Contents

11. ***Public sector***

12. ***Retail & Consumer***

13. ***Technology***

14. ***Telecommunications***

www.pwc.com/security

Changing the game

While tight budgets have forestalled updates to security programs, many businesses are confident they're winning the game. But the rules—and the players—have changed.

CIO Business Technology Leadership

CSO BUSINESS RISK LEADERSHIP

Key findings from The Global State of Information Security® Survey 2013

September 2012

pwc

> ***“You can’t succeed in today’s elevated threat environment if you don’t know the players and you don’t know the rules.”***
>
> ***—Gary Loveland, Principal, PwC***

Information security has always been a high-stakes game. One that demands a smart strategy, the right technology moves, and an unblinking eye on adversaries.

For many businesses, however, it has become a pursuit that is almost impossible to win. That’s because the rules have changed, and opponents—old and new—are armed with expert technology skills. As a result, the risks are greater than ever.

Businesses are fighting back by adopting new detection and prevention technologies. At the same time, governments around the world are enacting legislation to combat cyber threats. And regulatory bodies are issuing new guidance on disclosure obligations for cyber incidents.

Yet risks to data security continue to intensify—and show no signs of abating. Those keeping score agree that the bad guys appear to be in the lead.

Nonetheless, many businesses believe they are winning. The Global State of Information Security® Survey 2013 shows that most executives across industries are confident in the effectiveness of their information security practices. They believe their strategies are sound and many consider themselves to be leaders in the field.

The odds, however, are not in their favor: Diminished budgets have resulted in degraded security programs, reported security incidents are on the rise, and new technologies are being adopted faster than they can be safeguarded.

Given today's elevated threat environment, businesses can no longer afford to play a game of chance. They must prepare to play a new game, one that requires advanced levels of skill and strategy to win.

Agenda

Section 1. Methodology

Section 2. A game of confidence

Section 3. Meet the leaders

Section 4. A game of risk

Section 5. It's how you play the game

Section 6. The new world order

Section 7. What this means for your business

Section 1

Methodology

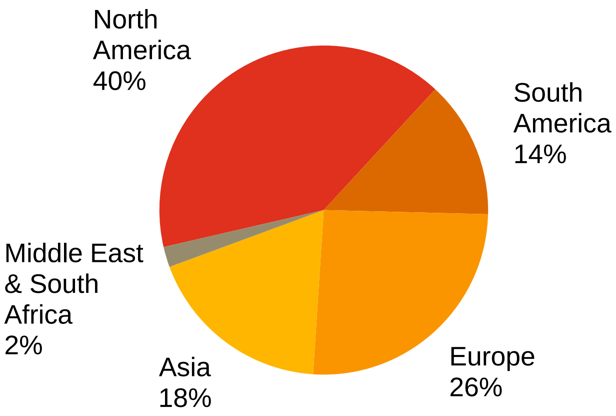
A worldwide study

The Global State of Information Security® Survey 2013, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 1, 2012 to April 15, 2012.

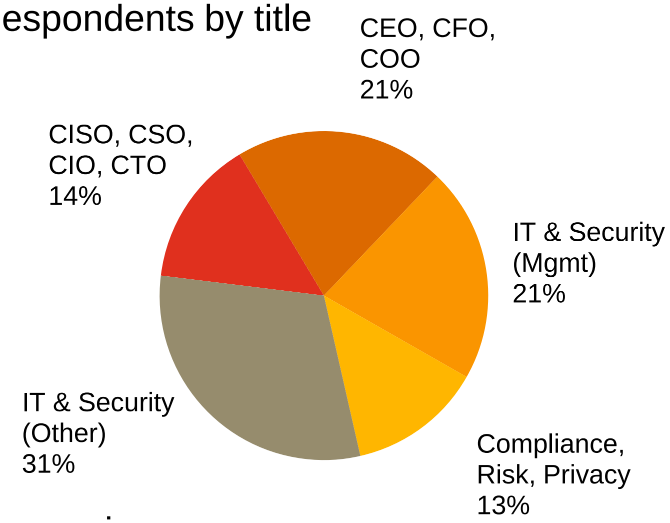
- PwC's 15th year conducting the online survey, 10th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 128 countries
- More than 9,300 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-three percent (33%) of respondents from companies with revenue of $500 million+
- Forty percent (40%) of respondents were from North America, 26% from Europe, 18% from Asia, 14% from South America, and 2% from the Middle East and South Africa
- Margin of error less than 1%

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

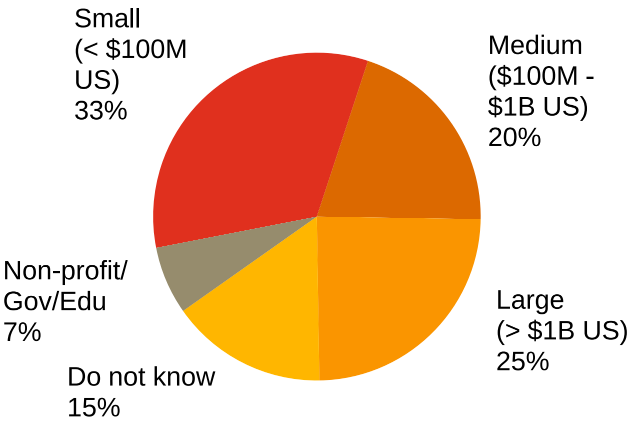
Respondents by region of employment



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

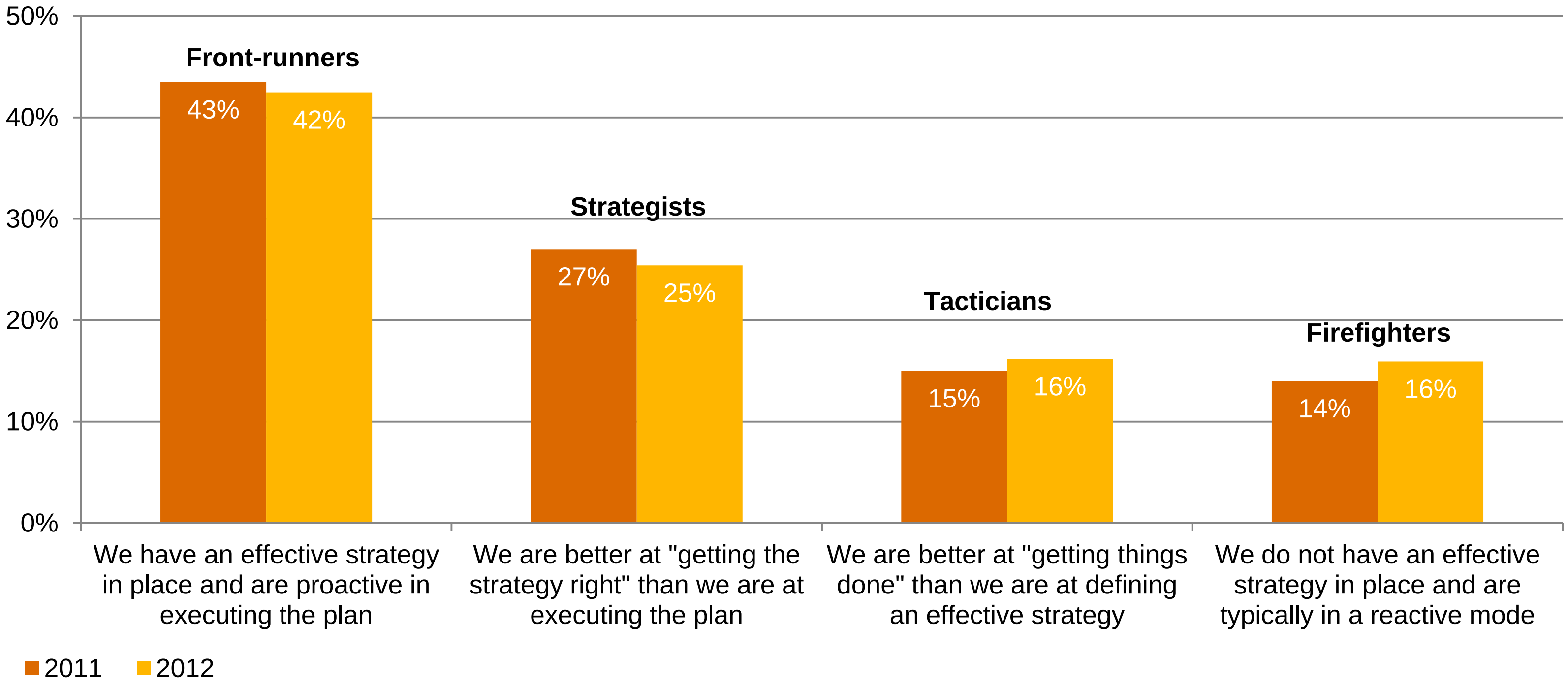
	Number of responses this year
Technology	1,469
Financial Services	1,338
Retail & Consumer Products	1,169
Industrial Products	775
Public Sector	730
Telecommunications	511
Healthcare Providers	467
Entertainment & Media	378
Aerospace & Defense	242
Automotive	218
Power & Utilities	201
Energy (Oil & Gas)	136
Pharmaceutical	112

Section 2

A game of confidence: Organizations assess their security practices

Respondents are confident in their security practices.

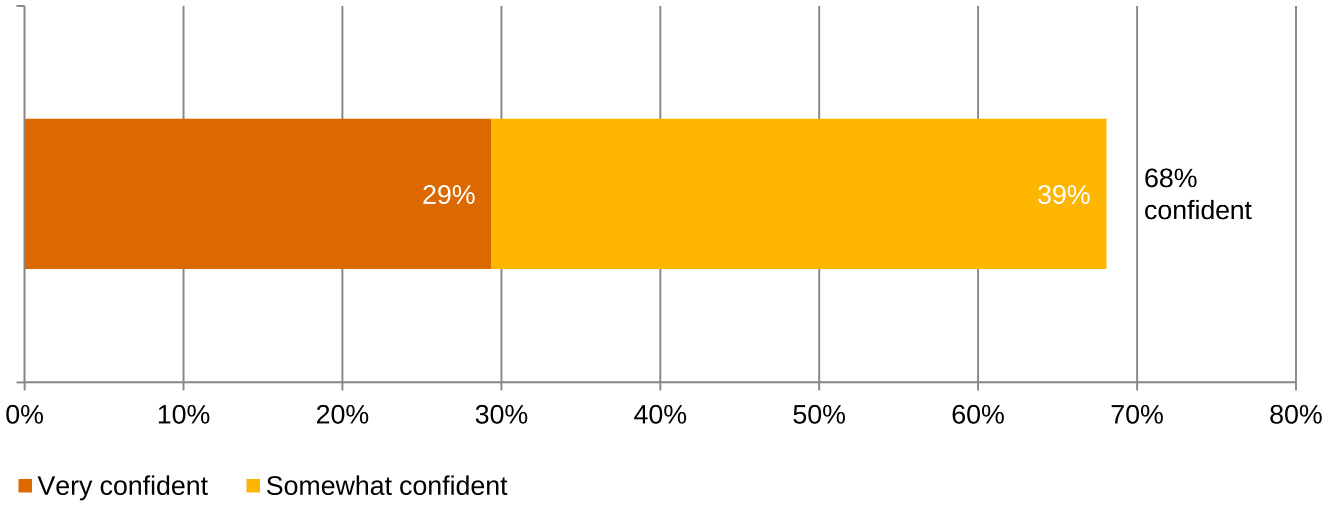
42% of respondents say their organization has a strategy in place and is proactive in executing it—exhibiting two distinctive attributes of a leader.



Question 28: "Which category below best characterizes your organization's approach to protecting information security?" (Numbers reported may not reconcile exactly with raw data due to rounding.)

Most believe they have instilled effective information security behaviors into organizational culture.

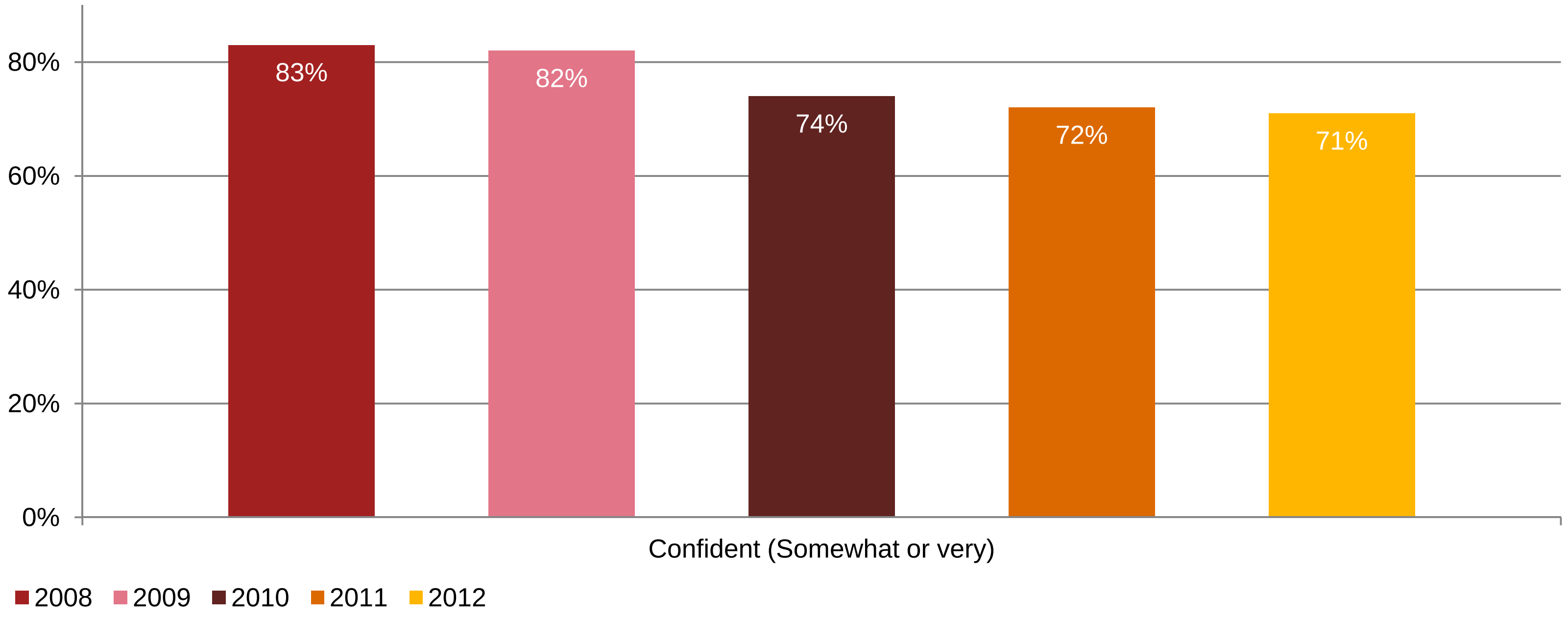
To be effective, security must be integral to the way people think and work, not just another item to be checked off a list. 68% of respondents are either very or somewhat confident they have instilled effective security behaviors into their organizational culture.



Question 35: "How confident are you that your organization has instilled effective information security behaviors into the organizational culture?"
(Not all factors shown. Totals do not add up to 100%.)

A majority of respondents say their information security activities are effective—but this confidence is eroding.

Confidence is a good thing. More than 70% of respondents are very (32%) or somewhat (39%) confident that their organization's information security activities are effective. Yet they may not realize that assurance has dropped since 2008.



Question 41: "How confident are you that your organization's information security activities are effective?"

Section 3

Meet the leaders: Measuring self-appraisals against our criteria for leadership

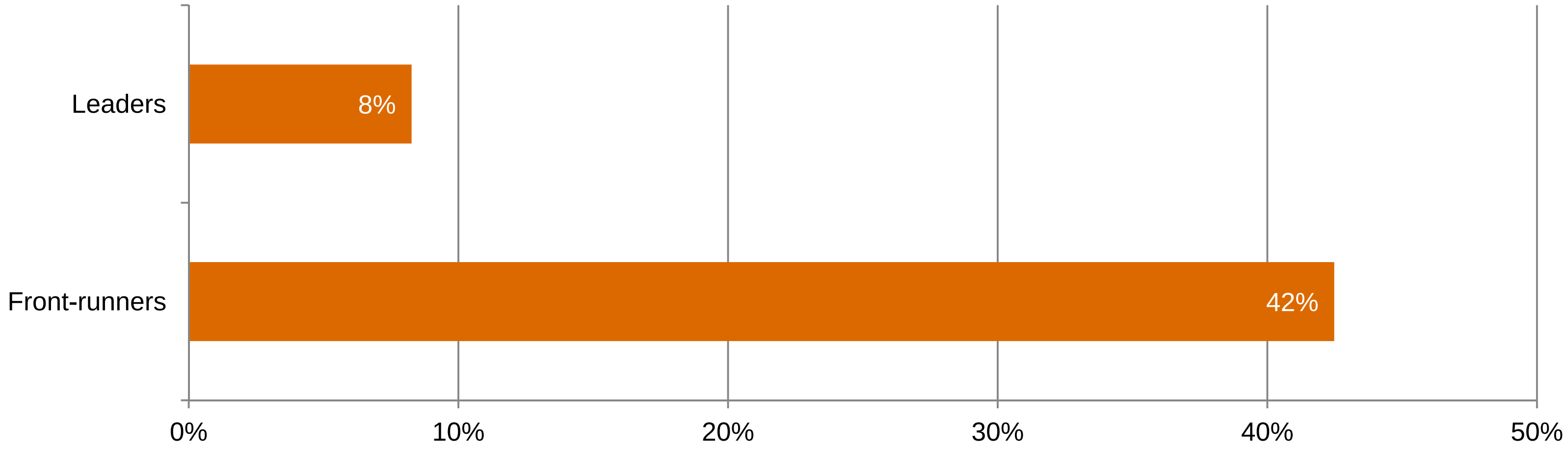
A check-list for defining information security leaders.

Self-appraisals can be misleading. To determine the real leaders in information security, we compared respondents' self-assessments against four key criteria to define leadership. To qualify as a leader, organizations must:

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

A reality check on real leaders.

Our analysis reveals that only 8% of respondents rank as real leaders. A comparison of this group with the much larger cohort of self-proclaimed front-runners suggests that many organizations have opportunities to improve their security practices.



Leaders are identified by responses to Question 13A: “Where / to whom does your CISO, CSO, or equivalent senior information security executive report?” Question 14: “What process information security safeguards does your organization currently have in place?” Question 18: “What types of security incidents (breach or downtime) occurred” and Question 31: “Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?”

How these leaders play a more competitive game.

Leaders are, by significant margins, more likely than all respondents to have a more mature security practice, implement strategies for newer technologies, and use sophisticated technology tools to safeguard data.

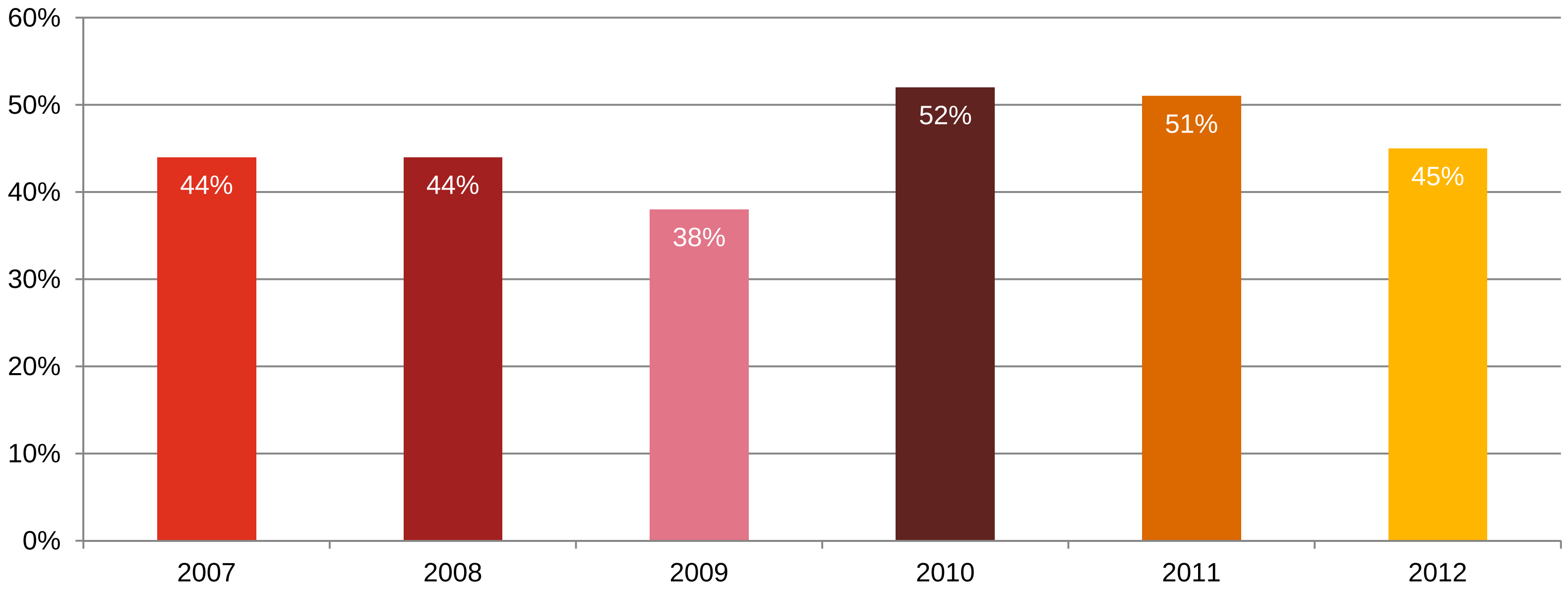
	Leaders	All survey
Expect security spending to increase over the next year	74%	45%
Employ a CISO or equivalent	90%	42%
Involve information security in major initiatives at project inception	45%	25%
Security spending is completely aligned with business goals	50%	30%
Confident that effective security behavior is instilled in company culture	94%	68%
Have framework integrating compliance, privacy/data use, security, ID theft	92%	60%
Have a mobile security strategy	57%	44%
Use malicious code detection tools	86%	71%
Use intrusion prevention tools	78%	59%
Have measured and reviewed security over the past year	100%	49%

Section 4

A game of risk: The decline of capabilities over time

Budget increases are slowing after recovery from the global economic crisis.

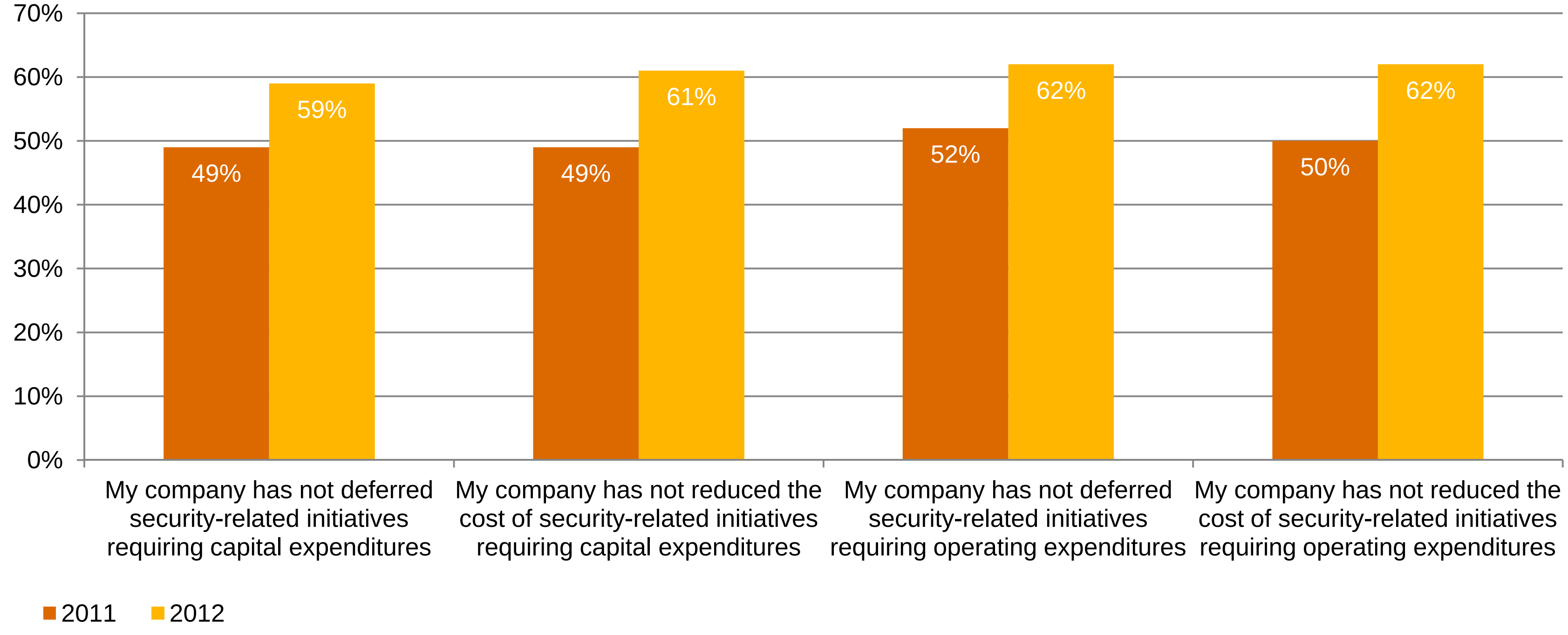
Purse strings are looser than they were during the recession, but the trend toward bigger security budgets has leveled off. Fewer than half of respondents expect budgets to increase over the next 12 months, while 18% say they don’t know where spending is headed.



Question 8: "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%”)

But there's good some news: Security projects are on track and companies are less likely to cut spending.

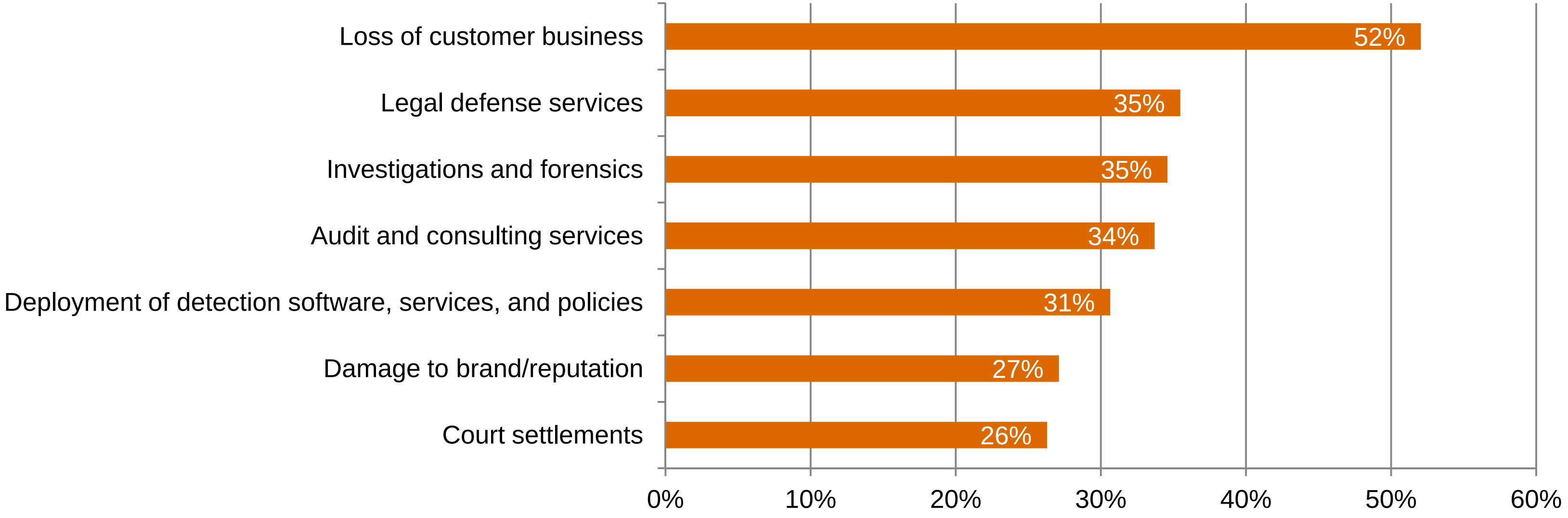
Encouragingly, respondents report fewer deferrals and fewer budget cutbacks for security initiatives. Compared with last year, for instance, 24% more respondents say they had not reduced costs of security programs requiring capital expenditures.



Questions 9A and 10A: "Has your company deferred capital and operating security-related initiatives?" Questions 9B and 10B: "Has your company reduced the capital and operating costs of security-related initiatives?"

Reported security incidents inch up, yet financial losses due to breaches decrease significantly.

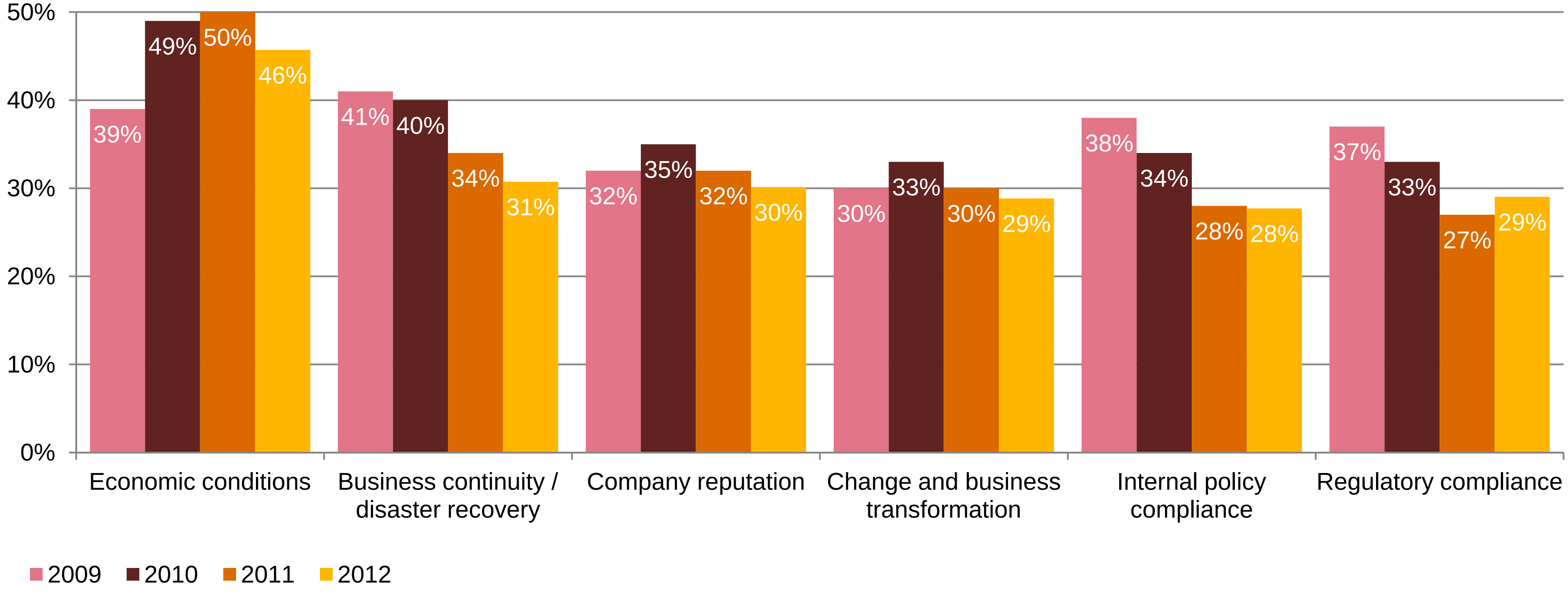
Respondents reporting 50 or more security incidents per year hit 13%—up slightly from last year and far above the levels of earlier years—yet respondents reporting financial losses dropped to 14% from 20% in 2011. These assessments of financial hits may be inaccurate due to incomplete appraisals of factors that contribute to losses. For instance, only 27% consider damage to brand/reputation and only 35% factor in legal defense costs.



Question 17: “Number of security incidents in the past 12 months.” Question 21: “How was your organization impacted by the security incident?” Question 21C: “What factors are included in your company’s calculation of these financial losses?” (Not all factors shown. Totals do not add up to 100%.)

Security budgets are driven by the economy, not security needs.

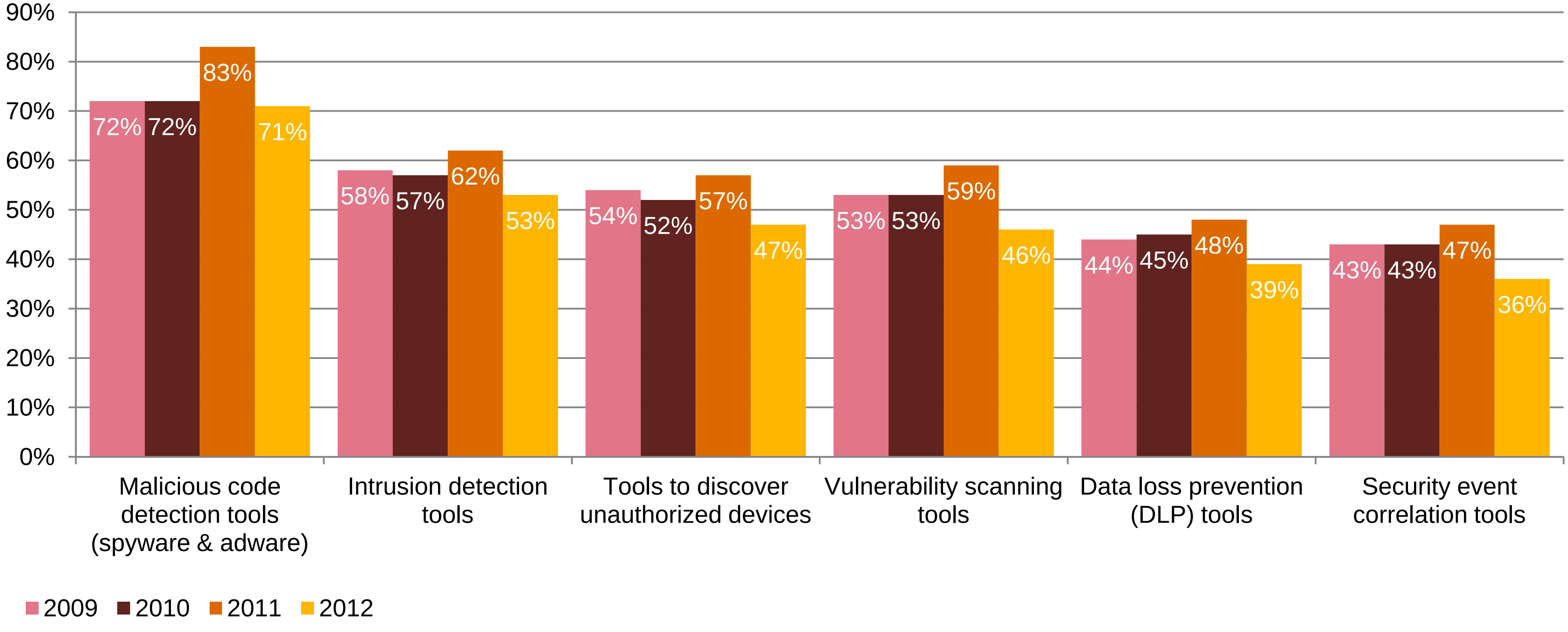
Almost half (46%) of respondents say economic conditions rank as the top driver of security spending. Business continuity/disaster recovery is the highest security-specific response.



Question 37: "What business issues or factors are driving your company's information security spending?" (Not all factors shown.)

Use of some key technology safeguards resumed a decline after last year's uptick.

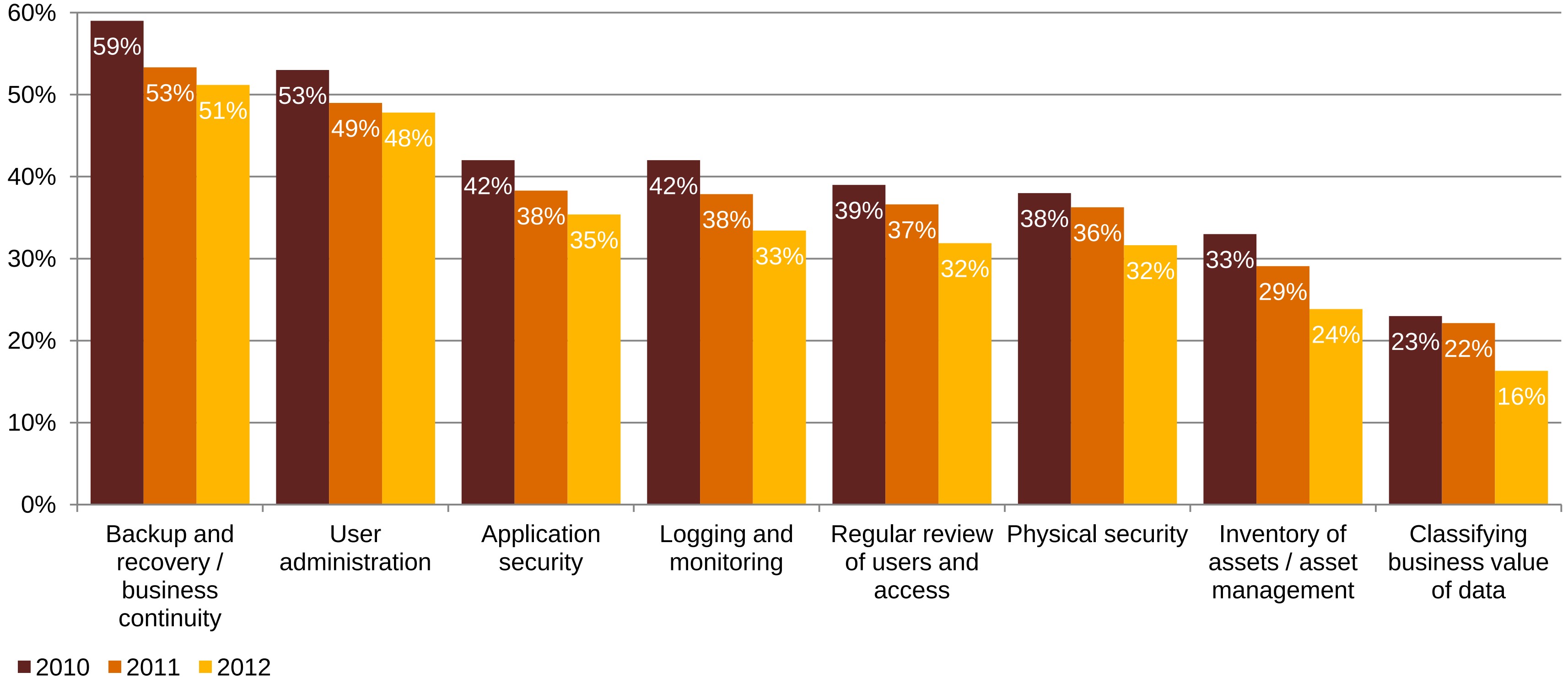
The future looked bright last year as many companies stepped up investments in prevention and detection safeguards. This year, however, saw a decrease in deployment of these important tools.



Question 15: “What technology information security safeguards does your organization currently have in place?” (Not all factors shown.)

Security policies have grown less robust and inclusive.

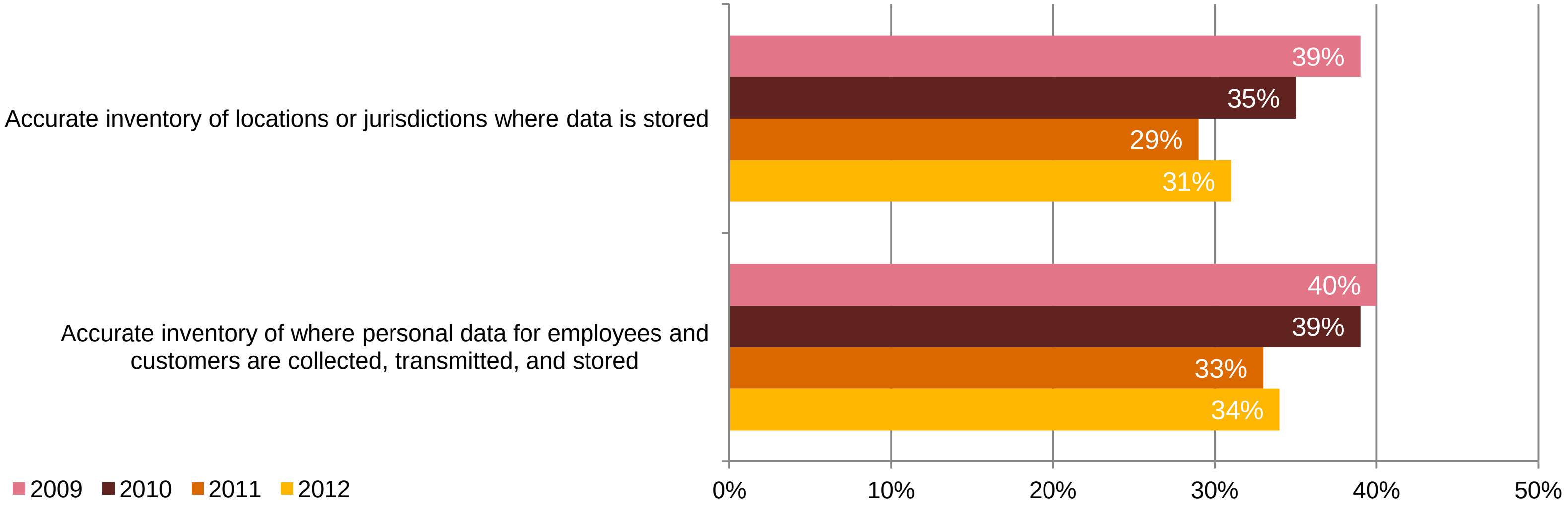
Many organizations are omitting fundamental elements of security from their overall policies.



Question 32: “Which of the following elements, if any, are included in your organization’s security policy?” (Not all factors shown.)

Respondents know less about their data now than they did three years ago.

While more than 80% of respondents say protecting employee and customer data is important, far fewer understand what that data entails and where it is stored. This is significant because, increasingly, consumers want to be in control of their personal data and "turn off" the flow of information from companies.[1]

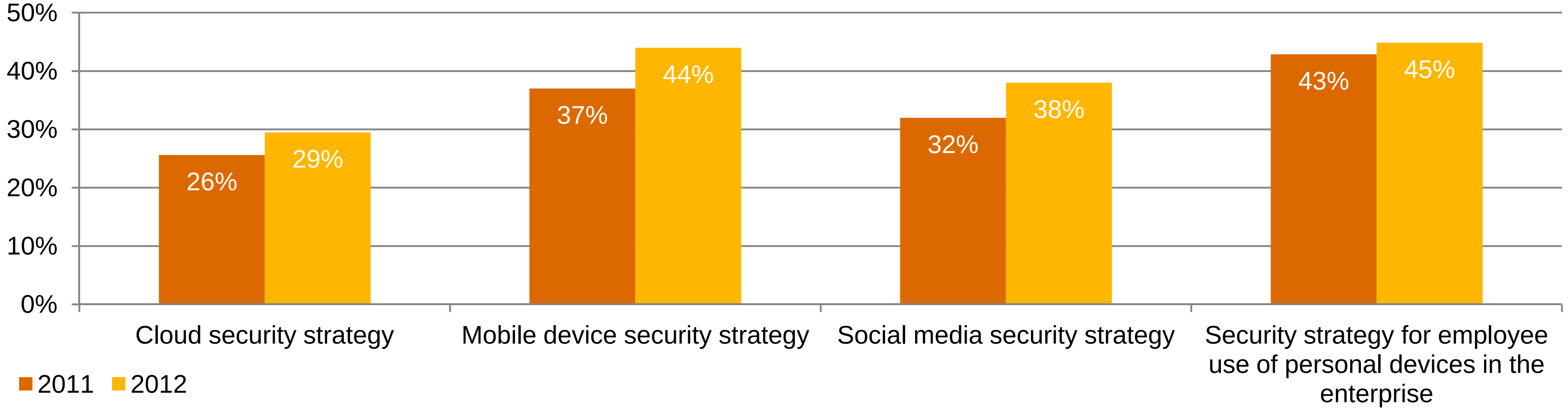


Question 38: "What level of importance does your company place on protecting the following types of information?" Question 11: "Which data privacy safeguards does your organization have in place?"

[1] PwC, Consumer privacy: What are consumers willing to share? July 2012

Technology adoption is moving faster than security implementation.

Across industries, organizations are struggling to keep pace with the adoption of cloud computing, social networking, mobility, and use of personal devices. Yet these new technologies often are not included in overall security plans even though they are widely used. In a recent survey, for instance, we found that 88% of consumers use a personal mobile device for both personal and work purposes.[2]



Question 14: What process information security safeguards does your organization currently have in place?" (Not all factors shown. Totals do not add up to 100%.)

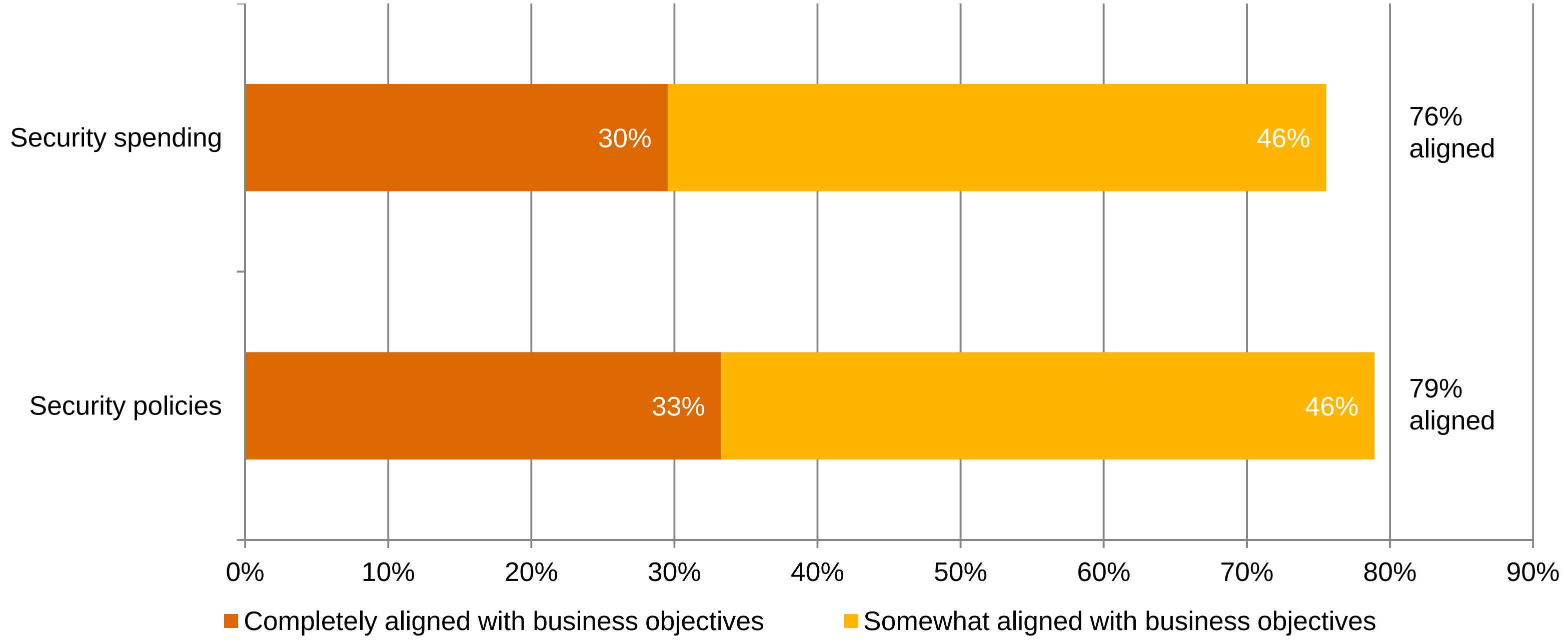
[2] PwC, Consumer privacy: What are consumers willing to share? July 2012

Section 5

It’s how you play the game: Alignment, leadership, and training are key

Respondents report that security strategies and security spending are well-aligned with business goals.

Strategies and budgets should be measured against their alignment with the goals of the larger organization. By that standard, most respondents believe their security efforts and security dollars are well-targeted.



Question 33: "In your opinion, how well are your company’s security policies aligned with your company’s business objectives? Question 34: "In your opinion, how well is your company’s security spending aligned with your company’s business objectives?” (Not all factors shown. Totals do not add up to 100%.)

What keeps security from being what it should be?

50% of respondents perceive top-level leadership to be an obstacle to improving information security. The most-cited single hindrance is insufficient capital expenditures, followed by lack of actionable vision.

	2011	2012
Leadership: CEO, president, board, or equivalent	23%	21%
Leadership: CIO or equivalent	17%	15%
Leadership: CISO, CSO, or equivalent	17%	14%
Insufficient capital expenditures	27%	26%
Lack of actionable vision or understanding	26%	24%
Lack of an effective information security strategy	26%	22%

Question 29: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?" (Not all factors shown. Totals do not add up to 100%.)

Less than half of respondents have security training programs for employees.

No security program can be effective without adequate training, yet only 49% of respondents have an employee security awareness training program in place. Even fewer have staff dedicated to security awareness.

Information security safeguards	2009	2010	2011	2012
Have employee security awareness training program	53%	49%	43%	49%
Have people dedicated to employee awareness programs	58%	55%	51%	47%

Question 13: “What information security safeguards related to people does your organization have in place?” Question 14: “What process information security safeguards does your organization currently have in place?” (Not all factors shown. Totals do not add up to 100%.)

Section 6

The new world order: Asia advances, South America makes its move, and other regions try to maintain

Years of investment pay off as Asia leads the world in security practices and performance.

Despite some degradation over last year and a mixed spending outlook, Asia's overall level of information security technologies, policies, and spending are higher than other regions.

	2011	2012
Employ a Chief Information Security Officer	48%	46%
CISO reports to CEO	40%	43%
Employ a Chief Privacy Officer	32%	36%
Have reduced budgets for security initiatives requiring capital expenditures	39%	35%
Have reduced budgets for security initiatives requiring operating expenditures	39%	34%
Have business continuity/disaster recovery plan	47%	49%
Information security becomes involved in major initiatives at project inception	N/A	28%
No downtime over the past 12 months as a result of security incidents	13%	17%
Have a mobile device security strategy	54%	47%
Have an effective strategy in place and are proactive in executing the plan	55%	46%
Security spending will increase over the next 12 months	74%	61%

(Not all factors shown.)

Security budgets are almost flat in North America, but certain strategies show gains.

Despite low expectations for security budgets, North America leads in keeping projects on track and makes some gains in practices like training, mobility, and business continuity/disaster recovery.

	2011	2012
Security spending will increase over the next 12 months	31%	34%
Have reduced budgets for security initiatives requiring capital expenditures	40%	30%
Have deferred security initiatives requiring capital expenditures	40%	32%
Have an effective strategy in place and are proactive in executing the plan	39%	42%
Have an overall information security strategy	58%	75%
Have an effective contingency plan for downtime due to security incidents	69%	73%
Have business continuity/disaster recovery plans	46%	56%
Have an accurate inventory of employees' and customers' personal data	30%	38%
Have employee security awareness training program	42%	54%
Have a mobile device security strategy	34%	47%
Have security strategy for use of personal devices on the enterprise	37%	46%

(Not all factors shown.)

As spending stalls in Europe and safeguards weaken, some security practices are improving.

Europe ranks low in the number of self-identified front-runners. But the Continent does lead in the percentage of Chief Privacy Officers on staff, and rates highly at employing CISOs and CSOs. It trails most other regions in security and privacy safeguards, however.

	2011	2012
Security spending will increase over the next 12 months	43%	43%
Have reduced budgets for security-related capital expenditures	57%	48%
Have reduced budgets for security-related operating expenditures	56%	48%
Have an effective strategy in place and are proactive in executing the plan	41%	40%
Employ a Chief Privacy Officer	31%	44%
Have business continuity/disaster recovery plans	32%	43%
Security policies are aligned with business objectives	70%	74%
Have an accurate inventory of employees' and customers' personal data	26%	29%
Have an employee security awareness training program	33%	42%
Have a mobile device security strategy	30%	39%
Have malicious code detection tools	80%	67%

(Not all factors shown.)

South America plays catch-up on security investments and emerges as a leader in some important categories.

Confidence is high South America, where spending is robust and initiatives for technologies like mobility and business continuity/disaster recovery are advancing.

	2011	2012
Security spending will increase over the next 12 months	65%	63%
Have reduced budgets for security-related capital expenditures	66%	47%
Have reduced budgets for security-related operating expenditures	66%	47%
Have an effective strategy in place and are proactive in executing the plan	42%	42%
Are confident that our information security activities are effective	71%	75%
Employ a Chief Information Security Officer	53%	50%
Have a mobile device security strategy	32%	41%
Have an accurate inventory of employees' and customers' personal data	29%	30%
Require third parties to comply with our data privacy policies	28%	36%
Cloud computing has improved security	56%	61%
Have business continuity/disaster recovery plan	30%	40%

(Not all factors shown.)

Section 7

What this means for your business

What you can do to improve your performance.

Information security today is a rapidly evolving game of advanced skill and strategy. As a result, the security models of the past decade are no longer sufficient.

Effective security requires a new way of thinking. The very survival of the business demands that security leaders understand, prepare for, and quickly respond to security threats.

Businesses seeking to strengthen their security practice must:

- Implement a comprehensive risk-assessment strategy and align security investments with identified risks.
- Understand the organization’s information, who wants it, and what tactics adversaries might use to get it.
- Understand that information security requirements – and, indeed, overall strategies for doing business – have reached a turning point.
- Embrace a new way of thinking in which information security is both a means to protect data as well as an opportunity to create value to the business.

For more information, please contact:

Gary Loveland
Products & Services Industries
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Products & Services Industries
646.471.5731
mark.a.lobel@us.pwc.com

Joe Nocera
Financial Services Industry
312.298.2745
joseph.nocera@us.pwc.com

Peter Harries
Health Industries
213.356.6760
peter.harries@us.pwc.com

John Hunt
Public Sector
703.918.3767
john.d.hunt@us.pwc.com

Dave Burg
Forensic Services
703.918.1067
david.b.burg@us.pwc.com

Dave Roath
Risk Assurance Services
646.471.5876
david.roath@us.pwc.com

Or visit www.pwc.com/giss2013 to explore the data for your industry and benchmark yourself.

The Global State of Information Security® is a registered trademark of International Data Group, Inc.

www.pwc.com/security

Changing the game

While tight budgets have forestalled updates to security programs, many businesses are confident they're winning the game. But the rules – and the players – have changed.

Aerospace & Defense

Key findings from The Global State of Information Security® Survey 2013

September 2012

"You can't succeed in today's elevated threat environment if you don't know the players and you don't know the rules."

– Gary Loveland, Principal, PwC

Information security has always been a high-stakes game. One that demands a smart strategy, the right technology moves, and an unblinking eye on adversaries.

For many businesses, however, it has become a pursuit that is almost impossible to win. That's because the rules have changed, and opponents—old and new—are armed with expert technology skills. As a result, the risks are greater than ever.

Businesses are fighting back by adopting new detection and prevention technologies. At the same time, governments around the world are enacting legislation to combat cyber threats. And regulatory bodies are issuing new guidance on disclosure obligations for cyber incidents.

Yet risks to data security continue to intensify – and show no signs of abating. Those keeping score agree that the bad guys appear to be in the lead.

Nonetheless, many businesses believe they are winning. The Global State of Information Security® Survey 2013 shows that most executives in the global aerospace and defense (A&D) industry are confident in the effectiveness of their information security practices. They believe their strategies are sound and many consider themselves to be leaders in the field.

The odds, however, are not in their favor: Diminished budgets have resulted in degraded security programs, reported security incidents are on the rise, and new technologies are being adopted faster than they can be safeguarded.

Given today's elevated threat environment, businesses can no longer afford to play a game of chance. They must prepare to play a new game, one that requires advanced levels of skill and strategy to win.

Agenda

Section 1. Methodology

Section 2. A game of confidence

Section 3. A game of risk

Section 4. It's how you play the game

Section 1

Methodology

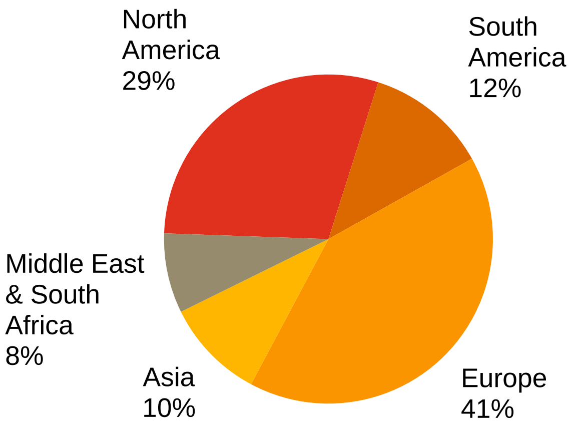
A worldwide study

The Global State of Information Security® Survey 2013, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 1, 2012 to April 15, 2012.

