of the downturn linger, the risks associated with weaker partners and suppliers have increased.



Question 10: “What impacts have the current economic conditions had on your company’s security function?” (Respondents who answered “Agree” or “Strongly Agree.”)

What strategies are organizations undertaking to reduce the enduring economy-related risks?

On a strategic level, the top three priorities have barely budged compared with last year. The greatest change, however, is reflected in tactical strategies that – in some cases – may be opening companies to new areas of risk.

Question 11: “To continue meeting your security objectives in the context of these harsher economic realities, how important are the following strategies?” (Respondents who answered “Important,” “Very Important” or “Top Priority.”) (Not all factors shown. Total does not add up to 100%.)

Agenda

1. Methodology
2. Spending: A subtle but enormously meaningful shift
3. Economic context: The leading impacts and strategies
4. Funding and budgets: A balance between caution and optimism
5. Capabilities and breaches: Trends too large to ignore
6. New areas of focus: Where the emerging opportunities lie
7. Regional trends: A changing of the guard
8. The road ahead: What this means for your business

Financial caution remains high as executives keep a tight lid on the budgetary coffers. At least for now.

Companies are almost as likely as they were last year to hold back on security's funding. Doing so for one year is sometimes necessary. Doing so for extended periods, however, can increase risks.

Has your company deferred security initiatives?	2009	2010
Yes, for capital expenditures	43%	46%
Yes, for operating expenditures	40%	42%

Has your company reduced budgets for security initiatives?	2009	2010
Yes, for capital expenditures	47%	47%
Yes, for operating expenditures	46%	46%

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

But take a closer look at these numbers.

This caution is “easing” for projects more than six months out and for reductions of 10% or more. And it’s “building up at the bow” for projects under six months or budget reductions under 10%.

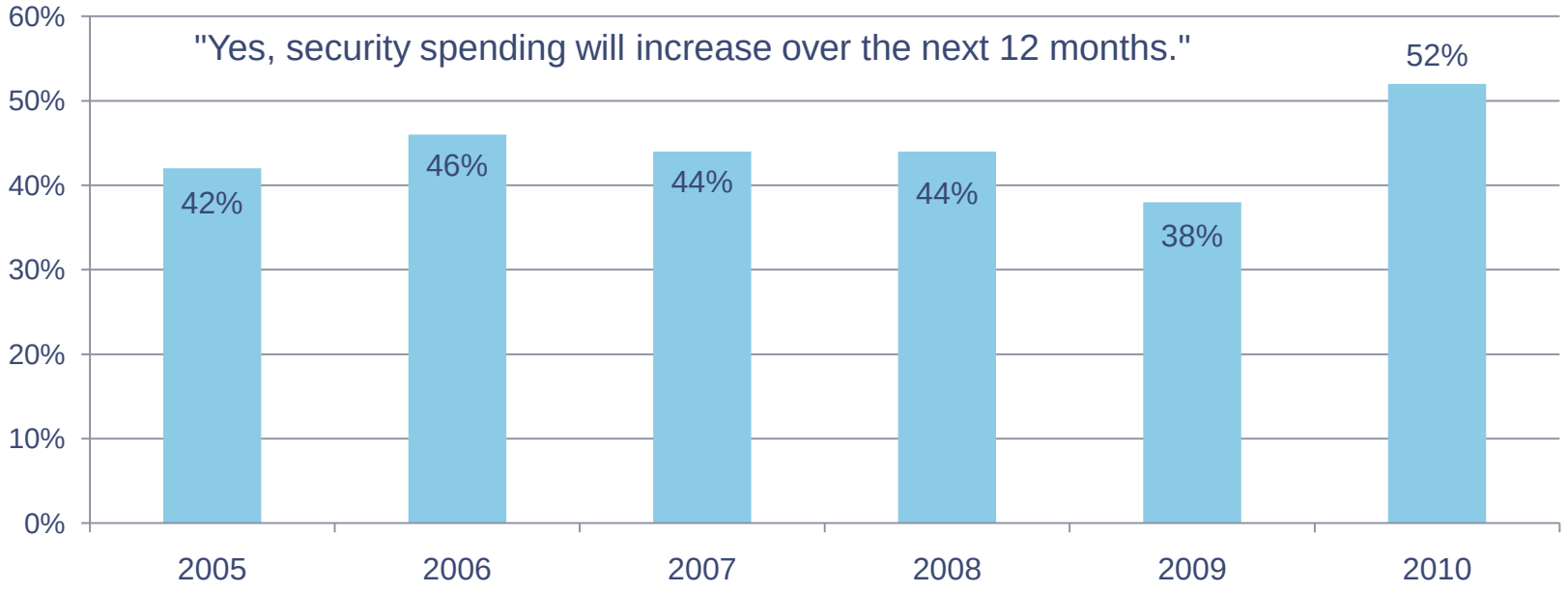
Has your company deferred security initiatives?	2009	2010
Yes, for capital expenditures	43%	46%
- By less than 6 months	**21%**	**27%**
- By more than 6 months	22%	19%
Yes, for operating expenditures	40%	42%
- By less than 6 months	**22%**	**26%**
- By more than 6 months	18%	16%