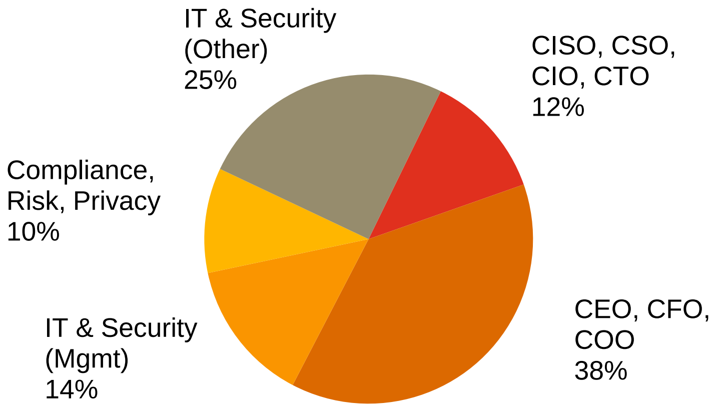
- PwC's 15th year conducting the online survey, 10th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 128 countries
- More than 9,300 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-three percent (33%) of respondents from companies with revenue of $500 million+
- Survey included 242 respondents from the aerospace and defense industry
- Margin of error less than 1%

Demographics

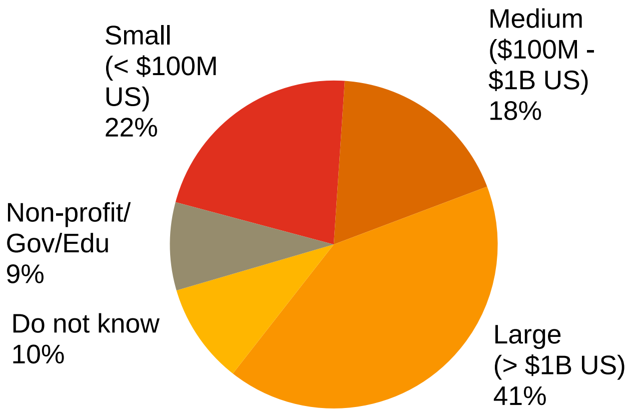
A&D respondents by region of employment



A&D respondents by title



A&D respondents by company revenue size



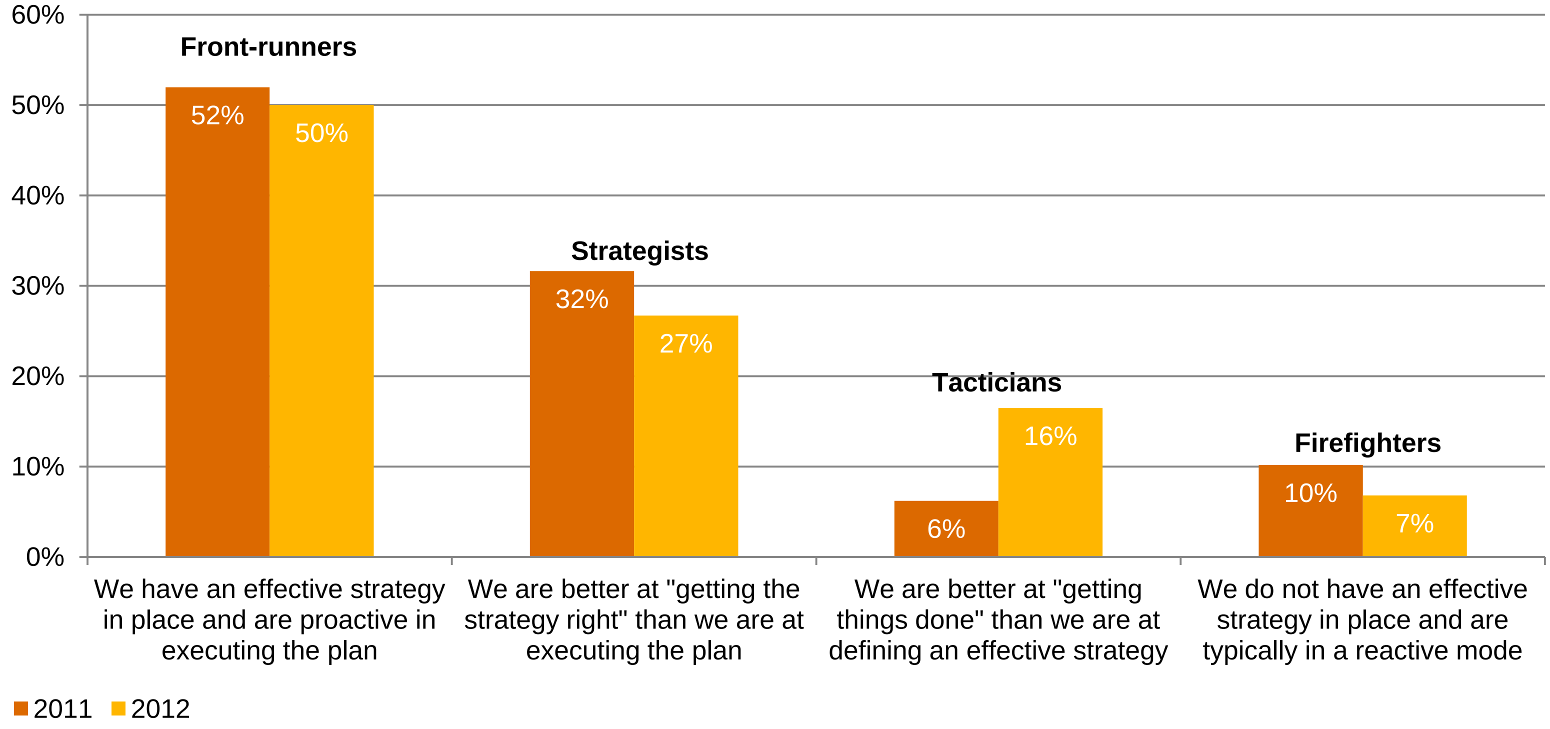
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

A game of confidence

A&D respondents are confident in their security practices.

50% of A&D respondents say their organization has a strategy in place and is proactive in executing it – exhibiting two distinctive attributes of a leader.



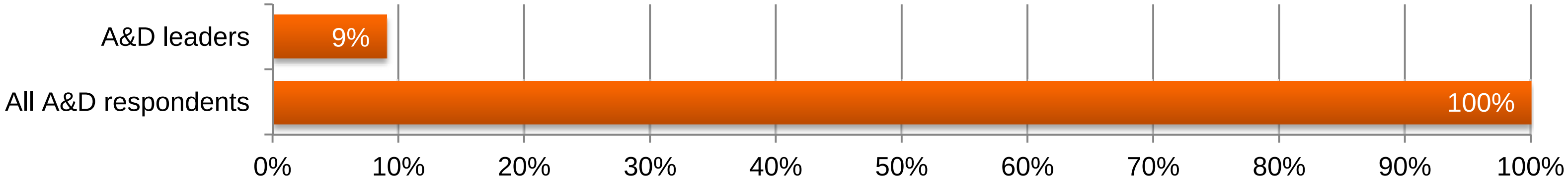
Question 28: "Which category below best characterizes your organization's approach to protecting information security?"

A reality check on real leaders.

But are they really leaders? We measured A&D respondents' self-appraisal against four key criteria to define leadership. To qualify, organizations must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the "top of the house" (e.g., to the CEO, CFO, COO, or legal counsel)
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

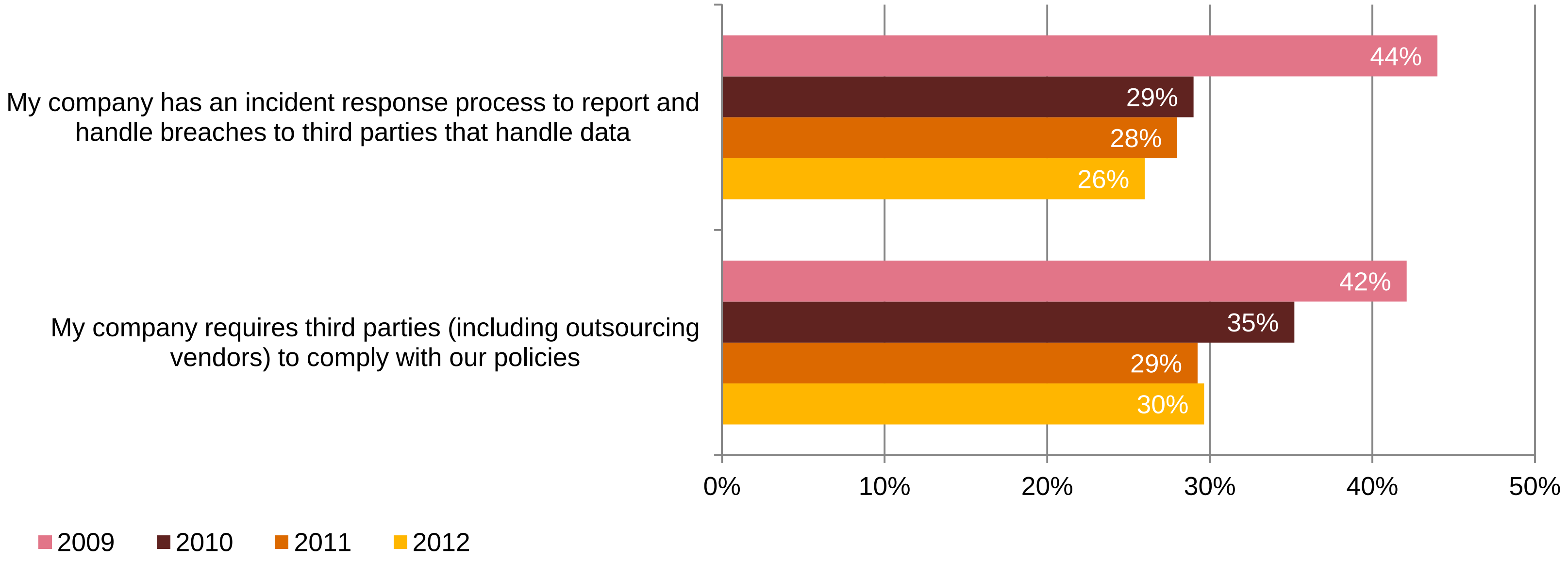
The result? Our analysis found that 9% of A&D respondents rank as leaders.



Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 18: "What types of security incidents (breach or downtime) occurred" and Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Many A&D respondents are over-confident in their organization's security program.

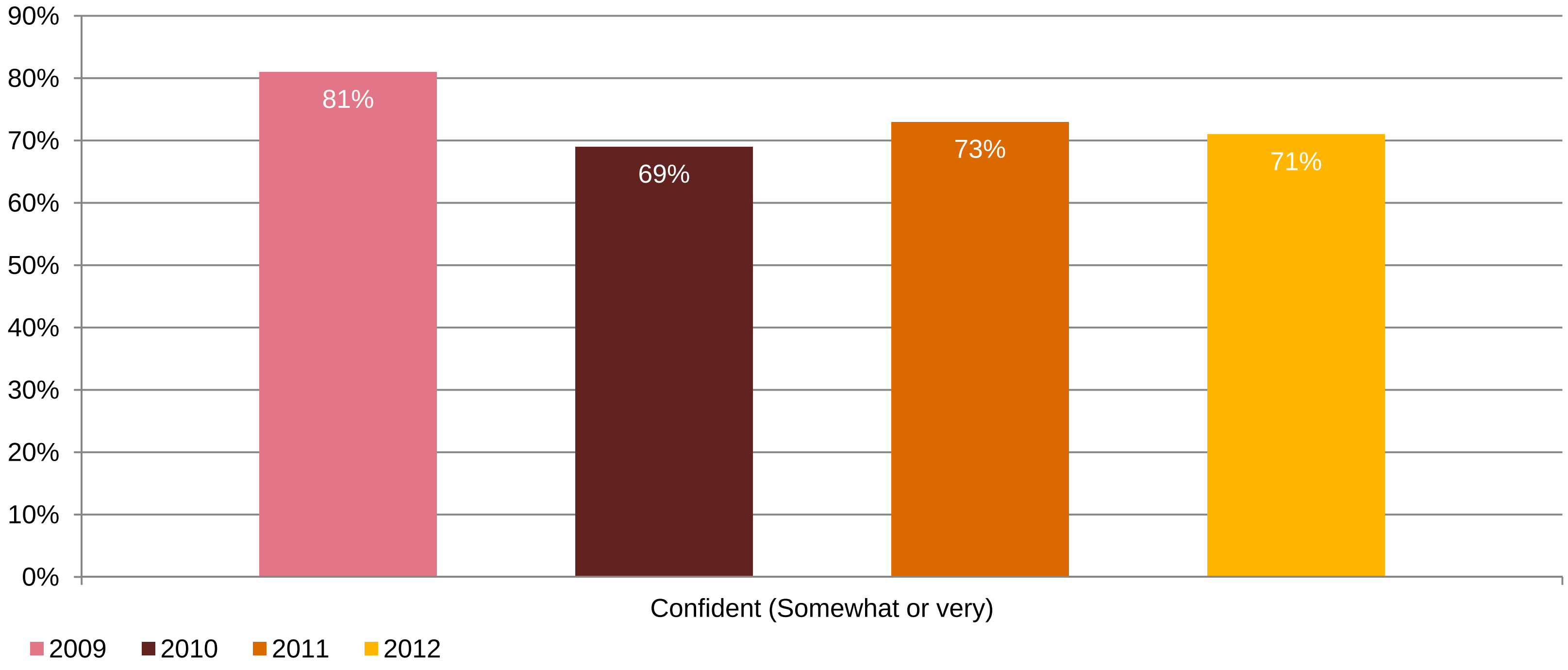
72% of respondents are confident that they have instilled effective security behaviors into their organization's culture, yet most do not have a process in place to handle third-party breaches. What's more, fewer than one-third require third parties to comply with their privacy policies. This suggests a troubling gap in perception.



Question 35: "How confident are you that your organization has instilled effective information security behaviors into the organizational culture?"
Question 11: "Which data privacy safeguards does your organization have in place?"

Most respondents say their information security activities are effective, but confidence is eroding.

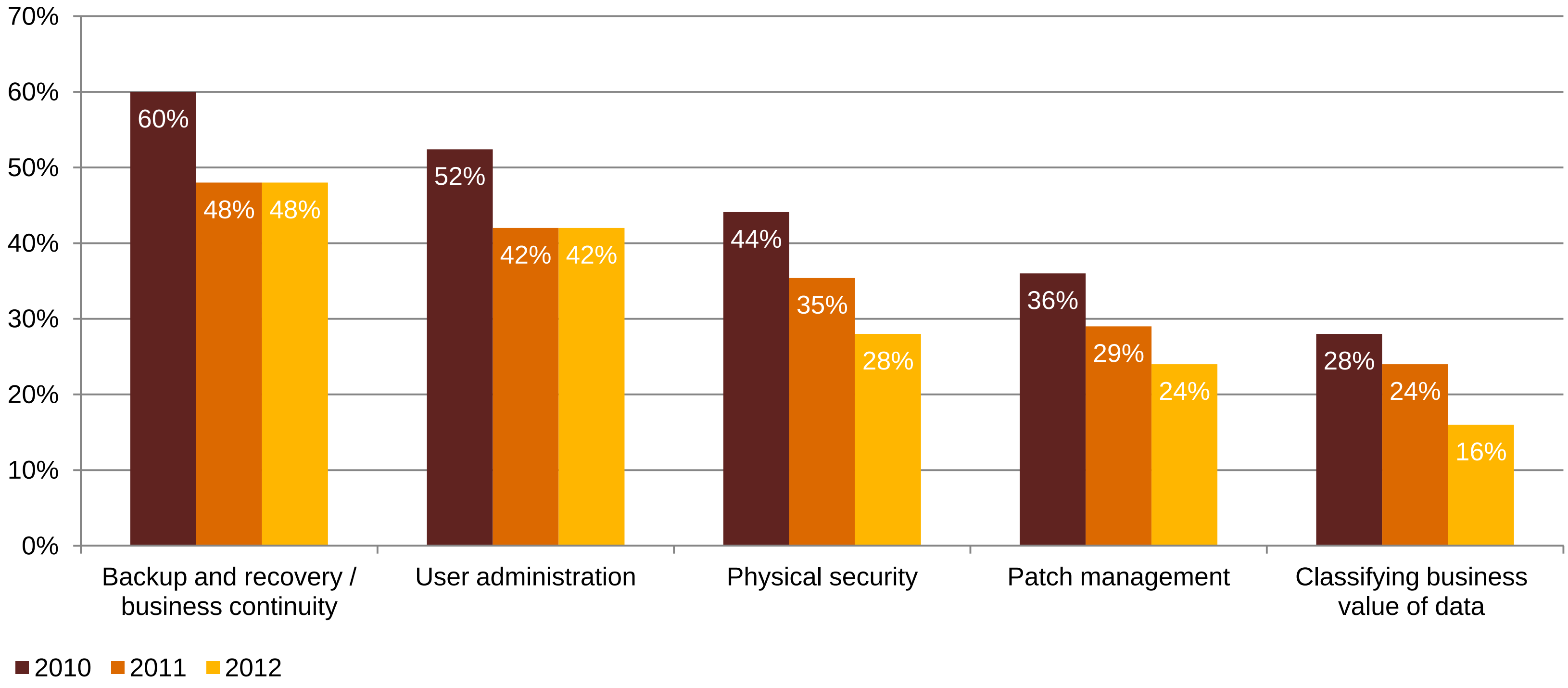
Confidence is a good thing. A strong 71% of A&D respondents say they are confident that their company's security activities are effective, but many may not realize that assurance has dropped since 2009.



Question 41: "How confident are you that your organization's information security activities are effective?"

Security policies have weakened over time.

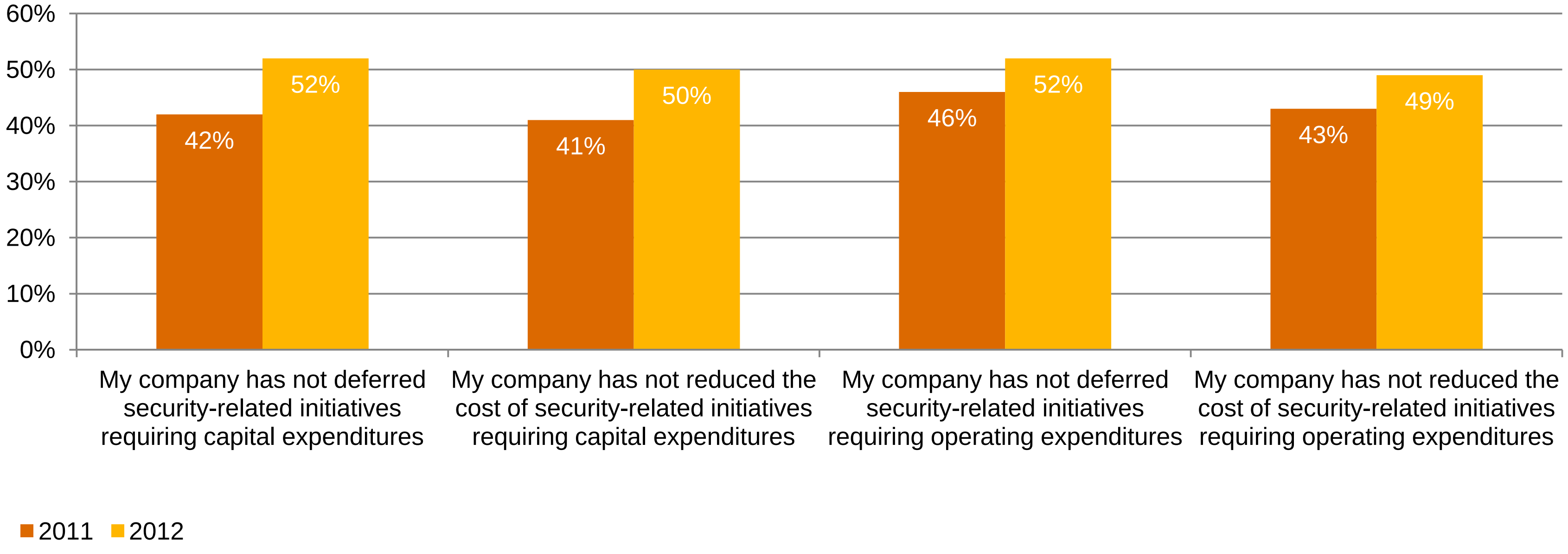
Some key elements of security show substantial degradation from earlier highs.



Question 32: "Which of the following elements, if any, are included in your organization's security policy?"

A&D respondents are optimistic about security spending over the next 12 months.

53% of A&D respondents expect security budgets to increase in the year ahead. More encouragingly, respondents report fewer deferrals and fewer budget cutbacks for security initiatives. Compared with last year, for instance, 22% more respondents say they have not cut capital expenditures for security programs.



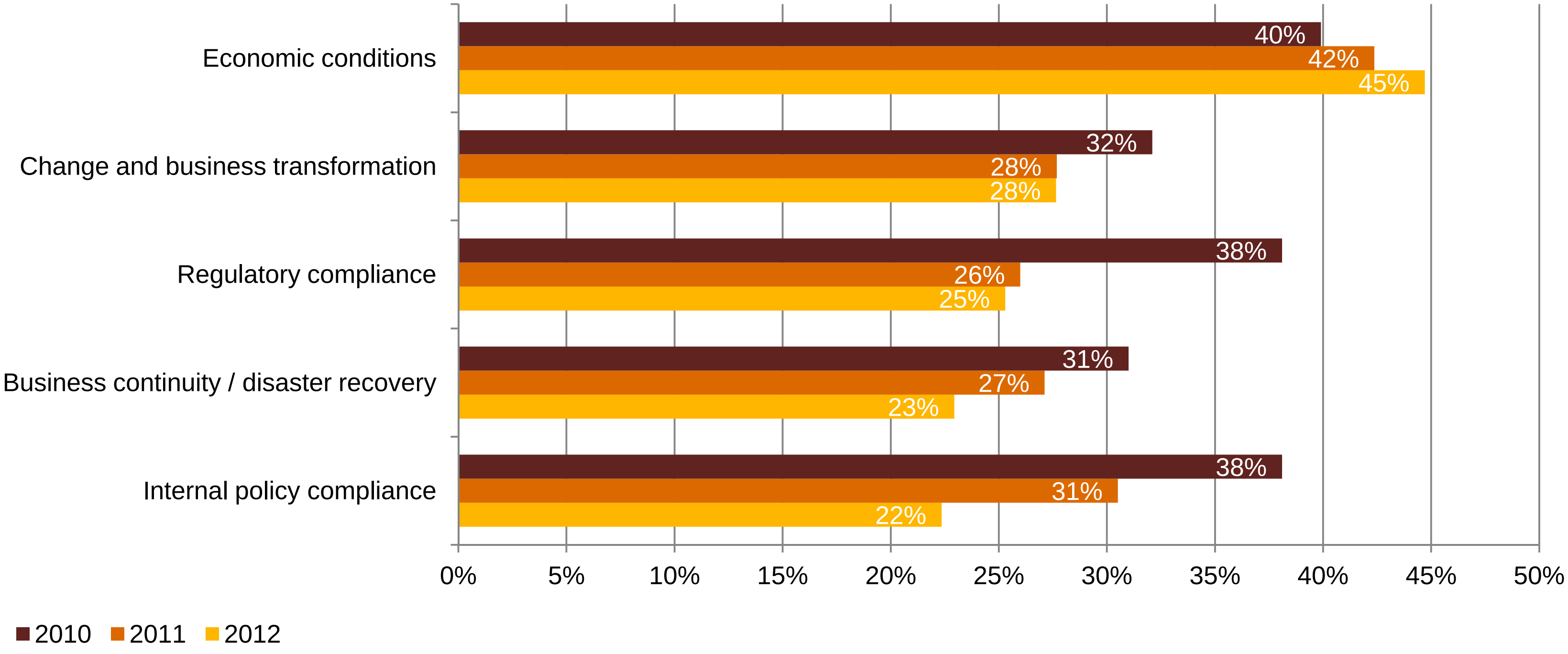
Question 8: “When compared with last year, security spending over the next 12 months will:” Questions 9A and 10A: “Has your company deferred capital and operating security-related initiatives?” Questions 9B and 10B: “Has your company reduced the capital and operating cost of security-related initiatives?”

Section 3

A game of risk

Security budgets are not driven by security needs.

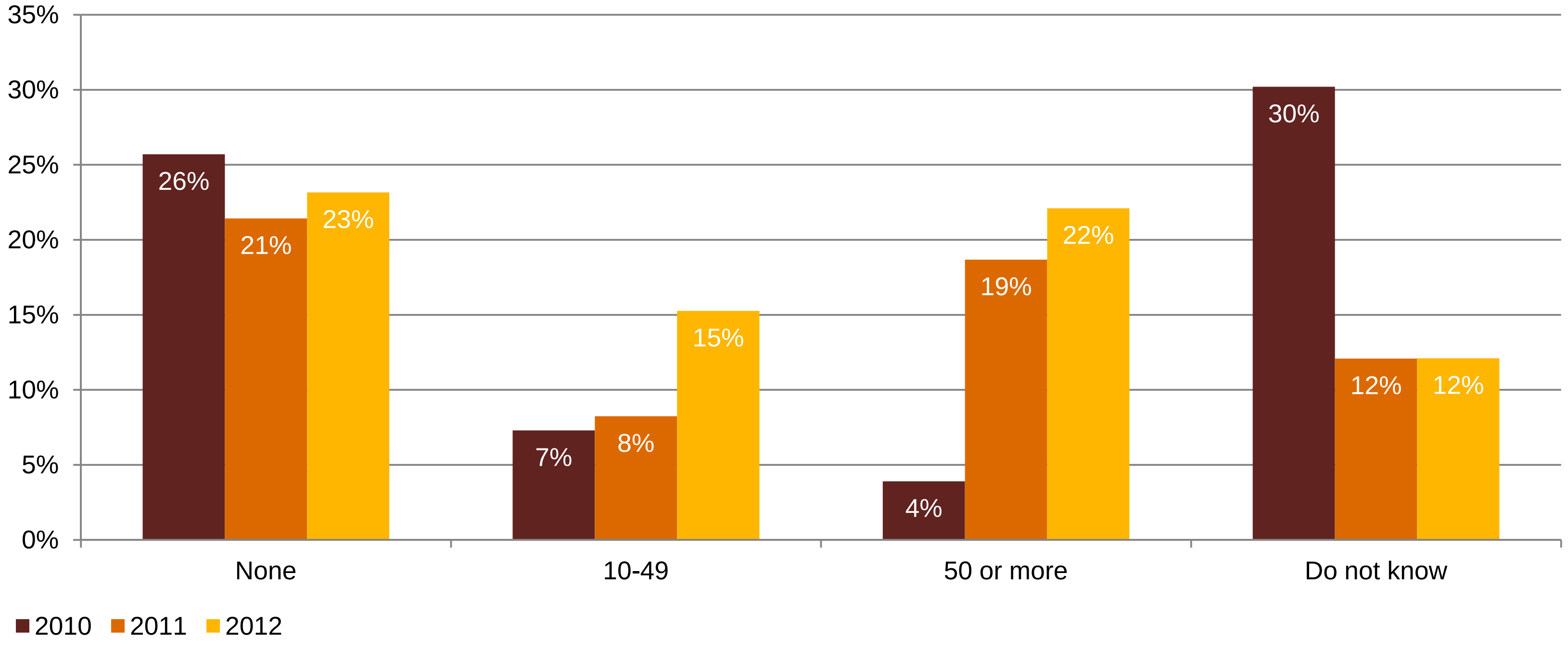
Economic conditions rank as the top driver of security spending for A&D respondents – an increase over recent years and a risky way to set priorities. One in four cite regulatory compliance as an important factor in spending.



Question 37: "What business issues or factors are driving your company's information security spending?" (Not all factors shown.)

Reported security incidents are on the rise.

The number of respondents reporting the most numerous category of security incidents – 50 or more per year – jumped 16% over 2011 and 450% over 2010. Those reporting 10-49 incidents almost doubled over last year.



Question 17: “Number of security incidents in the past 12 months.”

Just 55% of respondents have security training programs for employees.

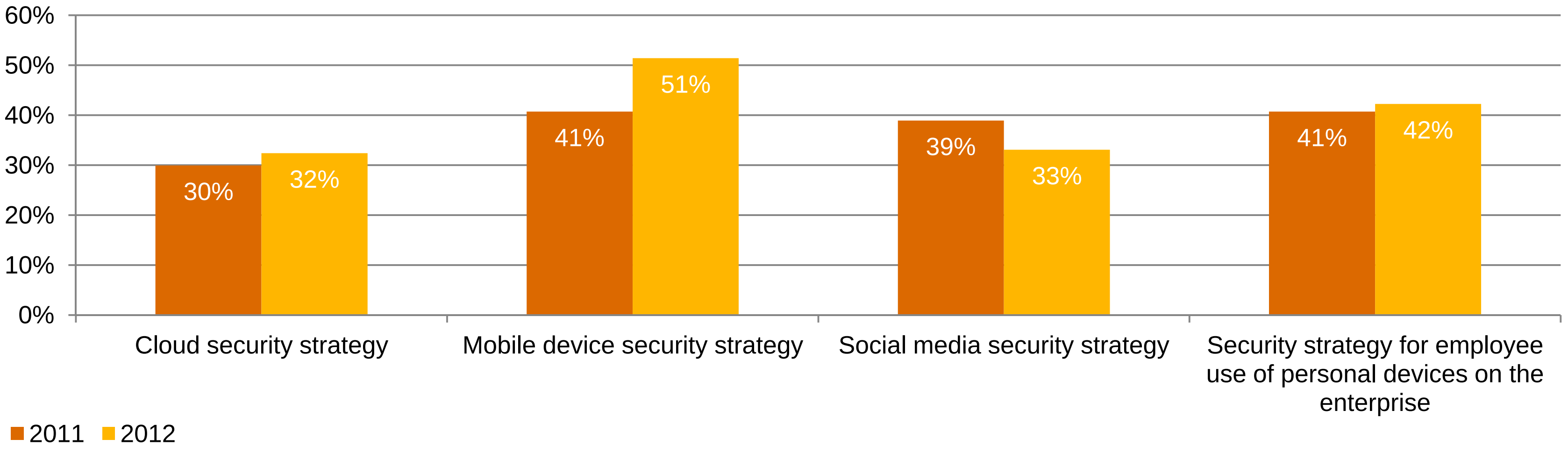
No security program can be effective without adequate training, yet only 55% of A&D respondents have an employee security awareness training program in place. Even fewer have staff dedicated to security awareness.

Information security safeguards	2009	2010	2011	2012
Have employee security awareness training program	69%	59%	43%	55%
Have people dedicated to employee awareness programs	73%	64%	57%	49%

Question 14: “What process information security safeguards does your organization currently have in place?” Question 13: “What information security safeguards related to people does your organization have in place?”

Technology adoption is moving faster than security implementation.

A&D respondents report some progress in implementing security strategies for mobility, social media, cloud computing, and use of employee-owned devices. But the numbers still lag adoption of the technologies themselves. We have found, for instance, that 88% of consumers use a personal mobile device for both personal and work purposes.[1]

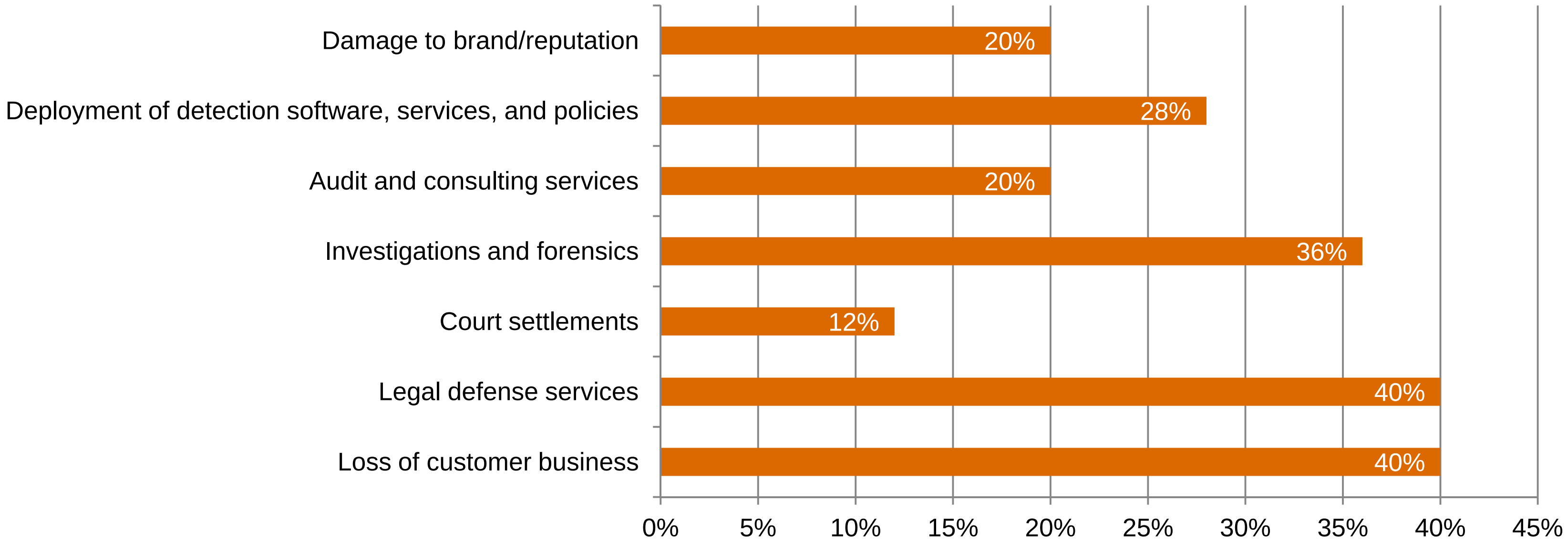


Question 14: “What process information security safeguards does your organization currently have in place?”

[1] PwC, Consumer privacy: What are consumers willing to share? July 2012

An inadequate assessment of security incidents can lead to a less-clear understanding of their impact.

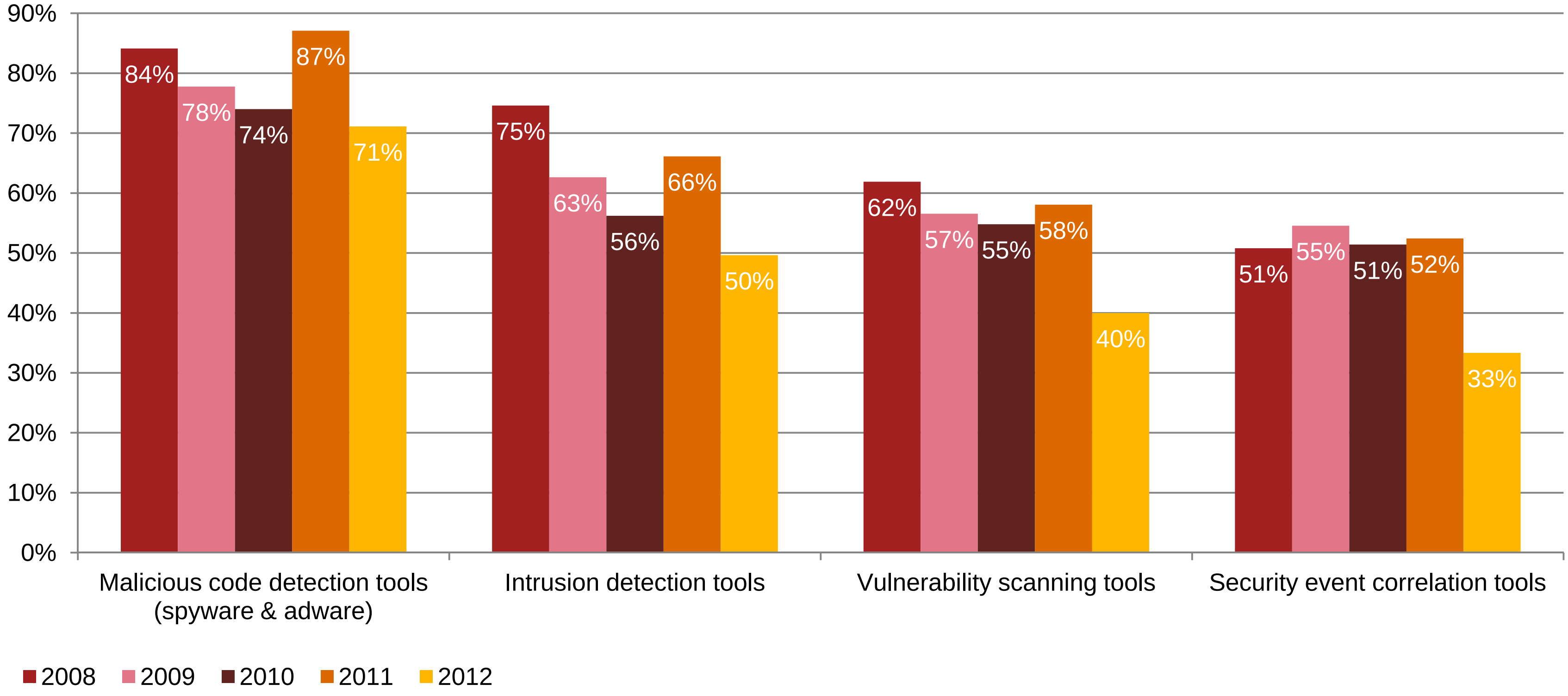
A&D respondents report a lower incidence of financial losses from security incidents than last year, yet many do not apply thorough or consistent analysis when appraising those costs. For example, only 20% consider damage to brand/reputation, while 40% factor in legal costs.



Question 21: “How was your organization impacted by the security incident?” Question 21C: “What factors are included in your company’s calculation of these financial losses?”

Use of some key technology safeguards resumed a long-term decline after last year's uptick.

Deployment of essential information security and privacy tools has atrophied over time.



Question 15: "What technology information security safeguards related to detection does your organization have in place?"

Section 4

It’s how you play the game

What keeps security from being what it should be?

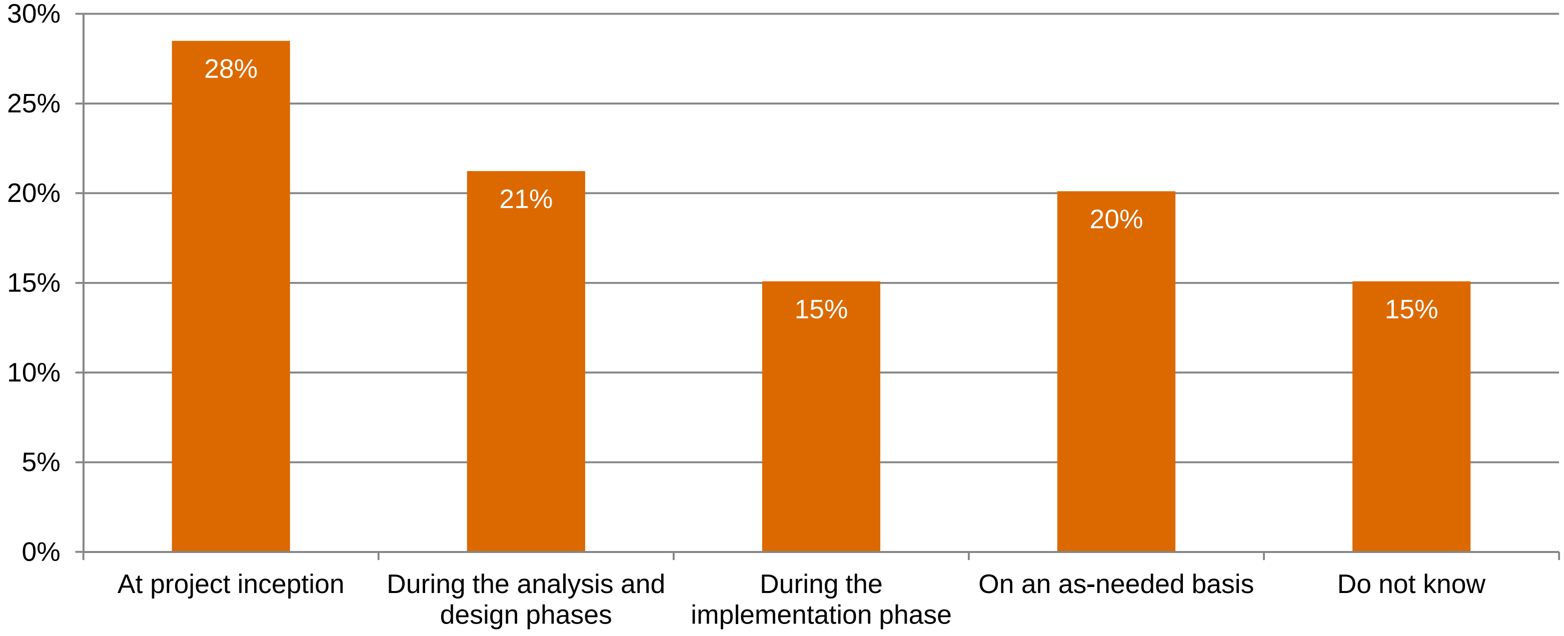
Company leadership is seen as less an obstacle than in the past, although 61% of respondents still point to C-level executives and Boards. A lack of capital funding and inadequate vision continue to be top concerns.

	2011	2012
Leadership – CEO, President, Board, or equivalent	29%	23%
Leadership – CIO or equivalent	21%	21%
Leadership – CISO, CSO, or equivalent	20%	17%
Insufficient capital expenditures	27%	24%
Lack of an actionable vision or understanding	25%	22%
Lack of an effective information security strategy	26%	20%
Absence or shortage of in-house technical expertise	22%	18%

Question 29: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?"

Security is not always baked into major projects from the beginning.

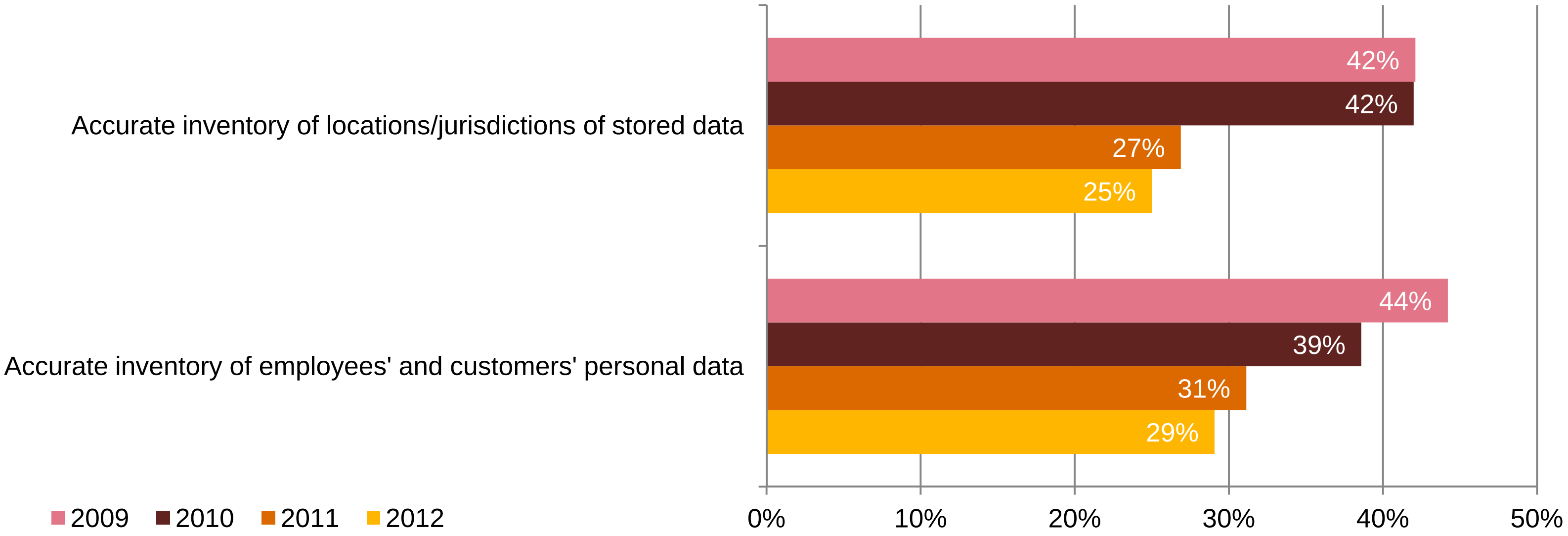
More than one-third of respondents involve security only during the implementation phase or on an as-needed basis.



Question 30: “When does information security become involved in major projects?”

A&D respondents know less about their data now than they did three years ago.

While approximately 80% of respondents say protecting customer and employee data is important, far fewer understand what that data entails and where it is stored. This is significant because, increasingly, consumers want to be in control of their personal data and "turn off" the flow of information from companies.[2]



Question 38: "What level of importance does your company place on protecting the following types of information?" Question 11: "Which data privacy safeguards does your organization have in place?"

[2] PwC, Consumer privacy: What are consumers willing to share? July 2012

What you can do to improve your performance.

Information security today is a rapidly evolving game of advanced skill and strategy. As a result, the security models of the past decade are no longer effective.

Effective security requires a new way of thinking. The very survival of the business demands that security leaders understand, prepare for, and quickly respond to security threats.

Businesses seeking to strengthen their security practice must:

- Implement a comprehensive risk-assessment strategy and align security investments with identified risks.
- Understand their organization's information, who wants it, and what tactics adversaries might use to get it.
- Understand that information security requirements – and, indeed, overall strategies for doing business – have reached a turning point.
- Embrace a new way of thinking in which information security is both a means to protect data as well as an opportunity to create value to the business.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
949.437.5380
gary.loveland@us.pwc.com

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

US Aerospace & Defense Contacts

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

John Pearce
Director
703.346.9071
john.pearce@us.pwc.com

Or visit www.pwc.com/giss2013

PwC

www.pwc.com/security

Changing the game

While tight budgets have forestalled updates to security programs, many businesses are confident they're winning the game. But the rules – and the players – have changed.

CIO Business Technology Leadership

CSO Business Risk Leadership

Automotive

Key findings from The Global State of Information Security® Survey 2013

September 2012

pwc

> ***“You can’t succeed in today’s elevated threat environment if you don’t know the players and you don’t know the rules.”***
>
> ***– Gary Loveland, Principal, PwC***

Information security has always been a high-stakes game. One that demands a smart strategy, the right technology moves, and an unblinking eye on adversaries.

For many businesses, however, it has become a pursuit that is daunting to achieve. That’s because the rules have changed, and opponents—old and new—are armed with expert technology skills. As a result, the risks are greater than ever.

Businesses are fighting back by adopting new detection and prevention techniques. At the same time, governments around the world are enacting legislation to combat the increasing cyber threats. And regulatory bodies are issuing new guidance on disclosure obligations for cyber risks and incidents.

Yet risks to data security continue to intensify – and show no signs of abating. Those keeping score agree that the bad guys appear to be in the lead.

Nonetheless, many businesses believe they are winning. The Global State of Information Security® Survey 2013 shows that most executives in the global automotive industry are confident in the effectiveness of their information security practices. They believe their strategies are sound and many consider themselves to be leaders in the field.

The odds, however, are not in their favor: Diminished budgets have resulted in degraded security programs, reported incidents are on the rise, and new technologies are being adopted faster than they can be safeguarded.

Given today's elevated threat environment, businesses can no longer afford to play a game of chance. They must prepare to play a new game, one that requires advanced levels of skill and strategy to win.

Agenda

Section 1. Methodology

Section 2. A game of confidence

Section 3. A game of risk

Section 4. It’s how you play the game

Section 1

Methodology

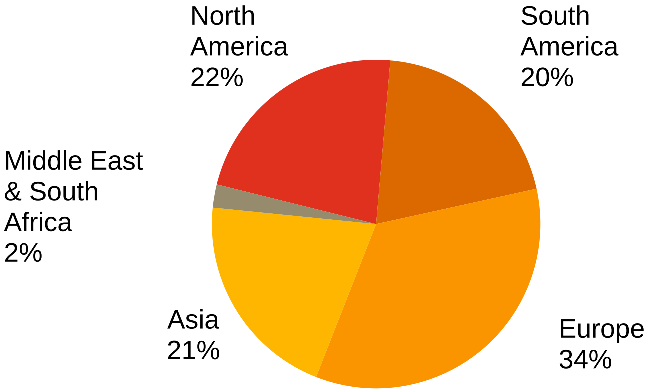
A worldwide study

The Global State of Information Security® Survey 2013, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 1, 2012 to April 15, 2012.

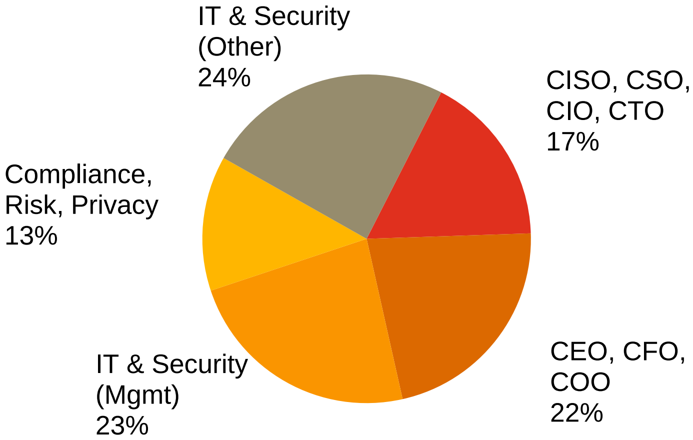
- PwC’s 15th year conducting the online survey, 10th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 128 countries
- More than 9,300 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-three percent (33%) of respondents from companies with revenue of $500 million+
- Survey included 218 respondents from the automotive industry
- Margin of error less than 1%

Demographics

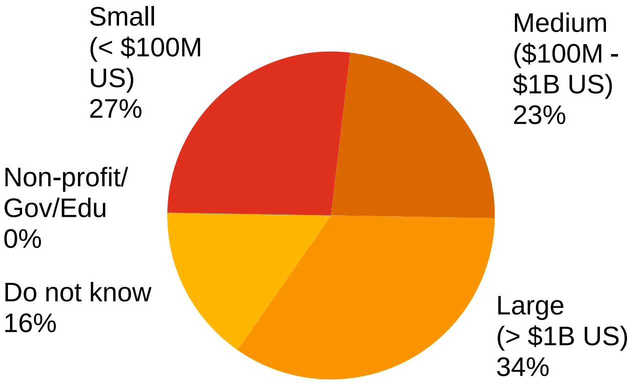
Automotive respondents by region of employment



Automotive respondents by title



Automotive respondents by company revenue size



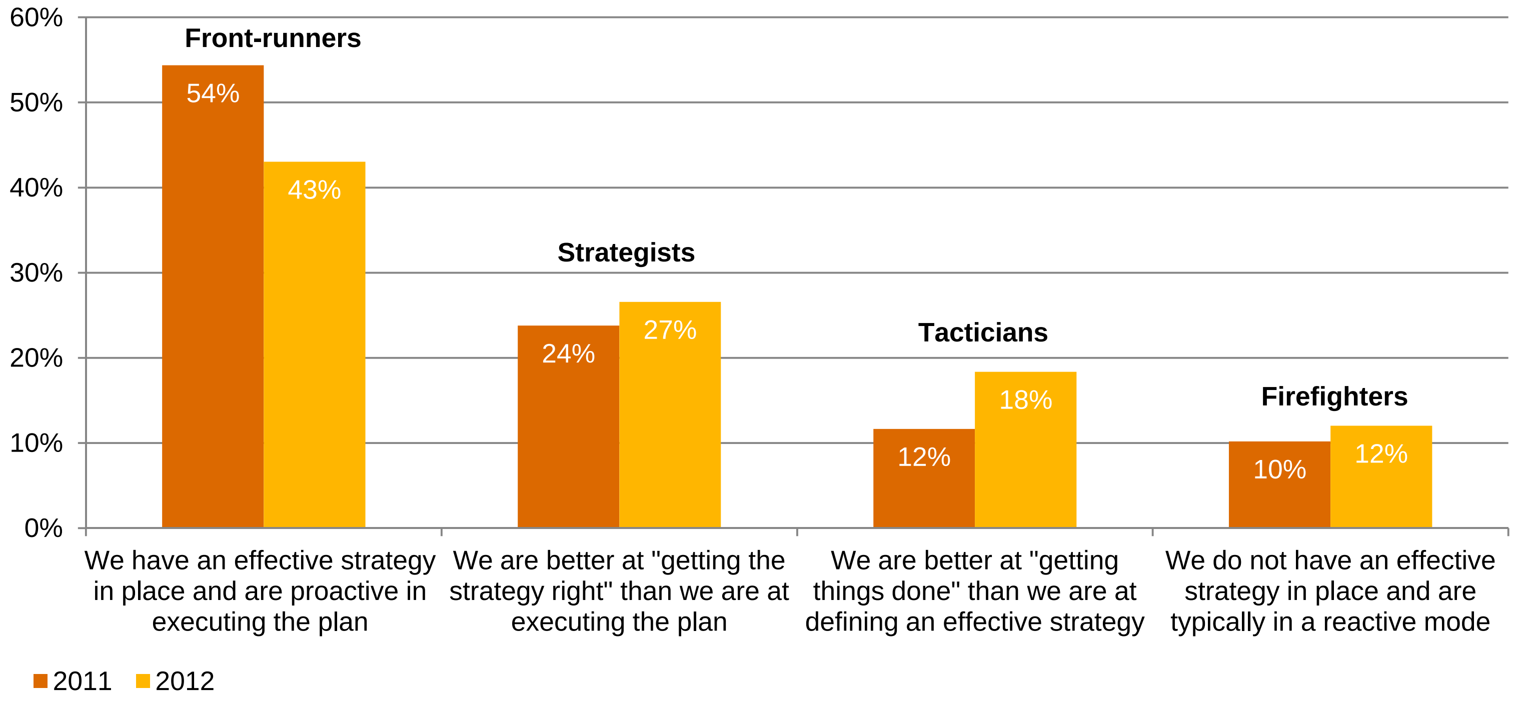
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

A game of confidence

While automotive respondents are confident in their security practices, fewer rank themselves at the top.

This year 43% of industry respondents say their organization has a strategy in place and is proactive in executing it – down from 54% in 2011.



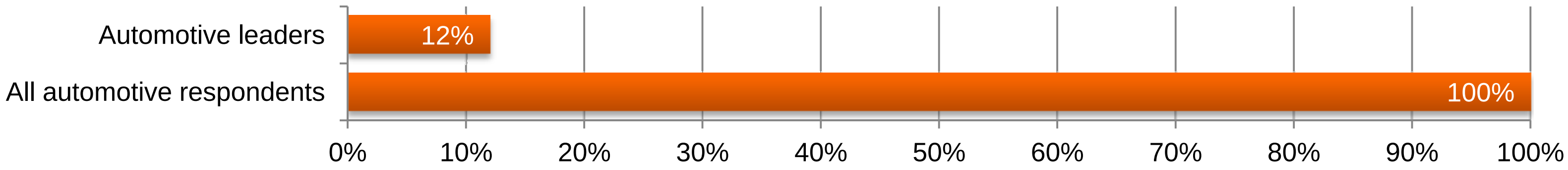
Question 28: "Which category below best characterizes your organization’s approach to protecting information security?"

A reality check on real leaders.

But are they really leaders? We measured automotive industry respondents' self-appraisal against four key criteria to define leadership. To qualify, organizations must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the "top of the house" (e.g., to the CEO, CFO, COO, or legal counsel)
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

The result? Our analysis found that 12% of automotive respondents rank as leaders.

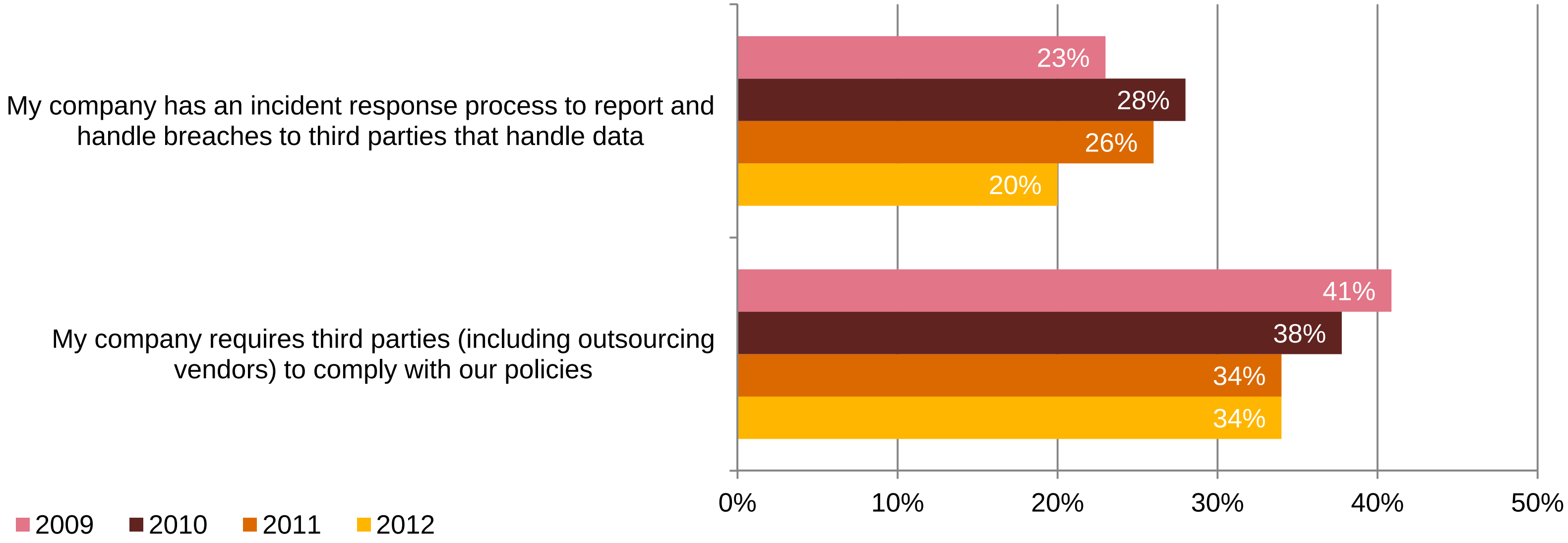


One notable finding is that 36% of automotive respondents report zero security incidents in the past year.

Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 18: "What types of security incidents (breach or downtime) occurred" and Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?" Question 17: "Number of security incidents in the past 12 months."

Many automotive industry respondents are over-confident in their organization's security program.