Has your company reduced budgets for security initiatives?	2009	2010
Yes, for capital expenditures	47%	47%
- By under 10%	**19%**	**22%**
- By more than 10%	28%	25%
Yes, for operating expenditures	46%	46%
- By under 10%	**19%**	**22%**
- By more than 10%	27%	24%

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

Respondents are *also* very optimistic about spending in the coming year – more so than at any time since before 2005.

Absent another global economic shock, we should expect to see a release of this pent-up demand “at the gate” and an increase in security-related capex and opex spending later this year.



Question 9: “Is security spending expected to increase over the next 12 months?” (Change in response points from prior year.)

Agenda

1. Methodology
2. Spending: A subtle but enormously meaningful shift
3. Economic context: The leading impacts and strategies
4. Funding and budgets: A balance between caution and optimism
5. Capabilities and breaches: Trends too large to ignore
6. New areas of focus: Where the emerging opportunities lie
7. Regional trends: A changing of the guard
8. The road ahead: What this means for your business

After posting solid process advances in the last several years, some firms are allowing these capabilities to degrade.

This year, on the whole, adoption levels for information security-related processes appear to have stalled – an unplanned consequence, perhaps, of the austerity in the funding environment. Where it occurs, the regression sometimes returns these capabilities to 2008 levels or below.

Examples of declines in process-related capabilities	2006	2007	2008	2009	2010
Have an overall information security strategy	37%	57%	59%	65%	65%
Have people dedicated to monitoring employee use of the Internet and information assets	40%	48%	50%	57%	53%
Integrate privacy and compliance plans	21%	28%	36%	44%	42%
Use vulnerability scanning tools	30%	50%	54%	53%	53%
Have wireless (cellular and Wi-Fi) security standards and procedures	29%	29%	40%	45%	45%
Conduct personnel background checks	51%	52%	51%	60%	56%
Use centralized security information management	34%	44%	51%	53%	48%
Conduct an employee security awareness program	39%	42%	54%	53%	49%

Questions 15 through 18: “What privacy or security safeguards does your organization currently have in place?”

As companies gain new visibility into security incidents, they are learning more about the real costs of breaches.

When the number of reported incidents jumped last year, we suspected the spike resulted from organizations gaining new-found knowledge into security incidents.

This year, it looks like the new visibility is paying off: The number of respondents reporting no incident at all leaped 42% – from 19% in 2009 to 27% in 2010. So, at minimum, it appears that organizations are more effectively reducing the frequency of incidents.

Number of security incidents	2007	2008	2009	2010
No incidents	22%	25%	19%	27%
1 to 9 incidents	28%	30%	35%	37%
10 to 49 incidents	7%	7%	9%	7%
50 or more incidents	4%	4%	5%	5%
Don't know	40%	35%	32%	23%

Question 19: "How many security incidents have occurred in the past 12 months?"