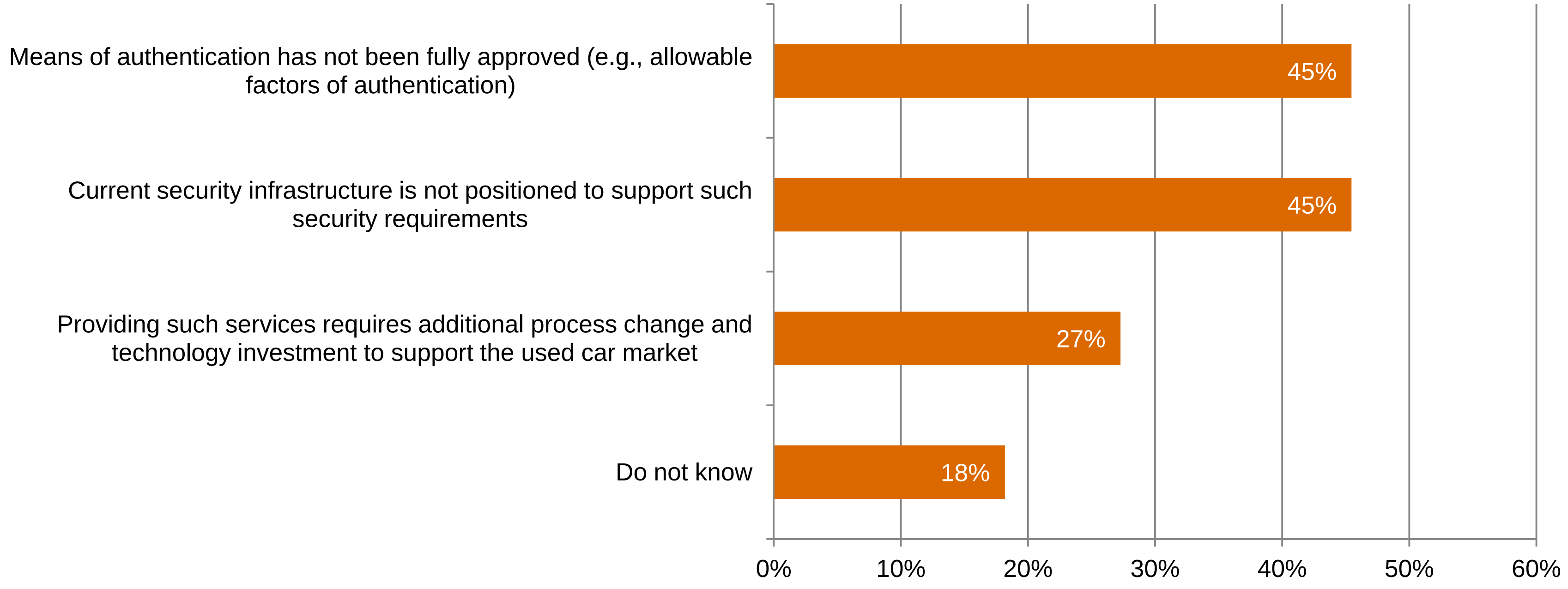
72% of respondents are confident that they have instilled effective security behaviors into their organization's culture, yet many do not have a process in place to handle third-party breaches. What's more, only 22% conduct compliance audits of third parties that handle data. This suggests a troubling gap in perception.



Question 35: "How confident are you that your organization has instilled effective information security behaviors into the organizational culture?"
Question 11: "Which data privacy safeguards does your organization have in place?"

Many automotive respondents are not prepared to handle customer data from in-vehicle information services.

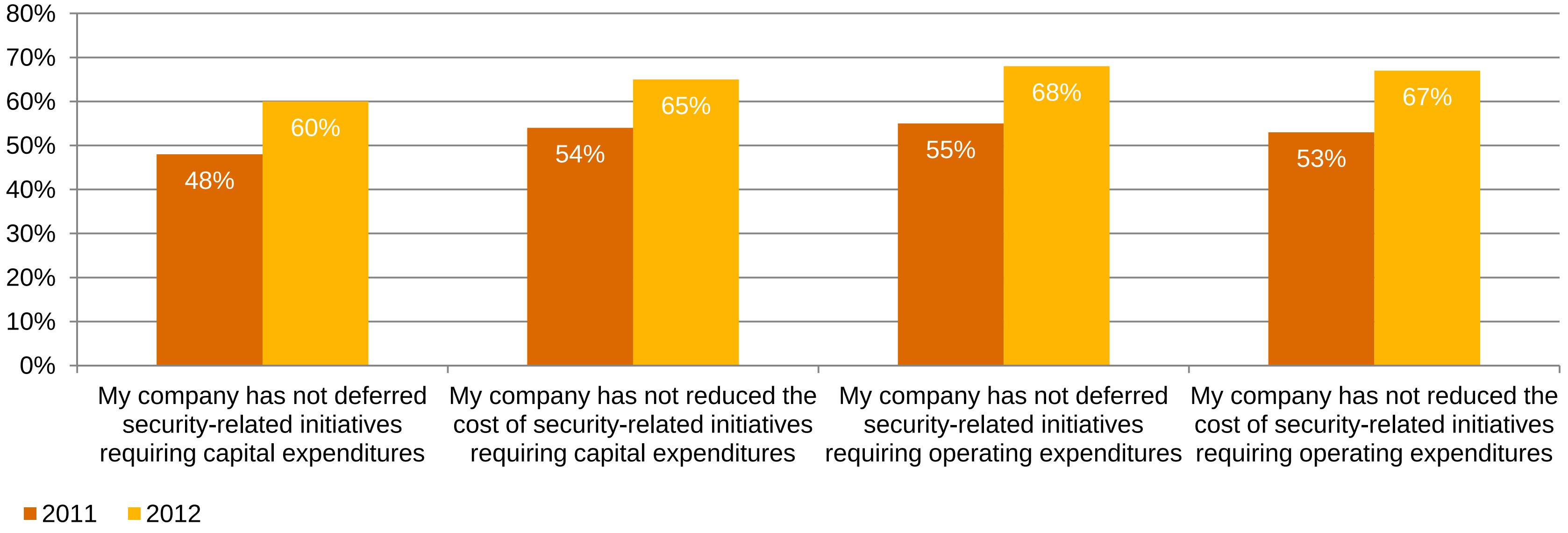
Telematics is expanding to on-the-go communications. Yet 43% of automotive respondents say they are not ready to secure this data or do not know if they can secure it. Many cite authentication and security infrastructure as top obstacles, as detailed below.



(Asked only of Automotive respondents) Question 4: “Is your organization positioned to securely provide these new technology services? Select all that apply.” Question 4A (Automotive): “Why is your organization not positioned to securely provide these services?”

Automotive respondents are cautiously optimistic about security spending over the next 12 months.

54% of industry respondents expect security budgets to increase in the year ahead and 27% say spending will stay the same as last year. Encouragingly, they report fewer deferrals and fewer budget cutbacks for security initiatives. Compared with last year, for instance, 20% more respondents say they had not cut capital spending for security.



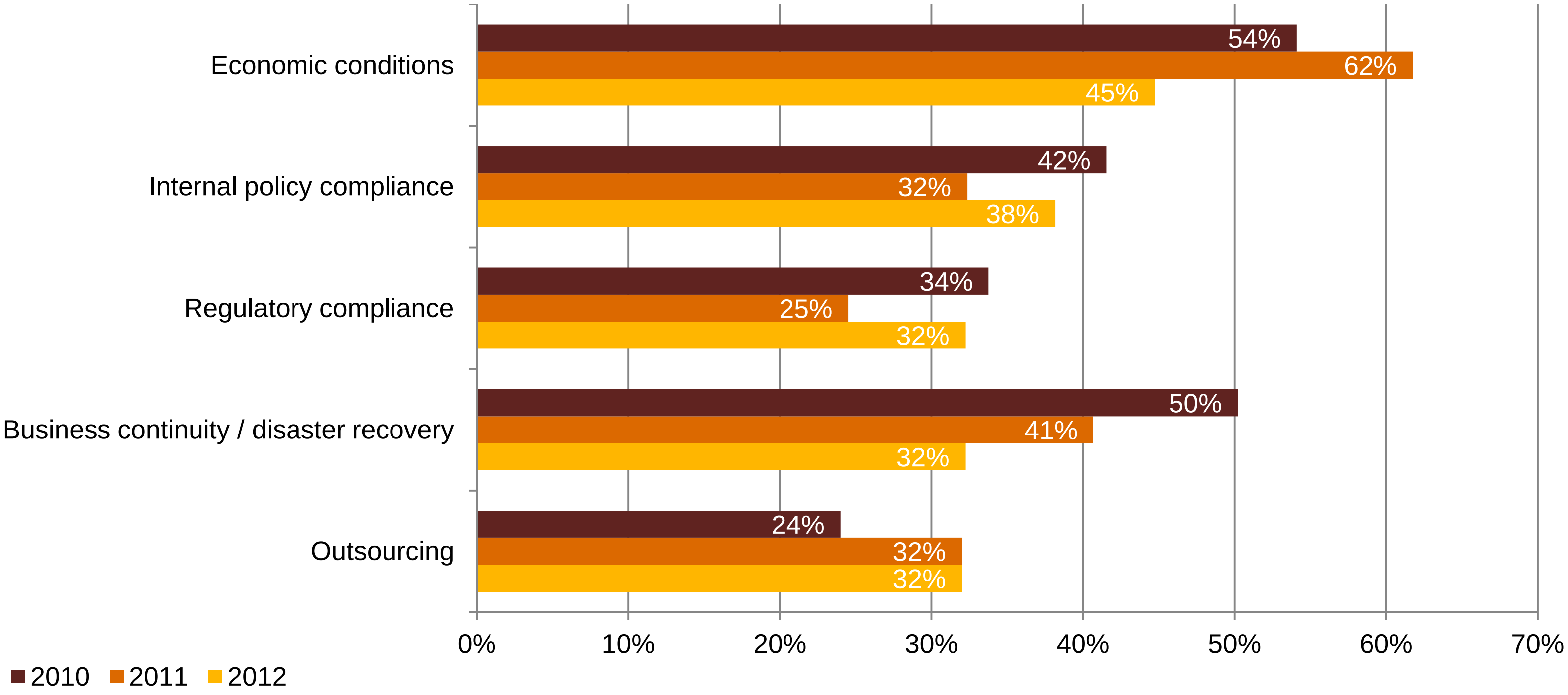
Question 8: “When compared with last year, security spending over the next 12 months will:” Questions 9A and 10A: “Has your company deferred capital and operating security-related initiatives?” Questions 9B and 10B: “Has your company reduced the capital and operating cost of security-related initiatives?”

Section 3

A game of risk

Security budgets are not driven by security needs.

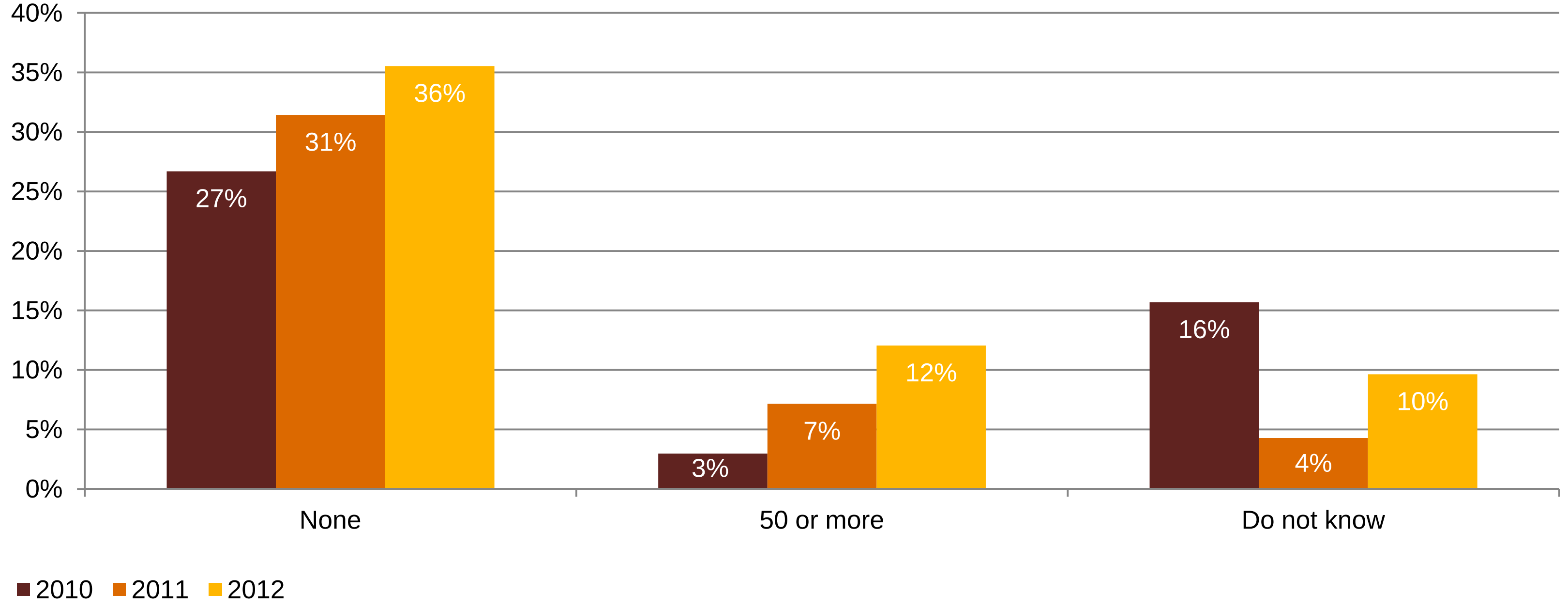
Economic conditions remain the leading driver of security spending, cited by 45% of respondents. Internal and external compliance were also top considerations, followed by business continuity/disaster recovery.



Question 37: “What business issues or factors are driving your company's information security spending?” (Not all factors shown.)

The frequency of reported security incidents is on the rise.

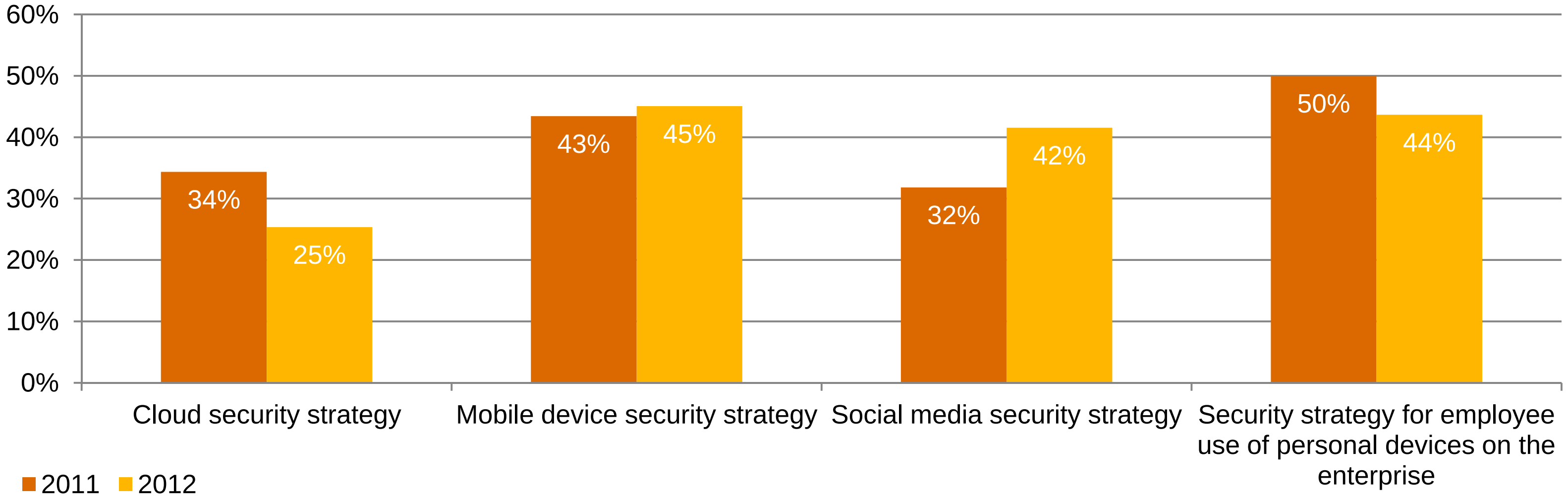
The number of respondents reporting the most numerous category of security incidents – 50 or more per year – soared 71% compared with last year. Those who do not know the number of incidents is also up dramatically, an alarming uncertainty that suggests ineffective security practices.



Question 17: “Number of security incidents in the past 12 months.”

Technology adoption is moving faster than security implementation.

As with many industries, automotive companies are struggling to keep pace with the adoption of cloud computing, social networking, mobility, and use of employee-owned devices. These new technologies often are not included in overall security plans even though they are widely used. We have found, for instance, that 88% of consumers use a personal mobile device for both personal and work purposes.[1]

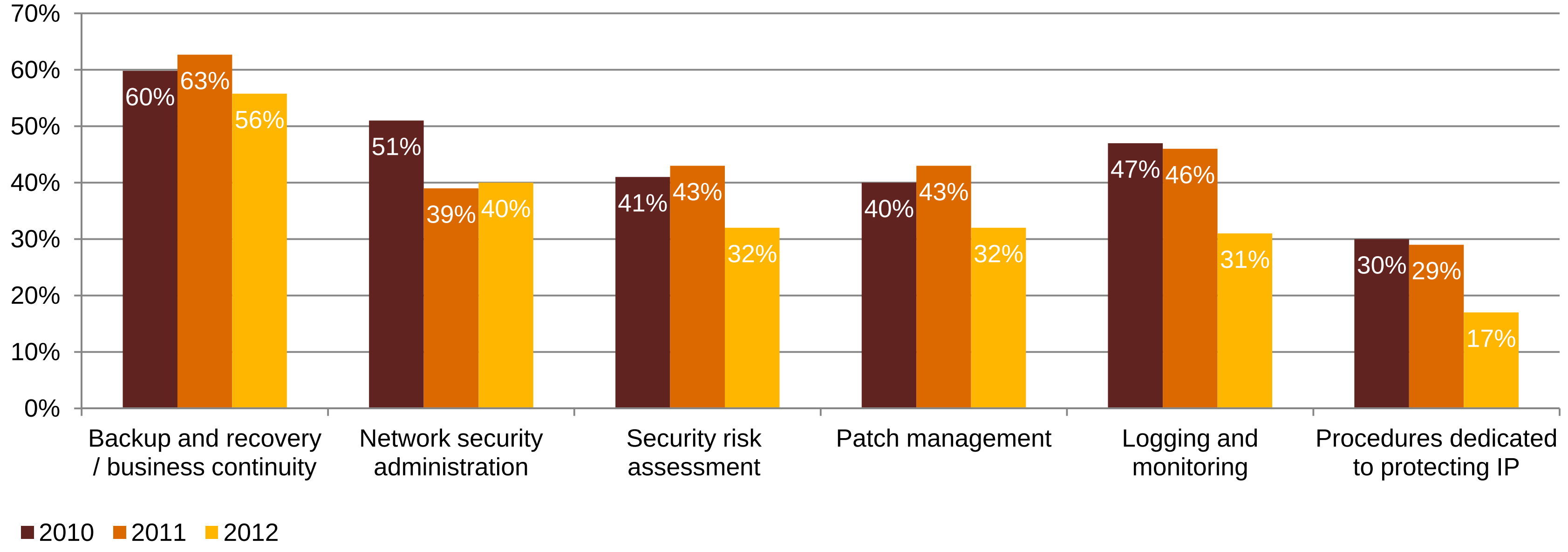


Question 14: “What process information security safeguards does your organization currently have in place?”

[1] PwC, Consumer privacy: What are consumers willing to share? July 2012

Security policies have grown less robust and inclusive.

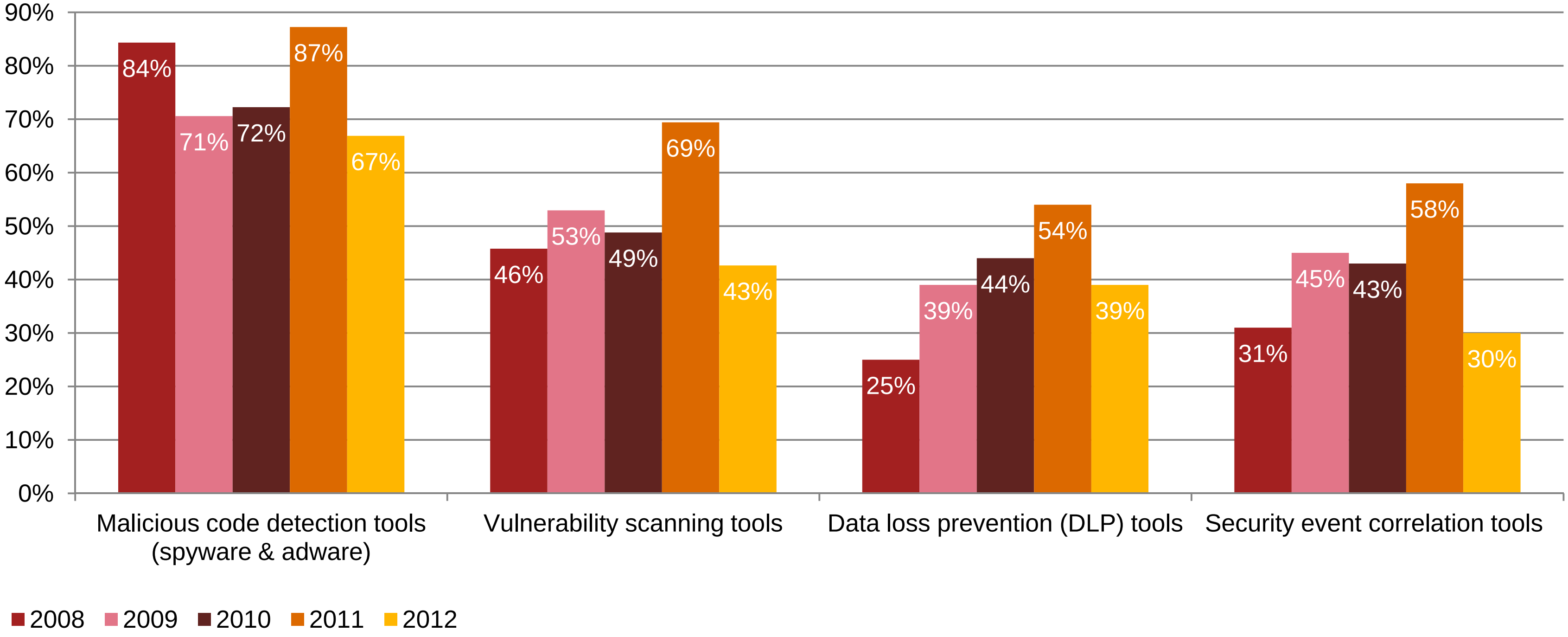
Despite industry trends and historical imperatives, fewer automotive respondents are including fundamental elements of security in their policies. In particular, it is troubling that only 17% of respondents have procedures to protect their intellectual property.



Question 32: “Which of the following elements, if any, are included in your organization’s security policy?”

Use of some key detection safeguards is lower after last year's uptick.

The future looked bright last year as many automotive firms stepped up investments in detection safeguards. This year, however, saw a decrease in use of important security and privacy tools across industries.



Question 15: "What technology information security safeguards related to detection does your organization have in place?"

Section 4

It’s how you play the game

What keeps security from being what it should be?

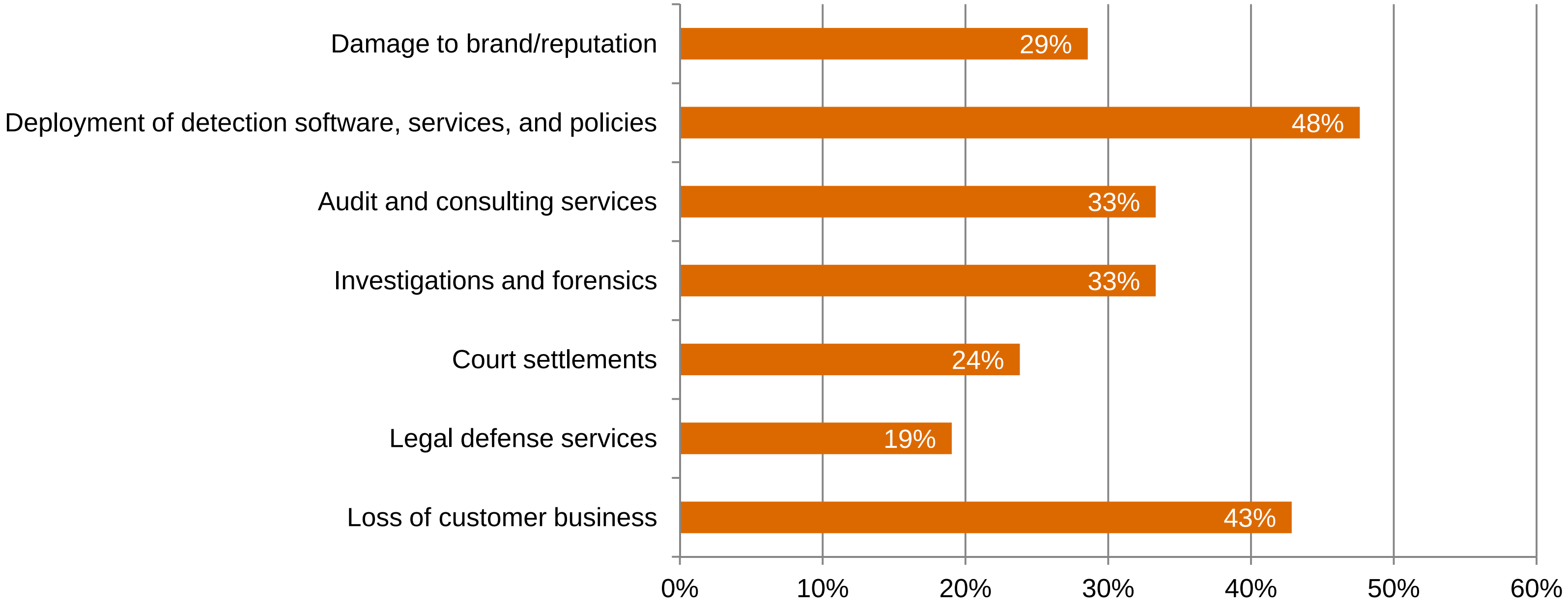
Top-level leadership – the CEO, President, or Board – is perceived to be an obstacle to effective security, according to 23% of respondents. But the most-cited single inhibitor to security is a lack of an actionable vision.

	2011	2012
Lack of an actionable vision or understanding	34%	30%
Leadership – CEO, President, Board, or equivalent	27%	23%
Lack of an effective information security strategy	28%	22%
Absence or shortage of in-house technical expertise	23%	21%
Insufficient operating expenditures	21%	20%
Insufficient capital expenditures	26%	19%

Question 29: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?"

An inadequate assessment of security incidents can lead to a less-clear understanding of their impact.

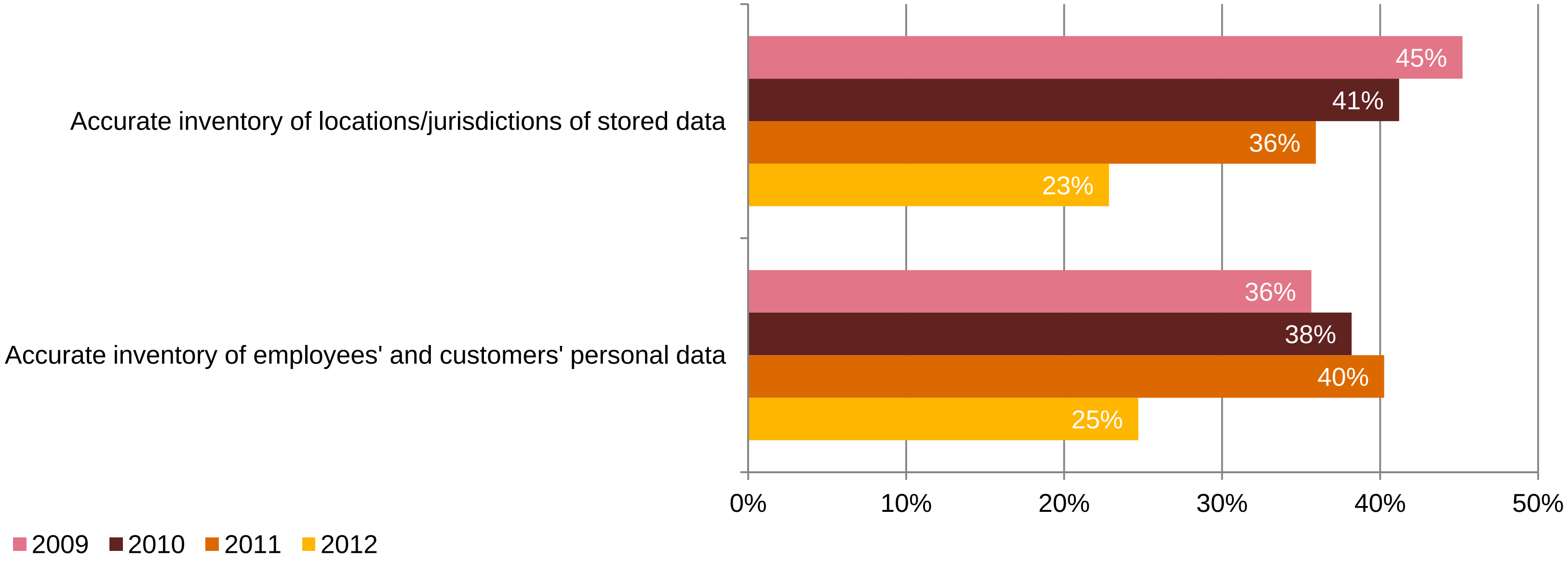
Automotive respondents reported a low impact from security incidents, yet many did not apply thorough or consistent analysis to appraising those costs. For example, only 19% considered legal defense services while 29% factored in damage to brand/reputation.



Question 21: "How was your organization impacted by the security incident?" Question 21C: "What factors are included in your company's calculation of these financial losses?"

Automotive respondents know less about their data now than they did three years ago.

While 88% of respondents say protecting customer and employee data is important, far fewer understand what that data entails and where it is stored. This is significant because, increasingly, consumers want to be in control of their personal data and “turn off” the flow of information from companies.[2]



Question 38: “What level of importance does your company place on protecting the following types of information?” Question 11: “Which data privacy safeguards does your organization have in place?”

[2] PwC, Consumer privacy: What are consumers willing to share? July 2012

What you can do to improve your performance.

Information security today is a rapidly evolving game of advanced skill and strategy. As a result, the security models of the past decade are no longer effective.

Effective security requires a new way of thinking. The very survival of the business demands that security leaders understand, prepare for, and quickly respond to security threats.

Businesses seeking to strengthen their security practice must:

- Implement a comprehensive risk-assessment strategy and align security investments with identified risks.
- Understand their organization's information, who wants it, and what tactics adversaries might use to get it.
- Understand that information security requirements – and, indeed, overall strategies for doing business – have reached a turning point.
- Embrace a new way of thinking in which information security is both a means to protect data as well as an opportunity to create value to the business.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
949.437.5380
gary.loveland@us.pwc.com

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

US Automotive Contacts

Brian Decker
Partner
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/giss2013

www.pwc.com/security

Changing the game

While tight budgets have forestalled updates to security programs, many businesses are confident they're winning the game. But the rules – and the players – have changed.

Oil & Gas

Key findings from The Global State of Information Security® Survey 2013

September 2012

> *"You can't succeed in today's elevated threat environment if you don't know the players and you don't know the rules."*
>
> *- Gary Loveland, Principal, PwC*

Information security has always been a high-stakes game. One that demands a smart strategy, the right technology moves, and an unblinking eye on adversaries.

For many businesses, however, it has become a pursuit that is almost impossible to win. That's because the rules have changed, and opponents—old and new—are armed with expert technology skills. As a result, the risks are greater than ever.

Businesses are fighting back by adopting new detection and prevention technologies. At the same time, governments around the world are enacting legislation to combat cyber threats. And regulatory bodies are issuing new guidance on disclosure obligations for cyber incidents.

Yet risks to data security continue to intensify – and show no signs of abating. Those keeping score agree that the bad guys appear to be in the lead.

Nonetheless, many businesses believe they are winning. The Global State of Information Security® Survey 2013 shows that most executives in the global oil and gas (O&G) industry are confident in the effectiveness of their information security practices. They believe their strategies are sound and many consider themselves to be leaders in the field.

The odds, however, are not in their favor: Diminished budgets have resulted in degraded security programs, reported security incidents are on the rise, and new technologies are being adopted faster than they can be safeguarded.

Given today's elevated threat environment, businesses can no longer afford to play a game of chance. They must prepare to play a new game, one that requires advanced levels of skill and strategy to win.

Agenda

Section 1. Methodology

Section 2. A game of confidence

Section 3. A game of risk

Section 4. It’s how you play the game

Section 1

Methodology

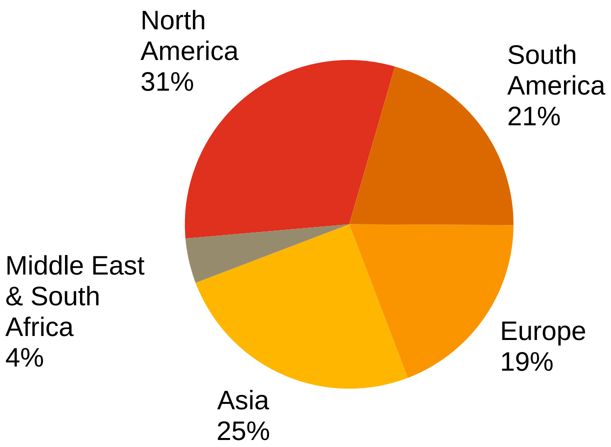
A worldwide study

The Global State of Information Security® Survey 2013, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 1, 2012 to April 15, 2012.

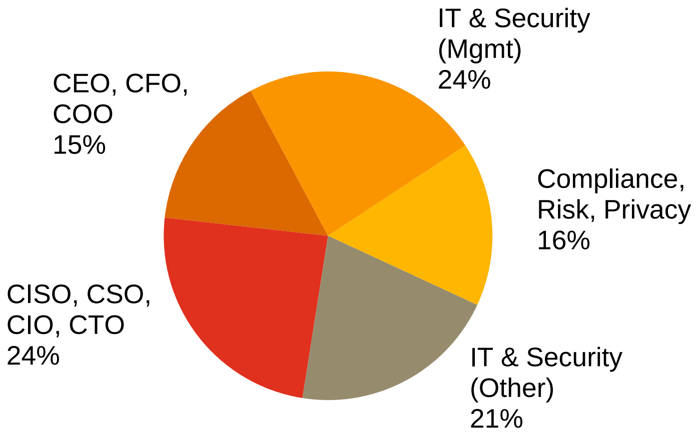
- PwC's 15th year conducting the online survey, 10th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 128 countries
- More than 9,300 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-three percent (33%) of respondents from companies with revenue of $500 million+
- Survey included 136 respondents from the oil and gas industry
- Margin of error less than 1%

Demographics

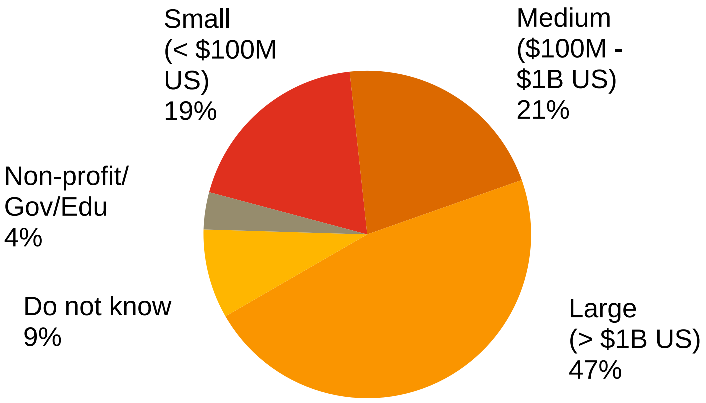
O&G respondents by region of employment



O&G respondents by title



O&G respondents by company revenue size



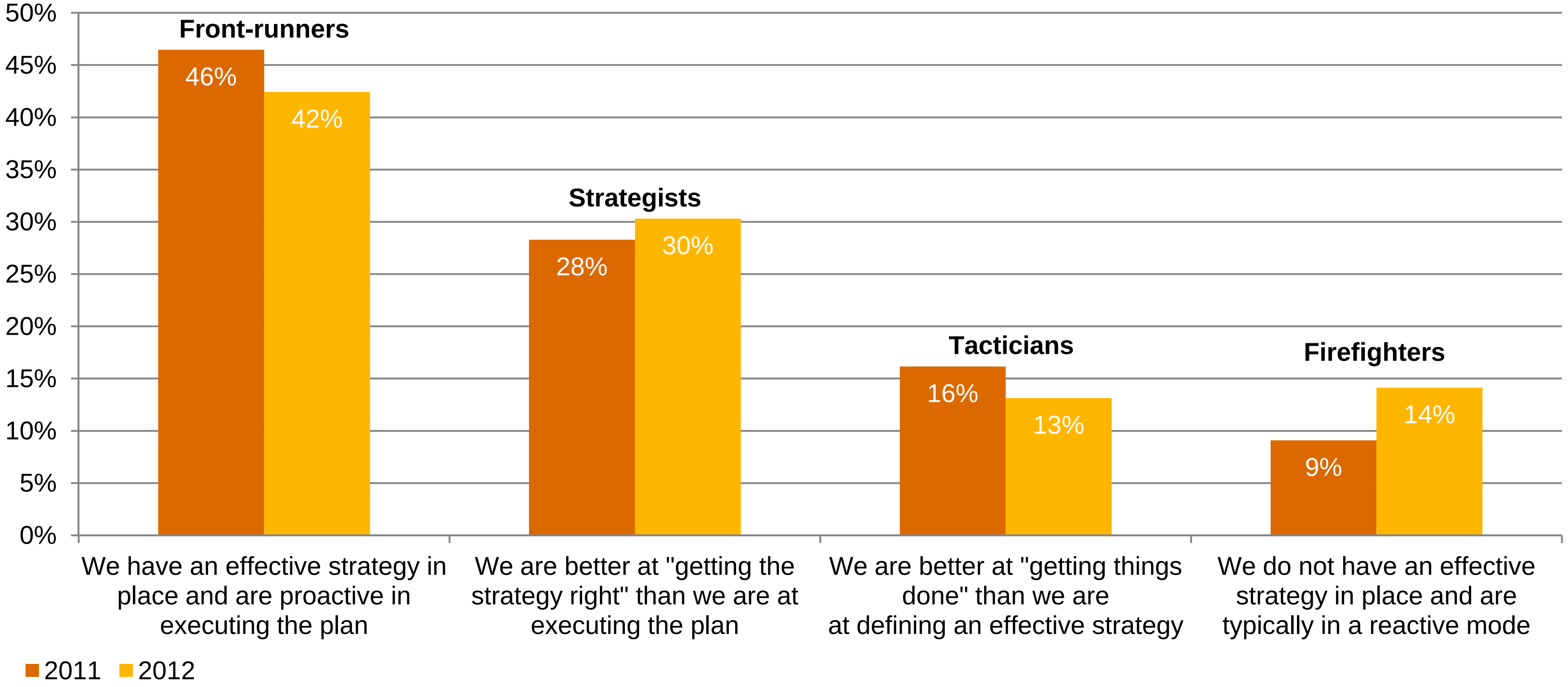
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

A game of confidence

O&G respondents are confident in their security practices.

42% of O&G respondents say their organization has a strategy in place and is proactive in executing it – exhibiting two distinctive attributes of a leader.



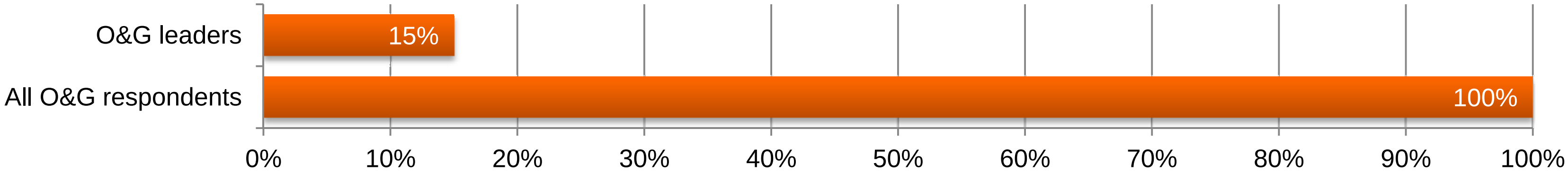
Question 28: "Which category below best characterizes your organization's approach to protecting information security?"

A reality check on real leaders.

But are they really leaders? We measured O&G respondents' self-appraisal against four key criteria to define leadership. To qualify, organizations must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the "top of the house" (e.g., to the CEO, CFO, COO, or legal counsel)
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

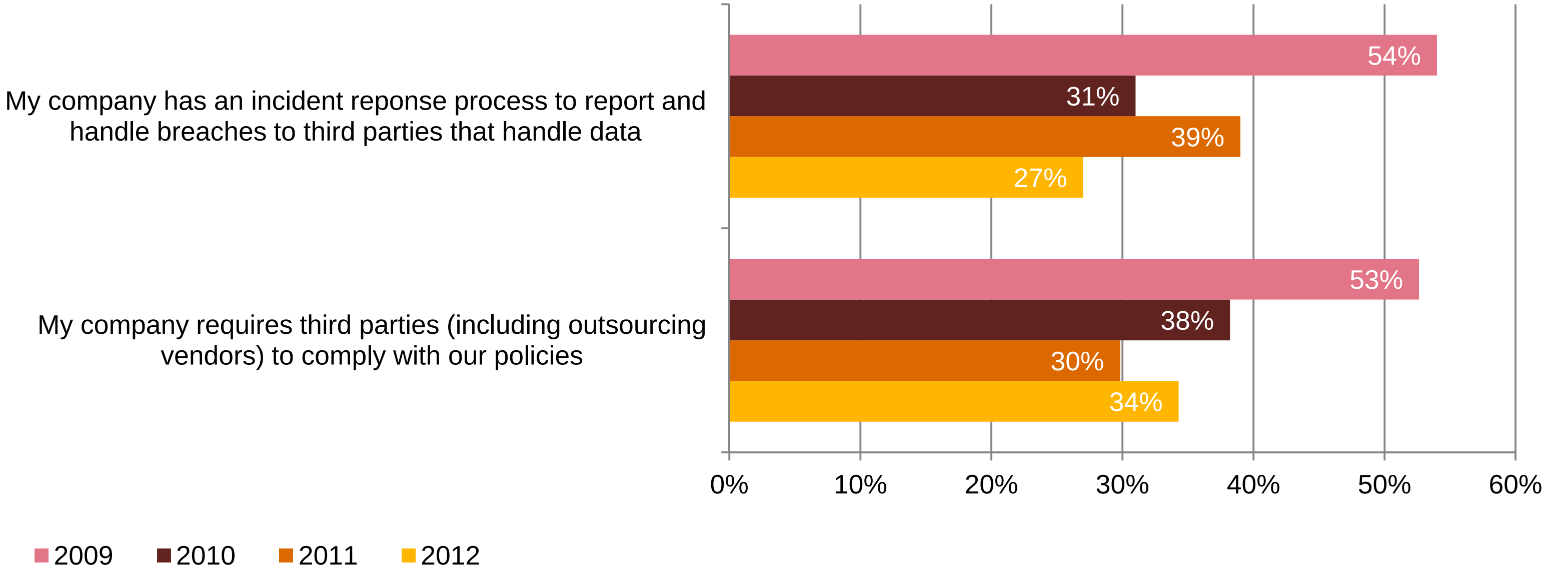
The result? Our analysis found that 15% of O&G respondents rank as leaders.



Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 18: "What types of security incidents (breach or downtime) occurred" and Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Many O&G respondents are over-confident in their organization's security program.

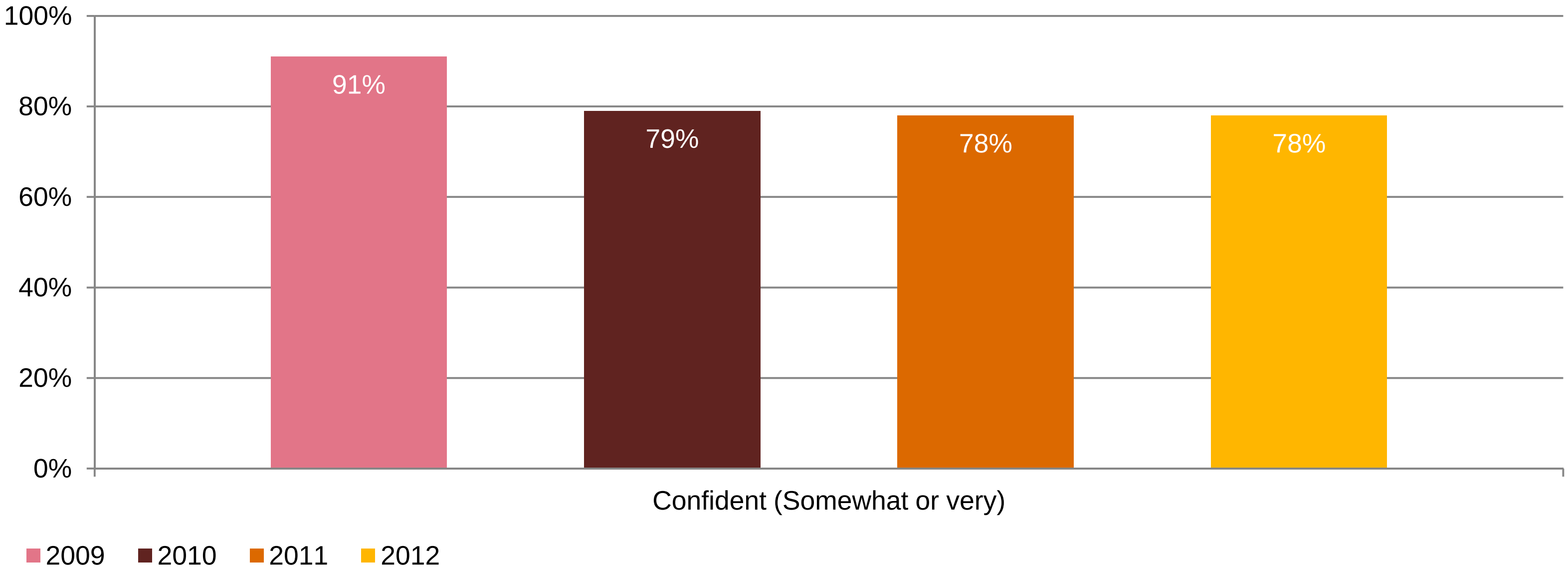
76% of respondents are confident that they have instilled effective security behaviors into their organization's culture, yet most do not have a process in place to handle third-party breaches. What's more, only one-third require third parties to comply with privacy policies. This suggests a troubling gap in perception.



Question 35: "How confident are you that your organization has instilled effective information security behaviors into the organizational culture?"
Question 11: "Which data privacy safeguards does your organization have in place?"

Most respondents say their information security activities are effective, but confidence is eroding.

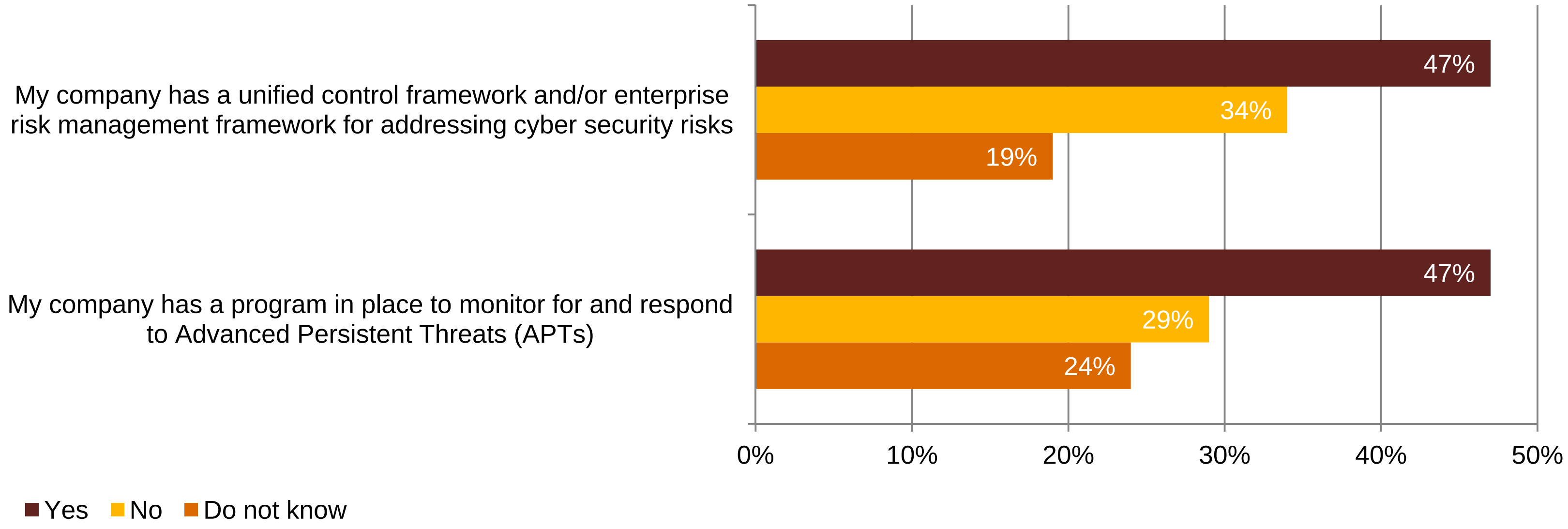
Confidence is a good thing. A strong 78% of O&G respondents say they are confident that their company’s security activities are effective, but many may not realize that assurance has dropped since 2009.



Question 41: “How confident are you that your organization’s information security activities are effective?”

O&G is trying to catch up to known cyber-security problems.

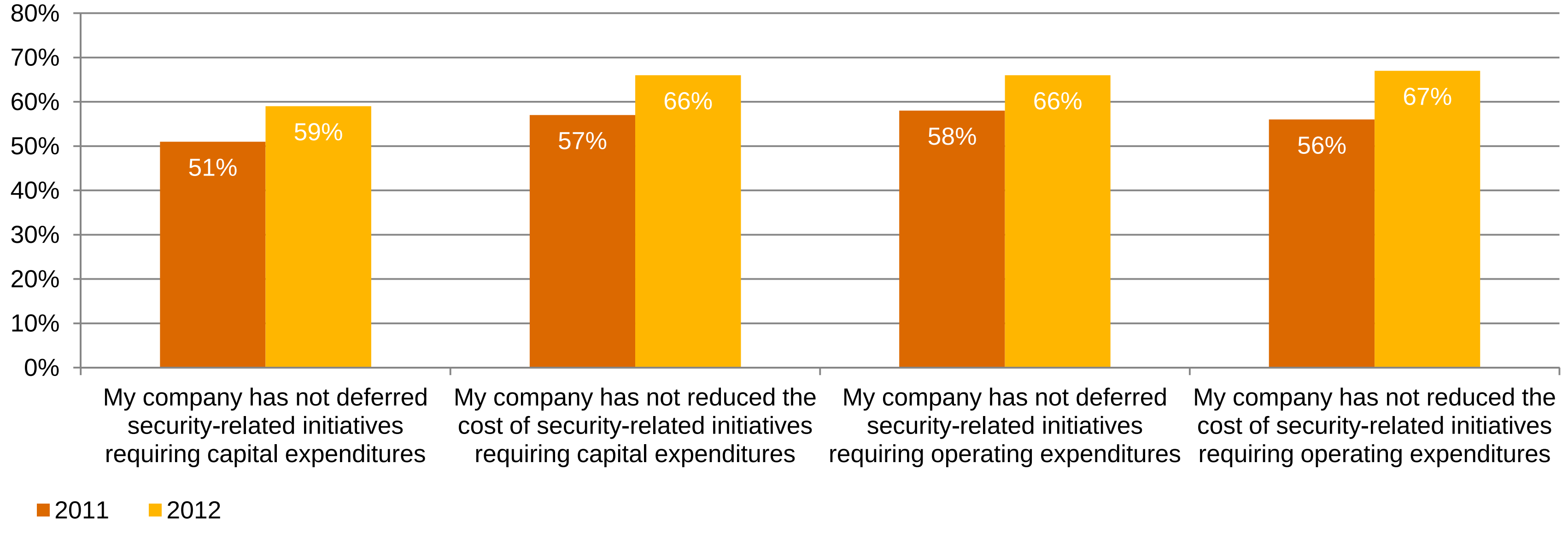
53% of O&G respondents say known weaknesses and incidents drive security spending, but just 47% address cyber security on an enterprise level. Similarly, 47% have programs in place to address Advanced Persistent Threats (APTs).



(Asked only of Oil & Gas respondents) Question 1: “What is the primary driver for cyber security spending at your company?” Question 2 (O&G): “Does your company employ a unified control framework and/or enterprise risk management framework for addressing cyber security risks?” Question 3 (O&G): “Does your company have a program in place to monitor for and respond to Advanced Persistent Threats (APTs)?"

O&G respondents are optimistic about security spending over the next 12 months.

54% of O&G respondents expect security budgets to increase in the year ahead. More encouragingly, they report fewer deferrals and fewer budget cutbacks for security initiatives. Compared with last year, for instance, 16% more respondents say they had not cut capital expenditures for security programs.



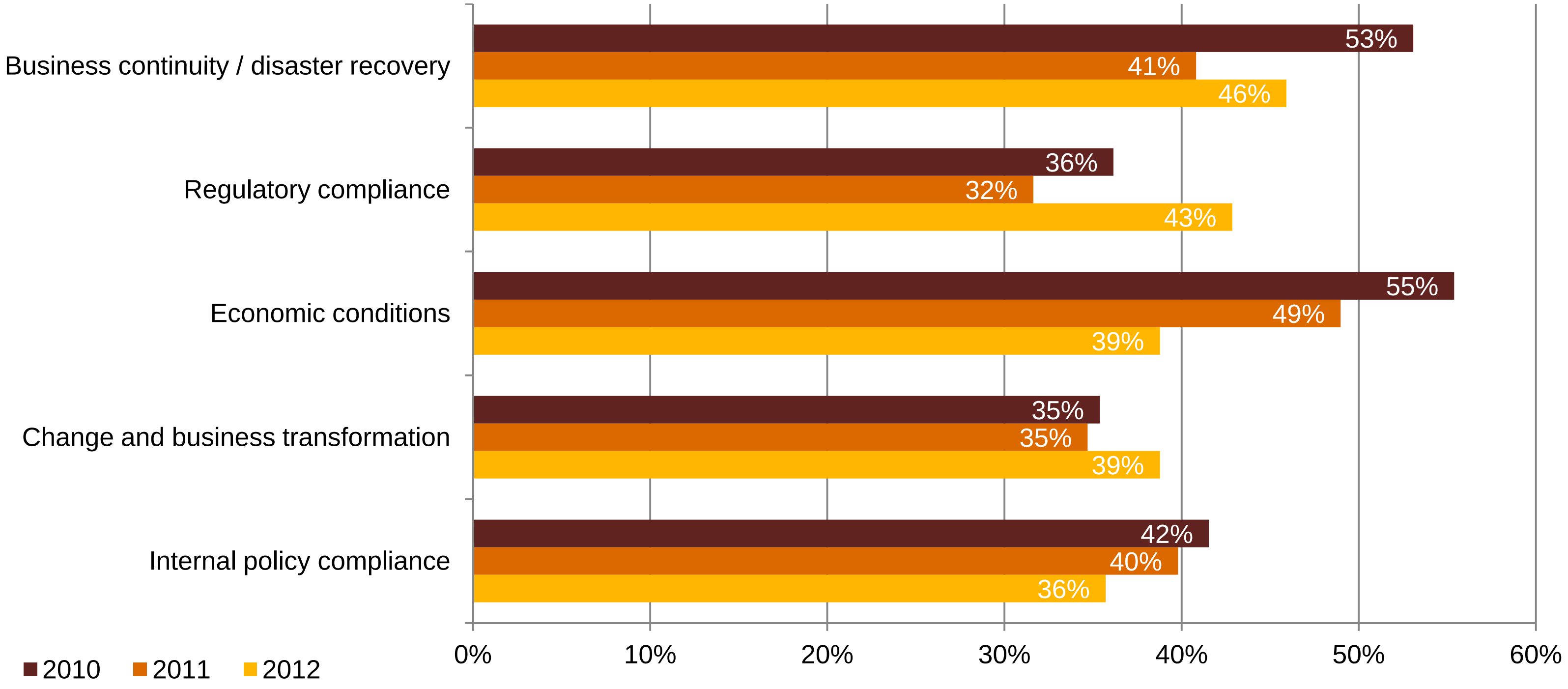
Question 8: “When compared with last year, security spending over the next 12 months will:” Questions 9A and 10A: “Has your company deferred capital and operating security-related initiatives?” Questions 9B and 10B: “Has your company reduced the capital and operating costs of security-related initiatives?”

Section 3

A game of risk

Security budgets are not driven by security needs.

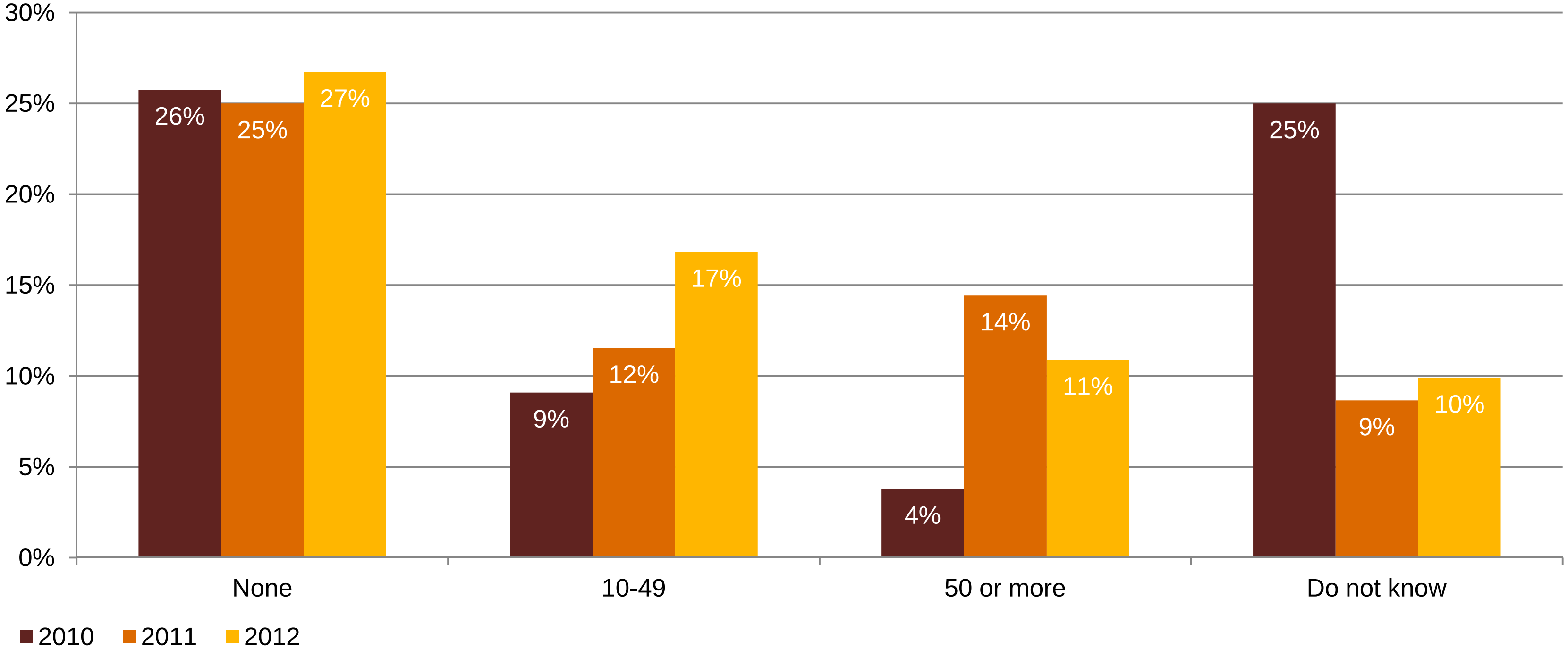
Business continuity/disaster recovery is the top driver of security spending, at 46%. Economic conditions weigh in at 39%. That's down from recent years, but still a risky way to set priorities.



Question 37: "What business issues or factors are driving your company's information security spending?" (Not all factors shown.)

Reported security incidents are on the rise.

17% of O&G respondents report 10-49 security incidents in the last 12 months, a 42% rise over 2011. 11% report 50 or more, a decline from last year but up sharply over previous years.



Question 17: “Number of security incidents in the past 12 months.”

Just half of respondents have security training programs for employees.

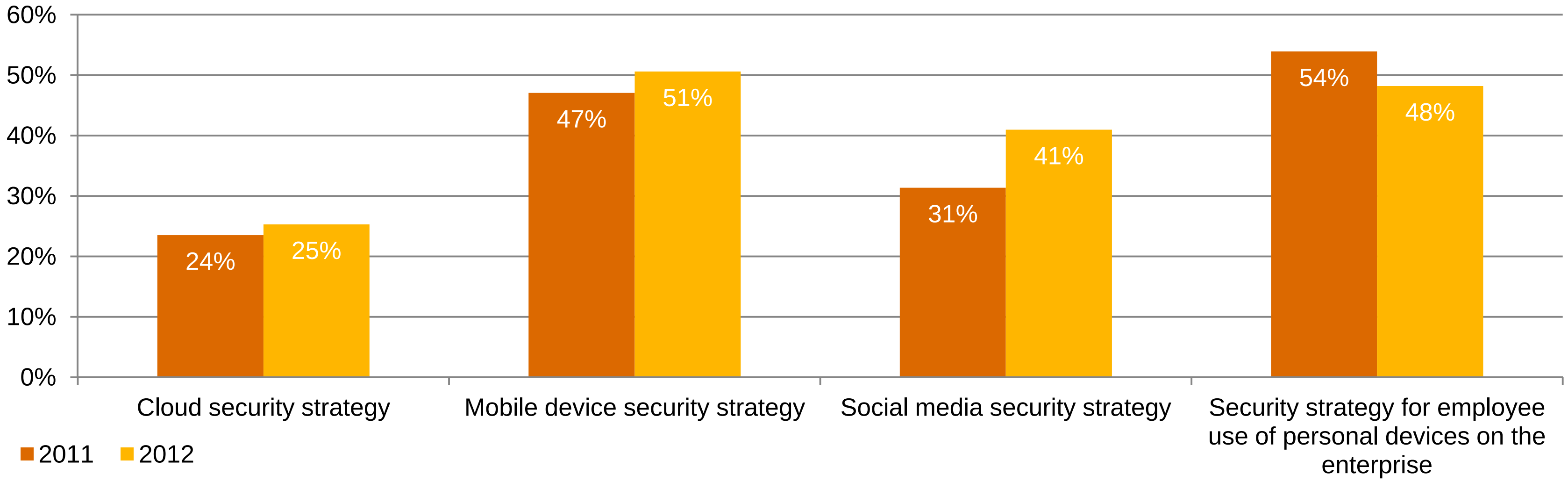
Just over half (53%) of O&G respondents have an employee security awareness training program – a fundamental element of an effective security culture. Staff dedicated to security awareness and training are in place at 56% of O&G companies, the lowest since 2007.

Information security safeguards	2007	2008	2009	2010	2011	2012
Have employee security awareness training program	45%	56%	48%	55%	54%	53%
Have people dedicated to employee awareness programs	46%	57%	64%	65%	61%	56%

Question 14: “What process information security safeguards does your organization currently have in place?” Question 13: “What information security safeguards related to people does your organization have in place?”

Technology adoption is moving faster than security implementation.

Compared with last year, more O&G respondents report that their organization has security strategies for mobile, social media, and cloud computing, although safeguards for use of employee-owned devices dropped. These numbers still lag adoption of the technologies themselves. We have found, for instance, that 88% of consumers use a personal mobile device for both personal and work purposes.[1]

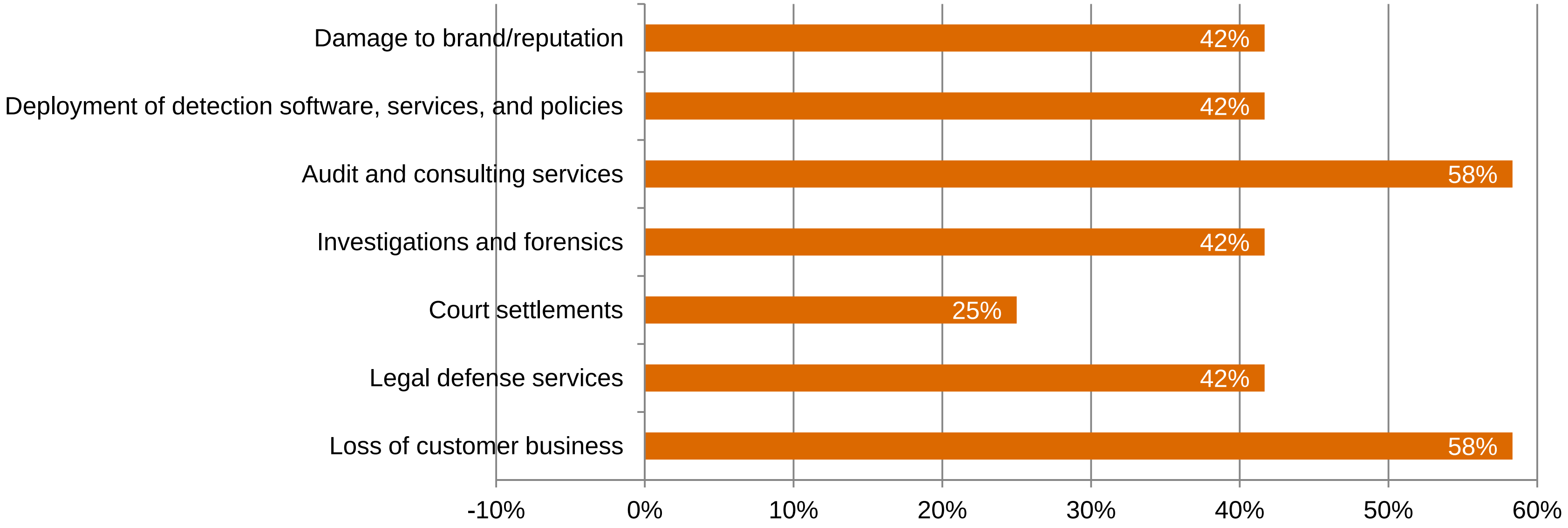


Question 14: “What process information security safeguards does your organization currently have in place?”

[1] PwC, Consumer privacy: What are consumers willing to share? July 2012

An inadequate assessment of security incidents can lead to a less-clear understanding of their impact.

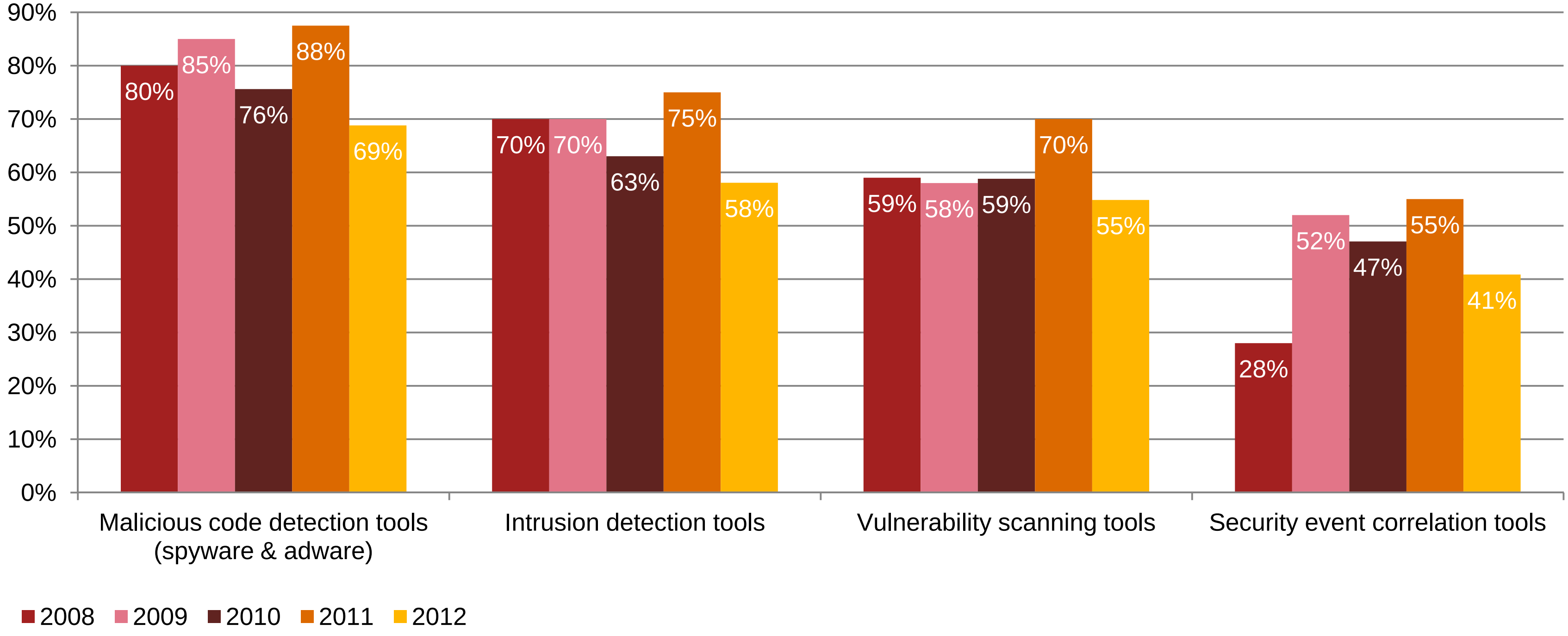
O&G respondents report a lower incidence of financial losses from security incidents than last year, yet many do not apply thorough or consistent analysis to appraising those costs. For example, only 42% consider damage to brand/reputation, while the same percentage factor in investigations and forensics.



Question 21: “How was your organization impacted by the security incident?” Question 21C: “What factors are included in your company’s calculation of these financial losses?”

Use of some key technology safeguards resumed a long-term decline after last year's uptick.

Respondents say that deployment, and therefore use, of many basic information security and privacy tools has atrophied over time.



Question 15: "What technology information security safeguards related to detection does your organization have in place?"

Section 4

It’s how you play the game

What keeps security from being what it should be?

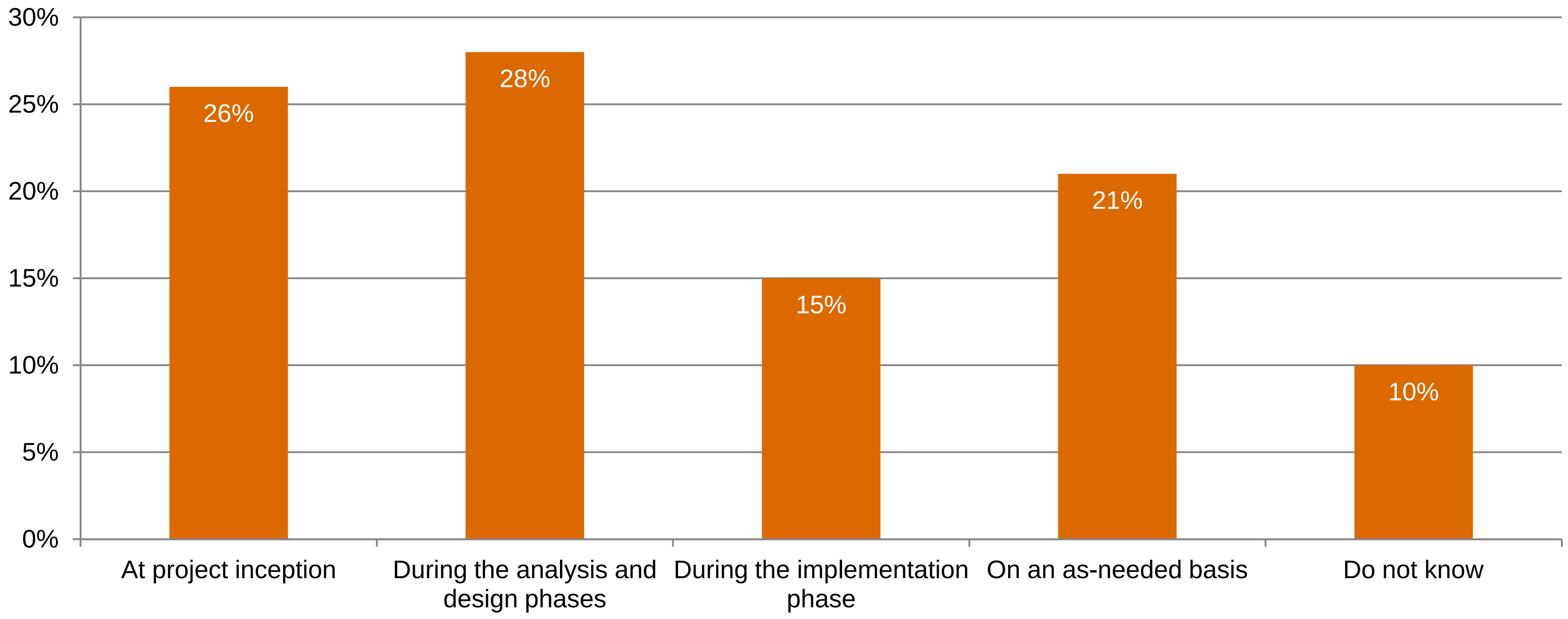
Top leadership is perceived to be less an obstacle than in the past, with senior executives and Boards singled out less frequently than in 2011; nonetheless, 46% of respondents still point to C-level executives and Boards. Lack of vision and strategy also remain top concerns.

	2011	**2012**
Leadership – CEO, President, Board, or equivalent	26%	13%
Leadership – CIO or equivalent	15%	15%
Leadership – CISO, CSO, or equivalent	21%	18%
Lack of an actionable vision or understanding	37%	34%
Absence or shortage of in-house technical expertise	19%	26%
Lack of an effective information security strategy	38%	25%
Poorly integrated or overly complex information/IT systems	23%	20%

Question 29: “What are the greatest obstacles to improving the overall strategic effectiveness of your organization’s information security function?”

Security is not always baked into major projects from the beginning.

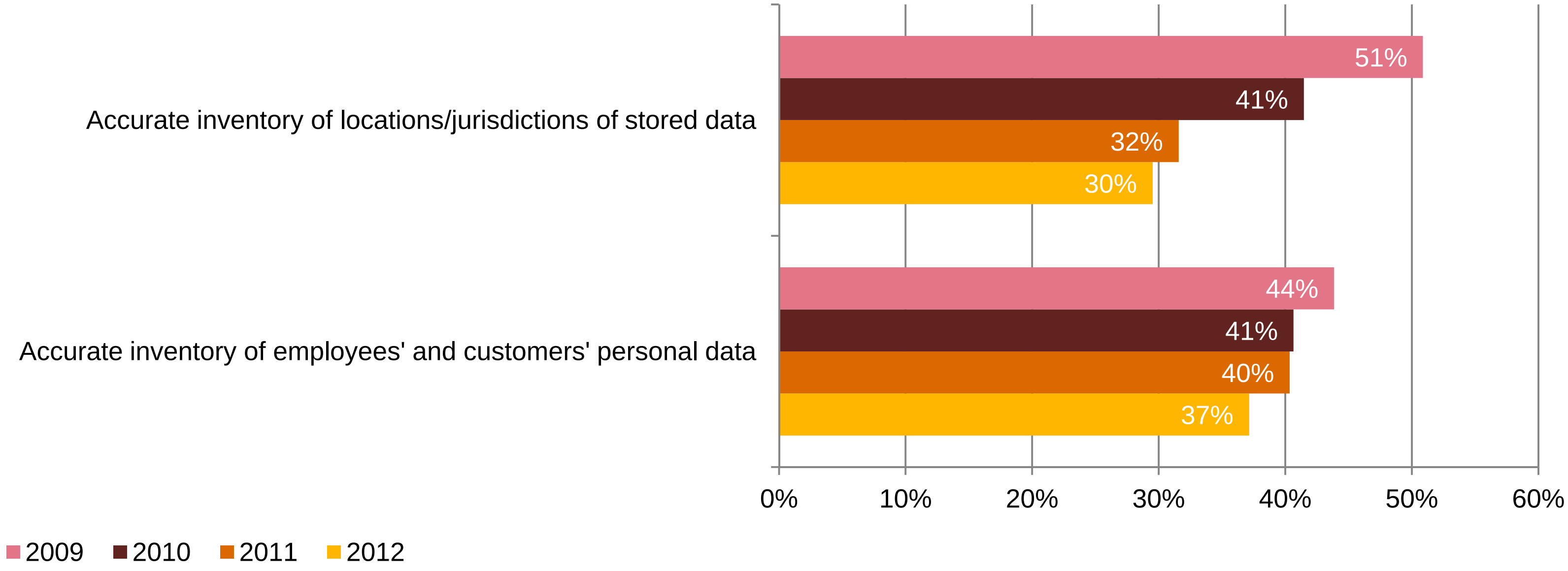
More than one-third (36%) of respondents involve security only during the implementation phase or on an as-needed basis.



Question 30: “When does information security become involved in major projects?”

O&G respondents know less about their data now than they did three years ago.

While 85% of respondents say protecting customer and employee data is important, far fewer understand what that data entails and where it is stored. This is significant because, increasingly, consumers want to be in control of their personal data and "turn off" the flow of information from companies.[2]



Question 38: "What level of importance does your company place on protecting the following types of information?" Q11: "Which data privacy safeguards does your organization have in place?"

[2] PwC, Consumer privacy: What are consumers willing to share? July 2012

What you can do to improve your performance.

Information security today is a rapidly evolving game of advanced skill and strategy. As a result, the security models of the past decade are no longer effective.

Effective security requires a new way of thinking. The very survival of the business demands that security leaders understand, prepare for, and quickly respond to security threats.

Businesses seeking to strengthen their security practice must:

- Implement a comprehensive risk-assessment strategy and align security investments with identified risks.
- Understand their organization's information, who wants it, and what tactics adversaries might use to get it.
- Understand that information security requirements – and, indeed, overall strategies for doing business – have reached a turning point.
- Embrace a new way of thinking in which information security is both a means to protect data as well as an opportunity to create value to the business.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
949.437.5380
gary.loveland@us.pwc.com

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

US Oil & Gas Contacts

Jim Guinn, II
Managing Director
832.656.8242
jim.guinn@us.pwc.com

Jamie Bass
Director
281.788.8263
james.bass@us.pwc.com

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

Or visit www.pwc.com/giss2013

www.pwc.com/security

Changing the game

While tight budgets have forestalled updates to security programs, many businesses are confident they're winning the game. But the rules – and the players – have changed.

Entertainment & Media

Key findings from The Global State of Information Security® Survey 2013

September 2012

"You can't succeed in today's elevated threat environment if you don't know the players and you don't know the rules."

- Gary Loveland, Principal, PwC

Information security has always been a high-stakes game. One that demands a smart strategy, the right technology moves, and an unblinking eye on adversaries.

For many businesses, however, it has become a pursuit that is almost impossible to win. That’s because the rules have changed, and opponents—old and new—are armed with expert technology skills. As a result, the risks are greater than ever.

Businesses are fighting back by adopting new detection and prevention technologies. At the same time, governments around the world are enacting legislation to combat cyber threats. And regulatory bodies are issuing new guidance on disclosure obligations for cyber incidents.

Yet risks to data security continue to intensify – and show no signs of abating. Those keeping score agree that the bad guys appear to be in the lead.

Nonetheless, many businesses believe they are winning. The Global State of Information Security® Survey 2013 shows that most executives in the global entertainment and media (E&M) industry are confident in the effectiveness of their information security practices. They believe their strategies are sound and many consider themselves to be leaders in the field.

The odds, however, are not in their favor: Diminished budgets have resulted in degraded security programs, reported security incidents are on the rise, and new technologies are being adopted faster than they can be safeguarded.

Given today's elevated threat environment, businesses can no longer afford to play a game of chance. They must prepare to play a new game, one that requires advanced levels of skill and strategy to win.

Agenda

Section 1. Methodology

Section 2. A game of confidence

Section 3. A game of risk

Section 4. It’s how you play the game

Section 1

Methodology

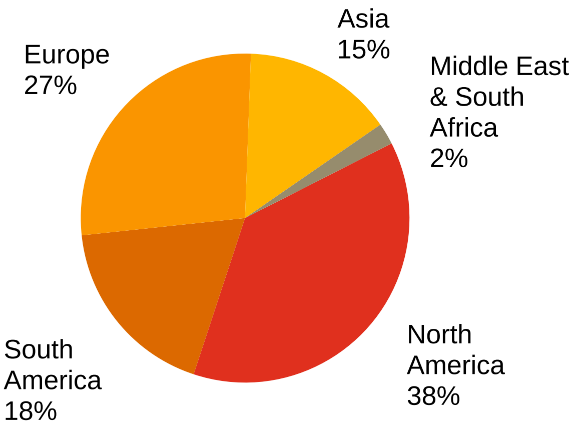
A worldwide study

The Global State of Information Security® Survey 2013, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 1, 2012 to April 15, 2012.

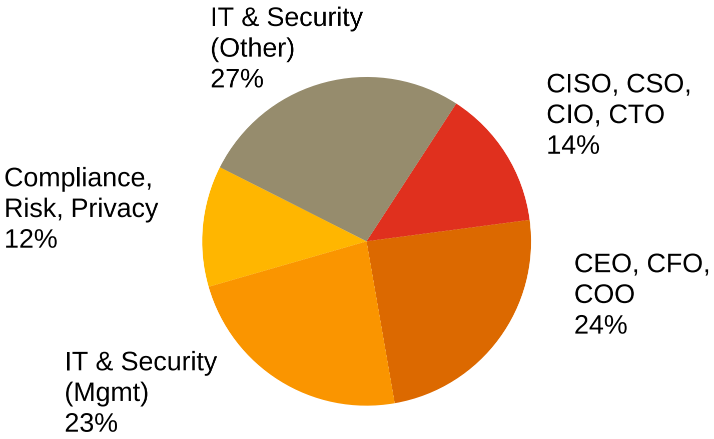
- PwC's 15th year conducting the online survey, 10th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 128 countries
- More than 9,300 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-three percent (33%) of respondents from companies with revenue of $500 million+
- Survey included 378 respondents from the entertainment and media industry
- Margin of error less than 1%

Demographics

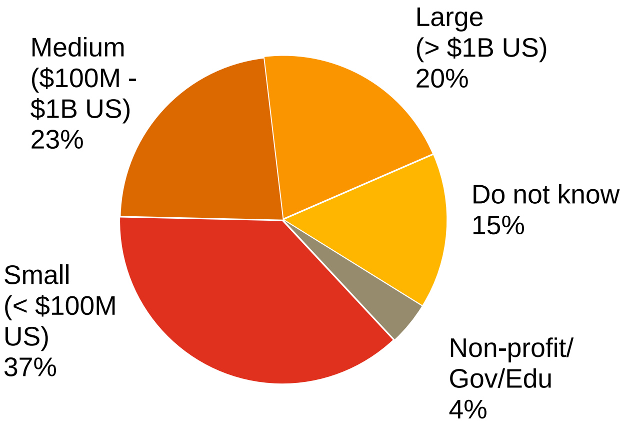
E&M respondents by region of employment



E&M respondents by title



E&M respondents by company revenue size



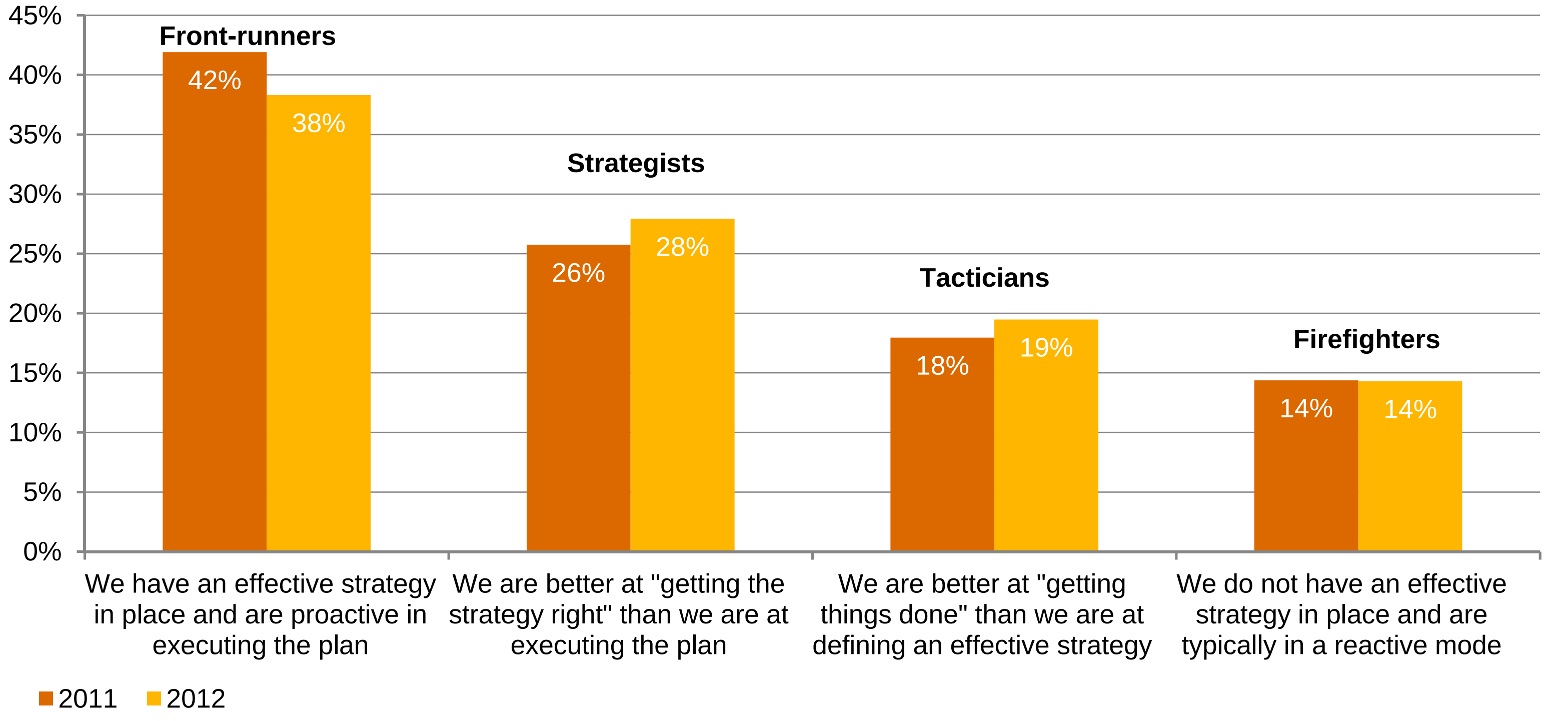
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

A game of confidence

E&M respondents are confident in their security practices.

38% of E&M respondents say their organization has a strategy in place and is proactive in executing it – exhibiting two distinctive attributes of a leader.



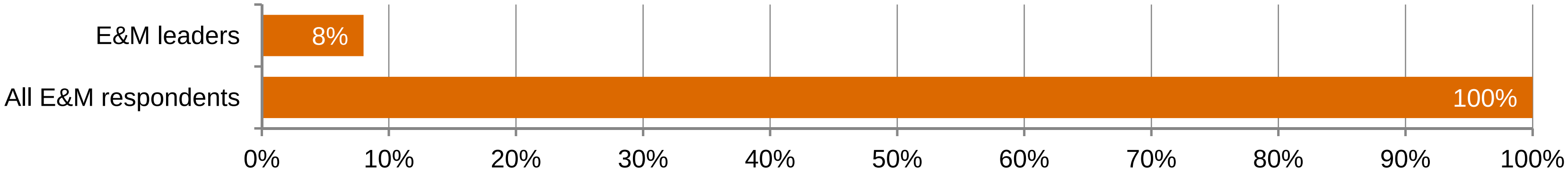
Question 28: "Which category below best characterizes your organization's approach to protecting information security?"

A reality check on real leaders.

But are they really leaders? We measured E&M respondents' self-appraisal against four key criteria to define leadership. To qualify, they must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the "top of the house" (e.g., to the CEO, CFO, COO, or legal counsel)
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

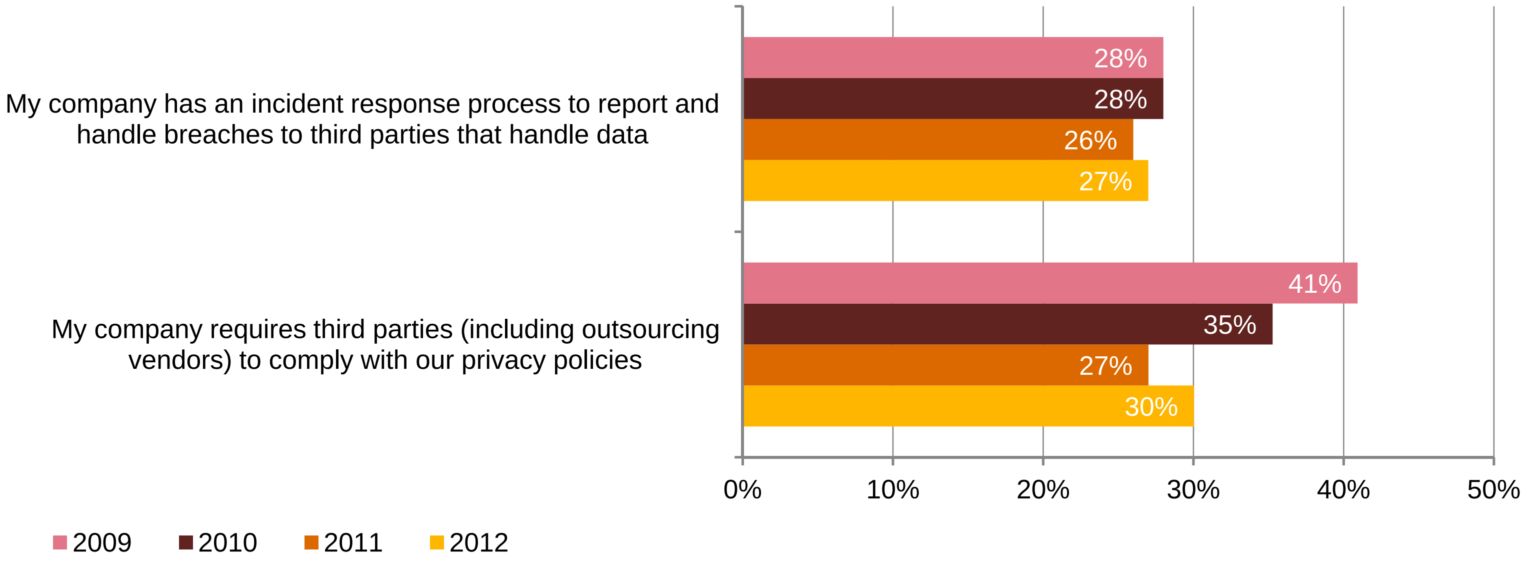
The result? Our analysis found that 8% of E&M respondents rank as leaders.



Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 18: "What types of security incidents (breach or downtime) occurred" and Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Many E&M respondents are over-confident in their organization's security program.

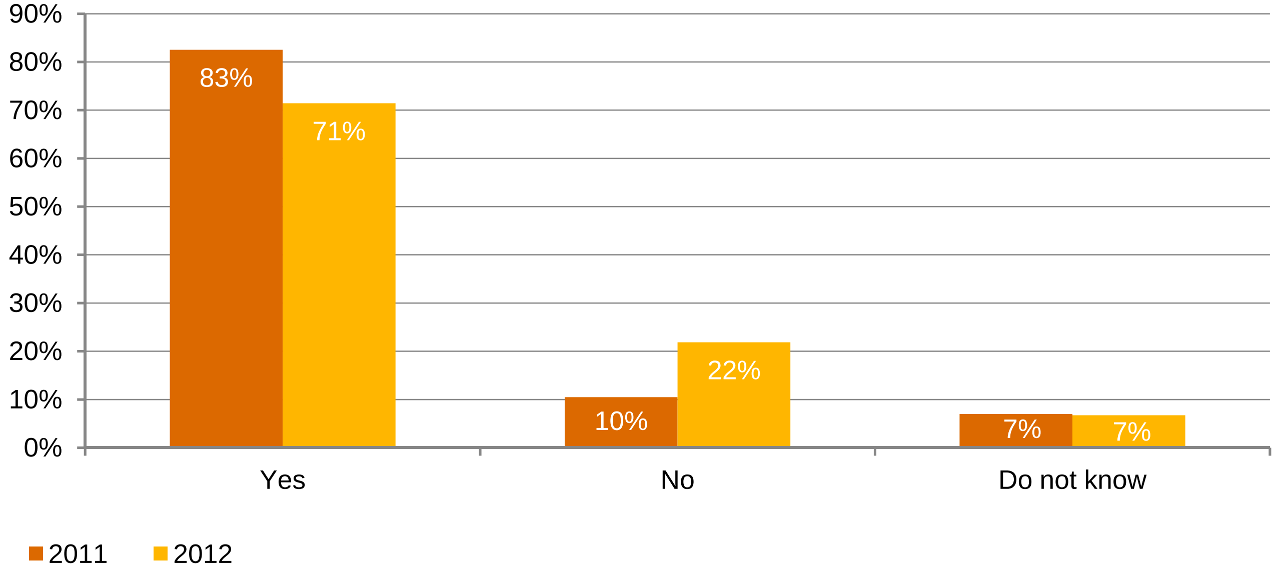
63% of respondents are confident that they have instilled effective security behaviors into their organization's culture, yet most do not have a process in place to handle third-party breaches. What's more, fewer than one-third require third parties to comply with privacy policies. This suggests a troubling gap in perception.



Question 35: "How confident are you that your organization has instilled effective information security behaviors into the organizational culture?"
Question 11: "Which data privacy safeguards does your organization have in place?"

And while most respondents say their customer information is secure, that confidence is eroding.

A strong 71% of E&M respondents say their organization has a solid strategy for protecting customer information – but that's down from last year's 83%. Protecting data is essential to customer loyalty. In fact, a recent PwC consumer survey found that 61% of respondents would stop using a company's products or services after a breach.[1]



(Asked only of Entertainment & Media respondents) Question 4A: "Do you believe your company has a solid strategy for protecting customer information?"

[1] PwC, Consumer privacy: What are consumers willing to share? July 2012

E&M executives are confident that distribution via the Internet is adequately secure.

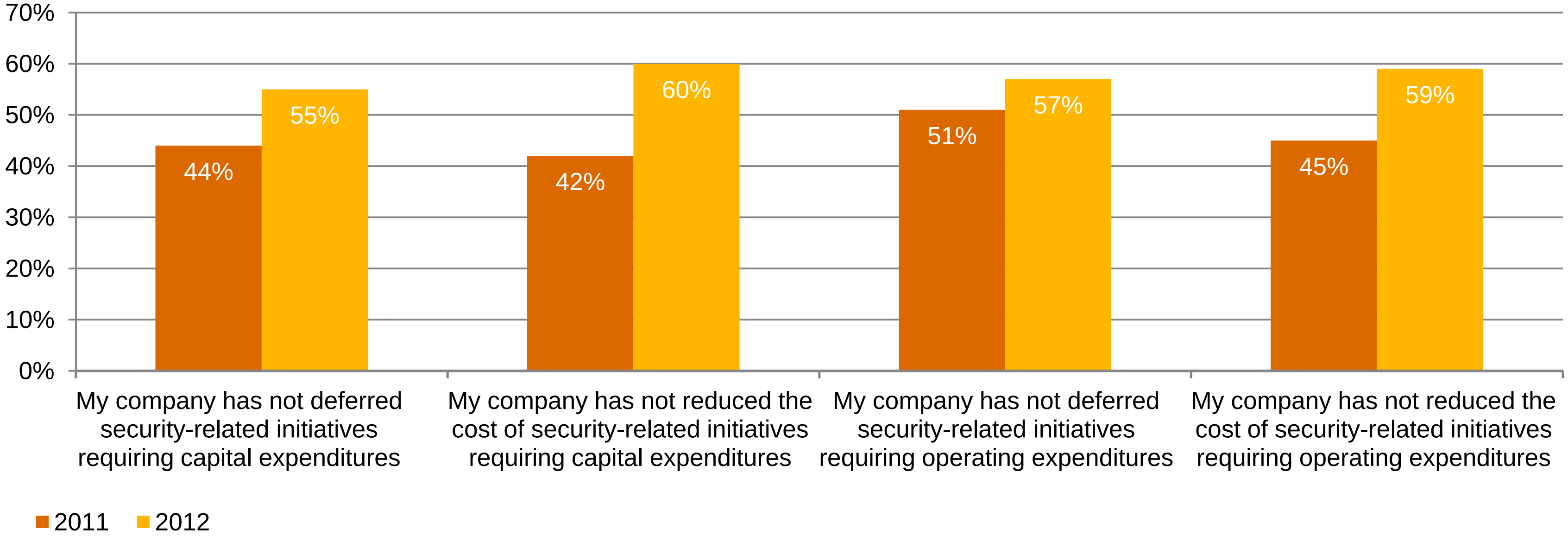
Fewer E&M respondents than last year say security is a significant factor in deciding whether to allow content to be distributed and/or viewed on the Internet.

	2011	2012
Yes	67%	62%
No	25%	24%
Do not know	8%	14%

Question 5 (E&M): “Is security a significant factor in deciding whether to allow content to be distributed and/or viewed on the Internet?”

E&M respondents are optimistic about security spending over the next 12 months.

49% of E&M respondents expect security budgets to increase in the year ahead. More encouragingly, respondents report fewer deferrals and fewer budget cutbacks for security initiatives. Compared with last year, 43% more respondents said they had not cut capital expenditures for security programs.



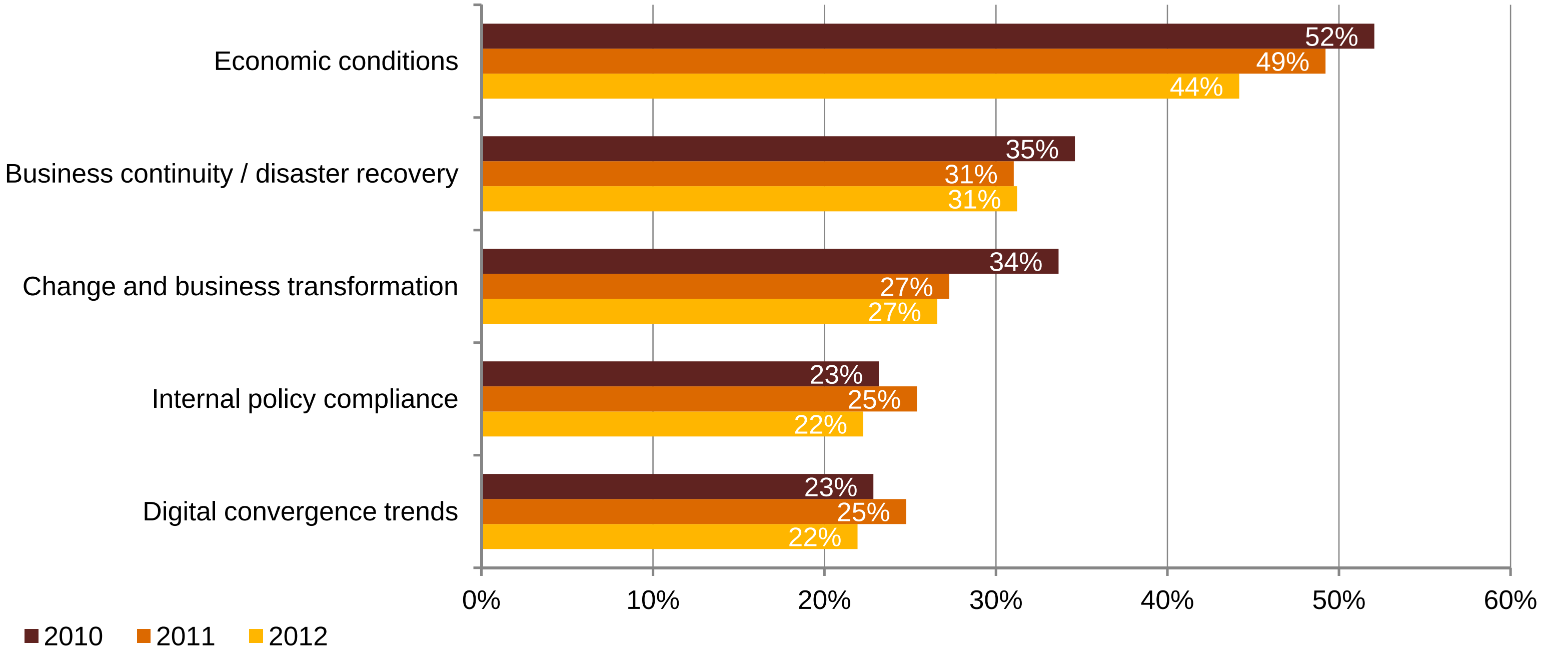
Question 8: “When compared with last year, security spending over the next 12 months will:” Questions 9A and 10A: “Has your company deferred capital and operating security-related initiatives?” Questions 9B and 10B: “Has your company reduced the capital and operating costs of security-related initiatives?”

Section 3

A game of risk

Security budgets are not driven by security needs.

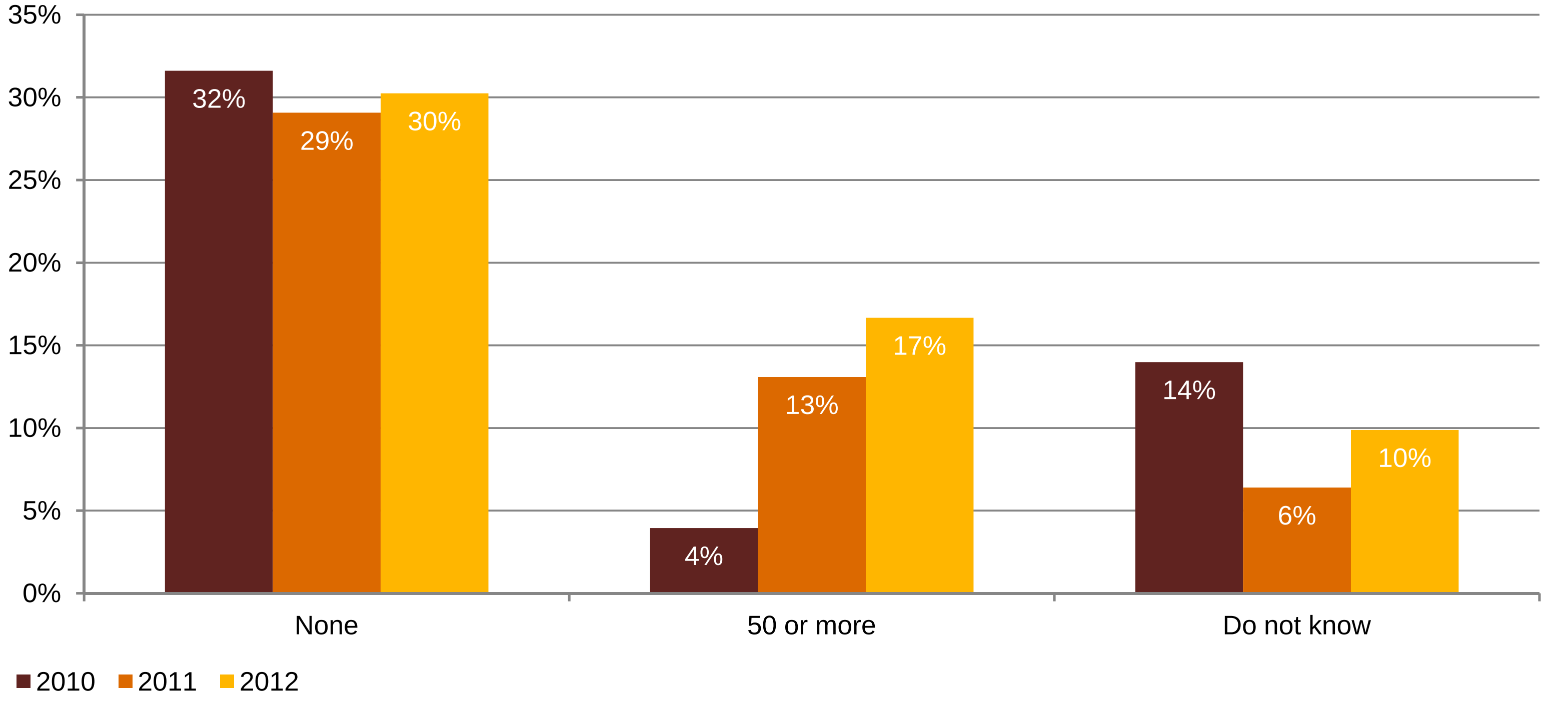
Economic conditions are by far the largest driver of security spending, at 44%. That's a lower percentage than 2011 and 2010, but still a risky way to set priorities. Business continuity/disaster recovery was the highest-rated security-specific response, at 31%.



Question 37: "What business issues or factors are driving your company's information security spending?" (Not all factors shown.)

Reported security incidents are on the rise.

The number of respondents reporting the most numerous category of security incidents – 50 or more per year – jumped 31% over 2011 and 325% over 2010. Almost one-third reported no security incidents in the last 12 months.



Question 17: “Number of security incidents in the past 12 months.”

Less than half of respondents have security training programs for employees.

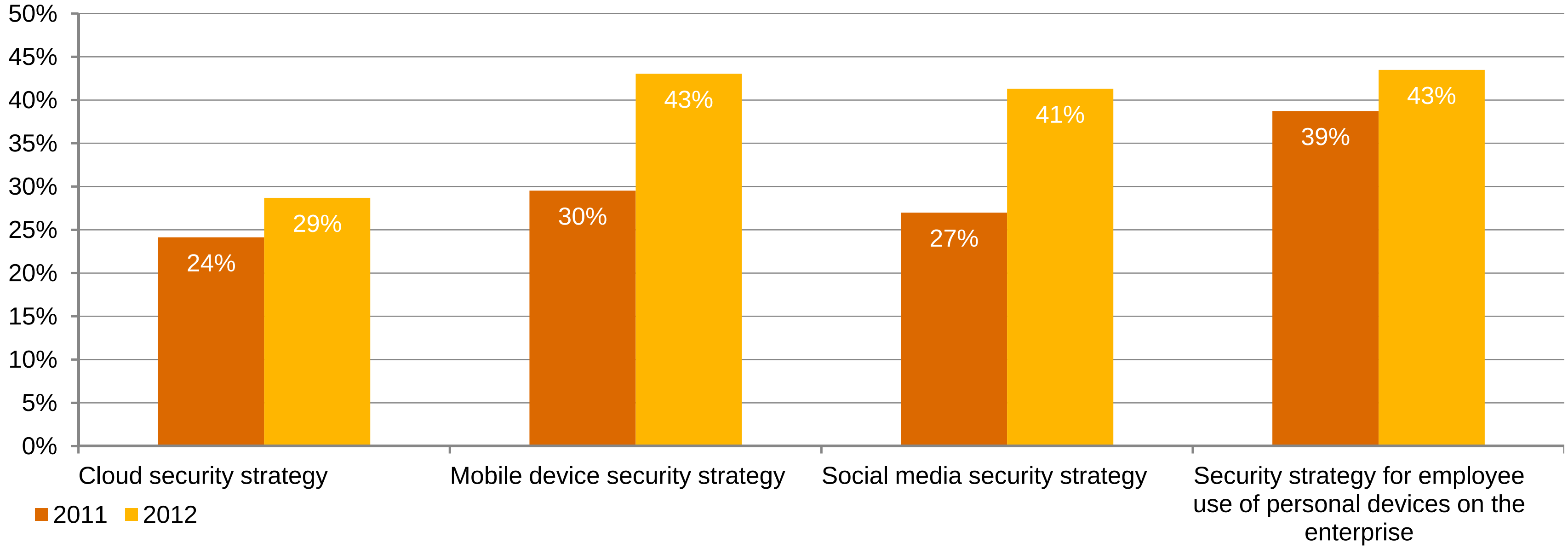
No security program can be effective without adequate training, yet only 45% of E&M respondents have an employee security awareness training program in place. Even fewer have staff dedicated to security awareness.

Information security safeguards	2009	2010	2011	2012
Have employee security awareness training program	48%	38%	35%	45%
Have people dedicated to employee awareness programs	53%	46%	43%	41%

Question 14: “What process information security safeguards does your organization currently have in place?” Question 13: “What information security safeguards related to people does your organization have in place?”

Technology adoption is moving faster than security implementation.

More E&M respondents report their organization has security strategies for mobile, social media, cloud computing, and use of employee-owned devices. But the numbers still lag adoption of the technologies themselves. We have found, for instance, that 88% of consumers use a personal mobile device for both personal and work purposes.[2]

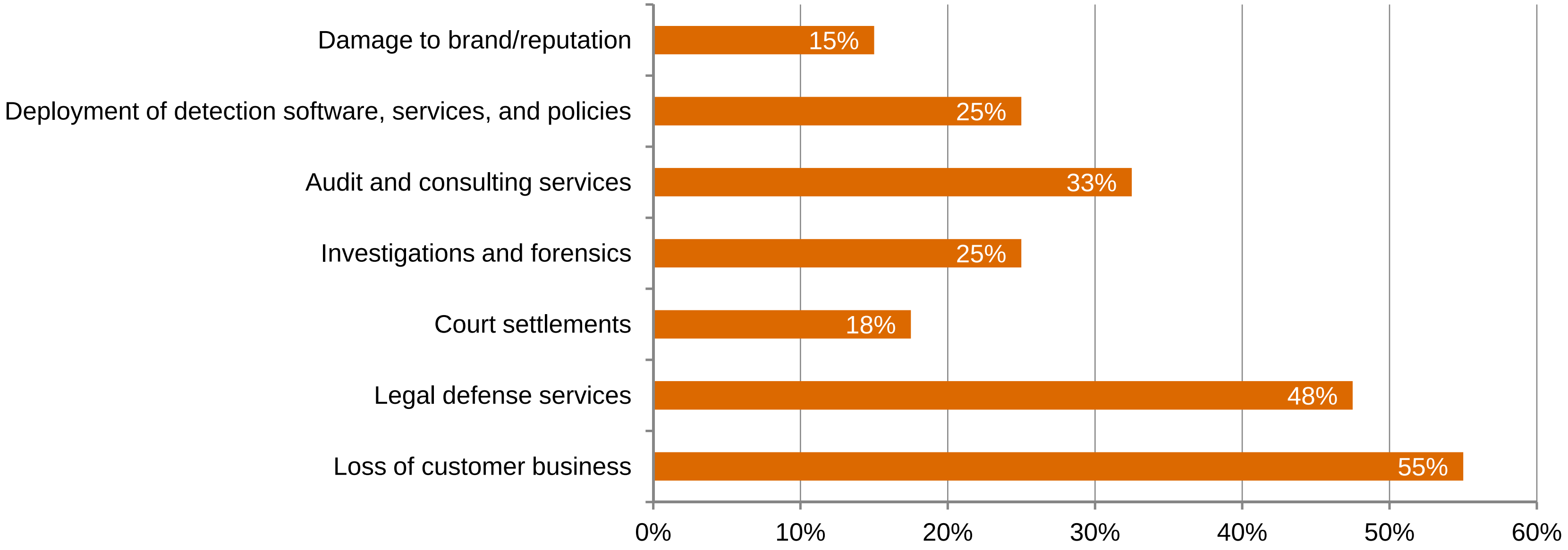


Question 14: “What process information security safeguards does your organization currently have in place?”

[2] PwC, Consumer privacy: What are consumers willing to share? July 2012

An inadequate assessment of security incidents can lead to a less-clear understanding of their financial impact.

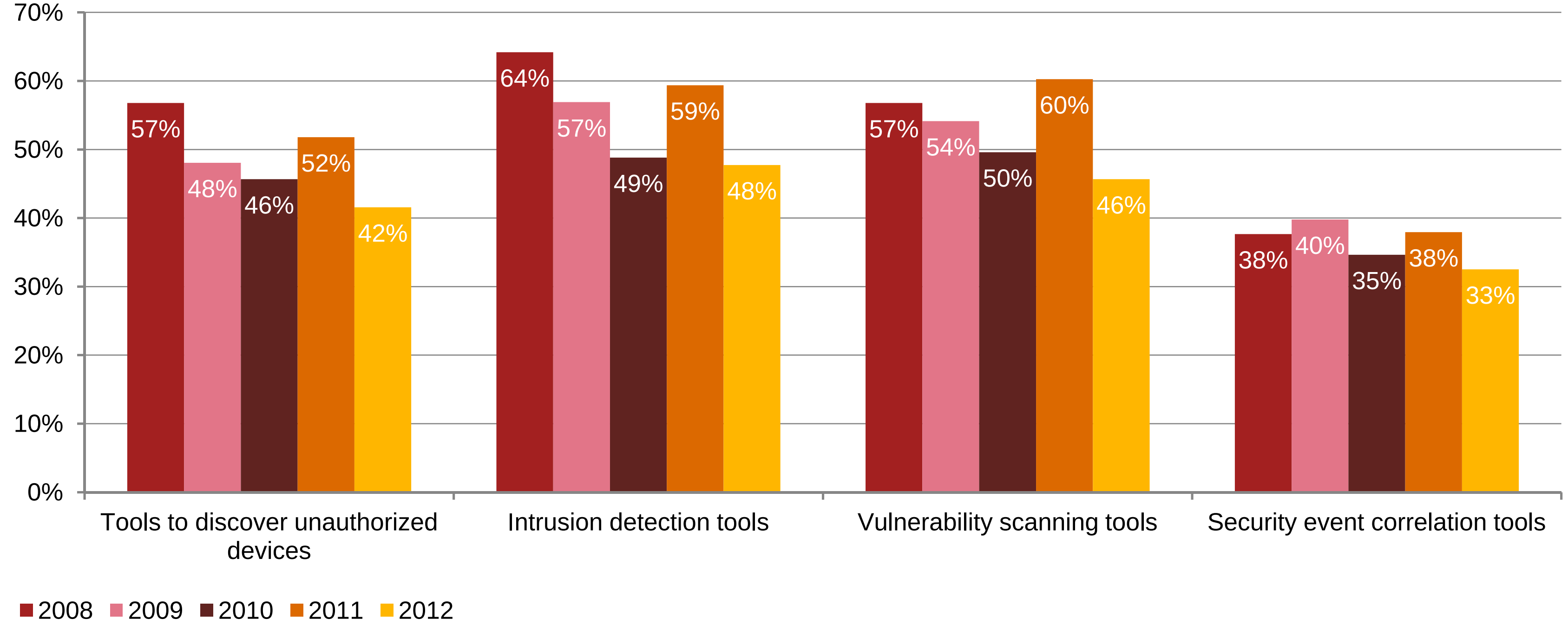
E&M respondents reported a lower incidence of financial losses from security incidents than last year, yet many did not perform a thorough or consistent appraisal of those losses. For example, only 15% considered damage to brand/reputation and 25% factored in investigations and forensics.



Question 21: "How was your organization impacted by the security incident?" Question 21C: "What factors are included in your company's calculation of these financial losses?"

Use of some key technology safeguards resumed a long-term decline after last year's uptick.

Deployment of many basic information security and privacy tools has atrophied since peaking in earlier years.



Question 15: "What technology information security safeguards related to detection does your organization have in place?"

Section 4

It's how you play the game

What keeps security from being what it should be?

Company leadership is seen as less of an obstacle than in the past, although 49% of respondents still point to C-level executives and Boards. Lack of vision and strategy continues to be a top concern.

	2011	2012
Leadership – CEO, President, Board, or equivalent	23%	19%
Leadership – CIO or equivalent	22%	17%
Leadership – CISO, CSO, or equivalent	18%	13%
Lack of an actionable vision or understanding	22%	25%
Lack of an effective information security strategy	25%	24%
Insufficient capital expenditures	31%	24%
Absence or shortage of in-house technical expertise	23%	21%

Question 29: “What are the greatest obstacles to improving the overall strategic effectiveness of your organization’s information security function?”

Fewer security leaders are reporting to the “top of the house.”

Effective security requires security presence at the executive level. Overall, fewer Chief Security Officers and equivalent senior information security executives are reporting directly to the Board, CEO, or CFO.