New insights into incidents are revealing higher levels of exploitation across the board – but especially to data.

As companies gain a much clearer perspective on the actual extent of security incidents, they're discovering that the greatest compromises are to data. In fact, the number of respondents reporting data exploitation has increased by nearly 70% since 2008. Mobile devices represent a significant new category of exploitation.

Types of security incidents	2007	2008	2009	2010
Data exploited	18%	16%	23%	27%
Network exploited	23%	20%	22%	25%
System exploited	18%	15%	18%	23%
Application exploited	14%	17%	16%	16%
Mobile device exploited	n/a	n/a	n/a	20%
Human exploited (social engineering)	16%	15%	13%	15%
Unknown	45%	44%	39%	33%

Question 20: "What types of security incidents occurred?" (Does not add up to 100%.)

As firms learn more about each event, attribution levels are climbing for all sources – including hackers and “insiders.”

Hackers were among the fastest-growing category of suspects. Also more likely to be suspected are “insiders.” This isn’t a surprise. Last year, we expected to see more incidents traced to employees and former employees, in line with the higher risks to security associated with salary freezes, job instability, layoffs and terminations and other HR challenges that rise during economic stress.

Likely source of incidents	2008	2009	2010
Current employee	34%	33%	32%
Former employee	16%	19%	23%
Hacker	28%	26%	31%
Customer	8%	10%	12%
Partner/supplier	7%	8%	11%
Unknown	42%	39%	34%

Question 22: “What is the estimated likely source of the incident?” (Does not add up to 100%.)

As business impacts rise, we expect demand for additional security-related funding to increase.

The number of incidents may be declining – but their impacts on the business have now risen to significant levels. In fact, over the last four years the business impacts – from financial losses to compromises to brands and reputations – have increased as much as 233%.

As these numbers continue to rise, we predict even greater pressure on the CFO to release funding – not just to maintain security capabilities at their current level but also to advance security's ability to protect and support the business.

Business impacts	2007	2008	2009	2010	Three-year change*
Financial losses	6%	8%	14%	20%	+ 233%
Intellectual property theft	5%	6%	10%	15%	+ 200%
Brand/reputation compromised	5%	6%	10%	14%	+ 180%

Question 23: "What were the business impacts to your organization as a result of the incident?" (Does not add up to 100%.)

* This calculation measures the difference between response levels over a three-year period from 2007 to 2010.

A major change in the CISO's reporting channel.

This year, there has been a significant shift in the ongoing evolution of the CISO's reporting channel – away from the CIO in favor of the company's senior decision-makers. What does this reveal? Across industries, there is growing recognition that security's strategic value is more closely aligned with the business than with IT.

Who the CISO reports to	2007	2008	2009	2010	Three-year change*
Chief Information Officer	38%	34%	32%	23%	- 39%
Board of Directors	21%	24%	28%	32%	+ 52%
Chief Executive Officer	32%	34%	35%	36%	+ 13%
Chief Financial Officer	11%	11%	13%	15%	+ 36%
Chief Operating Officer	9%	10%	12%	15%	+ 67%
Chief Privacy Officer	8%	8%	14%	17%	+ 113%

Question 16C: "Where or to whom does your CISO or equivalent senior information security officer report?"

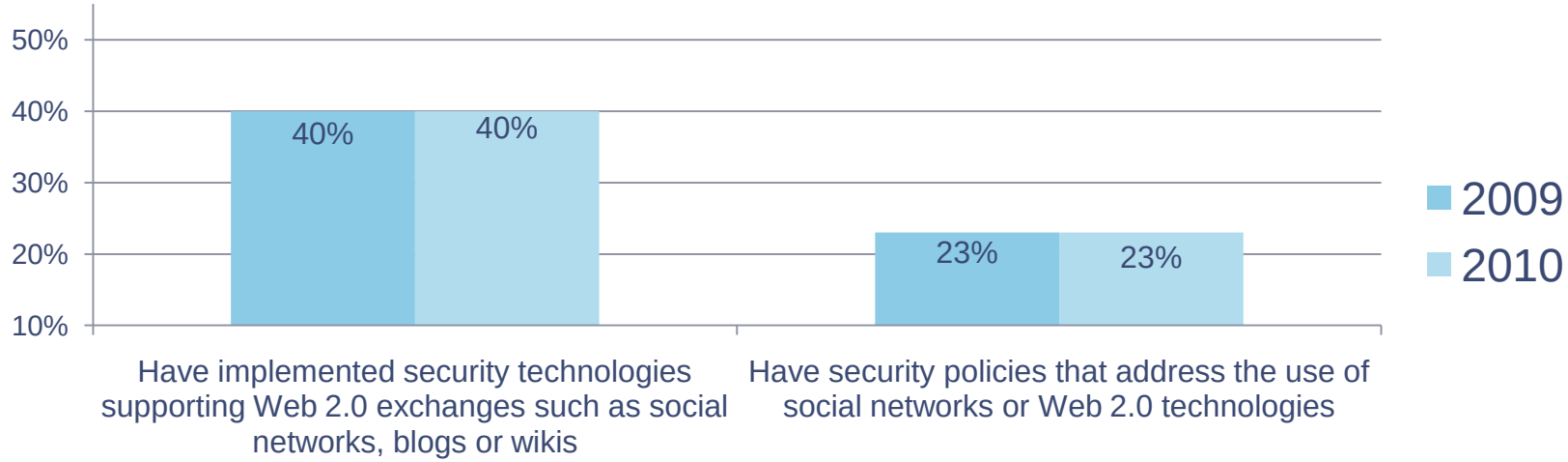
* This calculation measures the difference between response levels over a three-year period from 2007 to 2010.

Agenda

1. Methodology
2. Spending : A subtle but enormously meaningful shift
3. Economic context: The leading impacts and strategies
4. Funding and budgets: A balance between caution and optimism
5. Capabilities and breaches: Trends too large to ignore
6. New areas of focus: Where the emerging opportunities lie
7. Global trends: A changing of the guard
8. The road ahead: What this means for your business

Not surprisingly, social networking represents one of the fastest emerging new areas of risk.

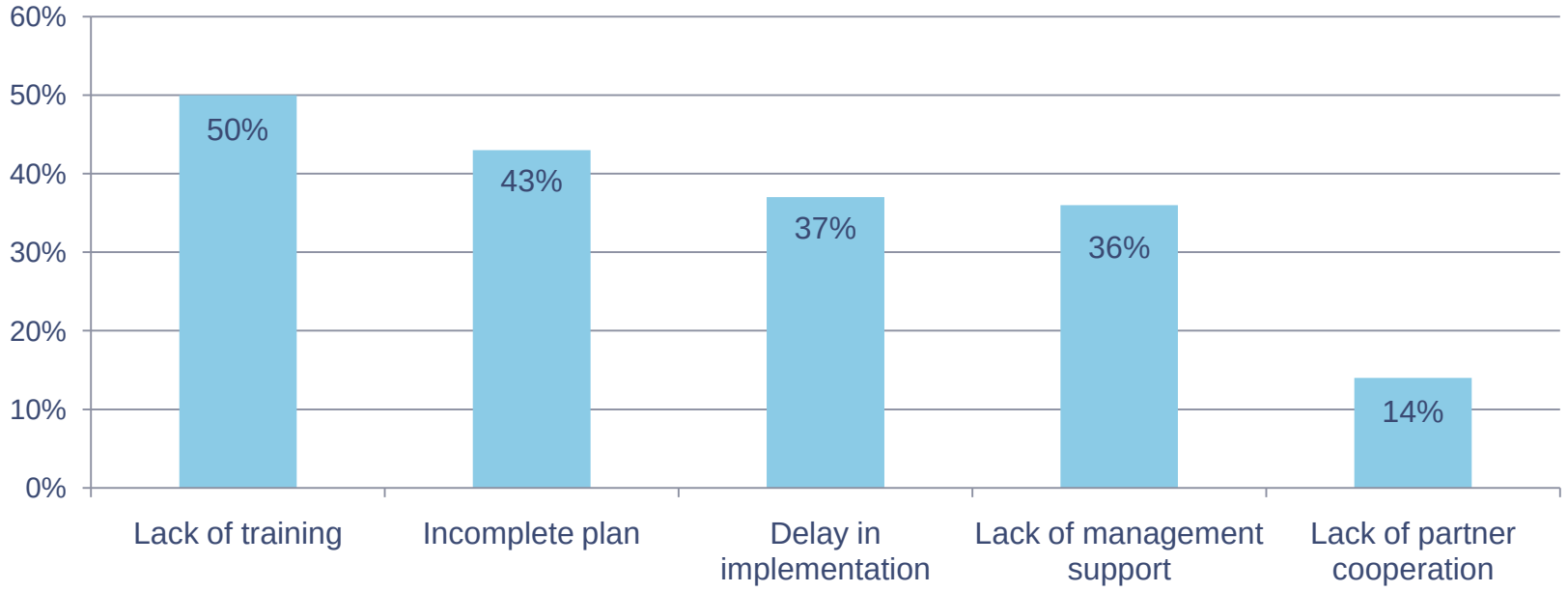
As if protecting data across applications, networks and mobile devices wasn't complex enough, social networking by employees is presenting companies with a new frontier of risk. Few, however, are adequately prepared to counter this threat.