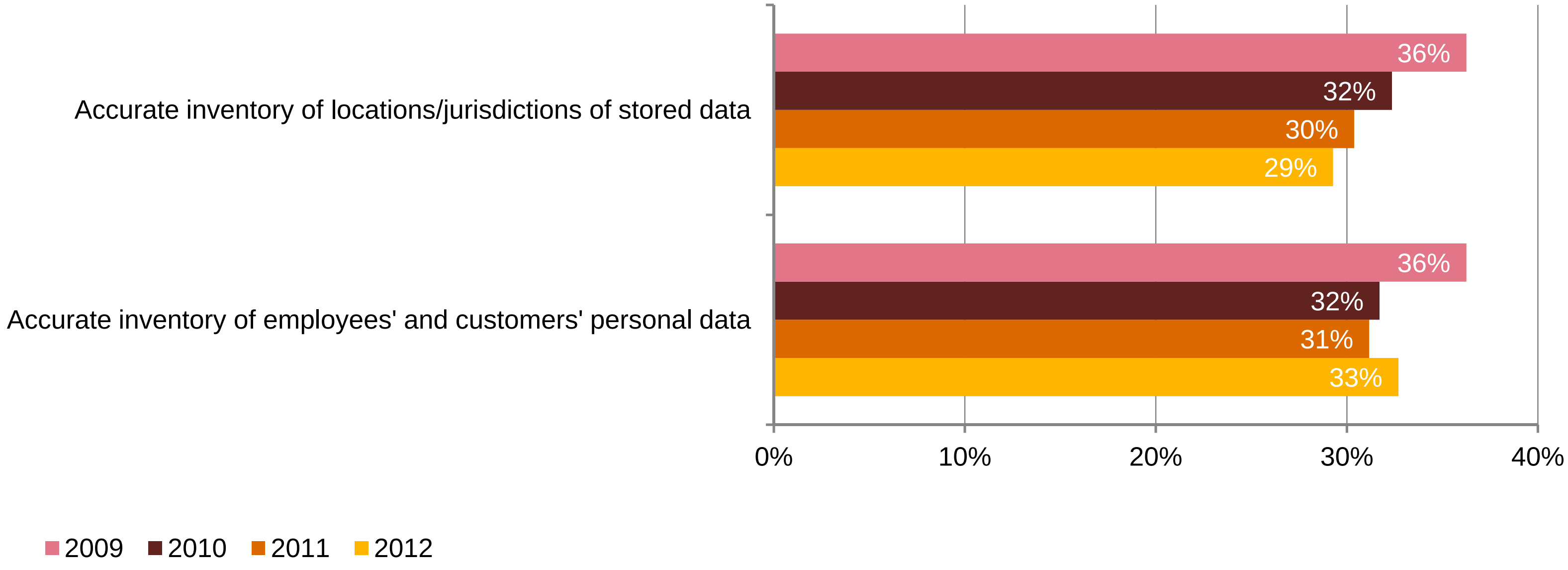
CISO, CSO, or equivalent senior information security executive reports to:	2010	2011	2012
Board of Directors	32%	32%	24%
CEO	31%	31%	28%
CFO	17%	20%	16%

CPO or equivalent senior privacy executive reports to:	2010	2011	2012
Board of Directors	41%	38%	30%
CEO	52%	40%	41%
CFO	23%	28%	21%

Question 13A: “Where / to whom does your CISO, CSO, or equivalent senior information security executive report?” Question 11A: “Where / to whom does your CPO or equivalent senior privacy executive report?”

E&M respondents know less about their data now than they did three years ago.

While approximately 80% of respondents say protecting customer and employee data is important, far fewer understand what that data entails and where it is stored. This is significant because, increasingly, consumers want to be in control of their personal data and “turn off” the flow of information from companies.[3]



Question 38: “What level of importance does your company place on protecting the following types of information?” Question 11: “Which data privacy safeguards does your organization have in place?”

[3] PwC, Consumer privacy: What are consumers willing to share? July 2012

What you can do to improve your performance.

Information security today is a rapidly evolving game of advanced skill and strategy. As a result, the security models of the past decade are no longer effective.

Effective security requires a new way of thinking. The very survival of the business demands that security leaders understand, prepare for, and quickly respond to security threats.

Businesses seeking to strengthen their security practice must:

- Implement a comprehensive risk-assessment strategy and align security investments with identified risks.
- Understand their organization's information, who wants it, and what tactics adversaries might use to get it.
- Understand that information security requirements – and, indeed, overall strategies for doing business – have reached a turning point.
- Embrace a new way of thinking in which information security is both a means to protect data as well as an opportunity to create value to the business.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
949.437.5380
gary.loveland@us.pwc.com

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

US Entertainment & Media Contact

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

Or visit www.pwc.com/giss2013

The Global State of Information Security® is a registered trademark of International Data Group, Inc.

www.pwc.com/security

Changing the game

While tight budgets have forestalled updates to security programs, many businesses are confident they're winning the game. But the rules – and the players – have changed.

CIO Business Technology Leadership

CSO BUSINESS RISK LEADERSHIP

Financial Services

Key findings from The Global State of Information Security® Survey 2013

September 2012

pwc

"You can't succeed in today's elevated threat environment if you don't know the players and you don't know the rules."

– Gary Loveland, Principal, PwC

Information security has always been a high-stakes game. One that demands a smart strategy, the right technology moves, and an unblinking eye on adversaries.

For many businesses, however, it has become a pursuit that is almost impossible to win. That’s because the rules have changed, and opponents—old and new—are armed with expert technology skills. As a result, the risks are greater than ever.

Businesses are fighting back by adopting new detection and prevention technologies. At the same time, governments around the world are enacting legislation to combat cyber threats. And regulatory bodies are issuing new guidance on disclosure obligations for cyber incidents.

Yet risks to data security continue to intensify – and show no signs of abating. Those keeping score agree that the bad guys appear to be in the lead.

Nonetheless, many businesses believe they are winning. The Global State of Information Security® Survey 2013 shows that most executives in the global financial services industry are confident in the effectiveness of their information security practices. They believe their strategies are sound and many consider themselves to be leaders in the field.

The odds, however, are not in their favor: Diminished budgets have resulted in degraded security programs, risks are not well understood or properly addressed, and new technologies are being adopted faster than they can be safeguarded.

Given today's elevated threat environment, businesses can no longer afford to play a game of chance. They must prepare to play a new game, one that requires advanced levels of skill and strategy to win.

Agenda

Section 1. Methodology

Section 2. A game of confidence

Section 3. A game of risk

Section 4. It’s how you play the game

Section 1

Methodology

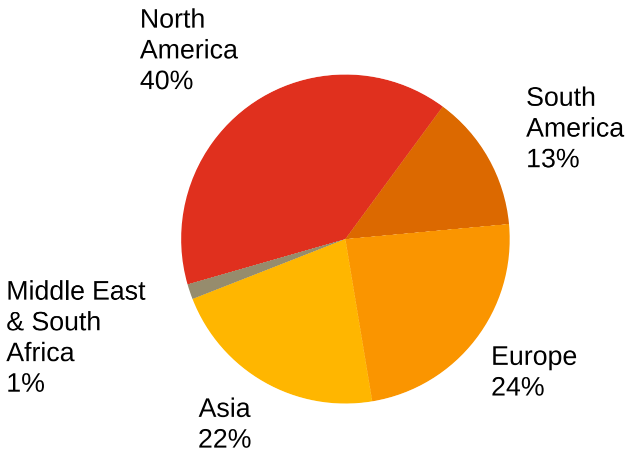
A worldwide study

The Global State of Information Security® Survey 2013, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 1, 2012 to April 15, 2012.

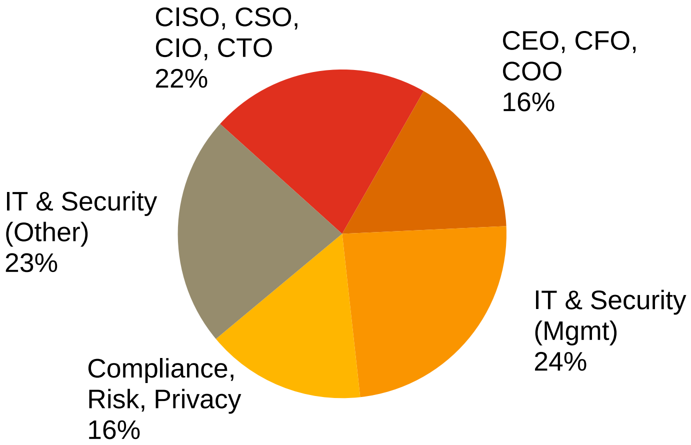
- PwC's 15th year conducting the online survey, 10th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 128 countries
- More than 9,300 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-three percent (33%) of respondents from companies with revenue of $500 million+
- Survey included 1,338 respondents from the financial services industry
- Margin of error less than 1%

Demographics

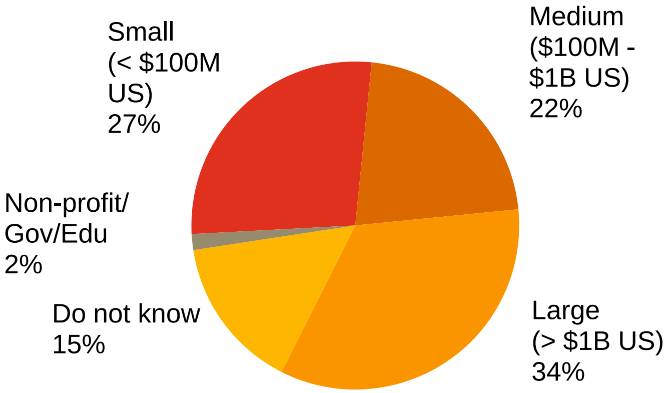
Financial services respondents by region of employment



Financial services respondents by title



Financial services respondents by company revenue size



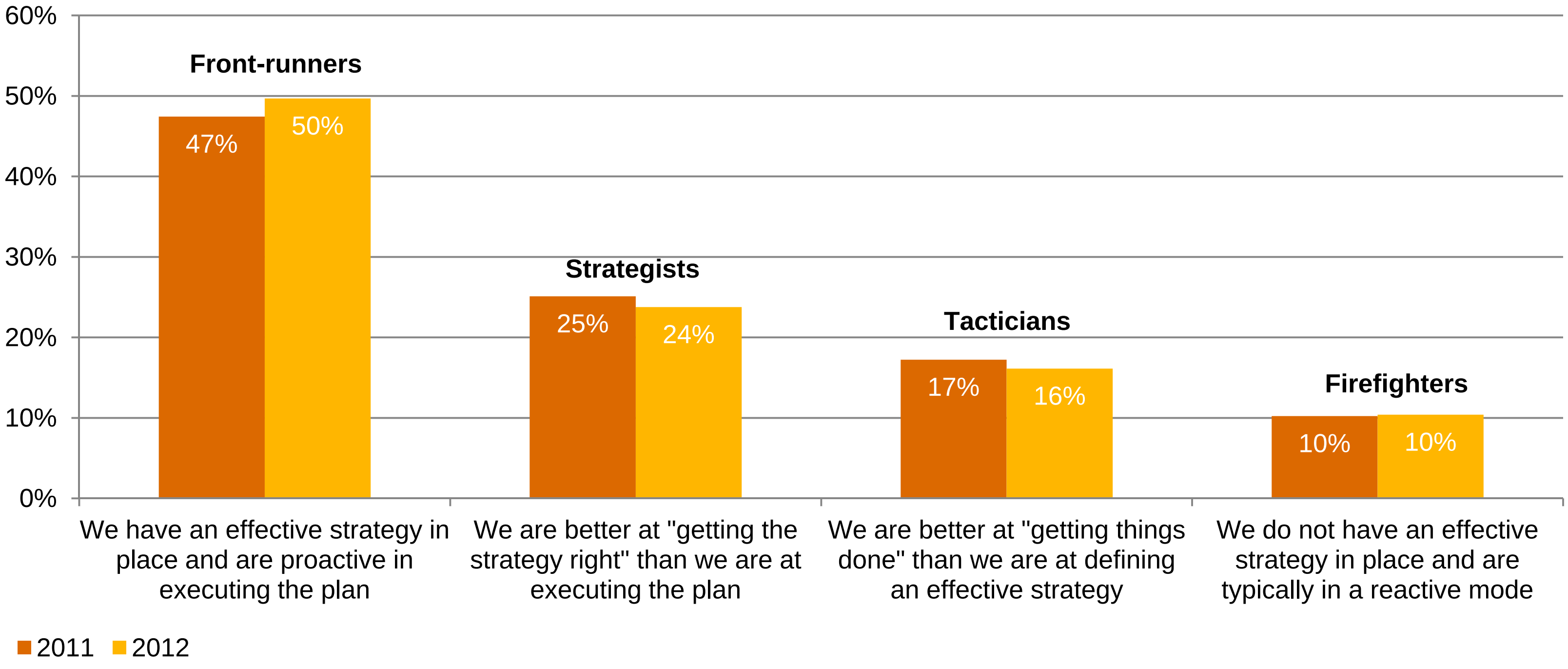
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

A game of confidence

Financial services respondents are confident in their security practices.

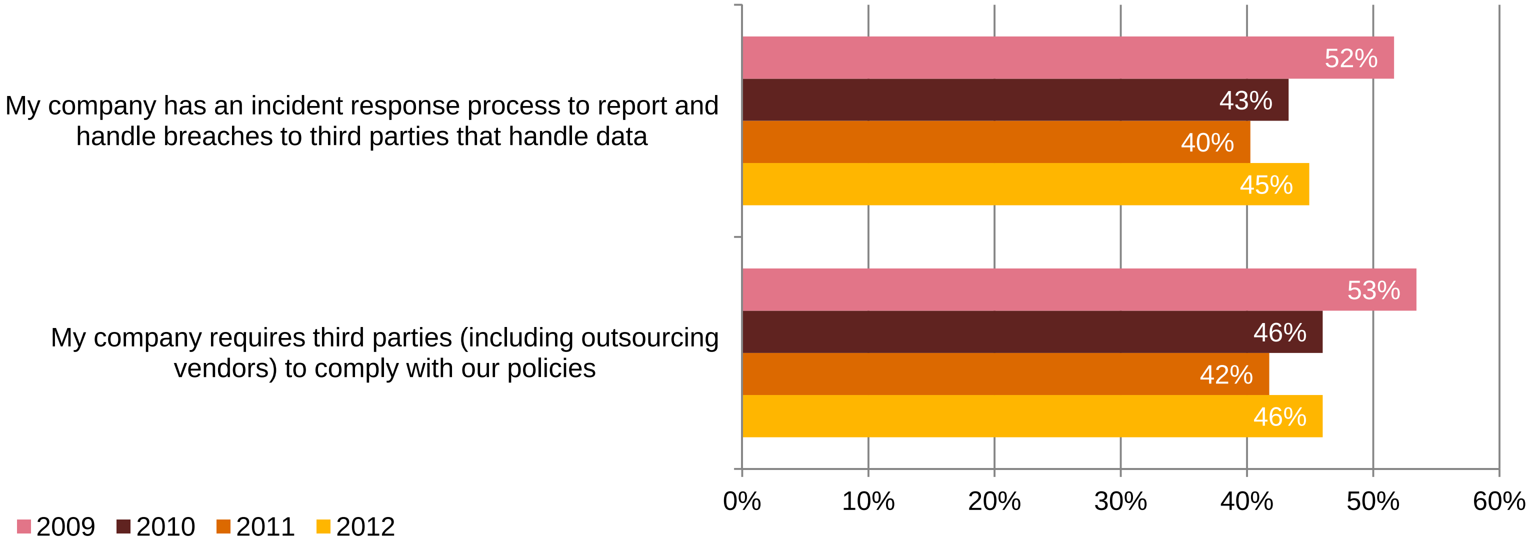
Half of financial services respondents say their organization has a strategy in place and is proactive in executing it – exhibiting two distinctive attributes of a leader.



Question 28: "Which category below best characterizes your organization’s approach to protecting information security?"

Many financial services respondents lack incident response processes and compliance policies for third-parties.

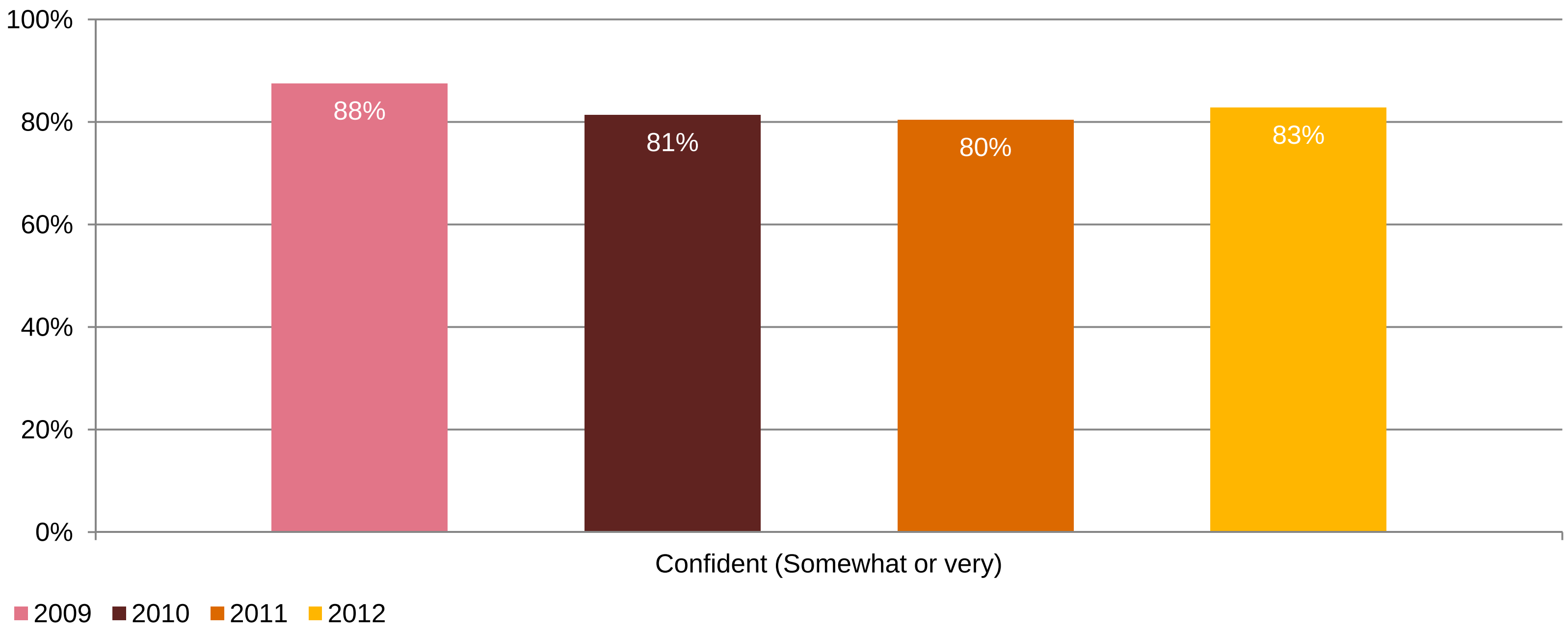
78% of respondents are confident that they have instilled effective security behaviors into their organization's culture, yet many do not have a process in place to handle third-party breaches. What's more, fewer than half require third parties to comply with privacy policies. This suggests a troubling gap in perception.



Question 35: "How confident are you that your organization has instilled effective information security behaviors into the organizational culture?"
Question 11: "Which data privacy safeguards does your organization have in place?"

Most respondents say their information security activities are effective, but confidence is eroding.

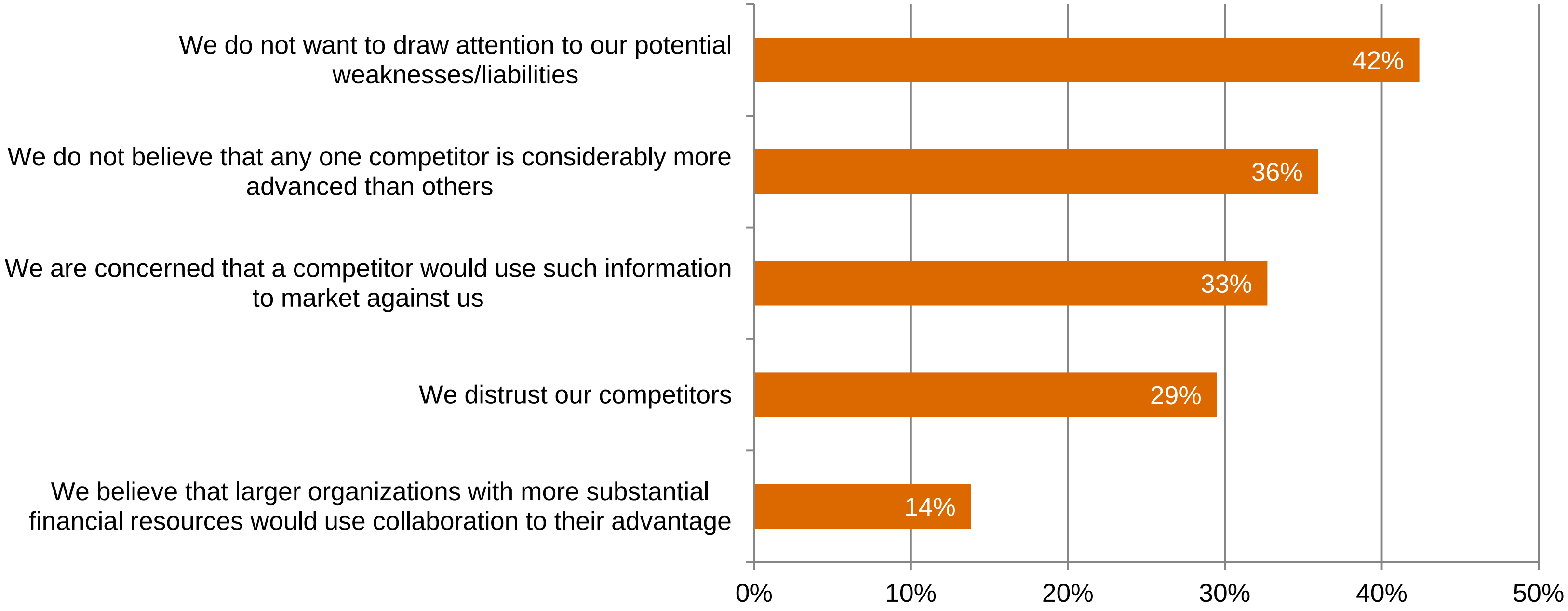
Confidence is a good thing. A strong 83% of financial services respondents say they are confident that their company's security activities are effective, but many may not realize that assurance is slowly dropping.



Question 41: "How confident are you that your organization's information security activities are effective?"

Why financial services firms are unwilling to collaborate with each other on strengthening security.

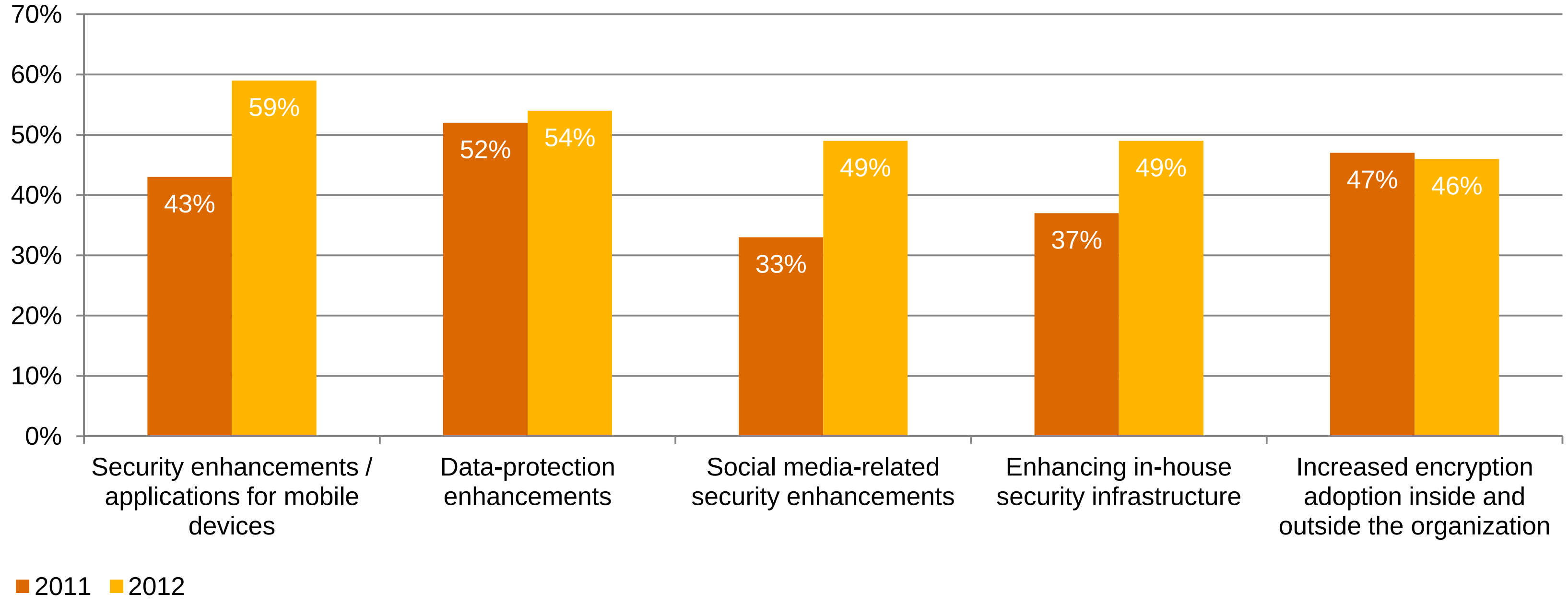
Only 55% of respondents say their firm works with other financial services companies to improve security practices. Why not more? It's all about competition.



(Asked only of Financial Services respondents) Question 6: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?" Question 6A (FS): "Why doesn't your organization collaborate with others in the industry to improve security and reduce the potential for future risks?"

Financial services firms target five areas for increased security spending.

The number of respondents planning to spend more on security for mobile devices increased by 37%, making mobile the year's top spending priority. Those planning to boost spending on social media increased by nearly 50% over 2011.



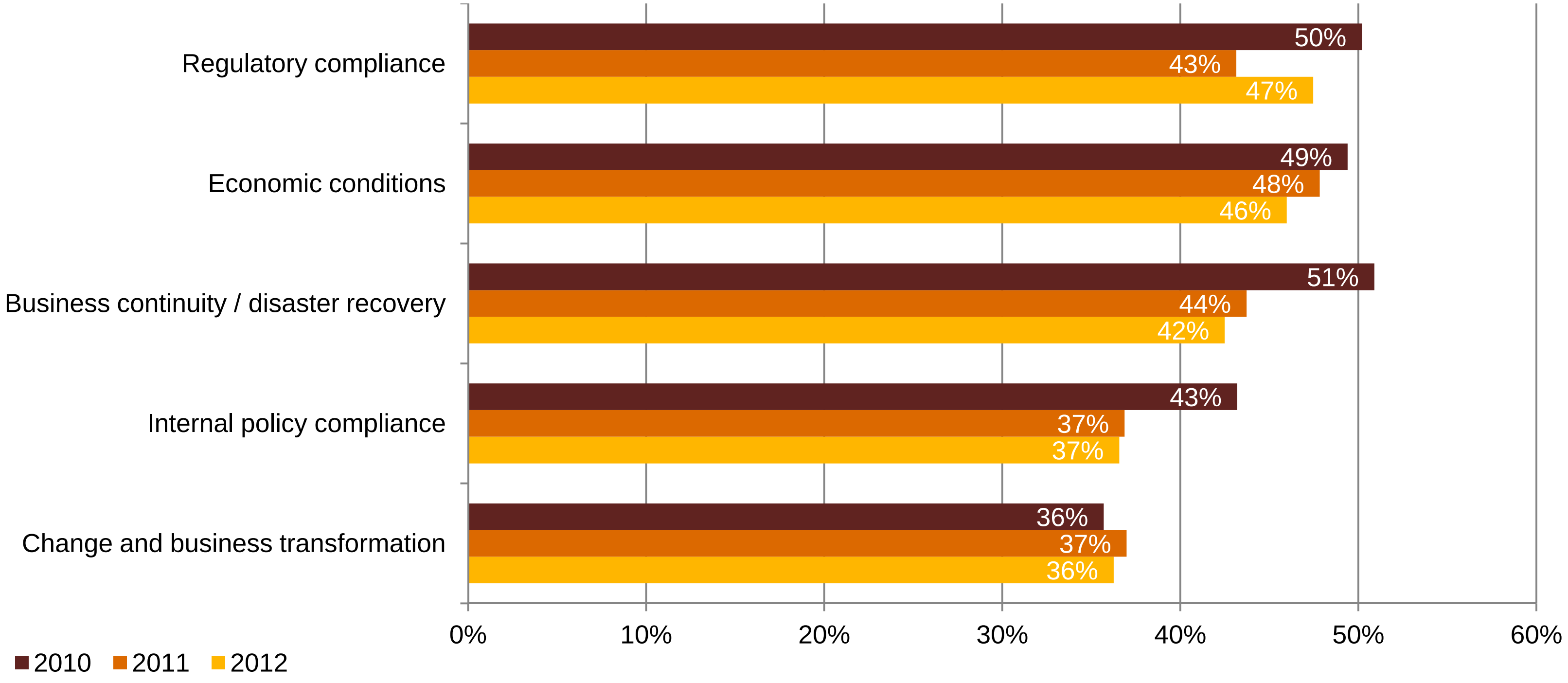
Question 3 (FS): "For each of the following areas, please indicate whether your organization will increase or decrease spending on information security over the next 12 months" (Not all factors shown.)

Section 3

A game of risk

Economic conditions continue to impact security budgets.

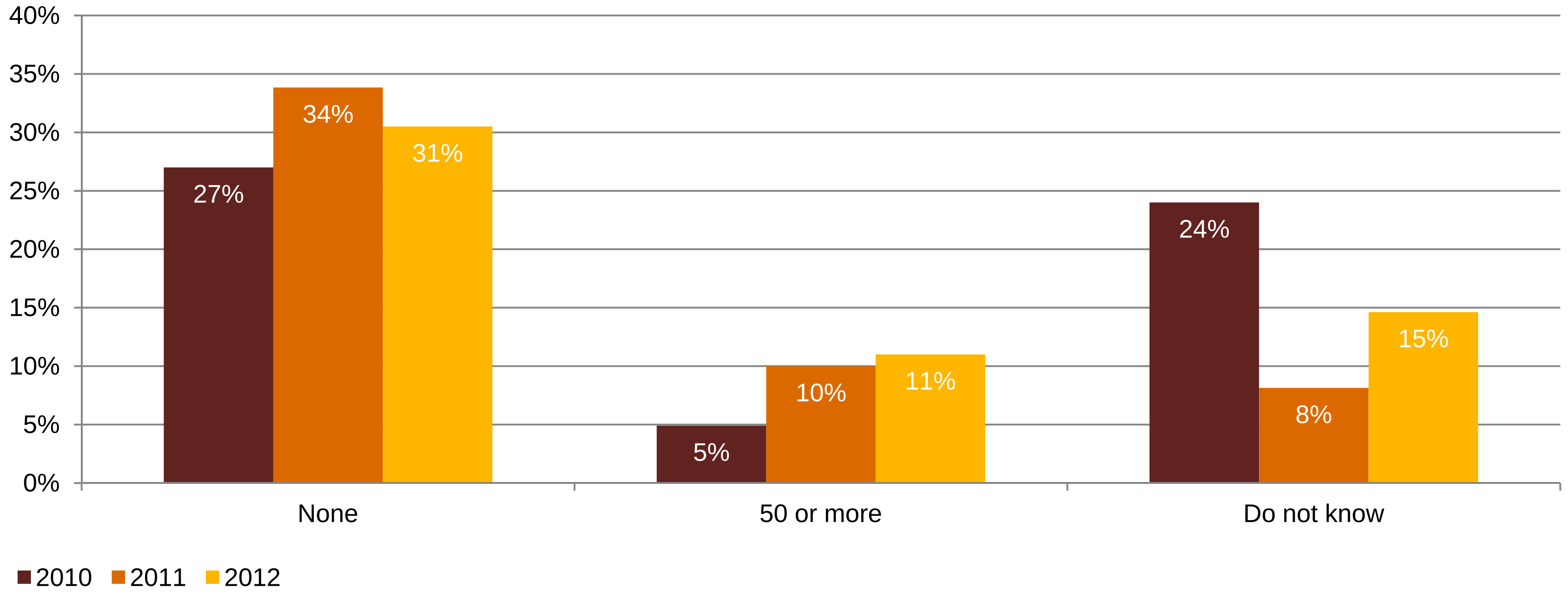
Lingering economic uncertainties continue to exercise a very significant influence on security budgets, according to financial services respondents. In fact, they say economic conditions are as important as regulatory compliance when determining security spending.



Question 37: “What business issues or factors are driving your company's information security spending?” (Not all factors shown.)

Reported security incidents show signs of leveling off after sharp increases.

Respondents reporting the most numerous category of security incidents – 50 or more annually – inched up over 2011, halting a steep increase from the year before. On the downside, those who do not know the number of incidents almost doubled, an uncertainty that suggests ineffective security practices.



Question 17: “Number of security incidents in the past 12 months.”

Many respondents do not have security training programs for employees.

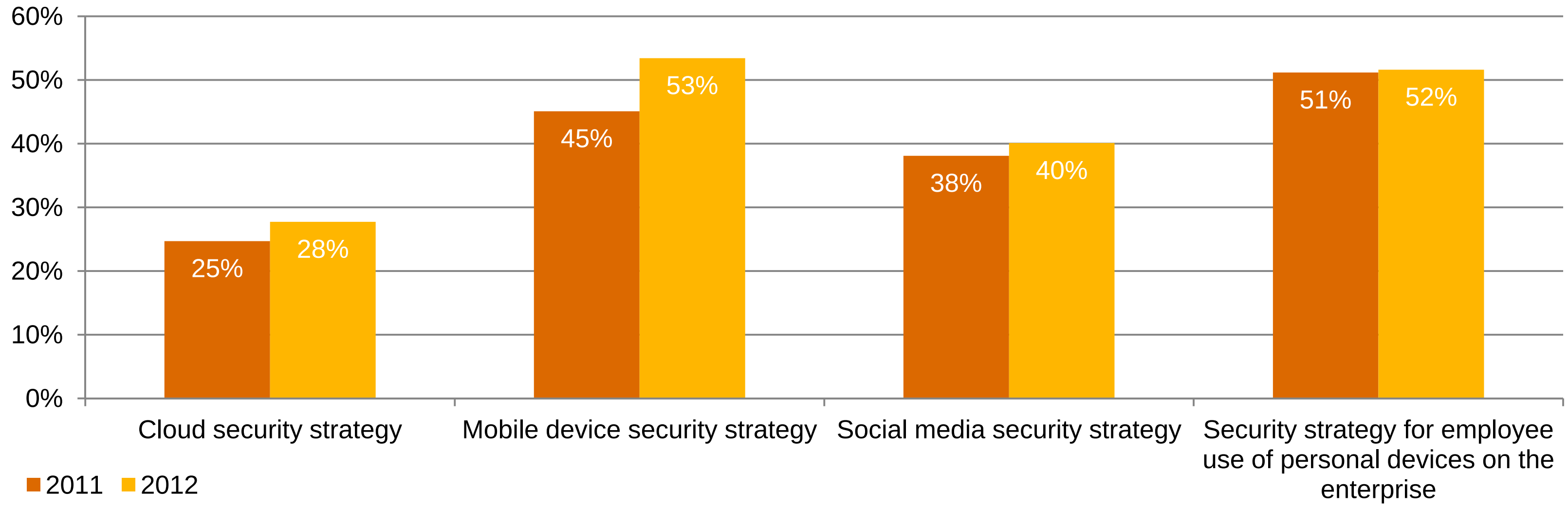
No security program can be effective without enterprise-wide training, yet 35% of financial services respondents say their firm does not have an employee security awareness training program. Staff dedicated to security awareness and training continued a multi-year downtrend.

Information security safeguards	2009	2010	2011	2012
Have employee security awareness training program	65%	61%	54%	65%
Have people dedicated to employee awareness programs	67%	64%	61%	59%

Question 14: “What process information security safeguards does your organization currently have in place?” Question 13: “What information security safeguards related to people does your organization have in place?”

Technology adoption is moving faster than security implementation.

As with many industries, financial services firms are struggling to keep pace with the adoption of cloud computing, social networking, mobility, and use of personal devices. These new technologies often are not included in overall security plans even though they are widely used. In a recent survey, for instance, we found that 88% of consumers use a personal mobile device for both personal and work purposes.[1]

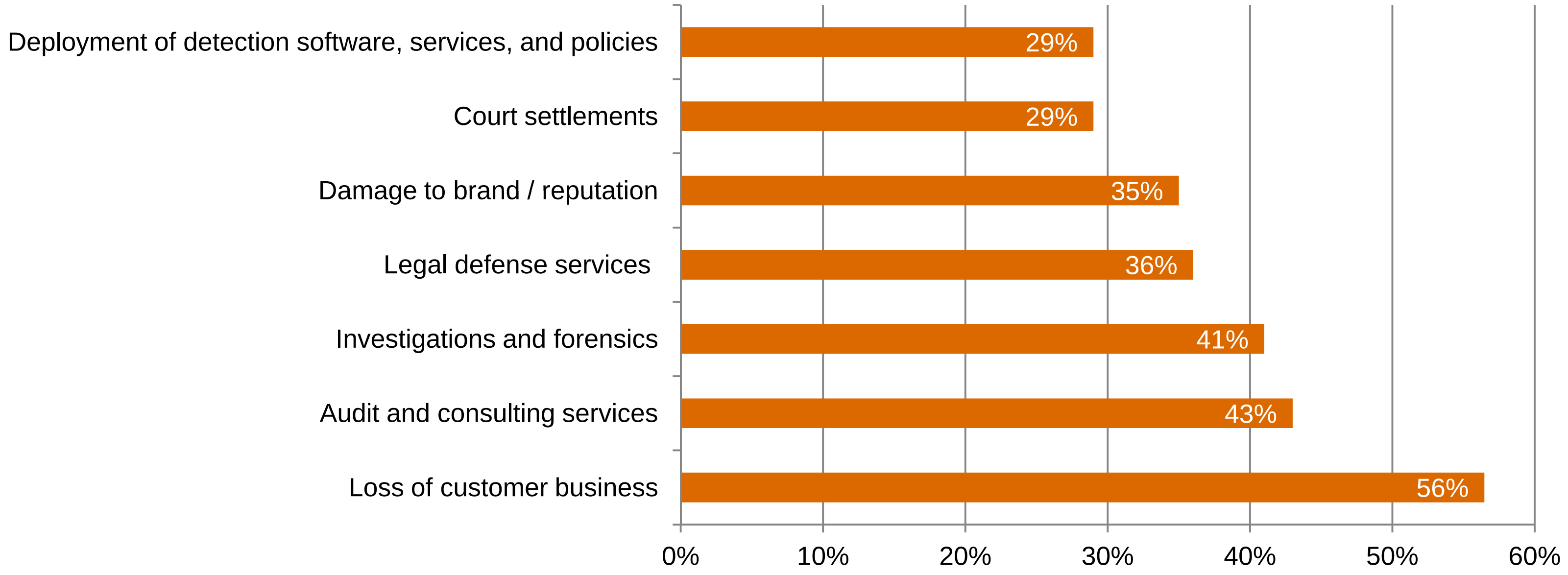


Question 14: “What process information security safeguards does your organization currently have in place?”

[1] PwC, Consumer privacy: What are consumers willing to share? July 2012

An inadequate assessment of security incidents can lead to a less-clear understanding of their impact.

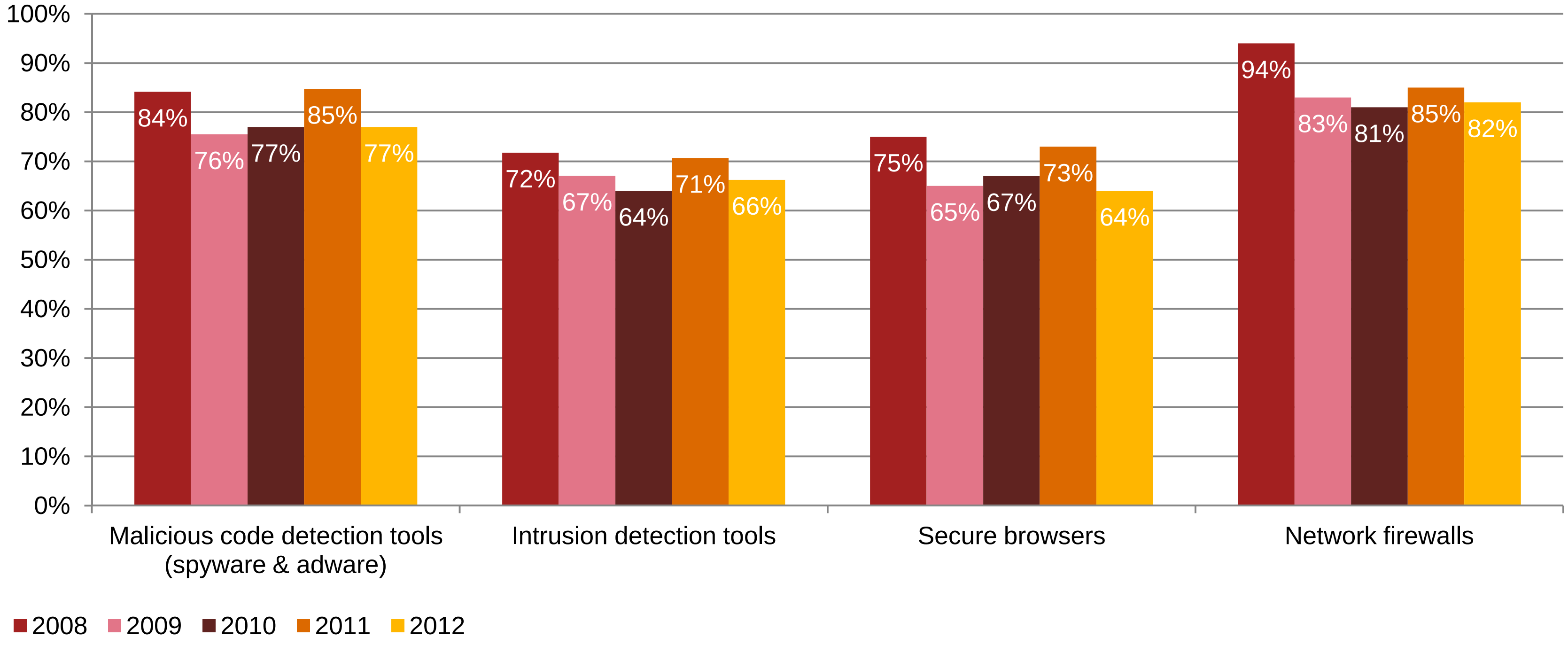
Financial services respondents reported a lower incidence of monetary losses from security incidents than last year, yet many do not apply thorough or consistent analysis to appraising those losses. For example, only 35% consider damage to brand/reputation, while 36% factor in legal costs.



Question 21: “How was your organization impacted by the security incident?” Question 21C: “What factors are included in your company’s calculation of these financial losses?”

Use of some key technology safeguards resumed a long-term decline after last year's uptick.

The future looked bright last year as many financial firms stepped up investments in technology safeguards. This year, however, saw a decrease in deployment of important security and privacy tools.



Question 15: "What technology information security safeguards does your organization have in place?"

Section 4

It's how you play the game

What keeps security from being what it should be?

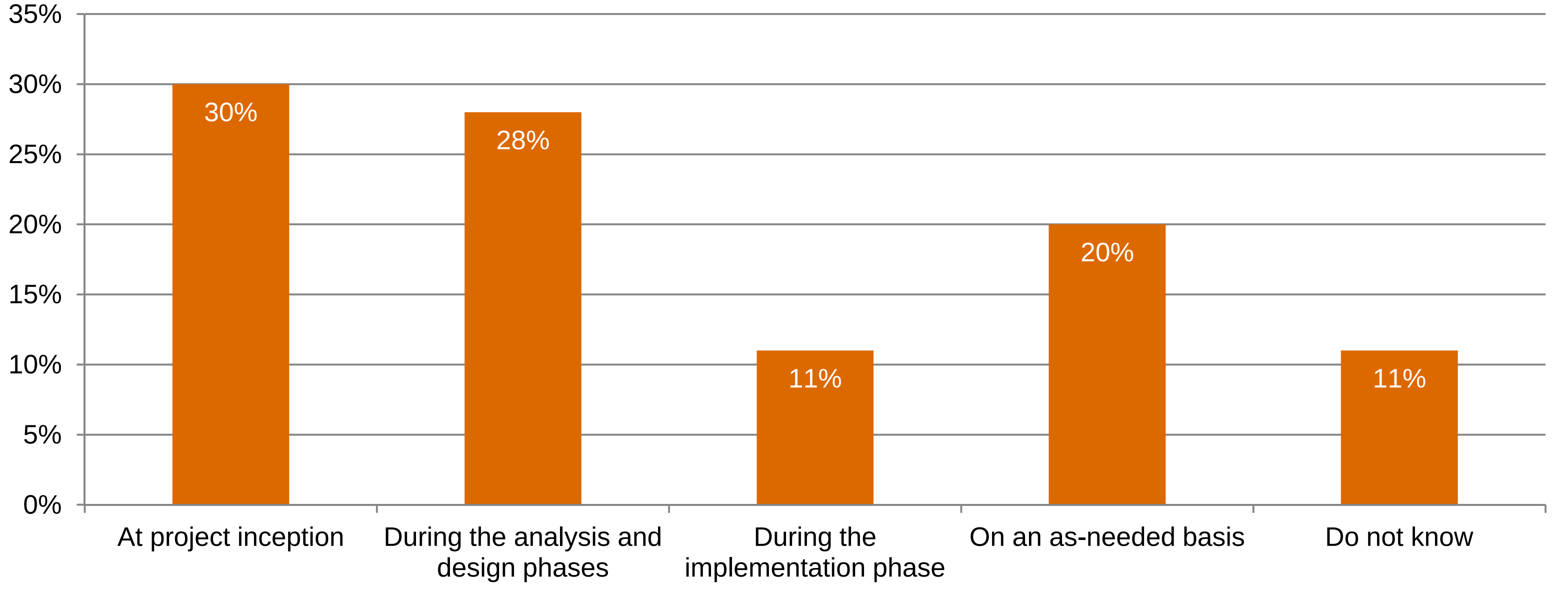
Company leadership is perceived to be an obstacle to effective security, according to 49% of financial services respondents. Other top concerns include a lack of vision and inadequate capital funding, both cited by more than one-quarter of respondents.

	2011	2012
Leadership – CEO, President, Board, or equivalent	21%	21%
Leadership – CIO or equivalent	15%	14%
Leadership – CISO, CSO, or equivalent	15%	14%
Lack of an actionable vision or understanding	28%	27%
Insufficient capital expenditures	25%	26%
Absence or shortage of in-house technical expertise	25%	23%
Poorly integrated or overly complex information/IT systems	25%	23%

Question 29: “What are the greatest obstacles to improving the overall strategic effectiveness of your organization’s information security function?”

Security is not always baked into major projects from the beginning.

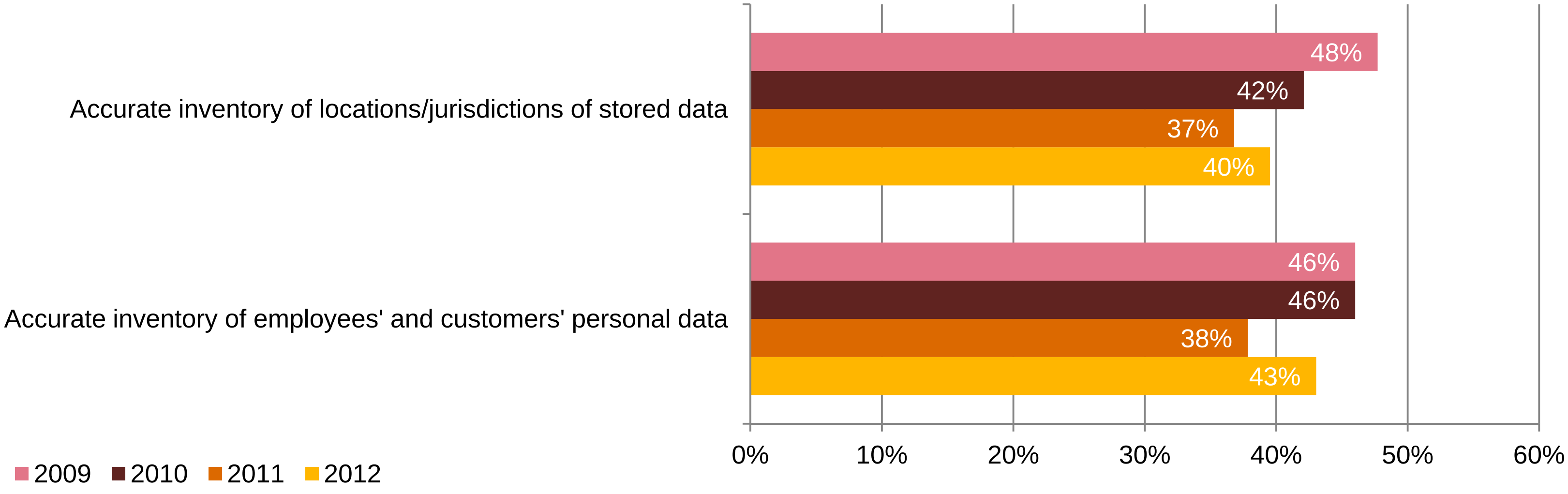
Any project should include security from the very start, and that's especially true in highly regulated industries like financial services. Yet almost one-third of respondents involve security only during the implementation phase or on an as-needed basis.



Question 30: "When does information security become involved in major projects?"

Financial services respondents know less about their data now than they did three years ago.

While approximately 90% of respondents say protecting employee and customer data is important, far fewer understand what that data entails and where it is stored. This is significant because, increasingly, consumers want to be in control of their personal data and "turn off" the flow of information from companies.[2]



Question 38: "What level of importance does your company place on protecting the following types of information?" Q11: "Which data privacy safeguards does your organization have in place?"

[2] PwC, Consumer privacy: What are consumers willing to share? July 2012

What you can do to improve your performance.

Information security today is a rapidly evolving game of advanced skill and strategy. As a result, the security models of the past decade are no longer effective.

Effective security requires a new way of thinking. The very survival of the business demands that security leaders understand, prepare for, and quickly respond to security threats.

Businesses seeking to strengthen their security practice must:

- Implement a comprehensive risk-assessment strategy and align security investments with identified risks.
- Understand their organization's information, who wants it, and what tactics adversaries might use to get it.
- Understand that information security requirements – and, indeed, overall strategies for doing business – have reached a turning point.
- Embrace a new way of thinking in which information security is both a means to protect data as well as an opportunity to create value to the business.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
949.437.5380
gary.loveland@us.pwc.com

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

US Financial Services Contacts

Joe Nocera
Principal
312.298.2745
joseph.nocera@us.pwc.com

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

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

Or visit www.pwc.com/giss2013

The Global State of Information Security® is a registered trademark of International Data Group, Inc.

PwC

www.pwc.com/security

Changing the game

While tight budgets have forestalled updates to security programs, many businesses are confident they're winning the game. But the rules – and the players – have changed.

Healthcare Providers

Key findings from The Global State of Information Security® Survey 2013

September 2012

"You can't succeed in today's elevated threat environment if you don't know the players and you don't know the rules."

– Gary Loveland, Principal, PwC

Information security has always been a high-stakes game. One that demands a smart strategy, the right technology moves, and an unblinking eye on adversaries.

For many businesses, however, it has become a pursuit that is almost impossible to win. That’s because the rules have changed, and opponents—old and new—are armed with expert technology skills. As a result, the risks are greater than ever.

Businesses are fighting back by adopting new detection and prevention technologies. At the same time, governments around the world are enacting legislation to combat cyber threats. And regulatory bodies are issuing new guidance on disclosure obligations for cyber incidents.

Yet risks to data security continue to intensify – and show no signs of abating. Those keeping score agree that the bad guys appear to be in the lead.

Nonetheless, many businesses believe they are winning. The Global State of Information Security® Survey 2013 shows that most executives in the global healthcare provider industry are confident in the effectiveness of their information security practices. They believe their strategies are sound and many consider themselves to be leaders in the field.

The odds, however, are not in their favor: Diminished budgets have resulted in degraded security programs, reported security incidents are on the rise, and new technologies are being adopted faster than they can be safeguarded.

Given today's elevated threat environment, businesses can no longer afford to play a game of chance. They must prepare to play a new game, one that requires advanced levels of skill and strategy to win.

Agenda

Section 1. Methodology

Section 2. A game of confidence

Section 3. A game of risk

Section 4. It’s how you play the game

Section 1

Methodology

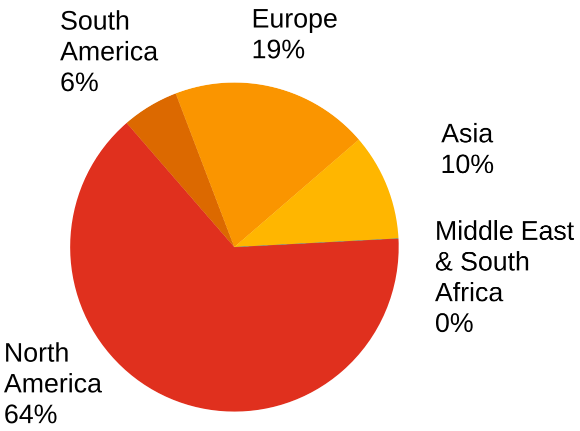
A worldwide study

The Global State of Information Security® Survey 2013, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 1, 2012 to April 15, 2012.

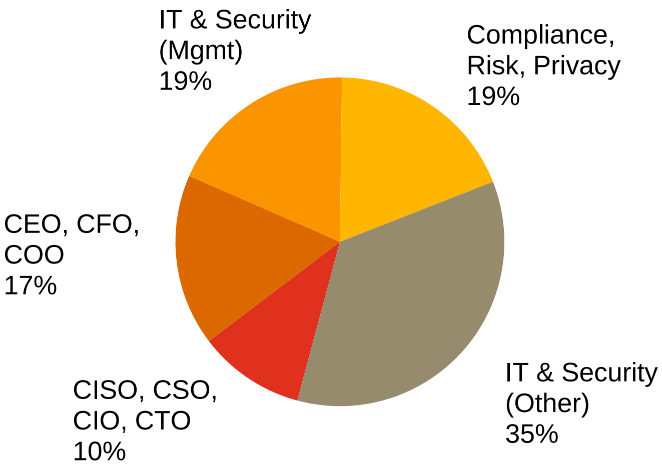
- PwC's 15th year conducting the online survey, 10th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 128 countries
- More than 9,300 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-three percent (33%) of respondents from companies with revenue of $500 million+
- Survey included 467 respondents from the healthcare provider industry
- Margin of error less than 1%

Demographics

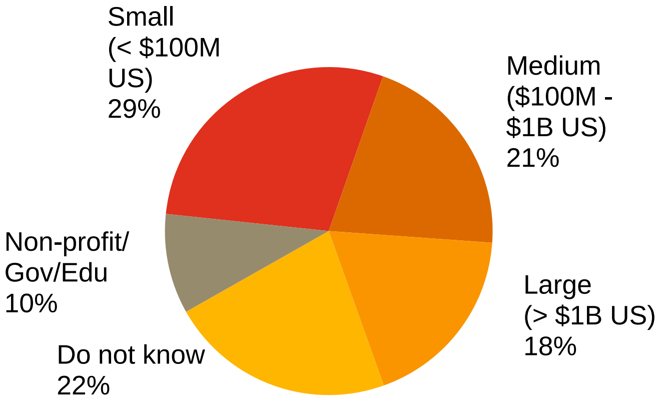
Healthcare provider respondents by region of employment



Healthcare provider respondents by title



Healthcare provider respondents by company revenue size



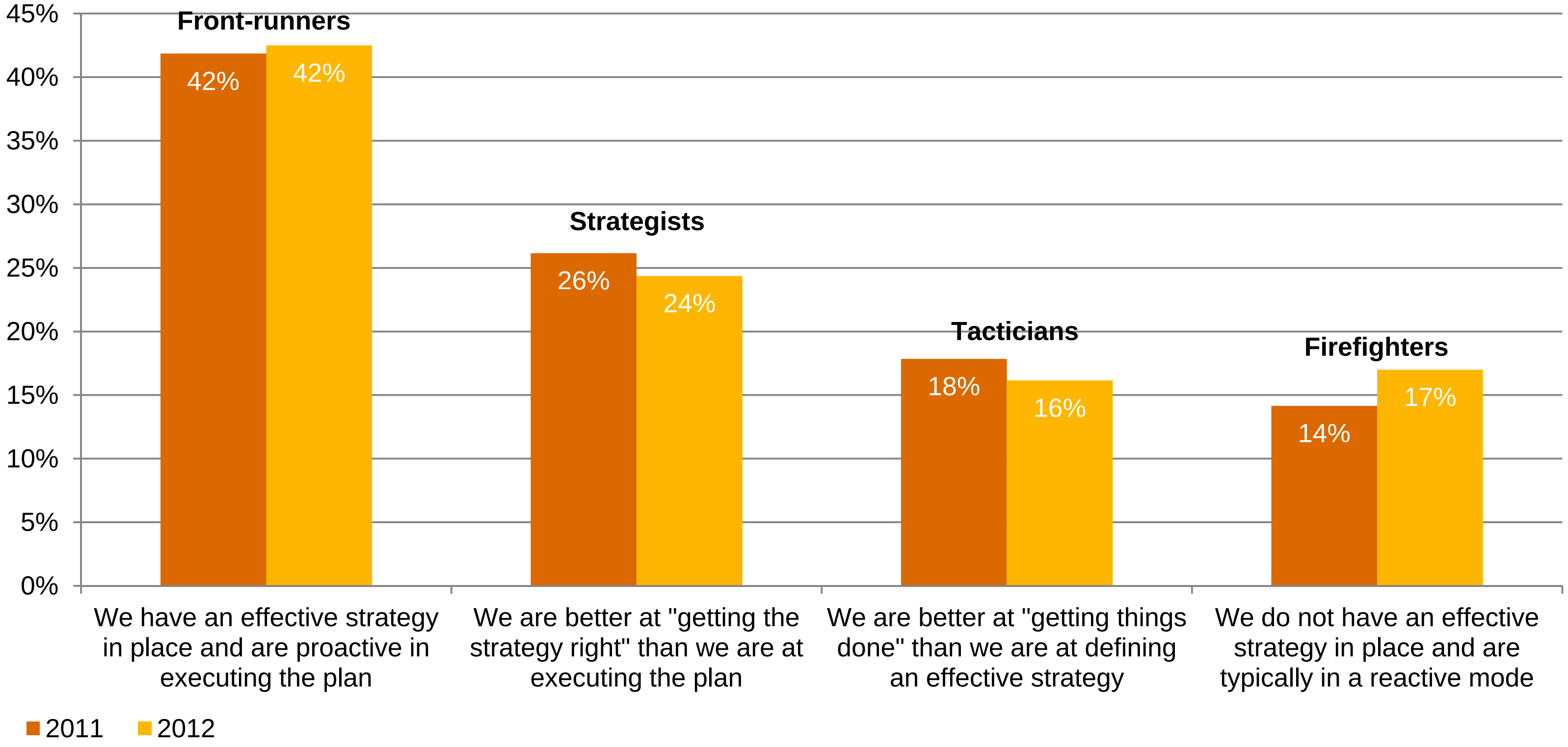
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

A game of confidence

Healthcare respondents are confident in their security practices

42% of healthcare provider respondents say their organization has a strategy in place and is proactive in executing it — exhibiting two distinctive attributes of a leader.