Questions 15 through 18: "What privacy or security safeguards does your organization currently have in place?" Question 28: "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%.)

If response becomes necessary, be prepared.

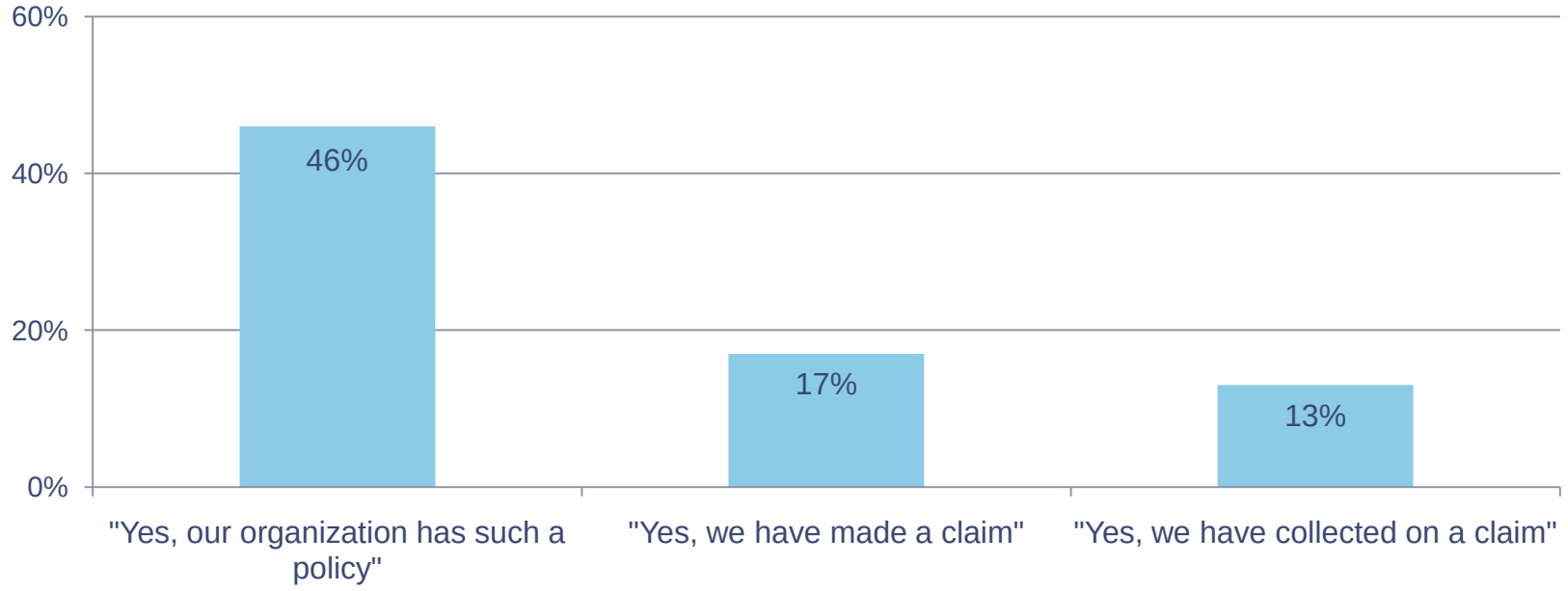
Nearly six out of 10 (58%) respondents report that their organization has a contingency plan for security incidents. But only 63% report that their plan is effective. In other words, most organizations (63%) either have no plan or the plan they have doesn't work. Why? Five principal reasons.



Question 26: "Why were your contingency plans not effective?" (Not all factors shown. Total does not add up to 100%.)

A newly popular tool in the CISO's arsenal? Insurance.

For the first time this year, we asked respondents whether their organization has an insurance policy that protects it from theft or misuse of assets such as electronic data or customer records. Almost half (46%) said "yes." And more than a few have made a claim – and collected on it. We expect to see these numbers rise significantly over the next several years.



Question 27: "Does your organization have an insurance policy that protects it from theft or misuse of electronic data, customer records, etc?"; "Have you made a claim?"; and "Have you collected on a claim?". Total does not add up to 100%.)

Agenda

1. Methodology
2. Spending : A subtle but enormously meaningful shift
3. Economic context: The leading impacts and strategies
4. Funding and budgets: A balance between caution and optimism
5. Capabilities and breaches: Trends too large to ignore
6. New areas of focus: Where the emerging opportunities lie
7. Regional trends: A changing of the guard
8. The road ahead: What this means for your business

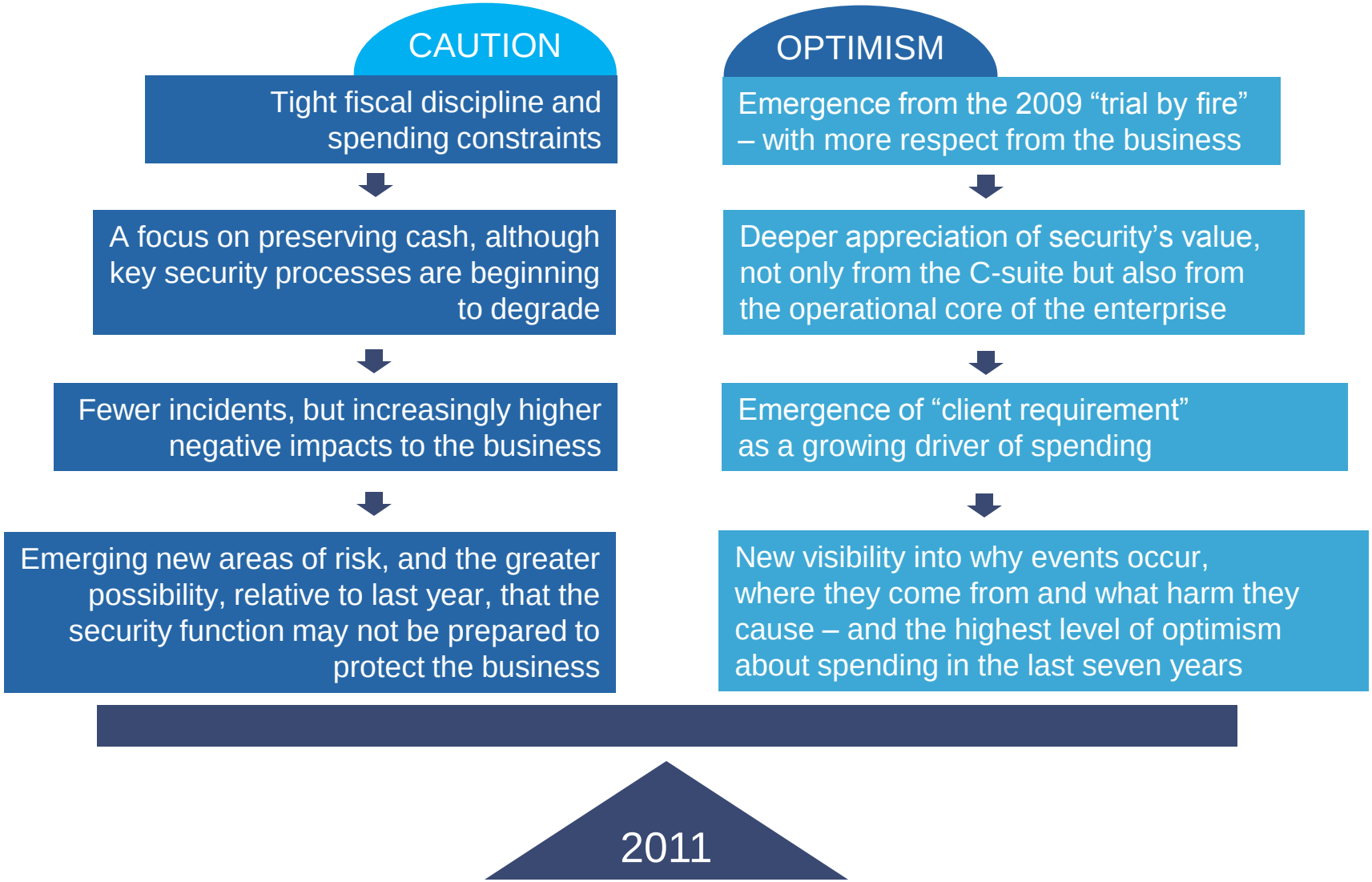
With confidence, persistence and momentum, Asia is becoming the new global leader in information security.

	Asia	North America	South America	Europe
A leading driver of security spending: Business continuity	50%	42%	35%	29%
A leading justification for security: Client requirement	52%	37%	39%	29%
Security spending will increase or stay the same	86%	71%	81%	68%