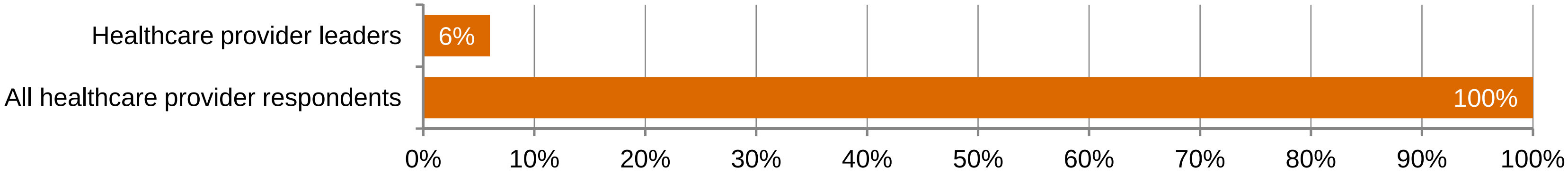
Question 28: "Which category below best characterizes your organization’s approach to protecting information security?"

A reality check on real leaders.

But are they really leaders? We measured healthcare provider respondents' self-appraisal against four key criteria to define leadership. To qualify, they must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the "top of the house" (e.g., to the CEO, CFO, COO, or legal counsel)
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

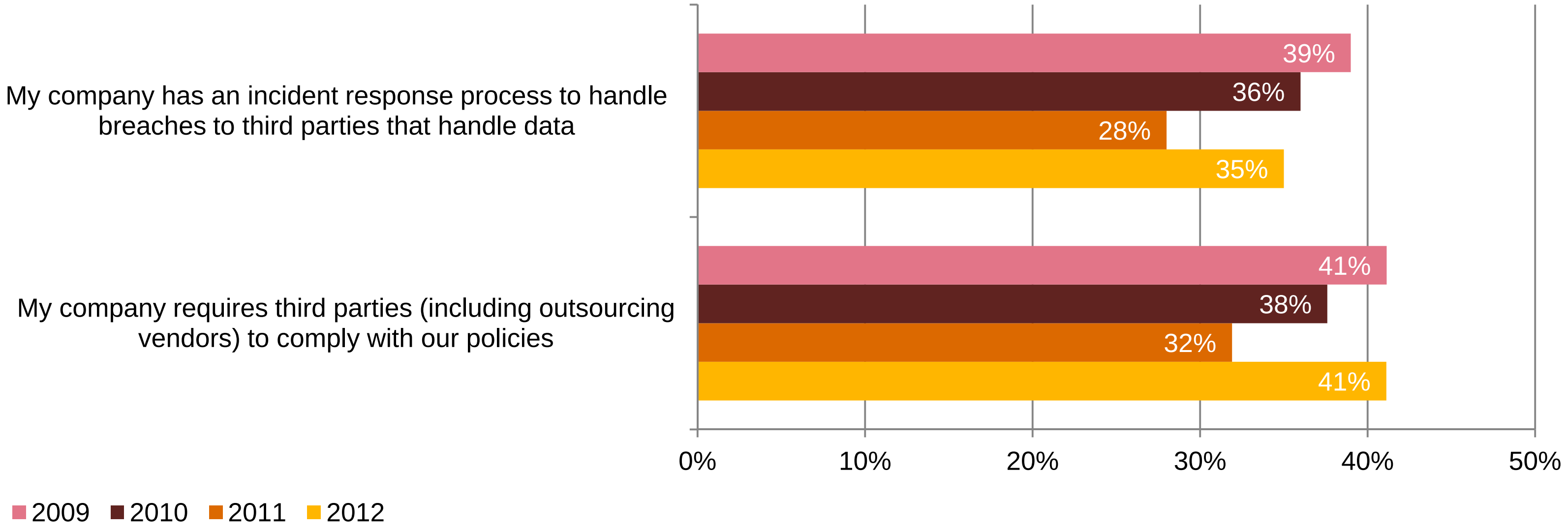
The result? Our analysis found that 6% of healthcare provider respondents rank as leaders.



Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 18: "What types of security incidents (breach or downtime) occurred" and Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Many healthcare providers lack incident response processes and compliance policies for third parties.

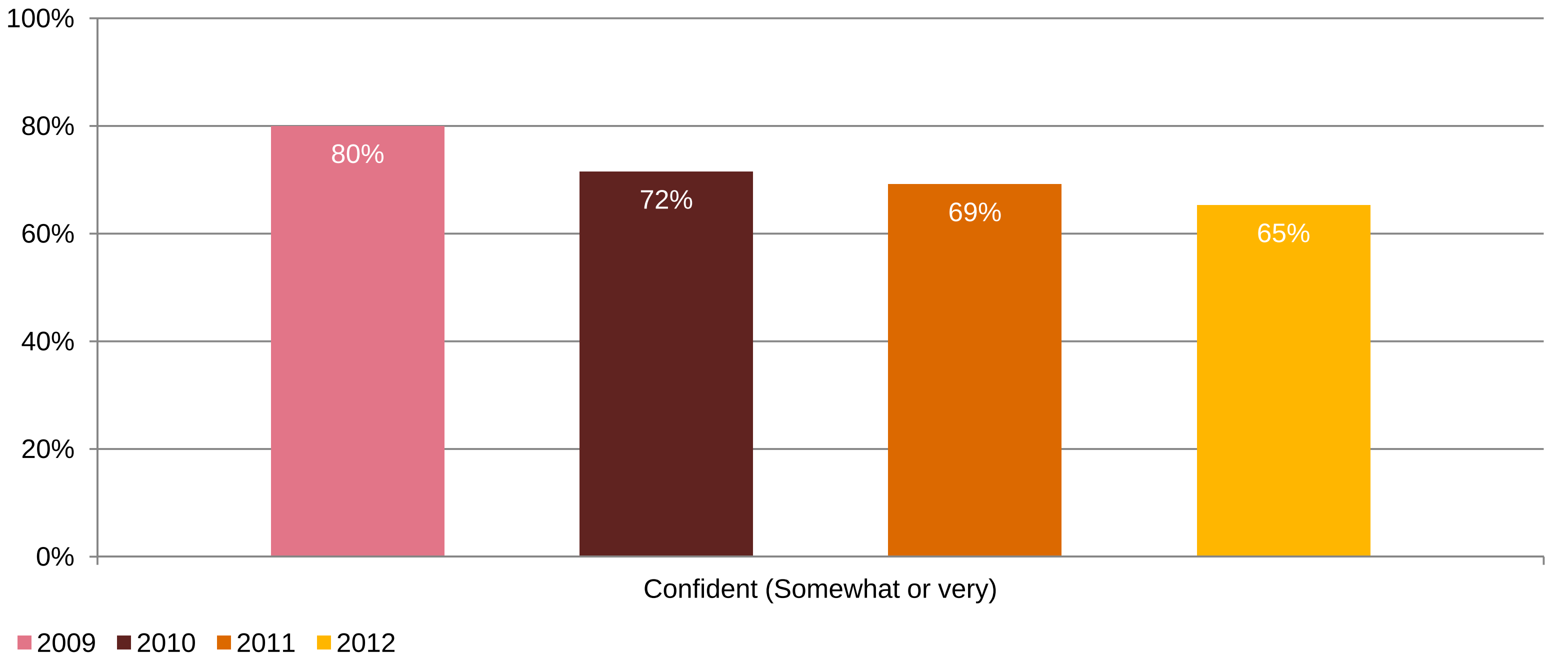
Data privacy is paramount in the healthcare provider industry, yet most respondents say they do not have a process in place to handle third-party breaches. What's more, only 41% require third parties to comply with their privacy policies.



Question 11: "Which data privacy safeguards does your organization have in place?"

Most respondents say their information security activities are effective, but this confidence is eroding.

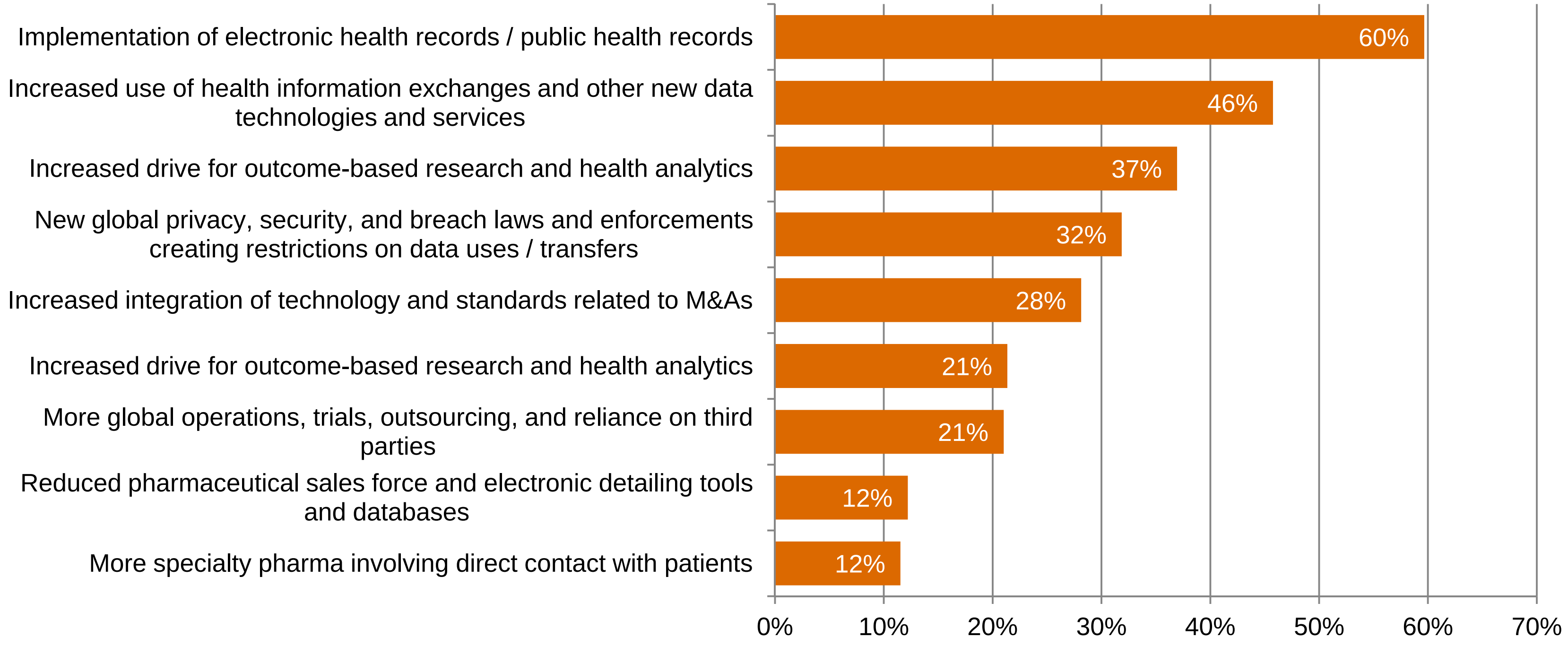
Confidence is a good thing. A strong 65% of healthcare provider respondents say they are confident their company's security activities are effective, but they may not realize that assurance has dropped considerably since 2009.



Question 41: "How confident are you that your organization's information security activities are effective?"

New electronic data technologies and services are driving spending.

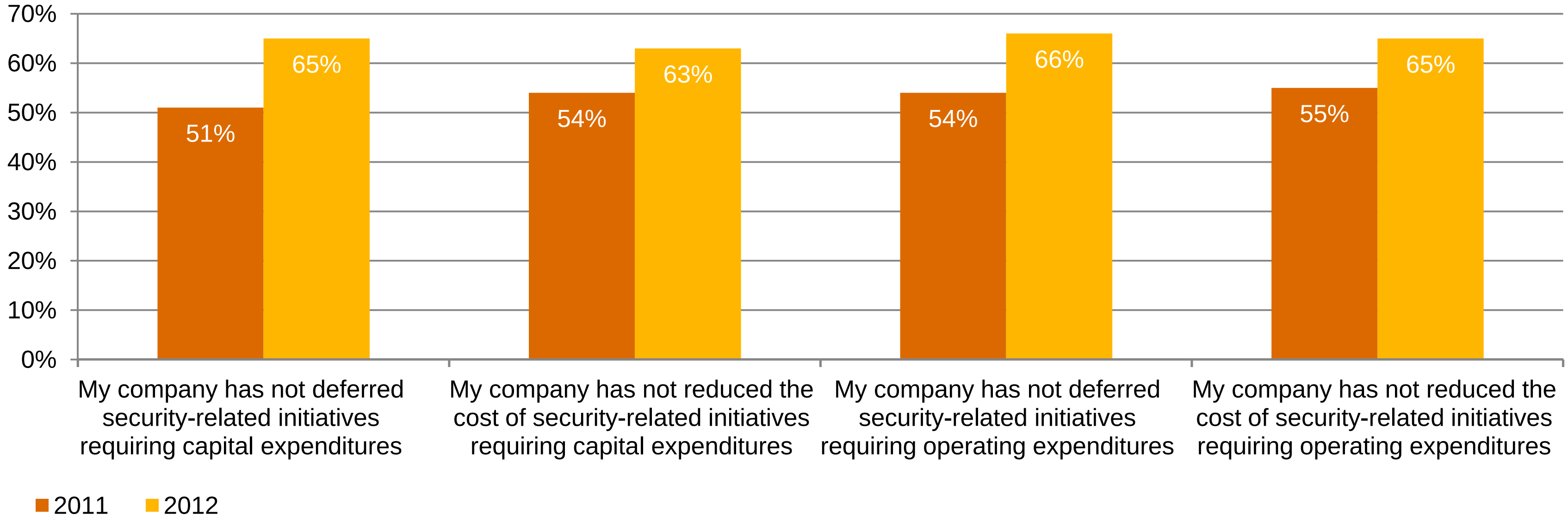
Implementation of electronic health records and public health records is, at 60%, the top driver of security spending, followed by the use of new health data technologies and services.



(Asked only of Healthcare Provider respondents) Question 1: “Which healthcare trends are driving your investment in information security?”

Among healthcare provider respondents, the outlook for security spending over the next 12 months is mixed.

37% of healthcare provider respondents expect security budgets to increase in the year ahead. More encouragingly, respondents report fewer deferrals and fewer budget cutbacks for security initiatives. Compared with last year, for instance, 27% more respondents say they had not deferred security programs requiring capital expenditures.



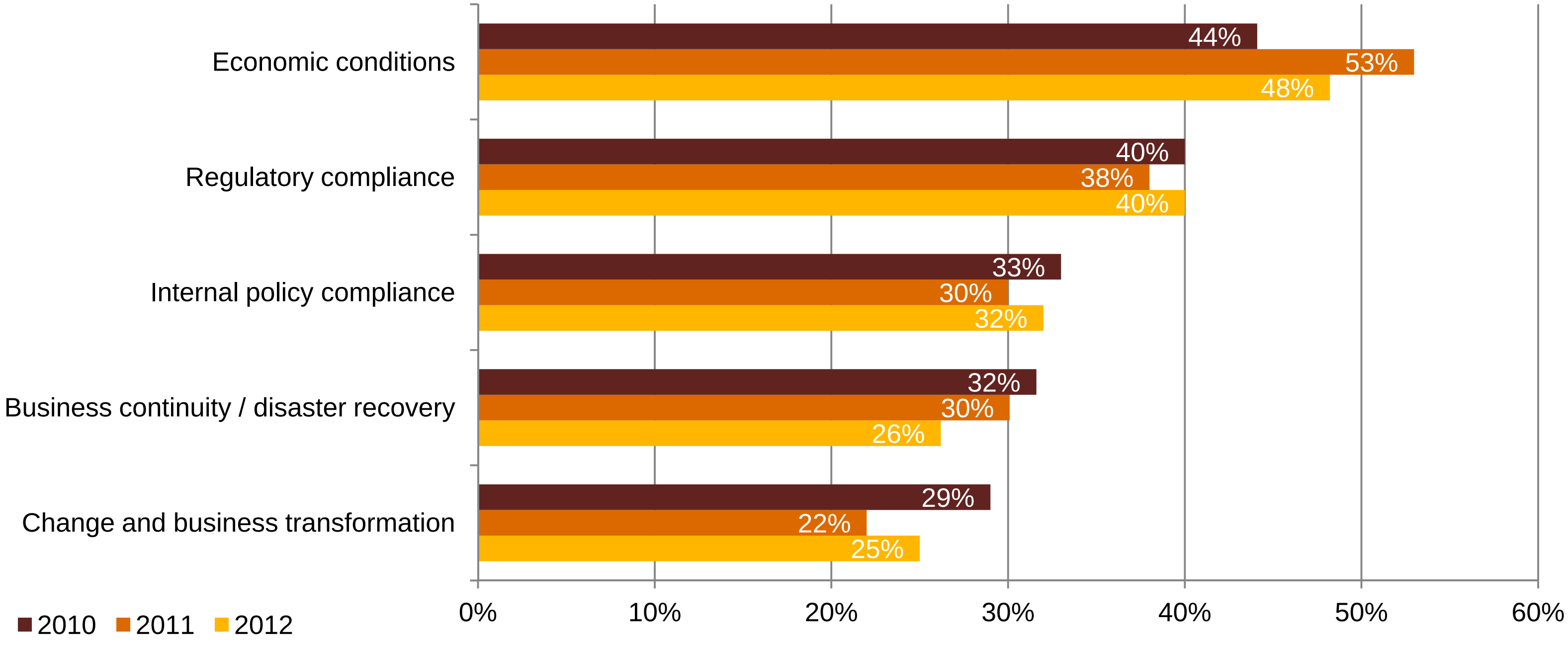
Question 8: “When compared with last year, security spending over the next 12 months will:” Questions 9A and 10A: “Has your company deferred capital and operating security-related initiatives?” Questions 9B and 10B: “Has your company reduced the capital and operating cost of security-related initiatives?”

Section 3

A game of risk

Security budgets are not driven by security needs.

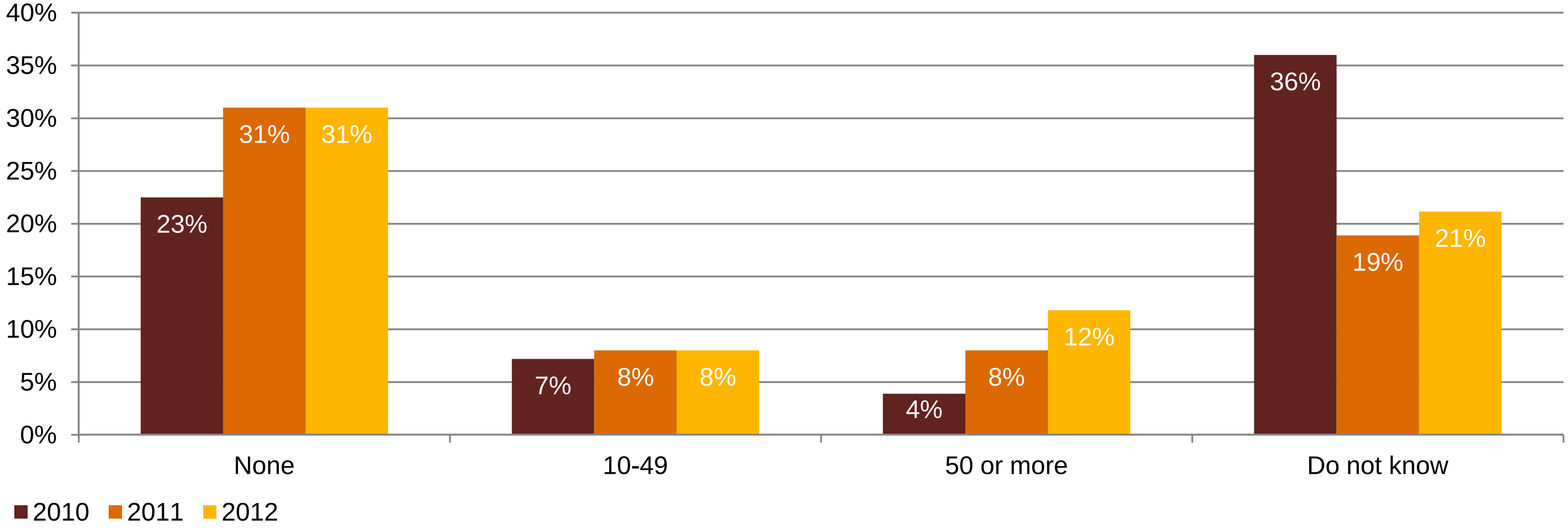
Economic conditions and compliance – both external and internal – are cited as the top drivers of security spending. At 26%, business continuity/disaster recovery is the highest-rated security-specific response.



Question 37: “What business issues or factors are driving your company's information security spending?” (Not all factors shown.)

Reported security incidents are on the rise.

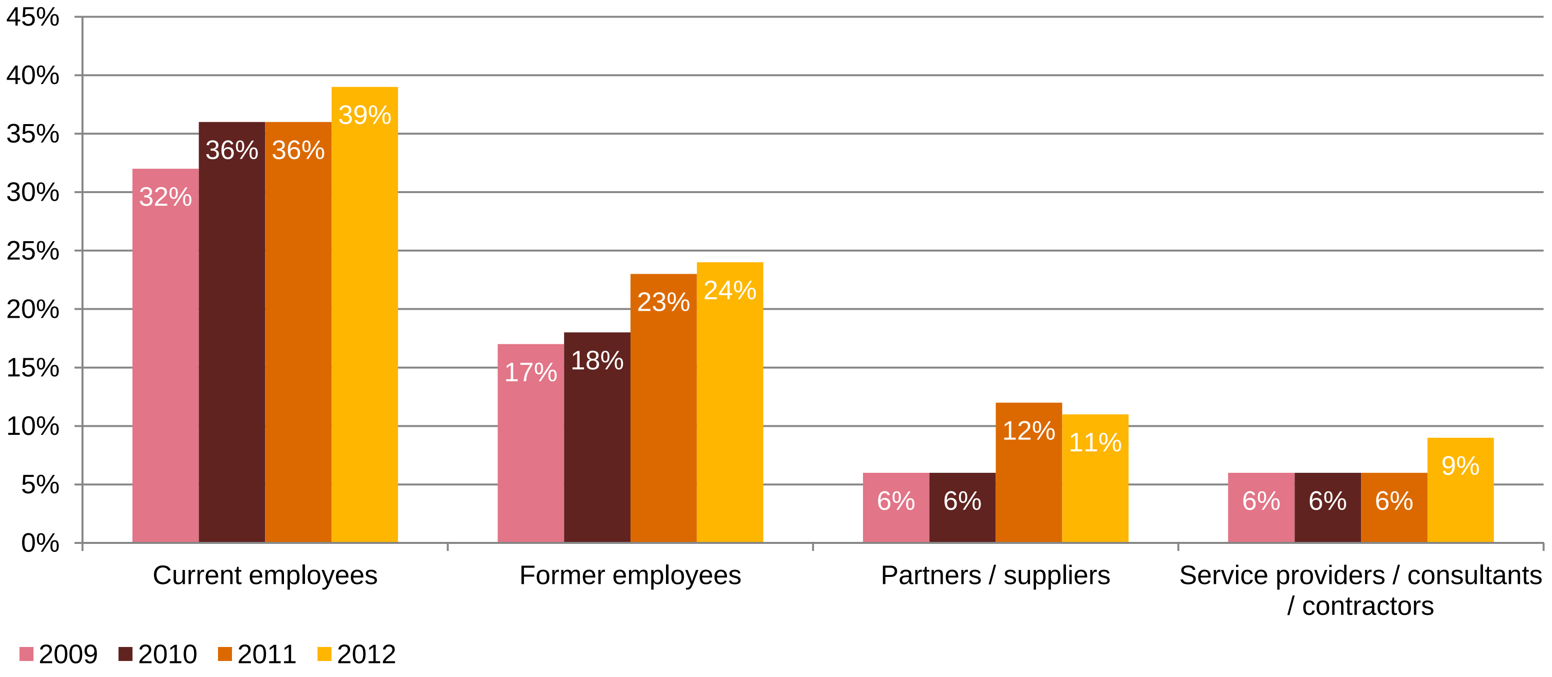
The most numerous category of reported security incidents – 50 or more per year – is the fastest growing among healthcare providers. The number of respondents that experienced 50 or more incidents in 2012 increased by 50% over the year before and 200% over 2010. One in five respondents do not know the number of incidents, an uncertainty that suggests ineffective security practices.



Question 17: “Number of security incidents in the past 12 months.”

Threats from insiders – including current and former employees – are increasing.

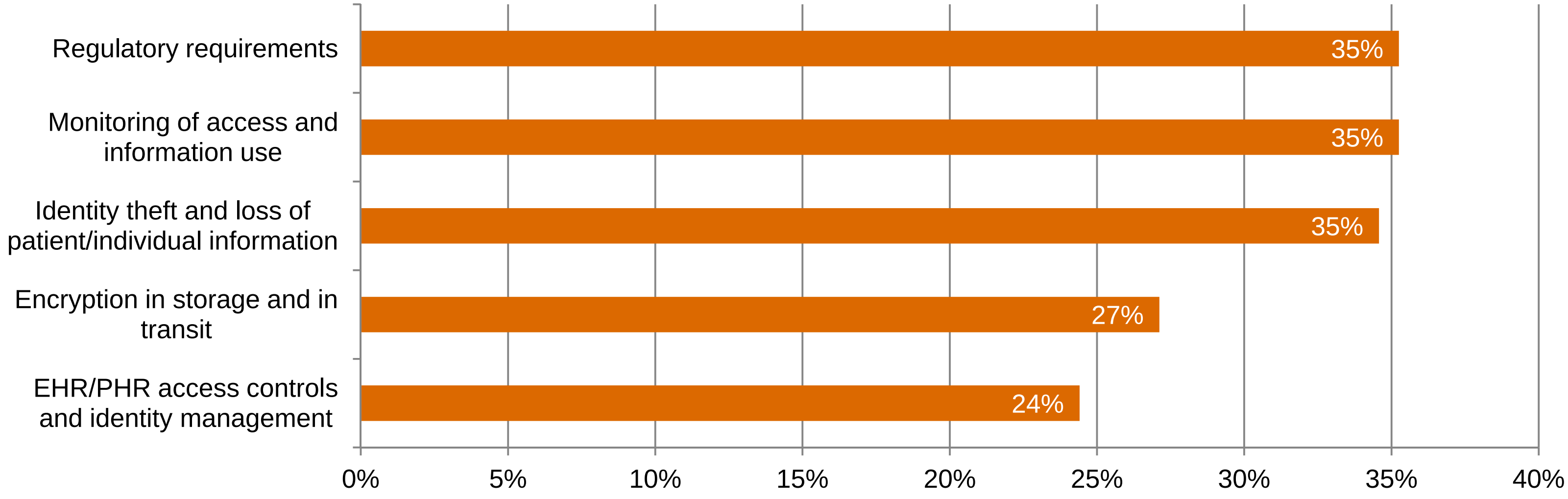
Security incidents attributed to current employees are at the highest level in years, as are those attributed to former workers. Also, more respondents point the finger at service providers/consultants/contractors this year.



Question 20: “Estimated likely source of incidents.”

Regulation and safeguarding of information are the top challenges for healthcare provider respondents.

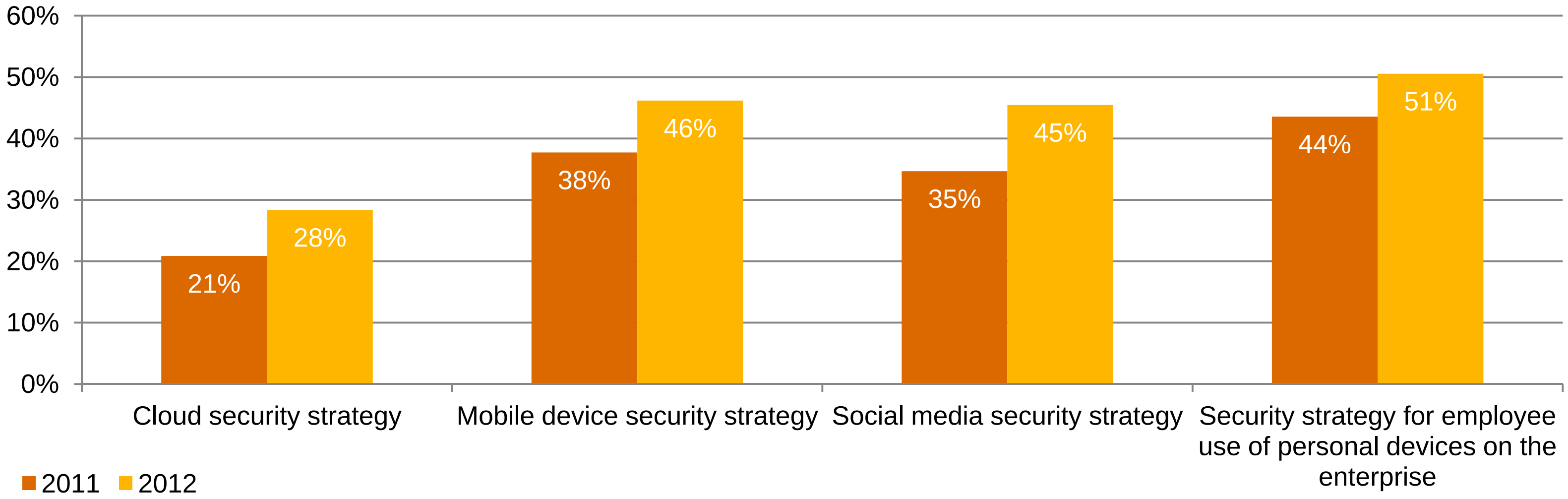
Respondents identified the top five security issues they face this year. Given increased global regulation and regulatory audits of patient data, it comes as no surprise that regulatory requirements top the list.



(Asked only of Healthcare Provider respondents) Question 2: “Please identify your top five security challenges.”

Technology adoption is moving faster than security implementation.

As with many industries, healthcare providers are struggling to keep pace with the adoption of cloud computing, social networking, mobility, and use of personal devices. These new technologies often are not included in overall security plans even though they are widely used. In a recent survey, for instance, we found that 88% of consumers use a personal mobile device for both personal and work purposes.[1]

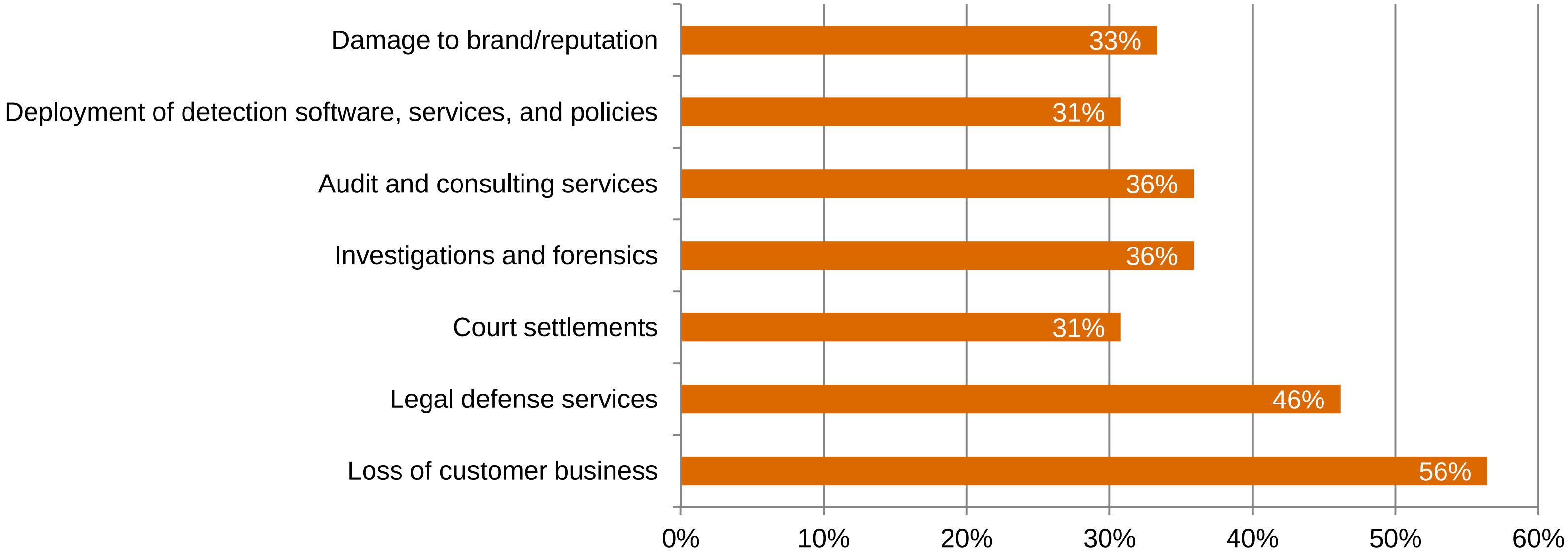


Question 14: “What process information security safeguards does your organization currently have in place?”

[1] PwC, Consumer privacy: What are consumers willing to share? July 2012

An inadequate assessment of security incidents can lead to a less-clear understanding of their financial impact.

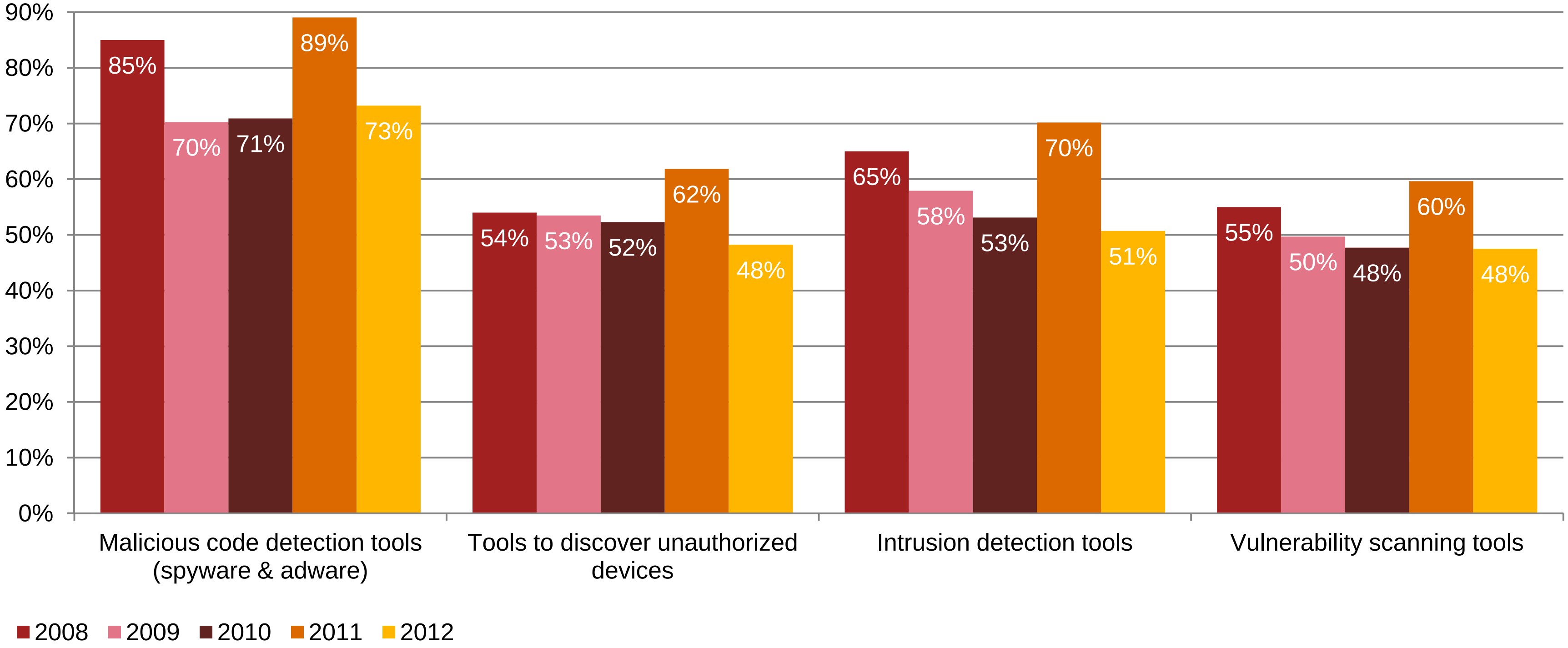
Respondents report a very low incidence of financial loss from security incidents, yet many do not perform a thorough or consistent appraisal of those losses. For example, only 33% consider damage to brand/reputation. Another factor that may lead to unmeasured financial losses: One in five respondents say security incidents result in identity theft.



Question 21: “How was your organization impacted by the security incident?” Question 21C: “What factors are included in your company’s calculation of these financial losses?”

Use of some key technology safeguards resumed a long-term decline after last year's uptick.

The future looked bright last year as many healthcare providers stepped up investments in detection safeguards. This year, however, saw a decrease in deployment of important security and privacy tools.



Question 15: "What technology information security safeguards related to detection does your organization have in place?"

Section 4

It's how you play the game

What keeps security from being what it should be?

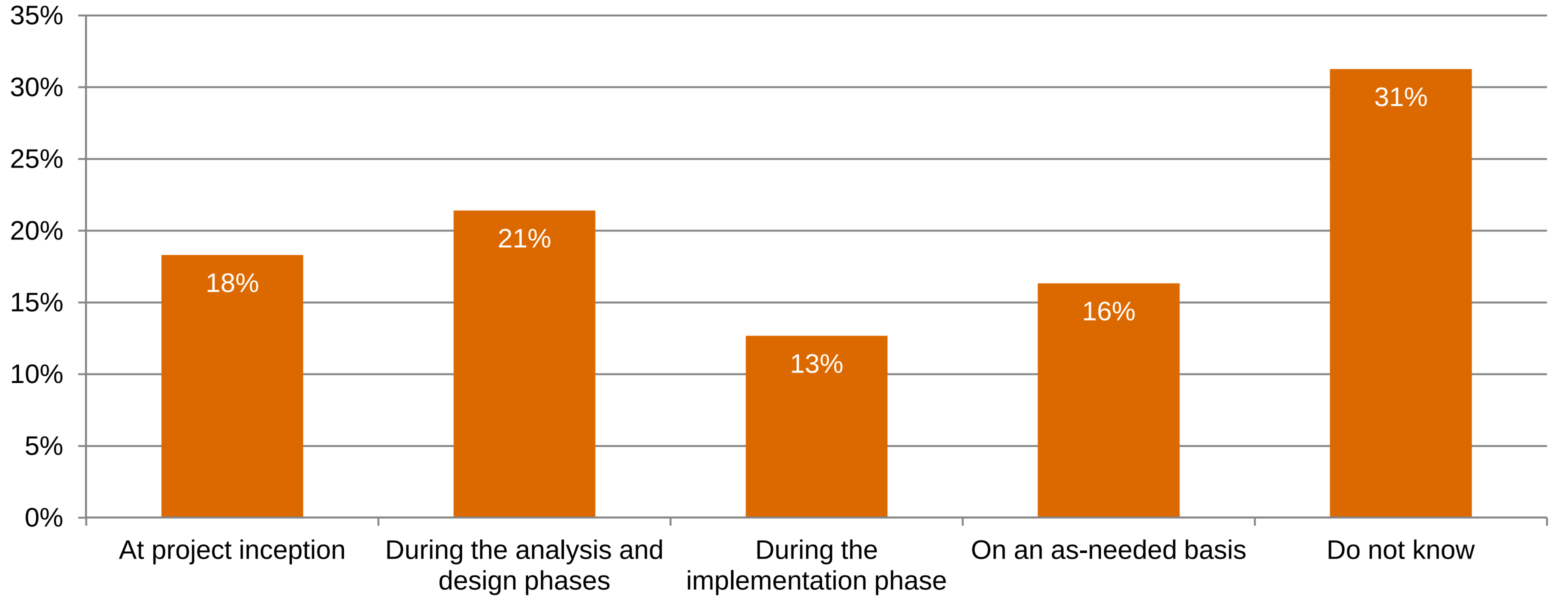
A lack of adequate funding, both capital and operating, was cited by 53% of healthcare provider respondents as the primary roadblocks to effective security. One in five respondents say top leadership – the CEO, President, or Board – is an impediment to improved security.

	2011	2012
Leadership – CEO, President, Board, or equivalent	21%	20%
Leadership – CIO or equivalent	15%	10%
Leadership – CISO, CSO, or equivalent	9%	10%
Insufficient capital expenditures	32%	27%
Insufficient operating expenditures	28%	26%
Absence or shortage of in-house technical expertise	22%	24%
Lack of actionable vision or understanding	19%	19%

Question 29: “What are the greatest obstacles to improving the overall strategic effectiveness of your organization’s information security function?”

Security is not always baked into major projects from the beginning.

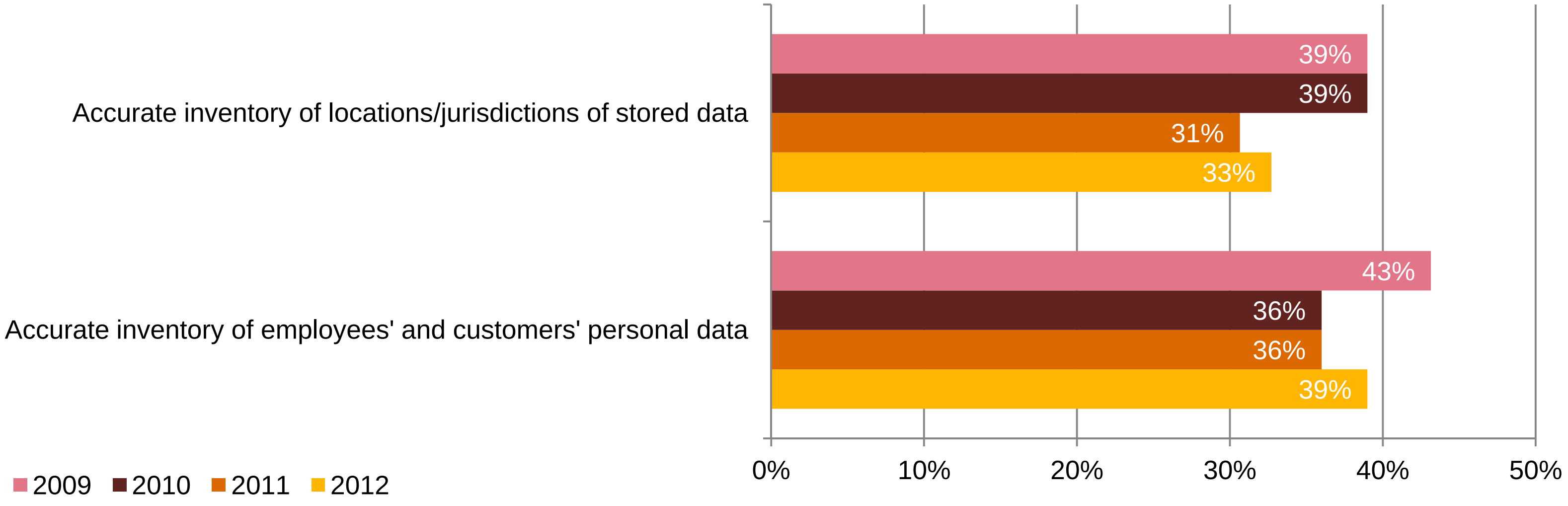
It is troubling that almost one-third (31%) of healthcare provider respondents do not know when information security becomes involved in major projects, demonstrating that security does not receive the attention it deserves. Only 18% involve security at project inception.



Question 30: “When does information security become involved in major projects?”

Healthcare provider respondents know less about their data now than they did three years ago.

While approximately 90% of respondents say protecting employee and customer data is important, far fewer know what that data entails and where it is stored. This is significant because, increasingly, understanding data, data flows, and data uses is a prerequisite to new healthcare treatment and business models. As regulations requiring disclosure of breaches increase, only 43% of respondents say they report security incidents.



Question 38: “What level of importance does your company place on protecting the following types of information?” Question 11: “Which data privacy safeguards does your organization have in place?” Question 19: “Did you report the incidents publicly, whether required by law or not?”

What you can do to improve your performance.

Information security today is a rapidly evolving game of advanced skill and strategy. As a result, the security models of the past decade are no longer effective.

Effective security requires a new way of thinking. The very survival of the business demands that security leaders understand, prepare for, and quickly respond to security threats.

Businesses seeking to strengthen their security practice must:

- Implement a comprehensive risk-assessment strategy and align security investments with identified risks.
- Understand their organization's information, who wants it, and what tactics adversaries might use to get it.
- Understand that information security requirements – and, indeed, overall strategies for doing business – have reached a turning point.
- Embrace a new way of thinking in which information security is both a means to protect data as well as an opportunity to create value to the business.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
949.437.5380
gary.loveland@us.pwc.com

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

US Healthcare Provider Contacts

Daniel Garrett
Principal
267.330.8202
daniel.garrett@us.pwc.com

Peter Harries
Principal
602.750.3404
peter.harries@us.pwc.com

Mick Coady
Principal
713.356.4366
mick.coady@us.pwc.com

Or visit www.pwc.com/giss2013

The Global State of Information Security® is a registered trademark of International Data Group, Inc.

PwC

www.pwc.com/security

Changing the game

While tight budgets have forestalled updates to security programs, many businesses are confident they're winning the game. But the rules – and the players – have changed.

Industrial Products

Key findings from The Global State of Information Security® Survey 2013

September 2012

> ***“You can’t succeed in today’s elevated threat environment if you don’t know the players and you don’t know the rules.”***
>
> ***– Gary Loveland, Principal, PwC***

Information security has always been a high-stakes game. One that demands a smart strategy, the right technology moves, and an unblinking eye on adversaries.

For many businesses, however, it has become a pursuit that is almost impossible to win. That’s because the rules have changed, and opponents—old and new—are armed with expert technology skills. As a result, the risks are greater than ever.

Businesses are fighting back by adopting new detection and prevention technologies. At the same time, governments around the world are enacting legislation to combat cyber threats. And regulatory bodies are issuing new guidance on disclosure obligations for cyber incidents.

Yet risks to data security continue to intensify – and show no signs of abating. Those keeping score agree that the bad guys appear to be in the lead.

Nonetheless, many businesses believe they are winning. The Global State of Information Security® Survey 2013 shows that most executives in the global industrial products industry are confident in the effectiveness of their information security practices. They believe their strategies are sound and many consider themselves to be leaders in the field.

The odds, however, are not in their favor: Diminished budgets have resulted in degraded security programs, reported security incidents are on the rise, and new technologies are being adopted faster than they can be safeguarded.

Given today's elevated threat environment, businesses can no longer afford to play a game of chance. They must prepare to play a new game, one that requires advanced levels of skill and strategy to win.

Agenda

Section 1. Methodology

Section 2. A game of confidence

Section 3. A game of risk

Section 4. It’s how you play the game

Section 1

Methodology

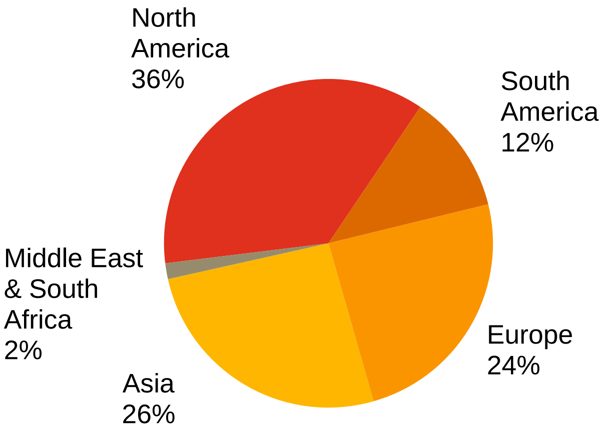
A worldwide study

The Global State of Information Security® Survey 2013, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 1, 2012 to April 15, 2012.

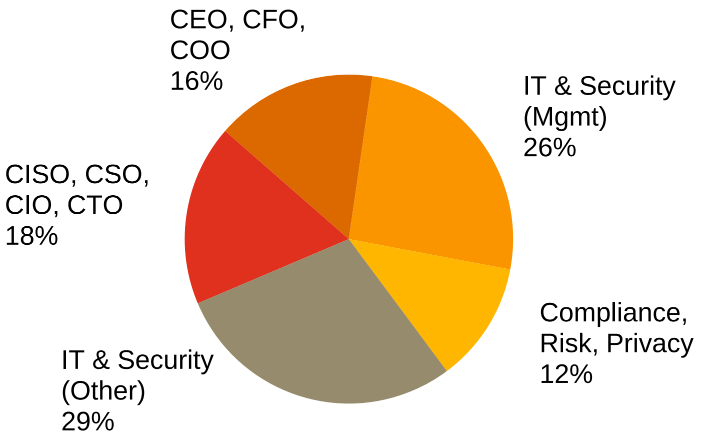
- PwC's 15th year conducting the online survey, 10th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 128 countries
- More than 9,300 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-three percent (33%) of respondents from companies with revenue of $500 million+
- Survey included 775 respondents from the industrial products industry
- Margin of error less than 1%

Demographics

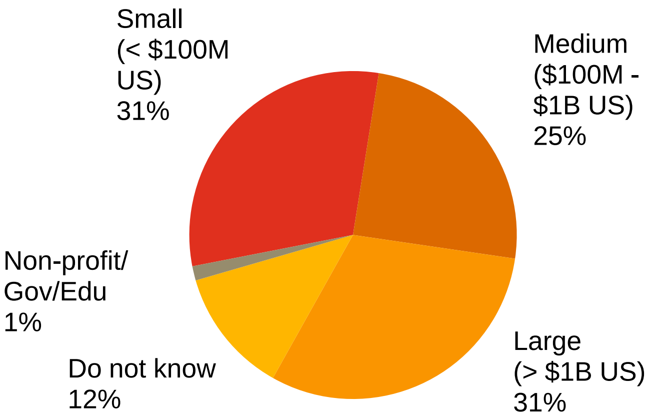
Industrial products respondents by region of employment



Industrial products respondents by title



Industrial products respondents by company revenue size



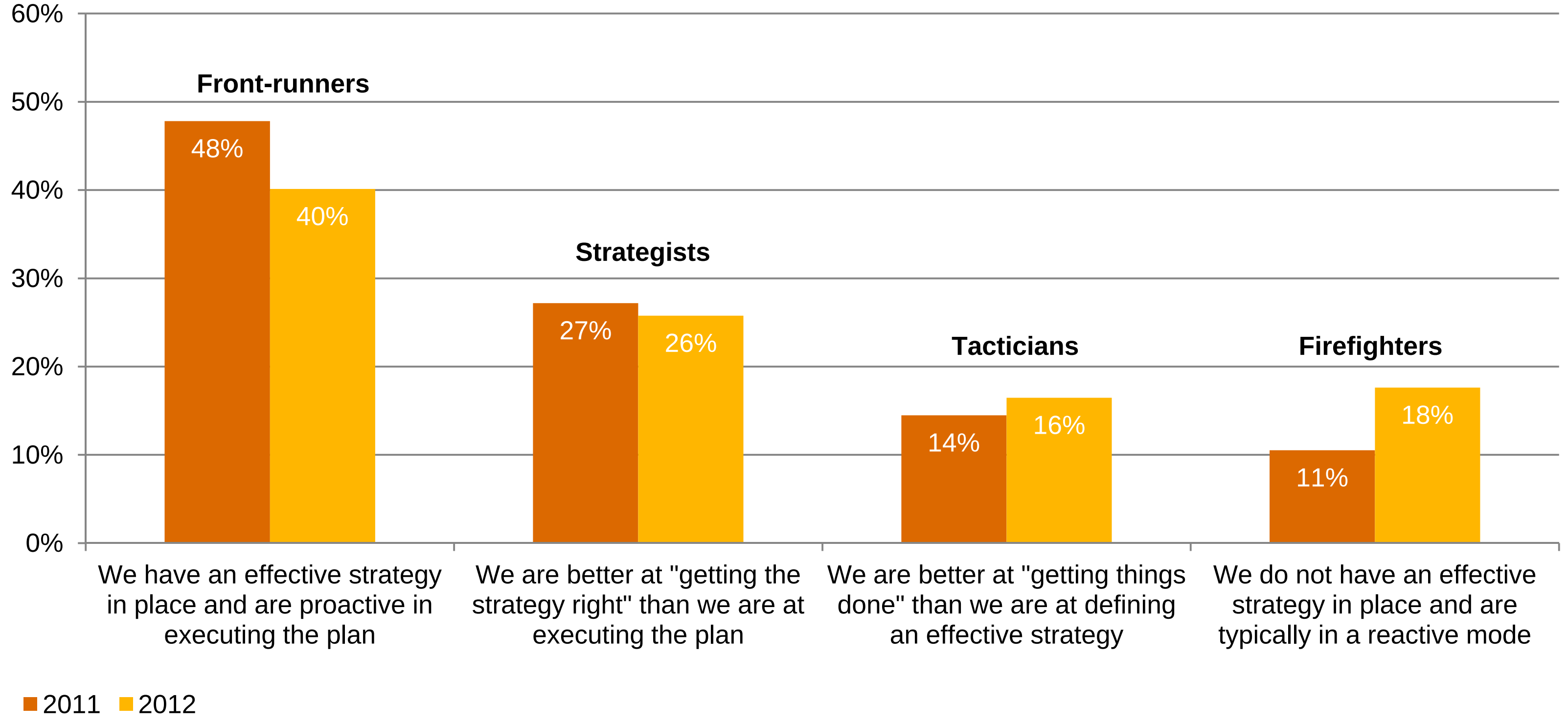
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

A game of confidence

Industrial products respondents are confident in their security practices.

40% of industry respondents say their organization has a strategy in place and is proactive in executing it – exhibiting two distinctive attributes of a leader.



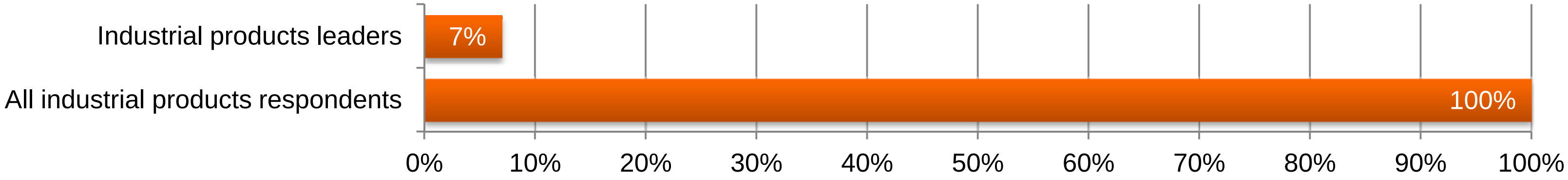
Question 28: "Which category below best characterizes your organization's approach to protecting information security?"

A reality check on real leaders.

But are they really leaders? We measured industrial products respondents' self-appraisal against four key criteria to define leadership. To qualify, organizations must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the "top of the house" (e.g., to the CEO, CFO, COO, or legal counsel)
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

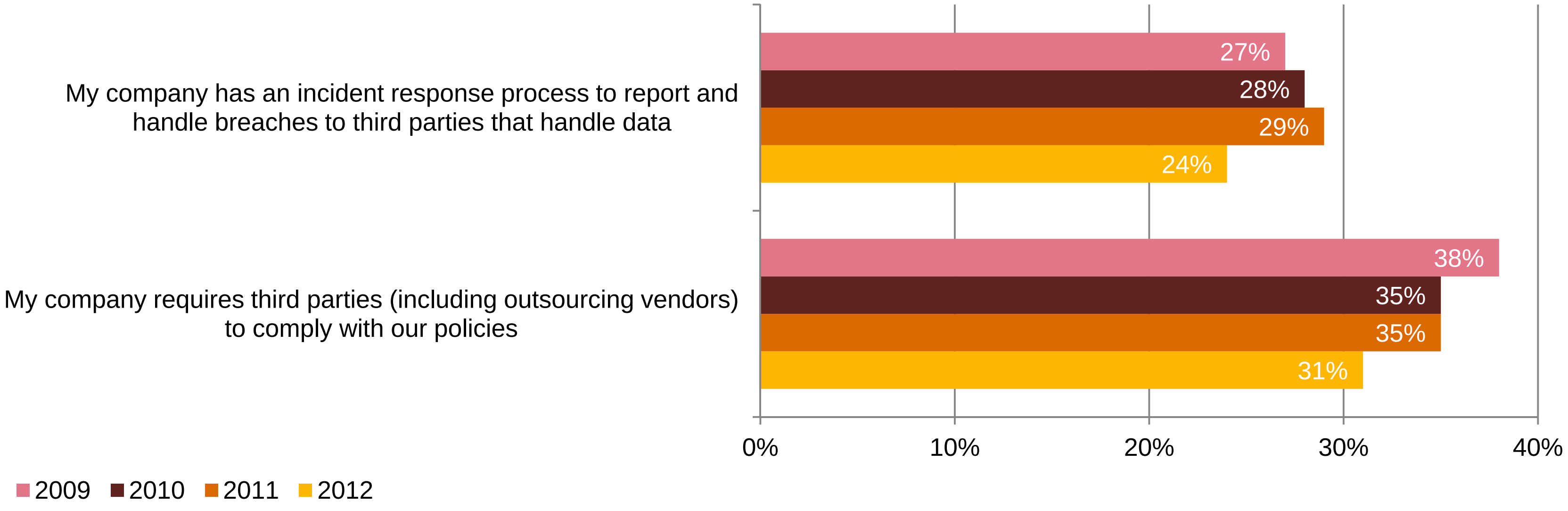
The result? Our analysis found that 7% of industrial products respondents rank as leaders.



Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 18: "What types of security incidents (breach or downtime) occurred" and Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Many industrial products respondents are over-confident in their organization's security program.

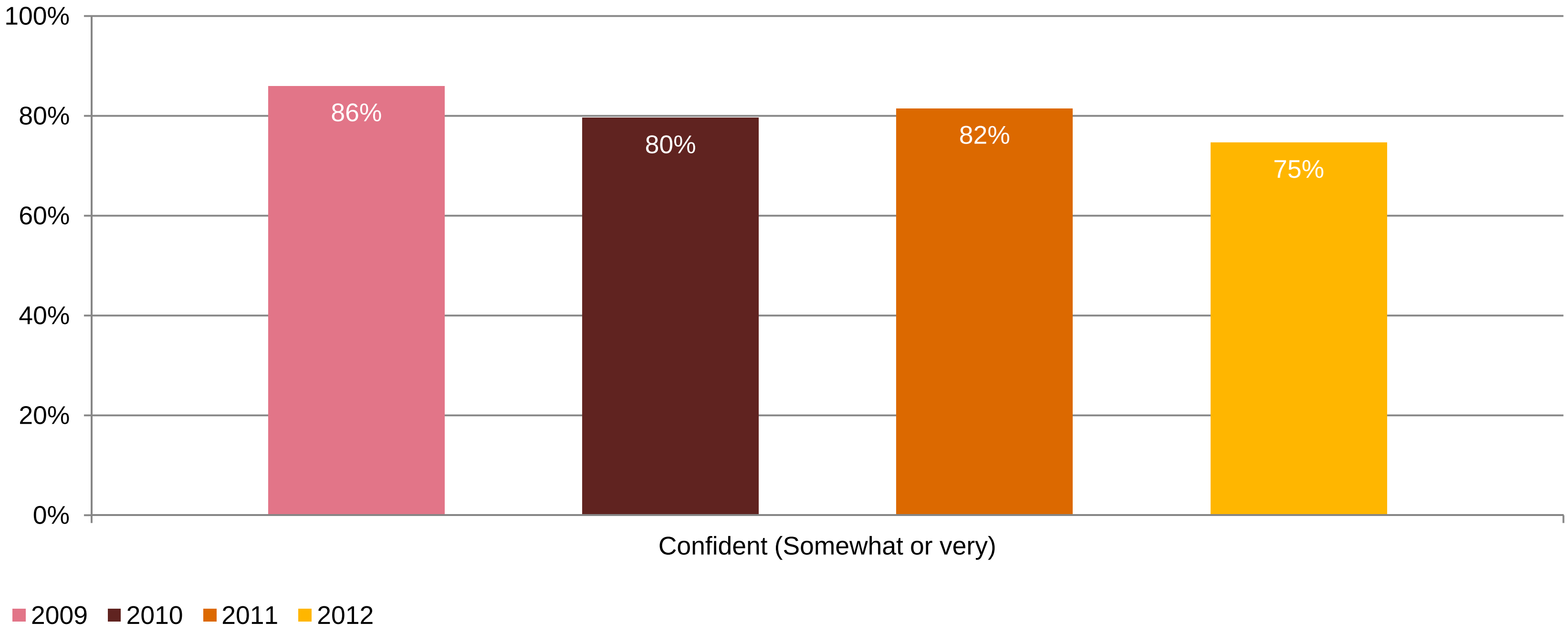
70% of respondents are confident that they have instilled effective security behaviors into their organization's culture, yet most do not have a process in place to handle third-party breaches. What's more, fewer than one-third require third parties to comply with security policies. This suggests a troubling gap in perception.



Question 35: "How confident are you that your organization has instilled effective information security behaviors into the organizational culture?"
Question 11: "Which data privacy safeguards does your organization have in place?"

Most respondents say their information security activities are effective, but confidence is eroding.

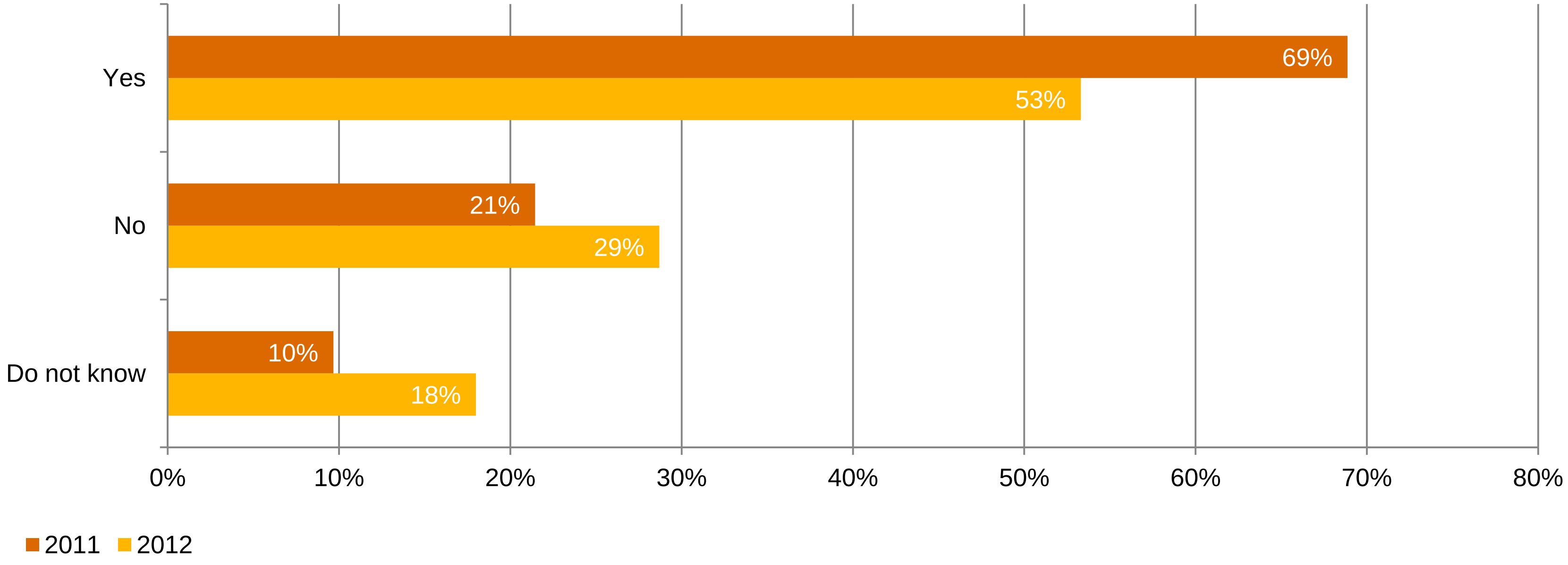
Confidence is a good thing. A strong three-quarters of industrial products respondents say they are confident that their company's security activities are effective, but many may not realize that assurance has dropped since 2009.



Question 41: "How confident are you that your organization's information security activities are effective?"

Security plans for manufacturing control systems have declined significantly.

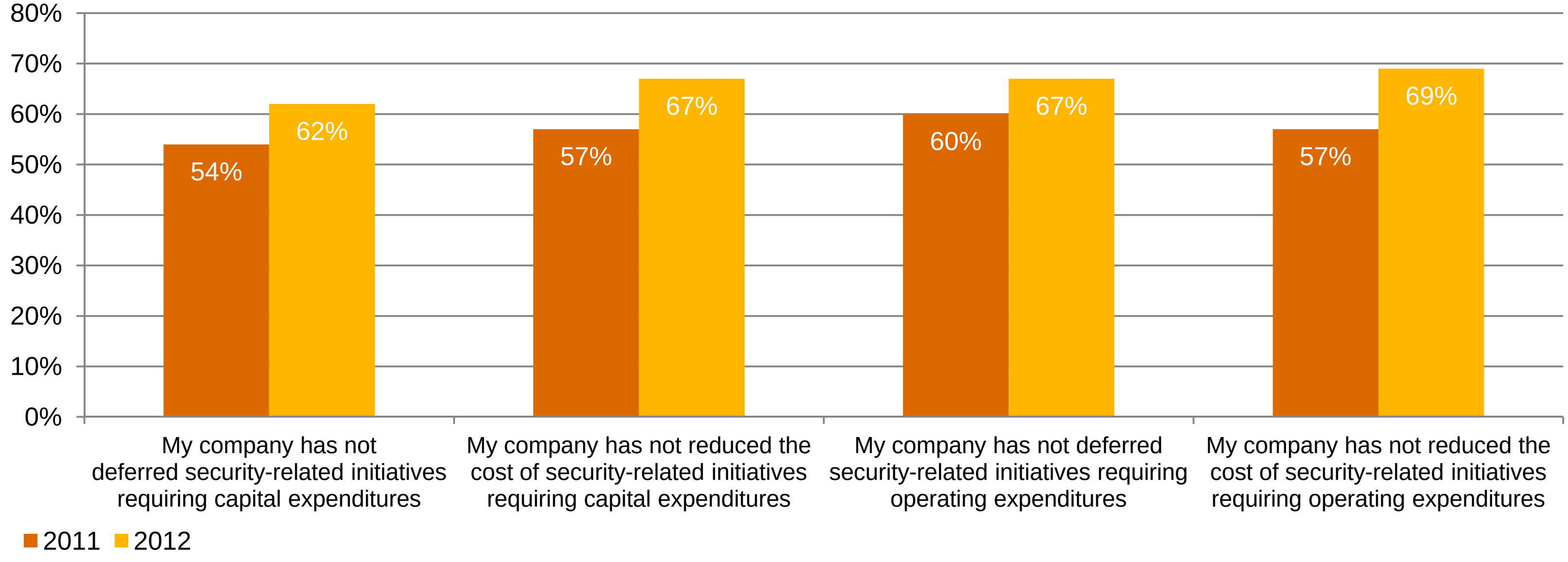
The number of industrial products respondents who have security policies for manufacturing control systems dropped 23% over last year. This is significant because these systems are increasingly linked to the Internet, which can leave them vulnerable to cyber attack.



(Asked only of Industrial Products respondents) Question 1: “Does your organization have a security plan in place to mitigate a breach of manufacturing control systems?”

Among industrial products respondents, the outlook for security spending over the next 12 months is mixed.

Only 45% of respondents expect security budgets to increase in the year ahead, a substantial decline over last year. More encouragingly, respondents report fewer deferrals and fewer budget cutbacks. Compared with last year, for instance, 23% fewer respondents say their company has cut capital spending for security initiatives.



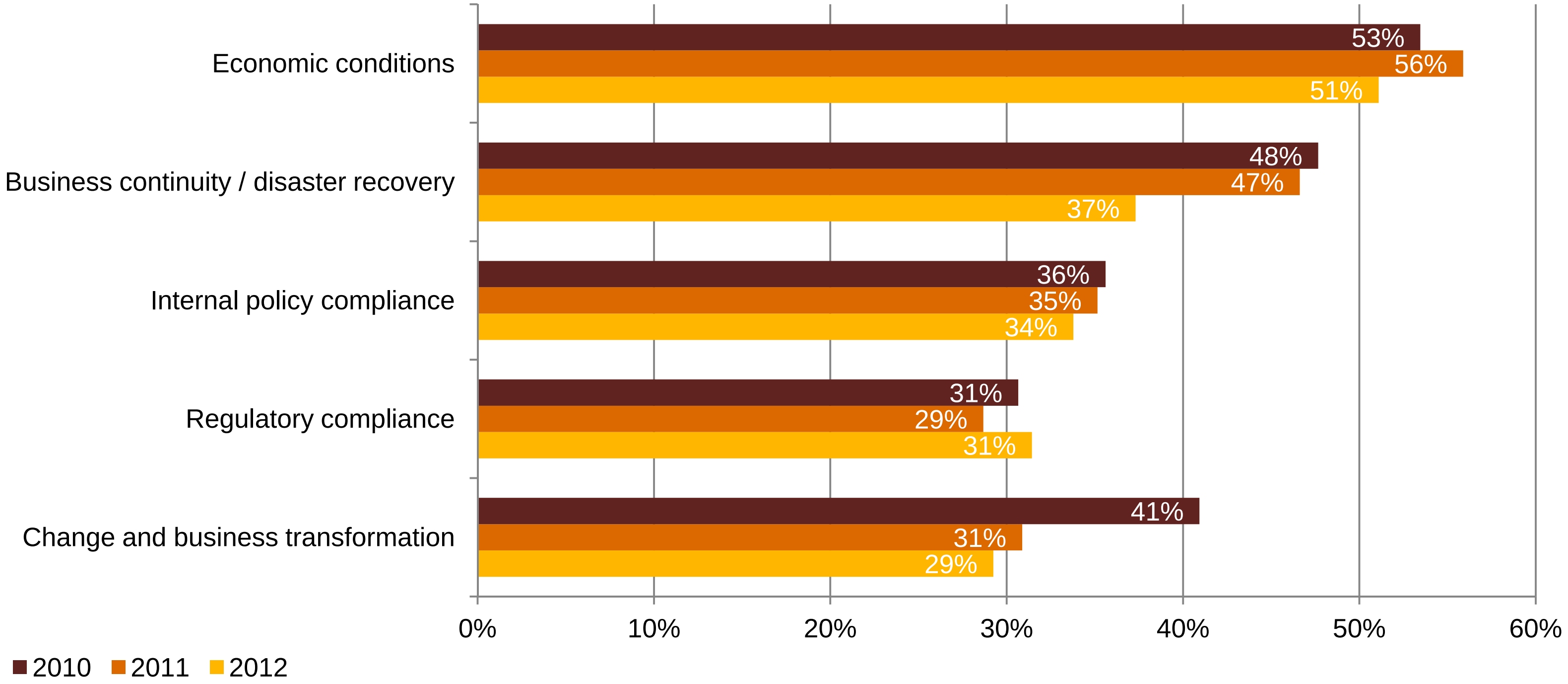
Question 8: “When compared with last year, security spending over the next 12 months will:” Questions 9A and 10A: “Has your company deferred capital and operating security-related initiatives?” Questions 9B and 10B: “Has your company reduced the capital and operating cost of security-related initiatives?”

Section 3

A game of risk

Security budgets are not driven by security needs.

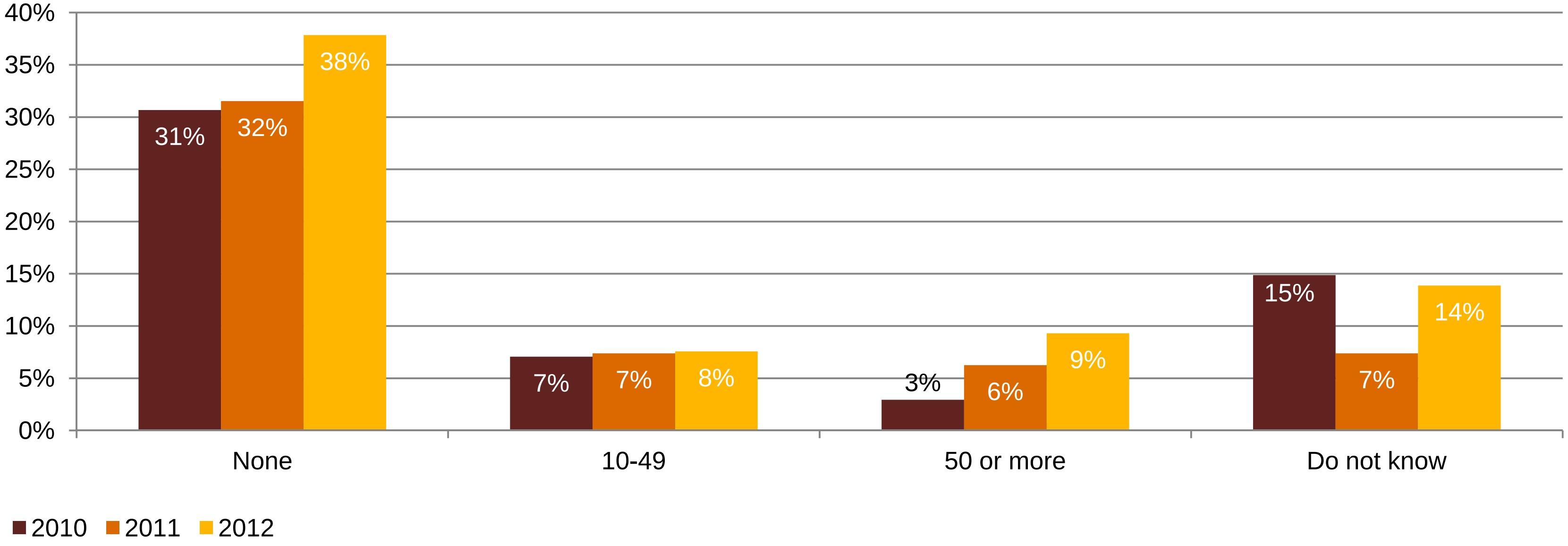
Economic conditions remain the leading driver of security spending, cited by 51% of respondents. That's a lower number than in 2011, but still a risky way to set priorities. Business continuity/disaster recovery is the highest security-specific response, at 37%.



Question 37: "What business issues or factors are driving your company's information security spending?" (Not all factors shown.)

Reported security incidents are on the rise.

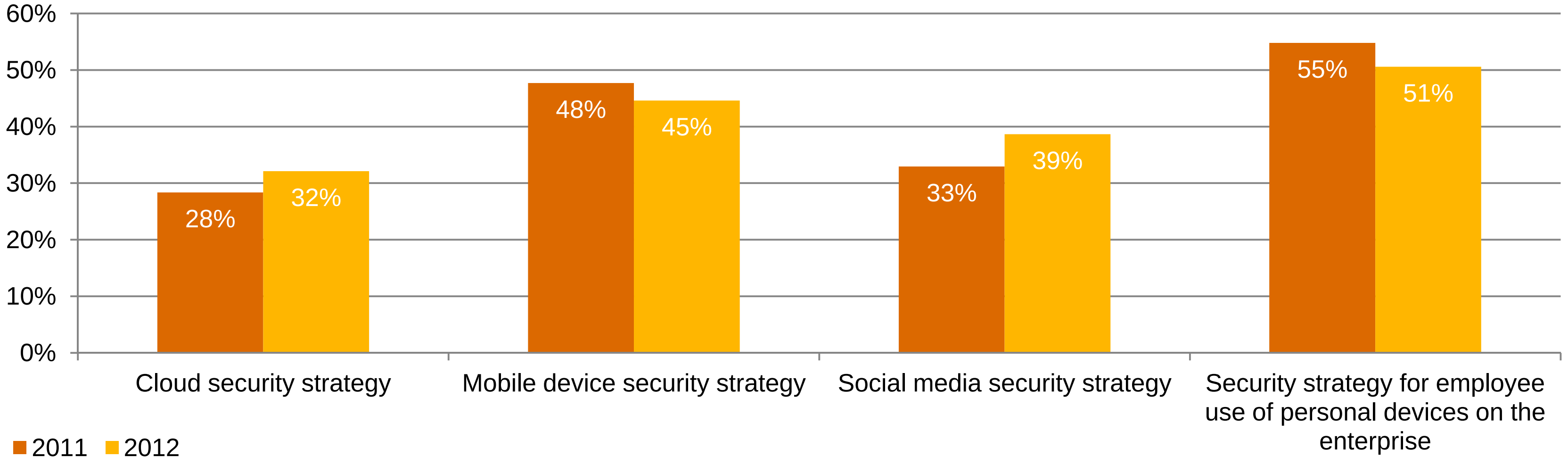
The most numerous category of reported security incidents – 50 or more per year – is growing fast. The number of respondents reporting 50-plus incidents increased by 50% over 2011 and 200% over 2010. Also up: The number of respondents who did not know the number of incidents, an uncertainty that suggests ineffective security practices.



Question 17: “Number of security incidents in the past 12 months.”

Technology adoption is moving faster than security implementation.

As with many industries, industrial products companies are struggling to keep pace with the adoption of cloud computing, social networking, mobility, and use of personal devices. These new technologies often are not included in overall security plans even though they are widely used. In a recent survey, for instance, we found that 88% of consumers use a personal mobile device for both personal and work purposes.[1]

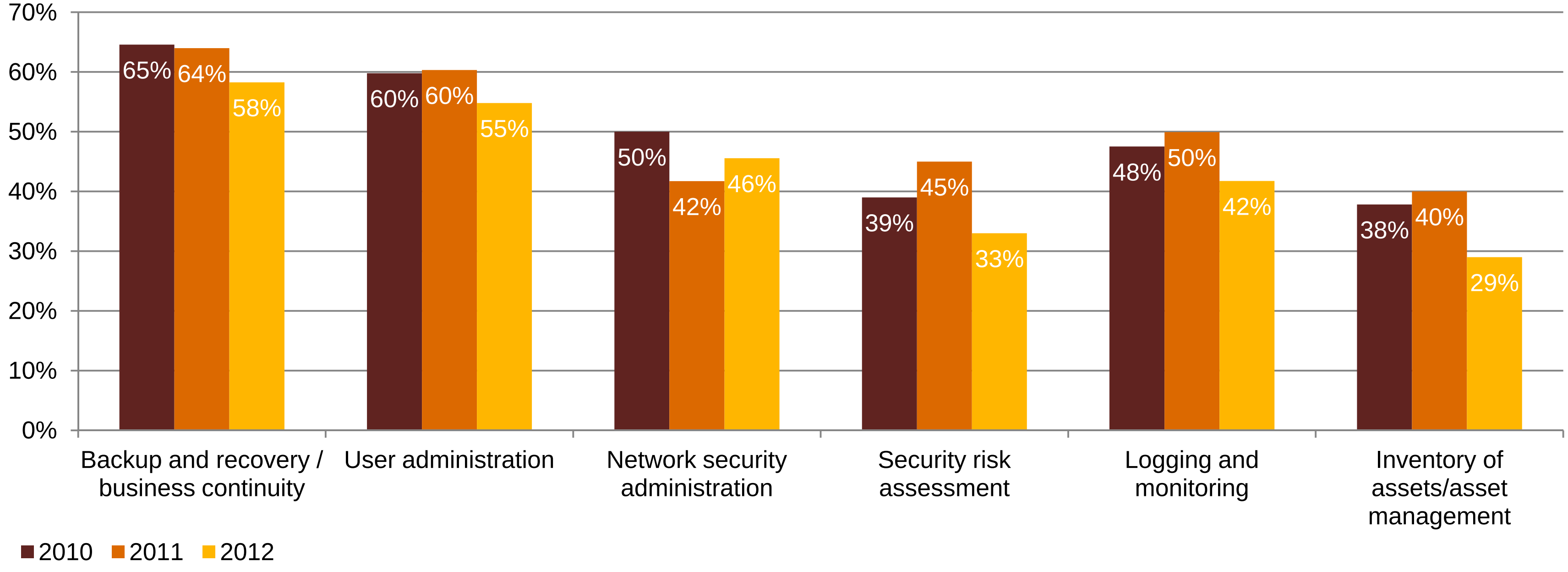


Question 14: “What process information security safeguards does your organization currently have in place?”

[1] PwC, Consumer privacy: What are consumers willing to share? July 2012

Security policies have grown less robust and inclusive.

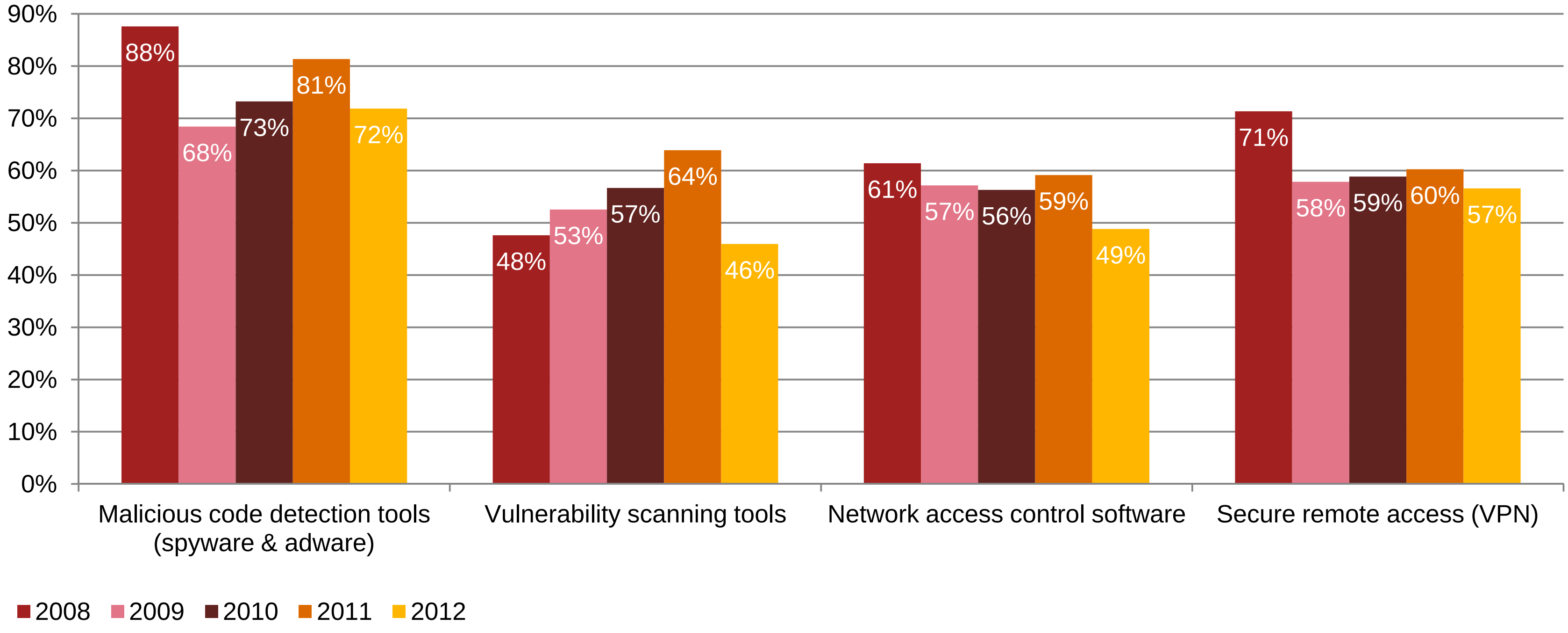
Many companies are omitting fundamental elements of security from their overall policies.



Question 32: “Which of the following elements, if any, are included in your organization’s security policy?”

Use of some key technology safeguards is lower after last year's uptick.

The future looked bright last year as many industrial products firms stepped up investments in technology safeguards. This year, however, saw a decrease in deployment of important security and privacy tools.



Question 15: "What technology information security safeguards related to detection does your organization have in place?"

Section 4

It’s how you play the game

What keeps security from being what it should be?

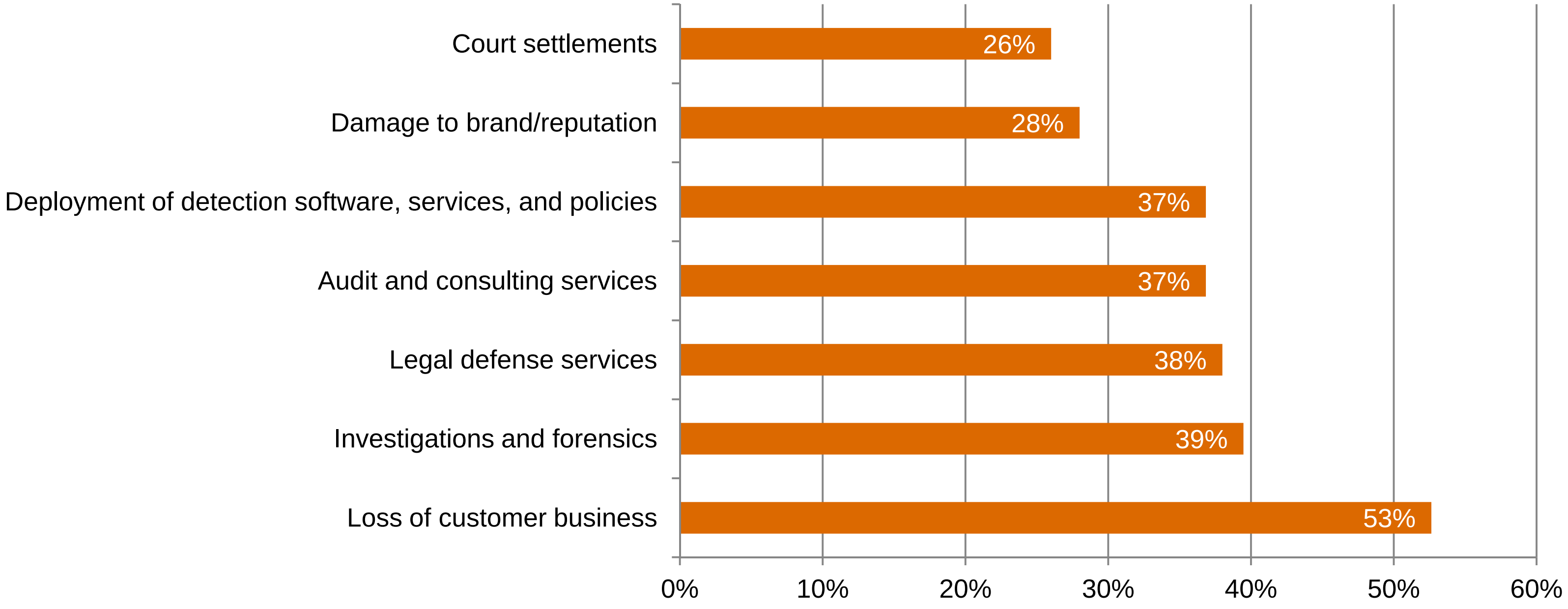
Company leadership is seen as less an obstacle to effective security than in the past, although 45% of respondents still point to C-level executives and Boards. Insufficient capital funding and a lack of vision continue to be top concerns.

	2011	2012
Leadership – CEO, President, Board, or equivalent	23%	20%
Leadership – CISO, CSO, or equivalent	16%	13%
Leadership – CIO or equivalent	17%	12%
Insufficient capital expenditures	27%	28%
Lack of an actionable vision or understanding	33%	28%
Absence or shortage of in-house technical expertise	20%	25%

Question 29: “What are the greatest obstacles to improving the overall strategic effectiveness of your organization’s information security function?”

An inadequate assessment of security incidents can lead to a less-clear understanding of their impact.

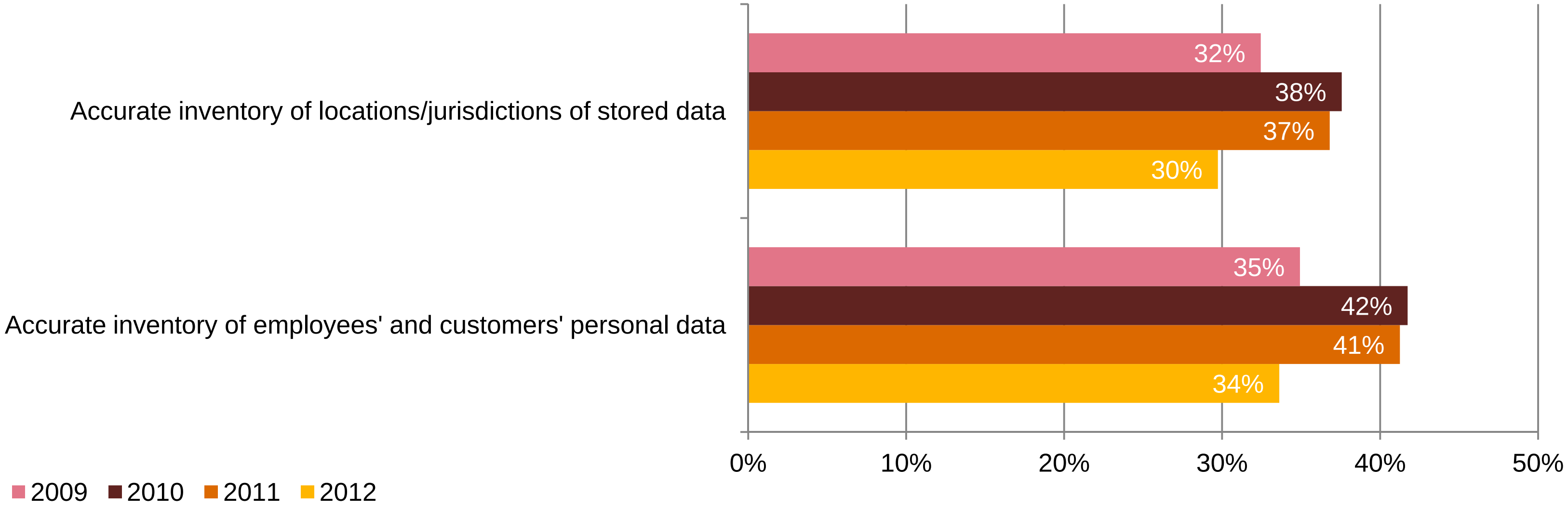
Industrial products respondents report a lower incidence of financial loss due to security incidents than last year, yet many do not apply a thorough or consistent analysis to appraise those costs. For example, only 28% consider damage to brand/reputation, while 38% factor in legal defense services.



Question 21: "How was your organization impacted by the security incident?" Question 21C: "What factors are included in your company's calculation of these financial losses?"

Industrial products respondents know less about their data now than they did three years ago.

While more than 80% of respondents say protecting employee and customer data is important, far fewer understand what that data entails and where it is stored. This is significant because, increasingly, consumers want to be in control of their personal data and "turn off" the flow of information from companies.[2]



Question 38: "What level of importance does your company place on protecting the following types of information?" Question 11: "Which data privacy safeguards does your organization have in place?"

[2] PwC, Consumer privacy: What are consumers willing to share? July 2012

What you can do to improve your performance.

Information security today is a rapidly evolving game of advanced skill and strategy. As a result, the security models of the past decade are no longer effective.

Effective security requires a new way of thinking. The very survival of the business demands that security leaders understand, prepare for, and quickly respond to security threats.

Businesses seeking to strengthen their security practice must:

- Implement a comprehensive risk-assessment strategy and align security investments with identified risks.
- Understand their organization's information, who wants it, and what tactics adversaries might use to get it.
- Understand that information security requirements – and, indeed, overall strategies for doing business – have reached a turning point.
- Embrace a new way of thinking in which information security is both a means to protect data as well as an opportunity to create value to the business.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
949.437.5380
gary.loveland@us.pwc.com

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

US Industrial Products Contacts

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

Joseph Marino
Managing Director
703.918.1188
joseph.marino@us.pwc.com

Or visit www.pwc.com/giss2013

The Global State of Information Security® is a registered trademark of International Data Group, Inc.

www.pwc.com/security

Changing the game

While tight budgets have forestalled updates to security programs, many businesses are confident they're winning the game. But the rules – and the players – have changed.

Pharmaceuticals

Key findings from The Global State of Information Security® Survey 2013

September 2012

> ***“You can’t succeed in today’s elevated threat environment if you don’t know the players and you don’t know the rules.”***
>
> ***– Gary Loveland, Principal, PwC***

Information security has always been a high-stakes game. One that demands a smart strategy, the right technology moves, and an unblinking eye on adversaries.

For many businesses, however, it has become a pursuit that is almost impossible to win. That’s because the rules have changed, and opponents—old and new—are armed with expert technology skills. As a result, the risks are greater than ever.

Businesses are fighting back by adopting new detection and prevention technologies. At the same time, governments around the world are enacting legislation to combat cyber threats. And regulatory bodies are issuing new guidance on disclosure obligations for cyber incidents.

Yet risks to data security continue to intensify – and show no signs of abating. Those keeping score agree that the bad guys appear to be in the lead.

Nonetheless, many businesses believe they are winning. The Global State of Information Security® Survey 2013 shows that most executives in the global pharmaceuticals industry are confident in the effectiveness of their information security practices. They believe their strategies are sound and many consider themselves to be leaders in the field.

The odds, however, are not in their favor: Diminished budgets have resulted in degraded security programs, reported security incidents are on the rise, and new technologies are being adopted faster than they can be safeguarded.

Given today's elevated threat environment, businesses can no longer afford to play a game of chance. They must prepare to play a new game, one that requires advanced levels of skill and strategy to win.

Agenda

Section 1. Methodology

Section 2. A game of confidence

Section 3. A game of risk

Section 4. It’s how you play the game

Section 1

Methodology

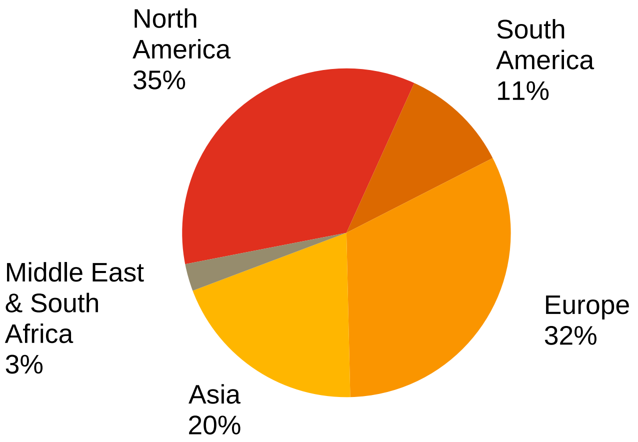
A worldwide study

The Global State of Information Security® Survey 2013, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 1, 2012 to April 15, 2012.

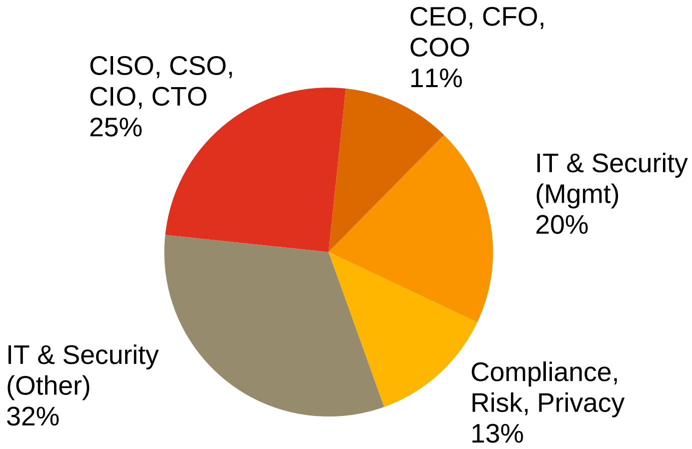
- PwC's 15th year conducting the online survey, 10th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 128 countries
- More than 9,300 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-three percent (33%) of respondents from companies with revenue of $500 million+
- Survey included 112 respondents from the pharmaceuticals industry
- Margin of error less than 1%

Demographics

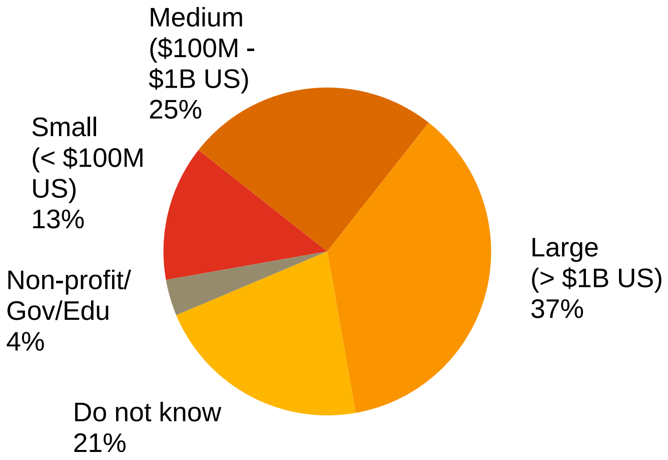
Pharma respondents by region of employment



Pharma respondents by title



Pharma respondents by company revenue size



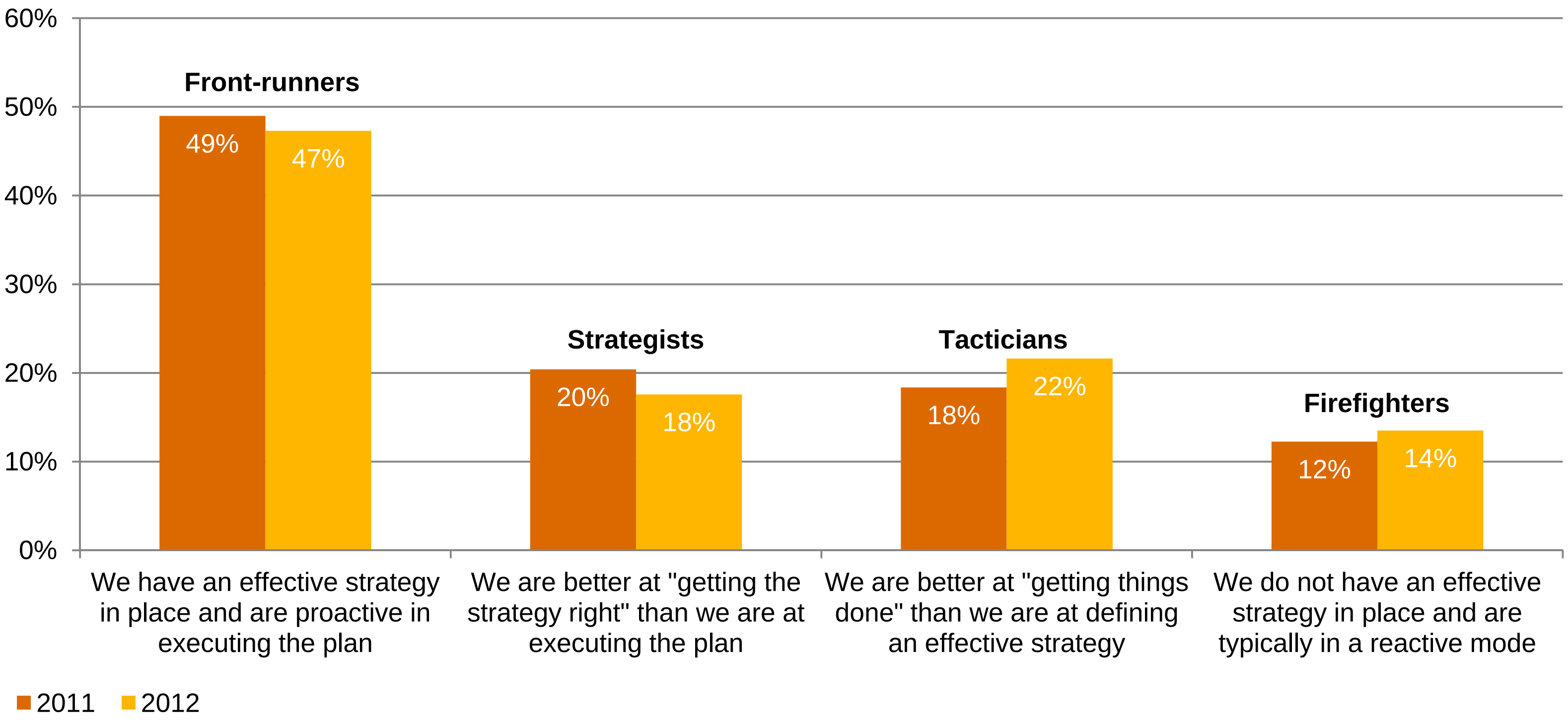
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

A game of confidence

Pharma respondents are confident in their security practices.

47% of pharma respondents say their organization has a strategy in place and is proactive in executing it – exhibiting two distinctive attributes of a leader.



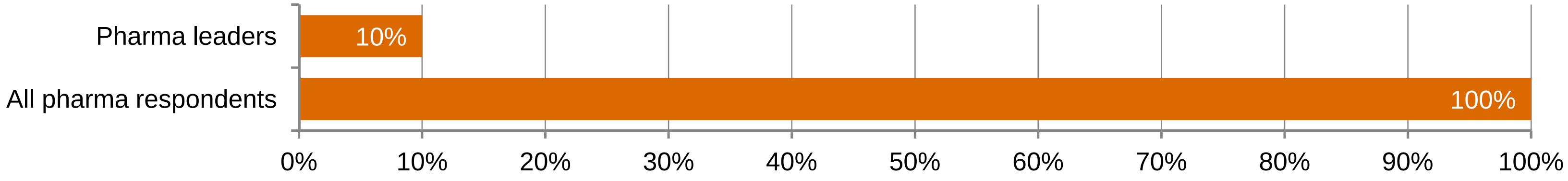
Question 28: "Which category below best characterizes your organization's approach to protecting information security?"

A reality check on real leaders.

But are they really leaders? We measured pharma respondents' self-appraisal against four key criteria to define leadership. To qualify, they must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the "top of the house" (e.g., to the CEO, CFO, COO, or legal counsel)
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

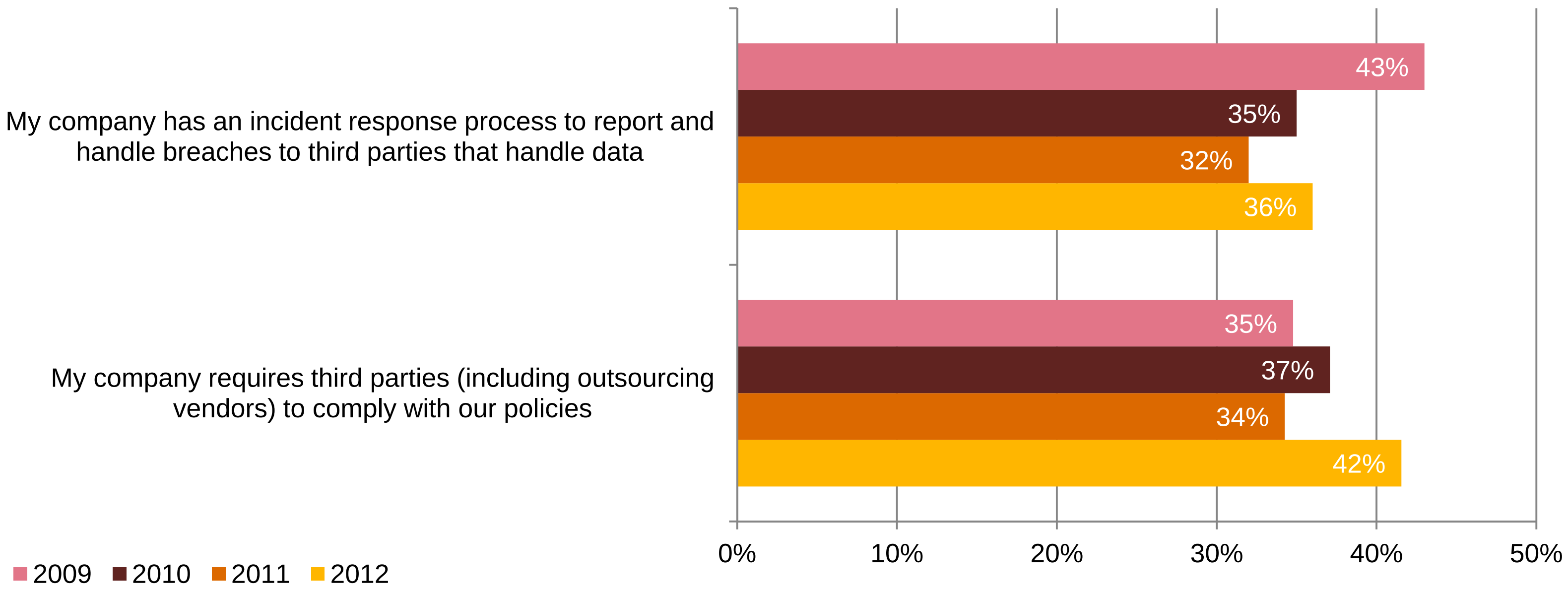
The result? Our analysis found that 10% of pharma respondents rank as leaders.



Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 18: "What types of security incidents (breach or downtime) occurred" and Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Many pharma companies lack incident response processes and compliance policies for third parties.

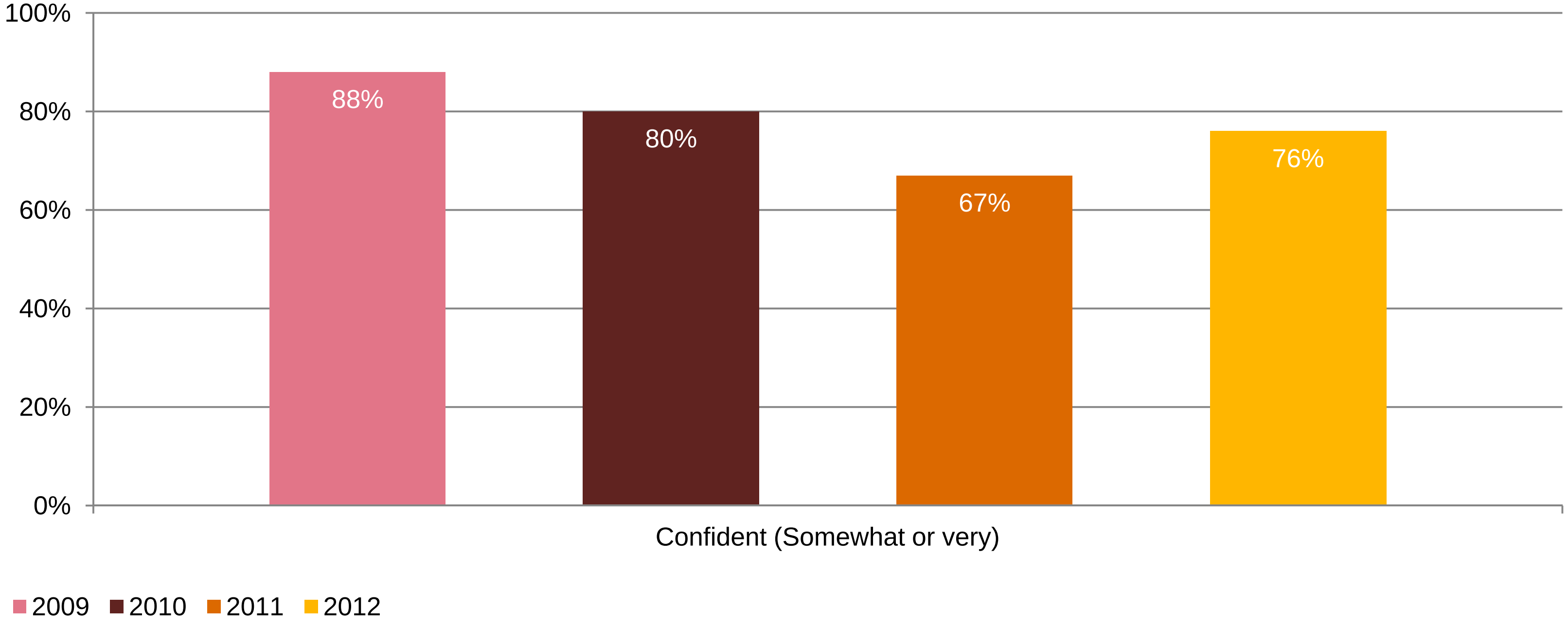
Data privacy is paramount in the pharmaceuticals industry, yet most respondents say they do not have a process in place to handle third-party breaches. What's more, only 42% require third parties to comply with their privacy policies.



Question 35: "How confident are you that your organization has instilled effective information security behaviors into the organizational culture?"
Question 11: "Which data privacy safeguards does your organization have in place?"

Most respondents say their information security activities are effective, but this confidence is eroding.

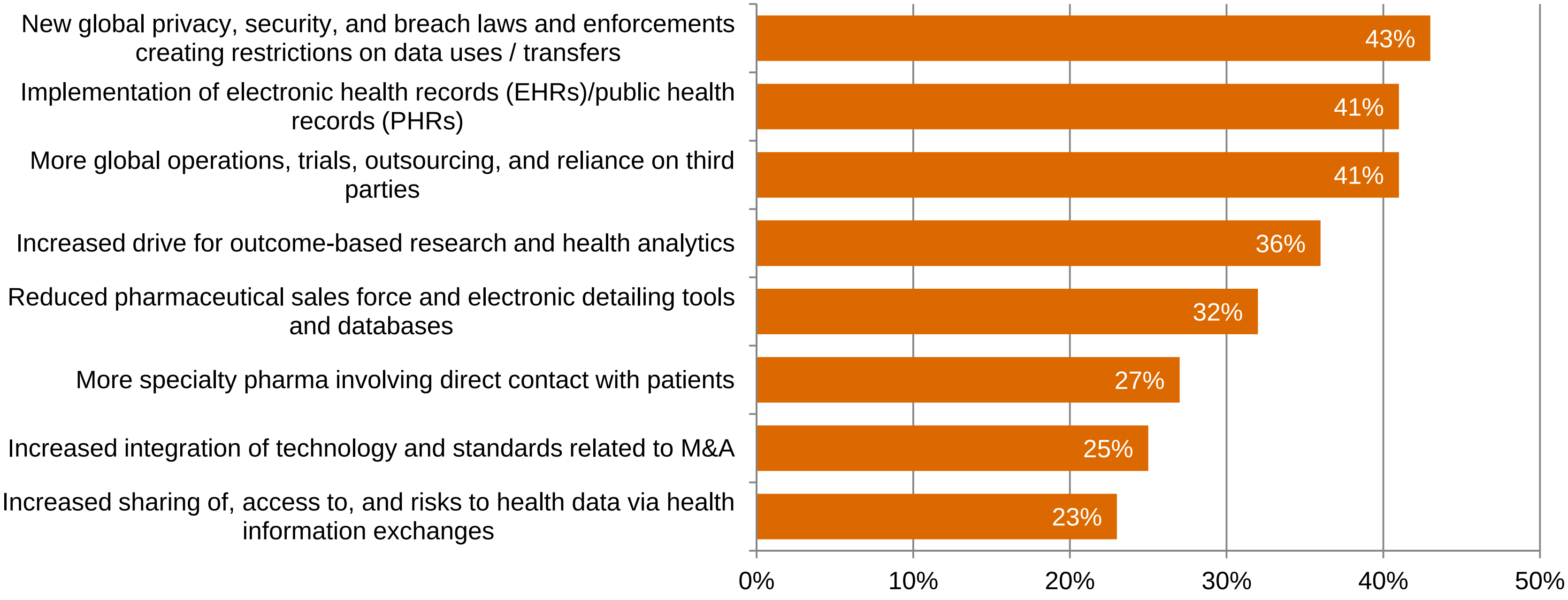
Confidence is a good thing. A strong 76% of pharma respondents say they are confident their company's security activities are effective, but they may not realize that assurance has dropped considerably since 2009.



Question 41: "How confident are you that your organization's information security activities are effective?"

New data regulations and electronic health records are the primary drivers of security spending.

Increased regulation of data – including privacy, security, and breach laws – is the top influence on security spending, followed by implementation of electronic health records and expanding global operations.



(Asked only of Pharmaceuticals respondents) Question 1: “Which trends are driving your investment in information security?”

Many pharma firms may be unprepared to solve their biggest security challenges.

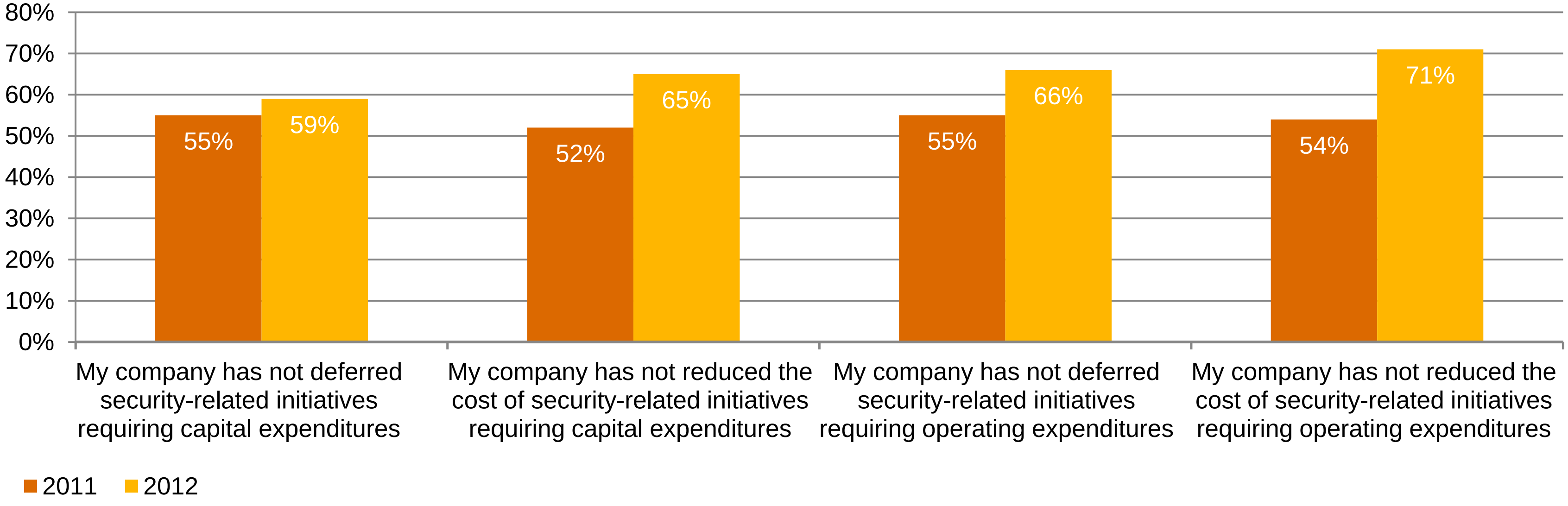
Respondents identified the top five security issues they face this year, but many may not have implemented the strategies necessary to address them.

Top 5 security challenges	What's holding them back?
1. Meeting regulatory requirements	Only 38% have a strategy for compliance with regulatory requirements
2. Protecting intellectual property	Only 24% have implemented procedures dedicated to protecting IP
3. Compliance with document-retention requirements	Only 45% have a security policy for data protection, disclosure, and destruction
4. Securing mobile devices	Only 58% have a mobile device security strategy
5. Cloud computing	Only 31% have a cloud security strategy

(Asked only of Pharmaceutical respondents) Question 2: “Please identify your top five security challenges” Question 14: “What process information security safeguards does your organization currently have in place?” Question 32: “Which of the following elements, if any, are included in your organization’s security policy?”

Among pharma respondents, the outlook for security spending over the next 12 months is mixed.