View protecting sensitive customer data “important/extremely important”	80%	80%	76%	68%
Have an accurate inventory of where sensitive data is stored	42%	40%	33%	24%
Have dedicated security personnel supporting internal business depts.	56%	45%	51%	38%
Use data leakage prevention (DLP) tools	50%	46%	41%	40%
Have security technologies supporting Web 2.0 exchanges	48%	36%	43%	32%
Number of security incidents in the past 12 months: Unknown	14%	37%	19%	29%
Have a centralized security information management process	52%	57%	44%	40%
Continuously prioritize information assets according to their risk level	24%	16%	20%	16%
Conduct enterprise risk assessment at least twice a year	41%	28%	42%	33%

Agenda

1. Methodology
2. Spending: A subtle but enormously meaningful shift
3. Economic context: The leading impacts and strategies
4. Funding and budgets: A balance between caution and optimism
5. Capabilities and breaches: Trends too large to ignore
6. New areas of focus: Where the emerging opportunities lie
7. Global trends: A changing of the guard
8. The road ahead: What this means for your business

It’s an uncertain year, and security hangs in the balance.



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/giss2011

© 2010 PricewaterhouseCoopers LLP. All rights reserved. "PricewaterhouseCoopers" refers to PricewaterhouseCoopers LLP, a Delaware limited liability. partnership, or, as the context requires, the PricewaterhouseCoopers global network or other member firms of the network, each of which is a separate and independent legal entity. This document is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

PRICEWATERHOUSECOOPERS