37% of respondents expect security budgets to increase in the year ahead. More encouragingly, respondents report fewer deferrals and fewer budget cutbacks for security initiatives. Compared with last year, for instance, 31% more respondents say they had not deferred security programs requiring operating expenditures.



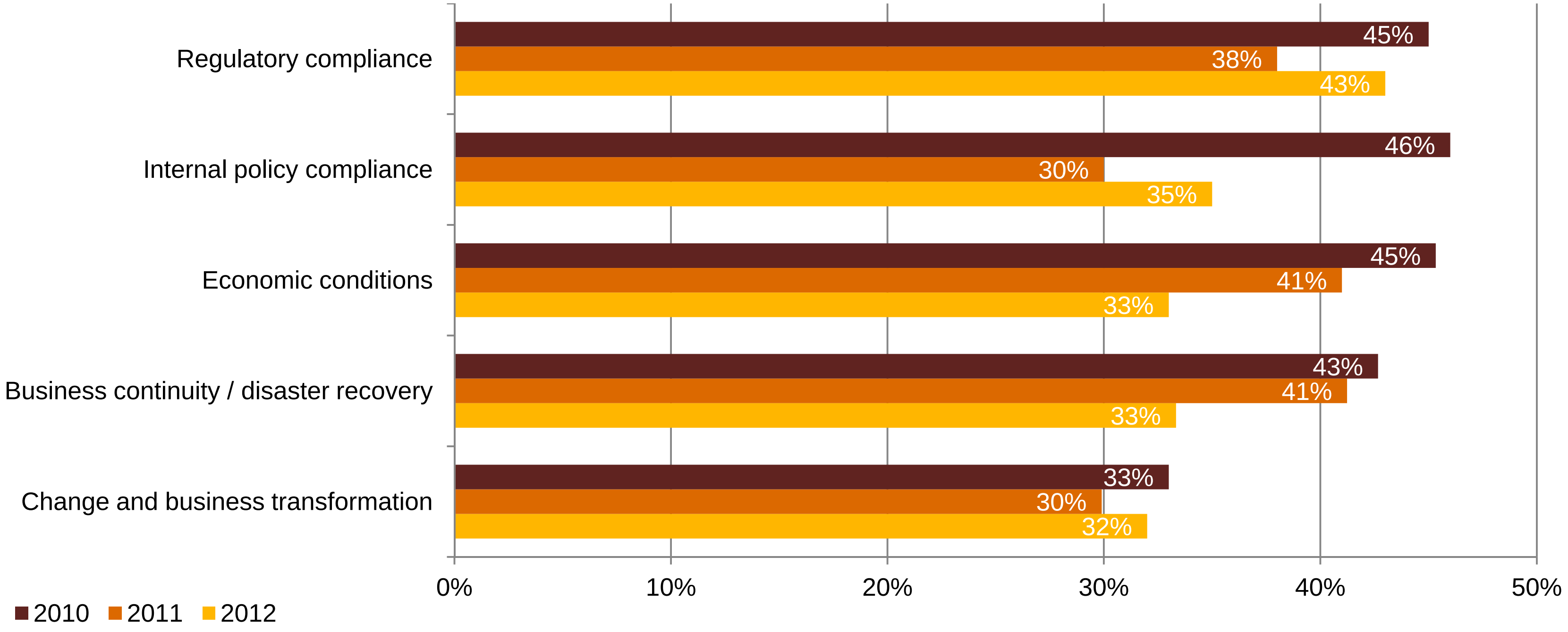
Question 8: “When compared with last year, security spending over the next 12 months will:” Questions 9A and 10A: “Has your company deferred capital and operating security-related initiatives?” Questions 9B and 10B: “Has your company reduced the capital and operating cost of security-related initiatives?”

Section 3

A game of risk

Security budgets are not driven by security needs.

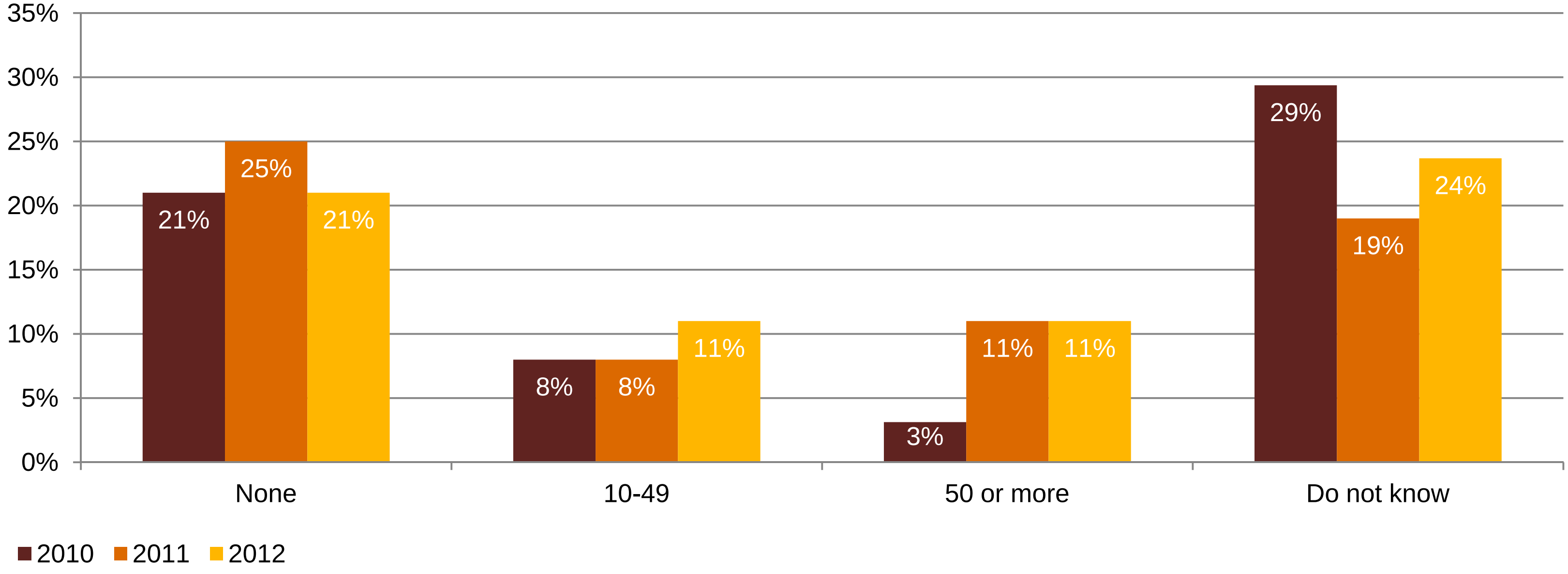
Compliance supplanted economic conditions as the top driver of security spending as new regulations governing data movement, global data access, and breach notifications were introduced. Business continuity/disaster recovery was the largest security-specific response, at 33%.



Question 37: “What business issues or factors are driving your company's information security spending?” (Not all factors shown.)

Reported security incidents are on the rise.

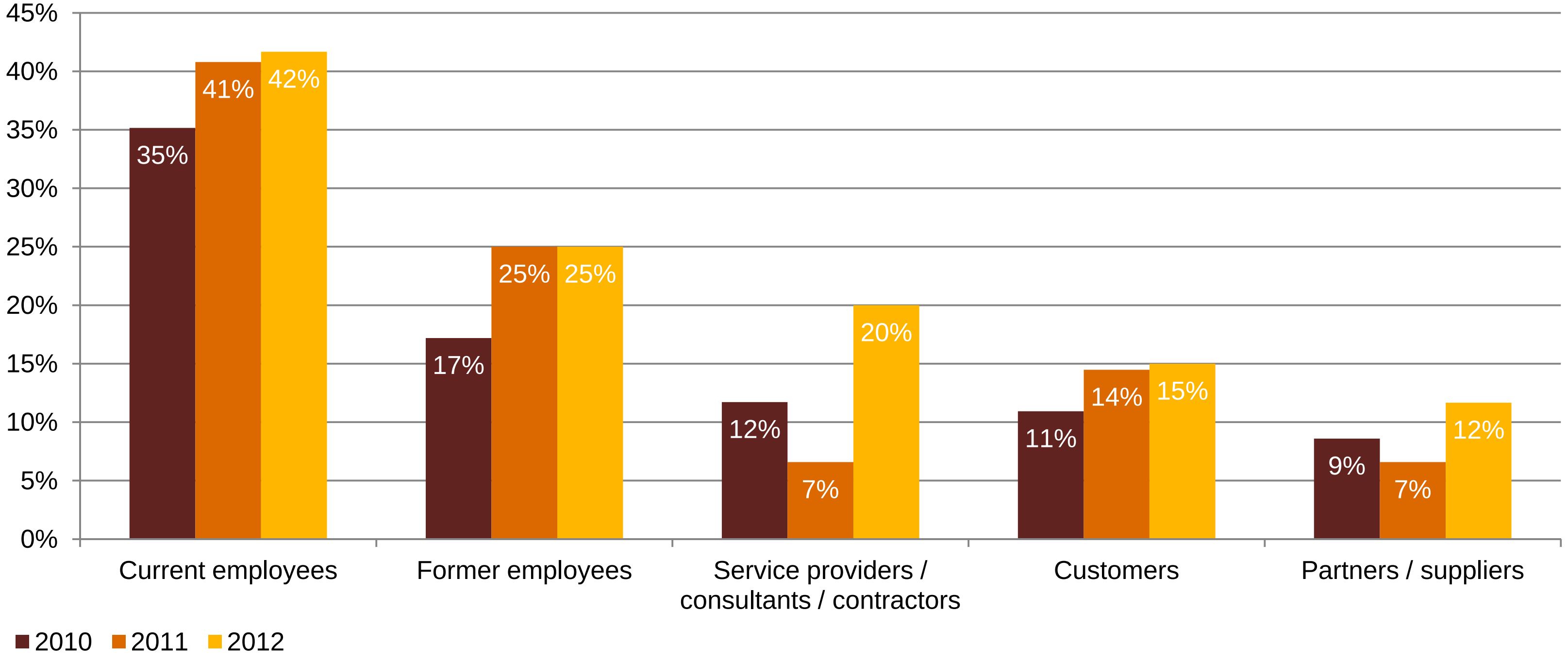
11% of pharma respondents report 10-49 security incidents in the last 12 months, up from 8% in 2011. Those reporting the most numerous category of incidents – 50 or more per year – leveled off at 11%, the same as last year but far above rates in previous years. One in four respondents do not know the number of incidents, an uncertainty that suggests ineffective security practices.



Question 17: “Number of security incidents in the past 12 months.”

Threats from 'insiders,' particularly current and former employees, are increasing.

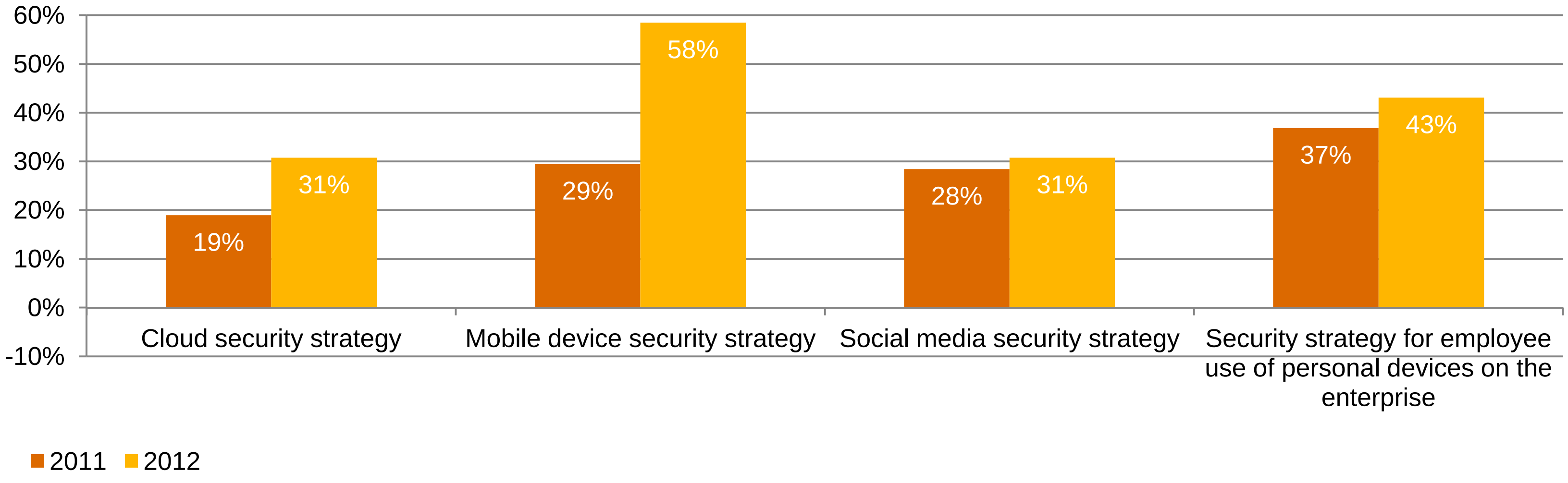
Security incidents attributed to current employees are at the highest level in years, as are those blamed on former workers. Threats from other insiders – providers, consultants, contractors, partners, and suppliers – are also rising.



Question 20: "Estimated likely source of incidents."

Technology adoption is moving faster than security implementation.

As with many industries, pharma is struggling to keep pace with the adoption of cloud computing, social networking, mobility, and use of personal devices. These new technologies often are not included in overall security plans even though they are widely used. In a recent survey, for instance, we found that 88% of consumers use a personal mobile device for both personal and work purposes.[1]

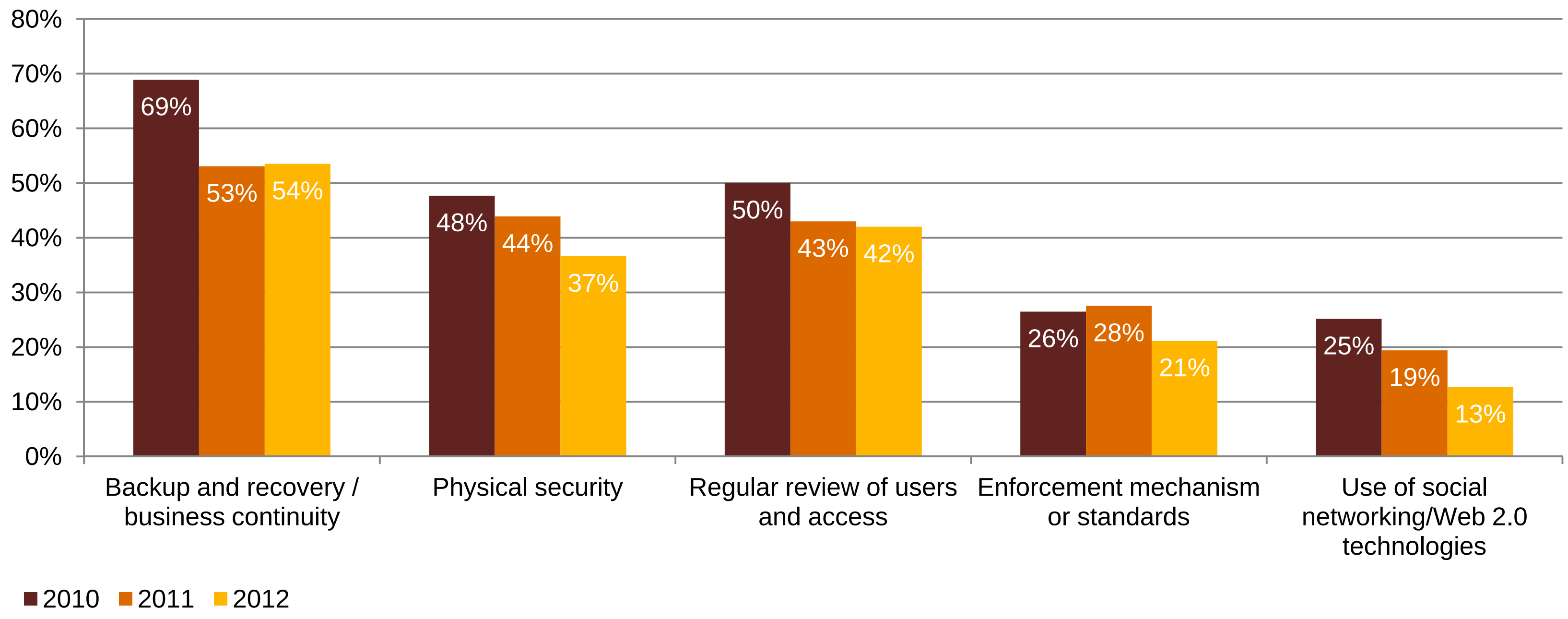


Question 14: “What process information security safeguards does your organization currently have in place?”

[1] PwC, Consumer privacy: What are consumers willing to share? July 2012

Security policies have grown less robust and inclusive.

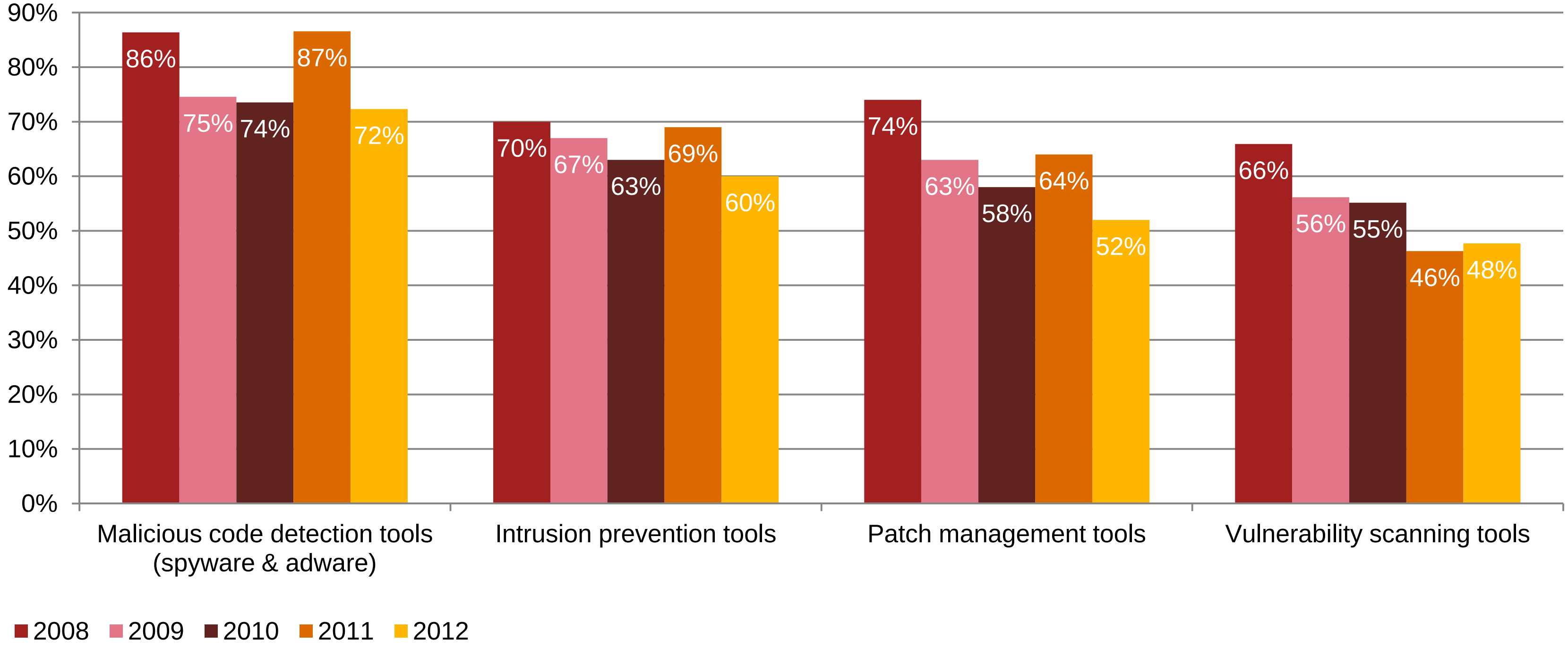
Many companies are omitting fundamental elements of security from their overall policies.



Question 32: “Which of the following elements, if any, are included in your organization’s security policy?”

Use of some key technology safeguards resumed a long-term decline after last year's uptick.

The future looked bright last year as many pharma companies stepped up investments in prevention and detection safeguards. This year, however, saw a decrease in deployment of these important tools.



Question 15: "What technology information security safeguards related to detection/prevention does your organization have in place?"

Section 4

It’s how you play the game

What keeps security from being what it should be?

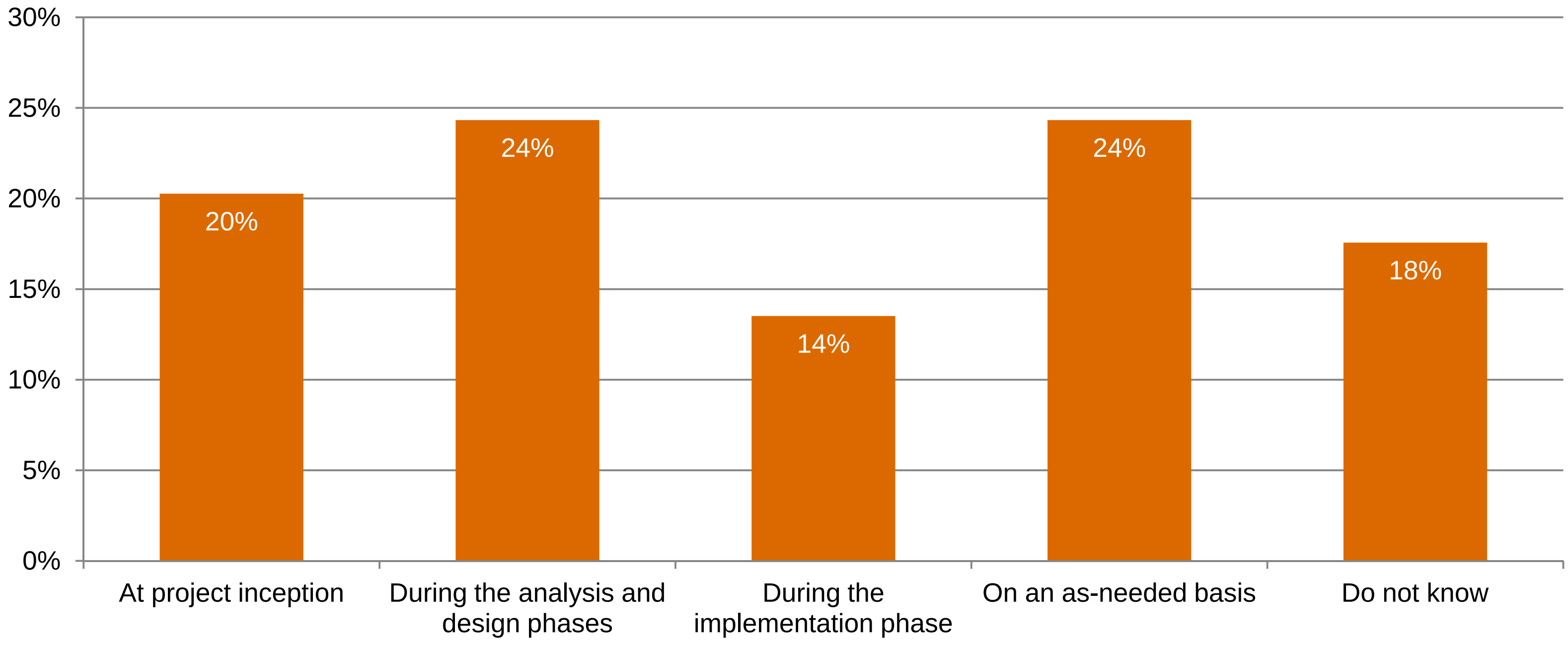
41% of pharma respondents perceive top-level leadership to be an obstacle to effective security. The most cited single hindrance is lack of an effective security strategy, followed by a shortage of in-house technical expertise.

	2011	2012
Leadership – CEO, President, Board, or equivalent	30%	12%
Leadership – CIO or equivalent	18%	20%
Leadership – CISO, CSO, or equivalent	17%	9%
Lack of an effective information security strategy	18%	34%
Absence or shortage of in-house technical expertise	19%	26%
Lack of actionable vision or understanding	28%	25%
Insufficient capital expenditures	27%	22%

Question 29: “What are the greatest obstacles to improving the overall strategic effectiveness of your organization’s information security function?”

Security is not always baked into major projects from the beginning.

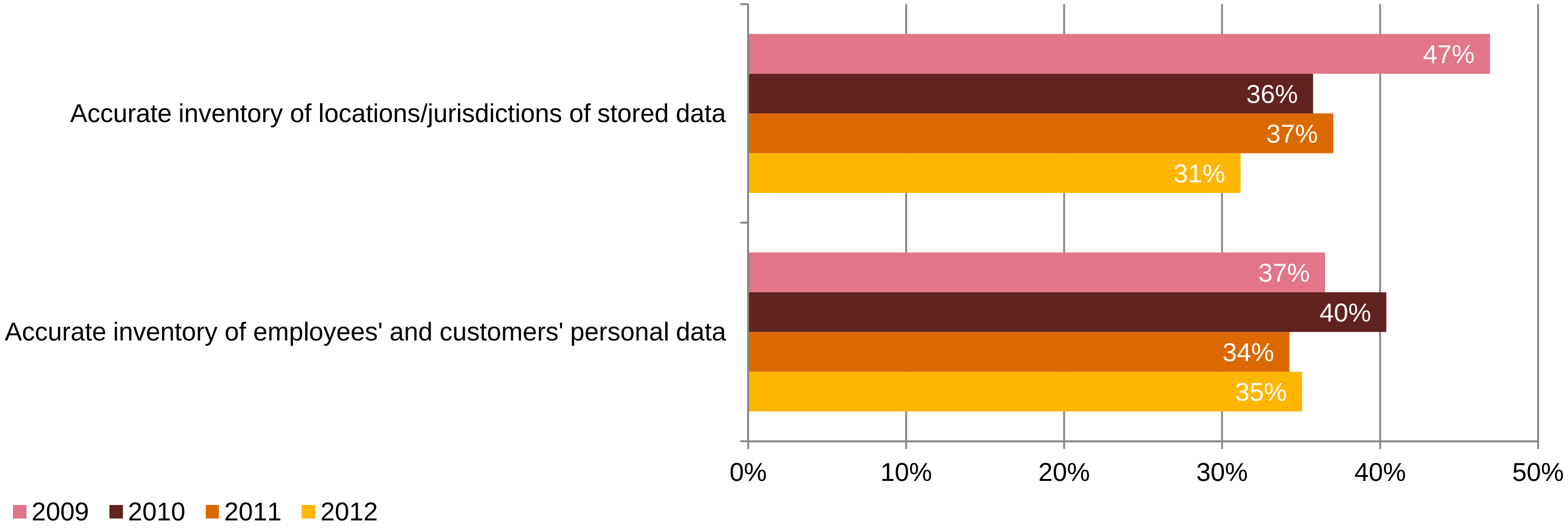
Information security sometimes seems like an afterthought, with more than one-third of respondents saying their organization involves security late in the process – during the implementation phase or on an as-needed basis.



Question 30: “When does information security become involved in major projects?”

Pharma respondents know less about their data now than they did three years ago.

While at least 84% of respondents say protecting customer and employee data is important, far fewer understand what that data entails and where it is stored. This is significant because, increasingly, understanding data, data flows, and data uses is a prerequisite to new pharmaceutical business models.



Question 38: “What level of importance does your company place on protecting the following types of information?” Question 11: “Which data privacy safeguards does your organization have in place?”

What you can do to improve your performance.

Information security today is a rapidly evolving game of advanced skill and strategy. As a result, the security models of the past decade are no longer effective.

Effective security requires a new way of thinking. The very survival of the business demands that security leaders understand, prepare for, and quickly respond to security threats.

Businesses seeking to strengthen their security practice must:

- Implement a comprehensive risk-assessment strategy and align security investments with identified risks.
- Understand their organization’s information, who wants it, and what tactics adversaries might use to get it.
- Understand that information security requirements – and, indeed, overall strategies for doing business – have reached a turning point.
- Embrace a new way of thinking in which information security is both a means to protect data as well as an opportunity to create value to the business.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
949.437.5380
gary.loveland@us.pwc.com

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

US Pharmaceuticals Contacts

Daniel Garrett
Principal
267.330.8202
daniel.garrett@us.pwc.com

Peter Harries
Principal
602.750.3404
peter.harries@us.pwc.com

Mick Coady
Principal
713.356.4366
mick.coady@us.pwc.com

Or visit www.pwc.com/giss2013

PwC

www.pwc.com/security

Changing the game

While tight budgets have forestalled updates to security programs, many businesses are confident they're winning the game. But the rules – and the players – have changed.

Power & Utilities

Key findings from The Global State of Information Security® Survey 2013

September 2012

"You can't succeed in today's elevated threat environment if you don't know the players and you don't know the rules."

- Gary Loveland, Principal, PwC

Information security has always been a high-stakes game. One that demands a smart strategy, the right technology moves, and an unblinking eye on adversaries.

For many businesses, however, it has become a pursuit that is almost impossible to win. That's because the rules have changed, and opponents—old and new—are armed with expert technology skills. As a result, the risks are greater than ever.

Businesses are fighting back by adopting new detection and prevention technologies. At the same time, governments around the world are enacting legislation to combat cyber threats. And regulatory bodies are issuing new guidance on disclosure obligations for cyber incidents.

Yet risks to data security continue to intensify – and show no signs of abating. Those keeping score agree that the bad guys appear to be in the lead.

Nonetheless, many businesses believe they are winning. The Global State of Information Security® Survey 2013 shows that most executives in the global utilities industry are confident in the effectiveness of their information security practices. They believe their strategies are sound and many consider themselves to be leaders in the field.

The odds, however, are not in their favor: Diminished budgets have resulted in degraded security programs, reported security incidents are on the rise, and new technologies are being adopted faster than they can be safeguarded.

Given today's elevated threat environment, businesses can no longer afford to play a game of chance. They must prepare to play a new game, one that requires advanced levels of skill and strategy to win.

Agenda

Section 1. Methodology

Section 2. A game of confidence

Section 3. A game of risk

Section 4. It’s how you play the game

Section 1

Methodology

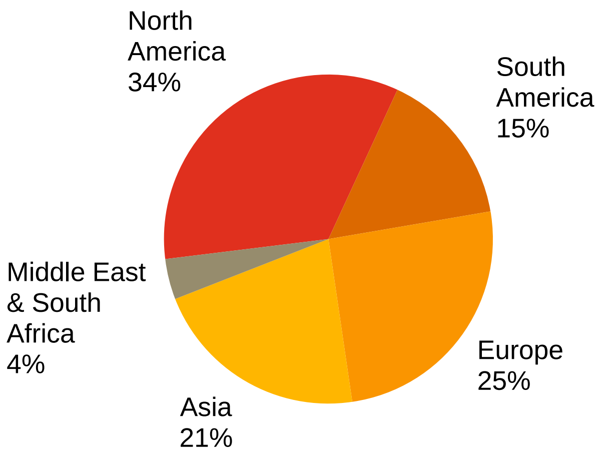
A worldwide study

The Global State of Information Security® Survey 2013, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 1, 2012 to April 15, 2012.

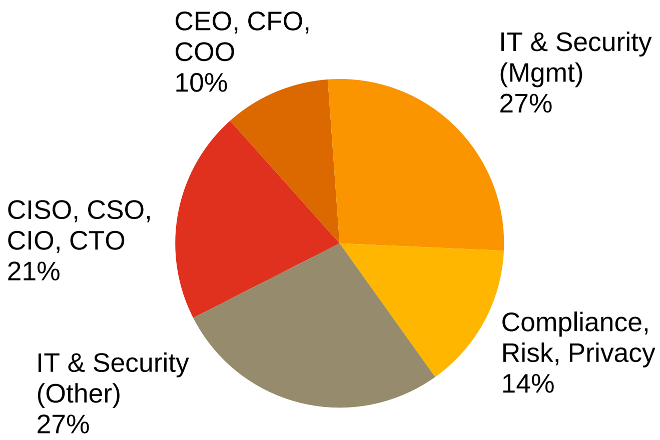
- PwC's 15th year conducting the online survey, 10th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 128 countries
- More than 9,300 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-three percent (33%) of respondents from companies with revenue of $500 million+
- Survey included 201 respondents from the utilities industry
- Margin of error less than 1%

Demographics

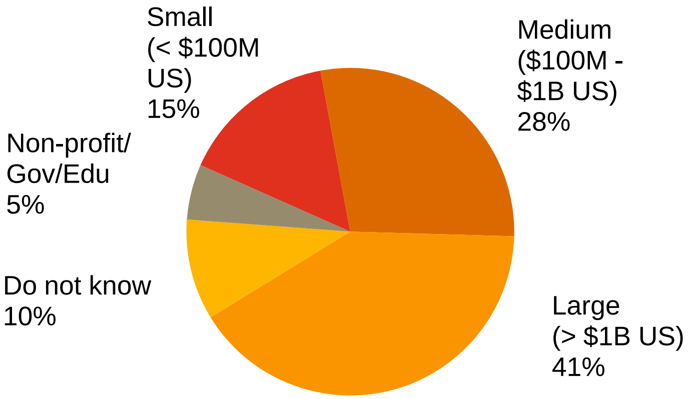
Utilities respondents by region of employment



Utilities respondents by title



Utilities respondents by company revenue size



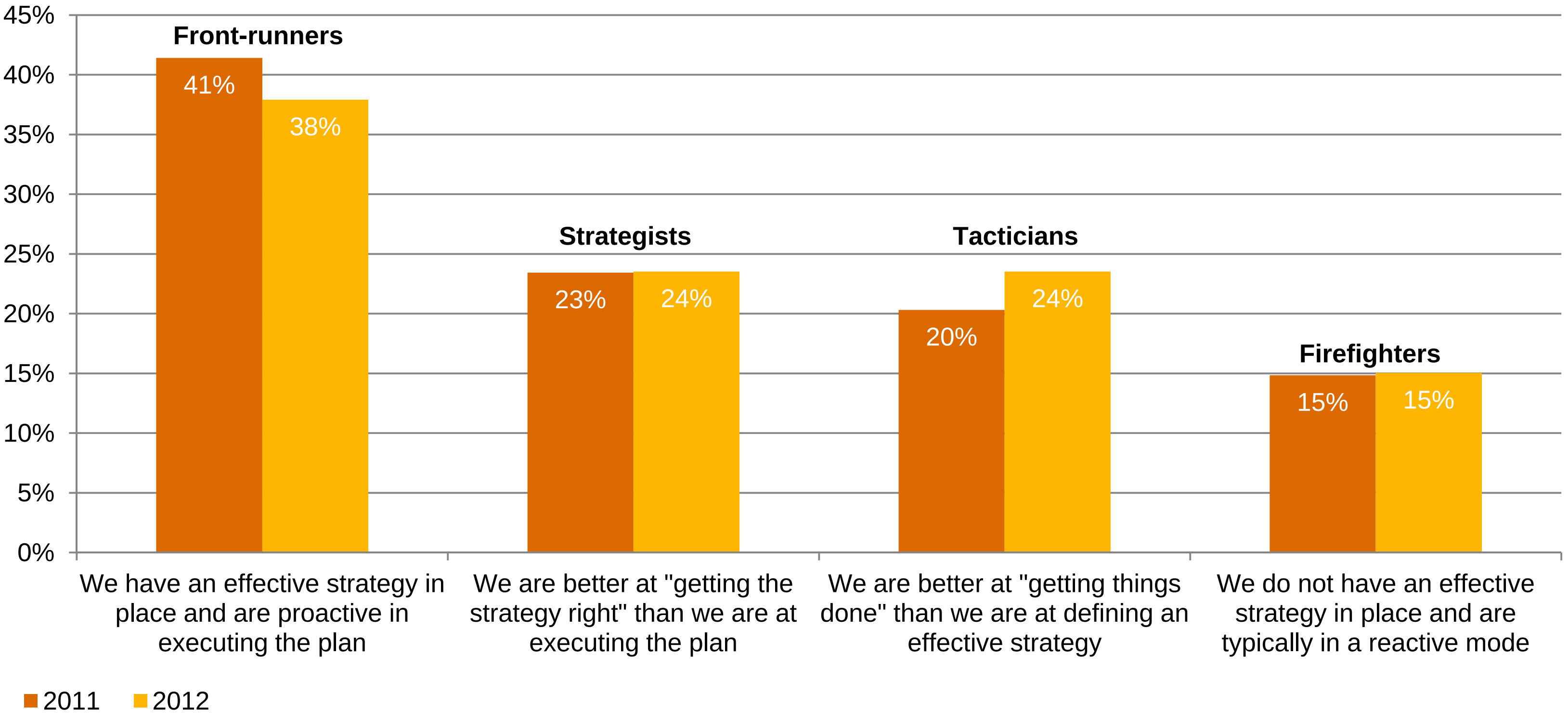
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

A game of confidence

Utilities respondents are confident in their security practices.

38% of utilities respondents say their organization has a strategy in place and is proactive in executing it – exhibiting two distinctive attributes of a leader.



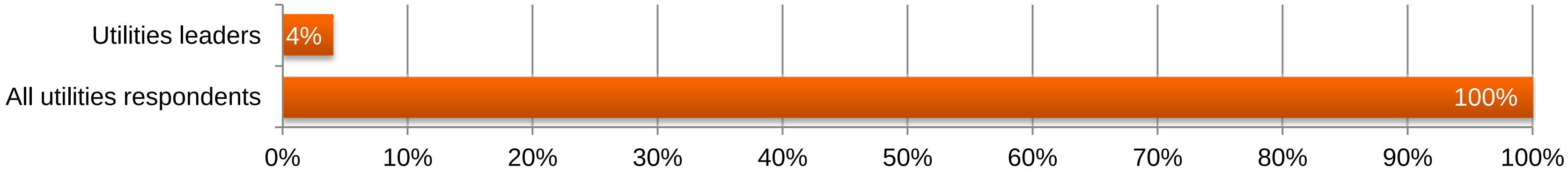
Question 28: "Which category below best characterizes your organization's approach to protecting information security?"

A reality check on real leaders.

But are they really leaders? We measured utilities respondents' self-appraisal against four key criteria to define leadership. To qualify, they must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the "top of the house" (e.g., to the CEO, CFO, COO, or legal counsel)
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

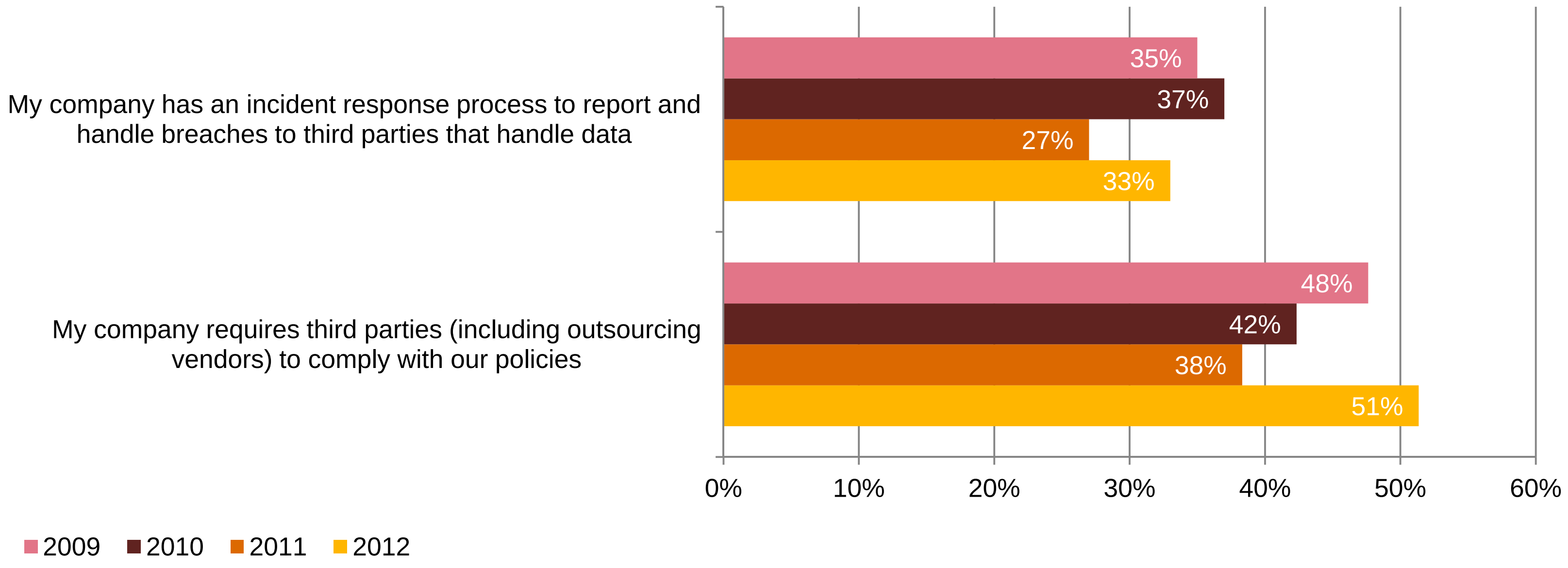
The result? Our analysis found that 4% of utilities respondents rank as leaders.



Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 18: "What types of security incidents (breach or downtime) occurred" and Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Many utilities respondents are over-confident in their organization’s security program.

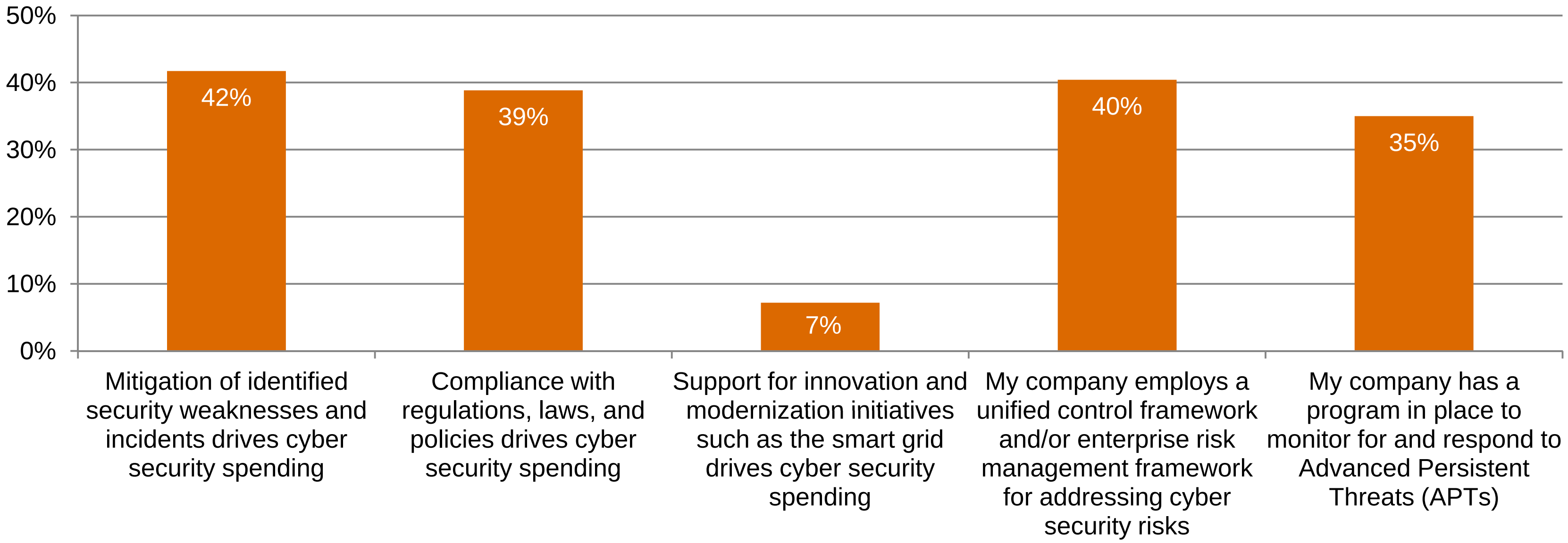
60% of respondents are confident that they have instilled effective security behaviors into their organization’s culture, yet most do not have a process in place to handle third-party breaches. What’s more, almost half do not require third parties to comply with privacy policies. This suggests a troubling gap in perception.



Question 35: “How confident are you that your organization has instilled effective information security behaviors into the organizational culture?”
Question 11: “Which data privacy safeguards does your organization have in place?”

Utilities are trying to catch up to known cyber-security problems.

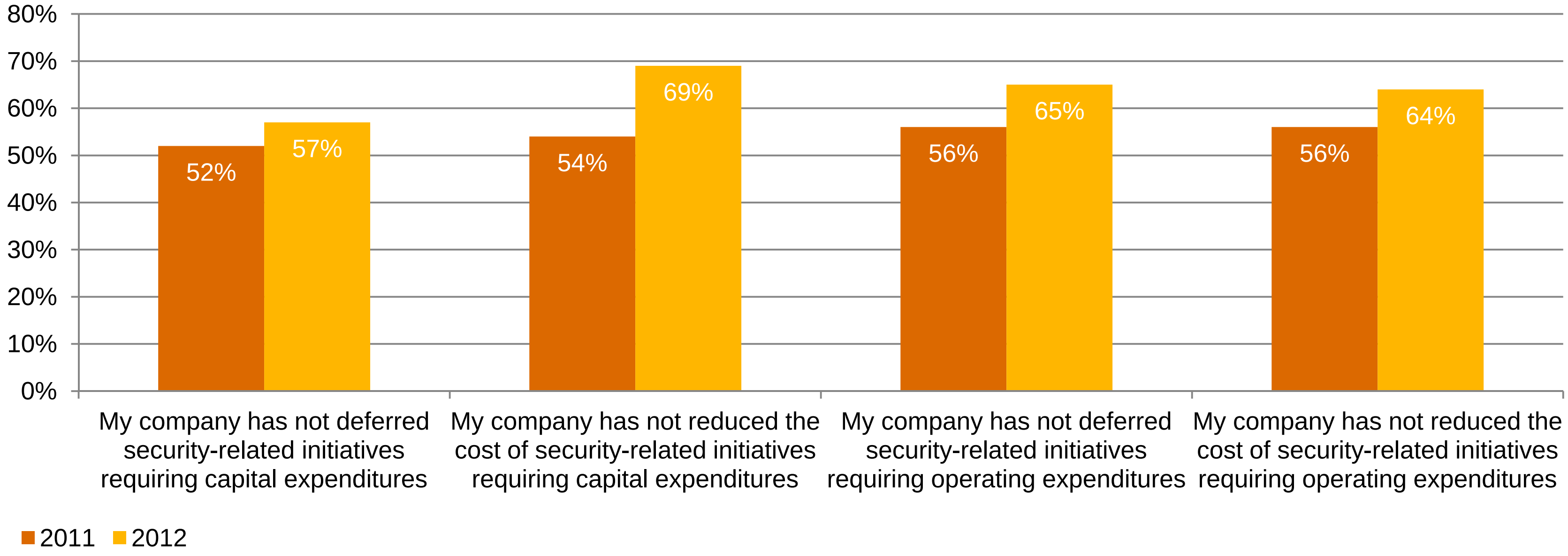
42% of utilities respondents invest in cyber security primarily to address known weaknesses and incidents. But just 40% address cyber security on an enterprise level and only 35% have programs in place to combat Advanced Persistent Threats (APTs).



(Asked only of Utilities respondents) Question 1: "What is the primary driver for cyber security spending at your company?" Question 2 (Utilities): "Does your company employ a unified control framework and/or enterprise risk management framework for addressing cyber security risks?" Question 3 (Utilities): "Does your company have a program in place to monitor for and respond to Advanced Persistent Threats (APTs)?"

Utilities respondents are optimistic about security spending over the next 12 months.

52% of utilities respondents expect security budgets to increase in the year ahead. More encouragingly, respondents report fewer deferrals and fewer budget cutbacks for security initiatives. Compared with last year, for instance, 28% more respondents say they had not cut capital expenditures for security programs.



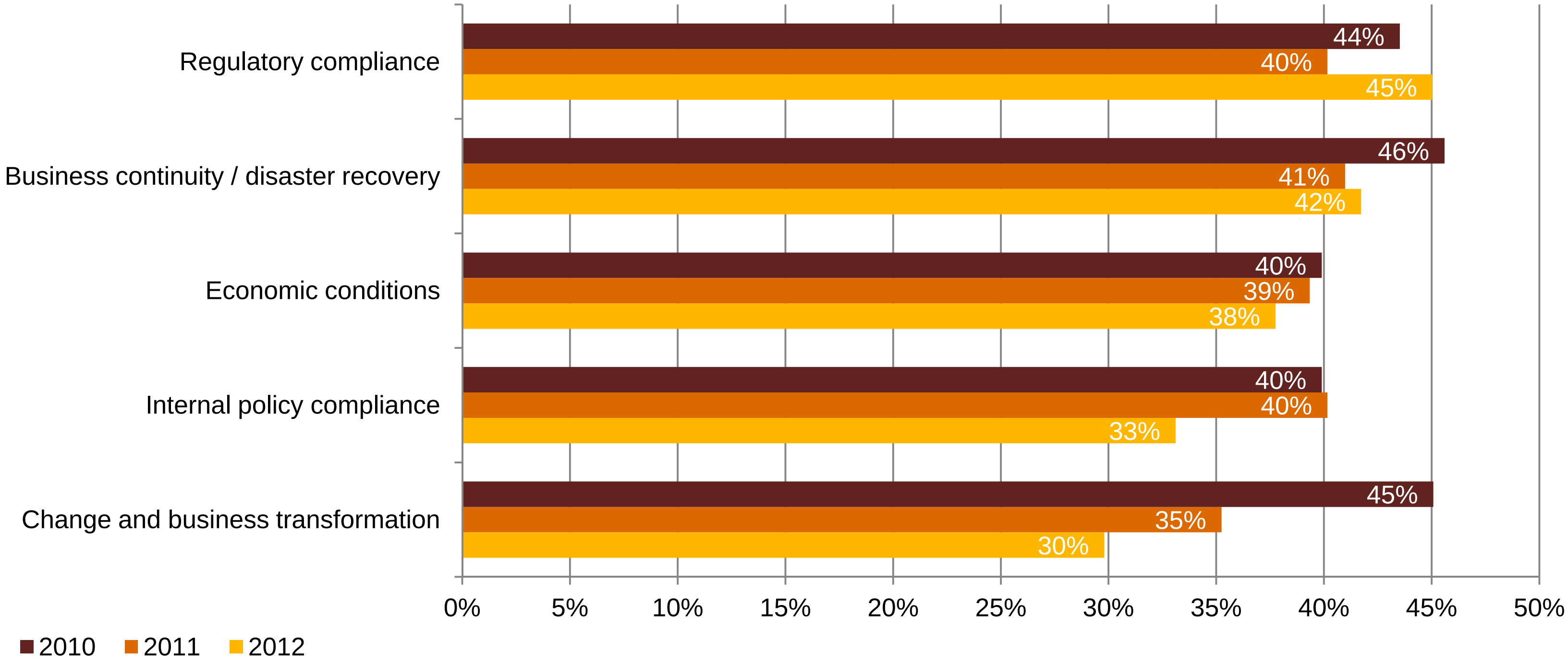
Question 8: “When compared with last year, security spending over the next 12 months will:” Questions 9A and 10A: “Has your company deferred capital and operating security-related initiatives?” Questions 9B and 10B: “Has your company reduced the capital and operating costs of security-related initiatives?”

Section 3

A game of risk

Security budgets are not driven by security needs.

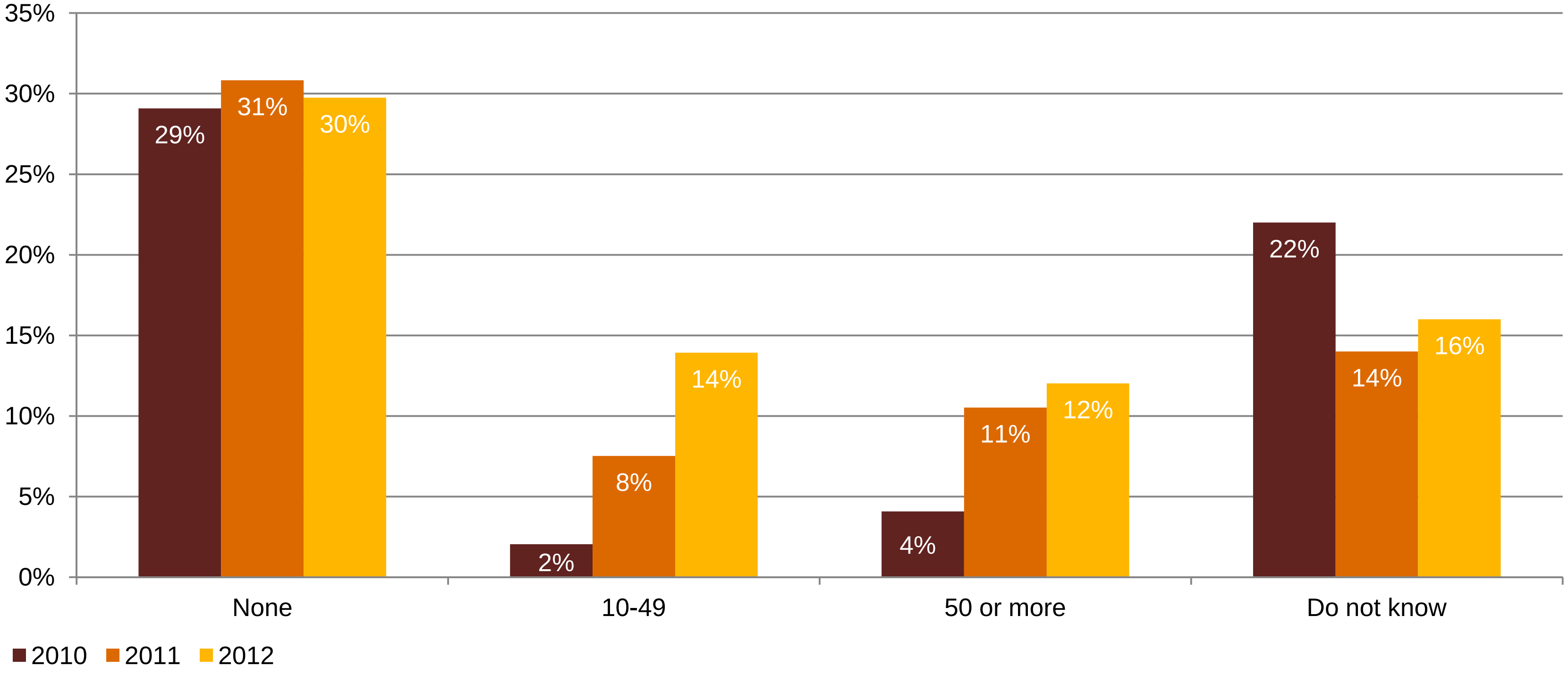
Regulatory compliance, at 45%, is the top driver of security spending – not surprising in a highly regulated industry such as utilities. Economic conditions weigh in at 38%, slightly down but still a risky way to set priorities.



Question 37: “What business issues or factors are driving your company's information security spending?” (Not all factors shown.)

Reported security incidents are on the rise.

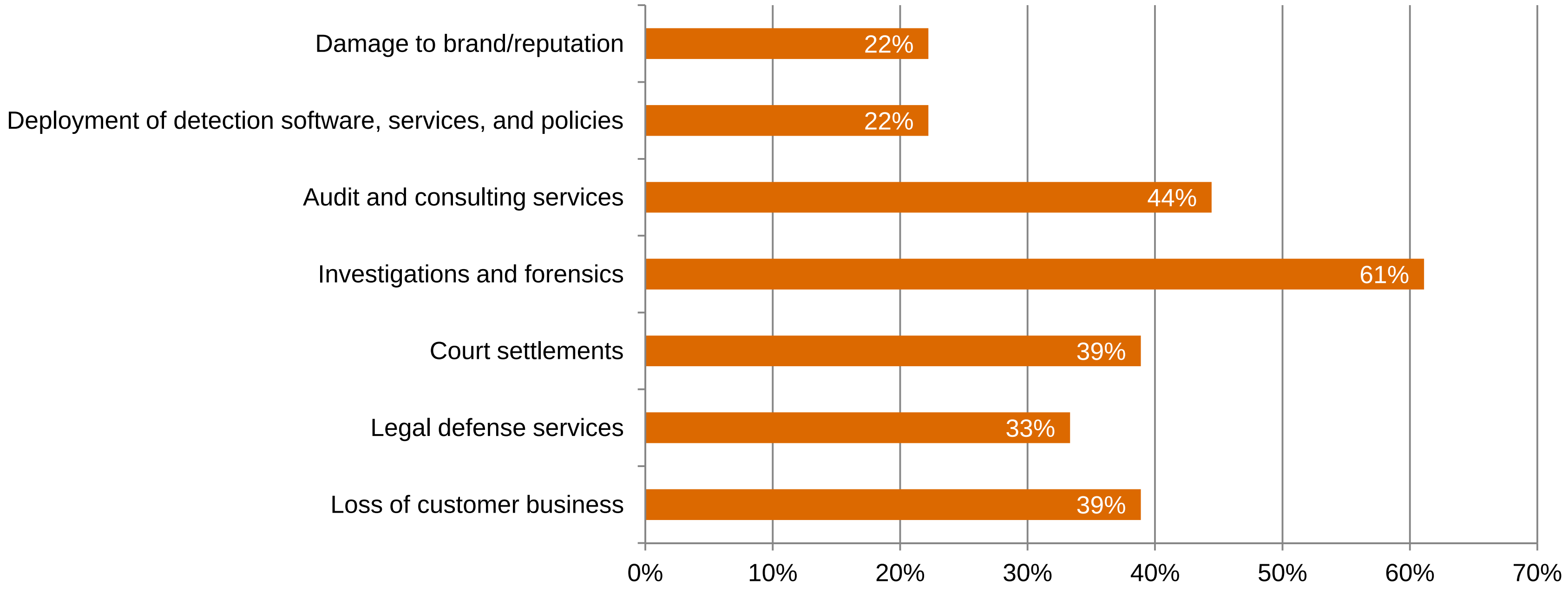
The number of respondents reporting 10-49 incidents jumped 75% over 2011 and 600% over 2010. Almost one-third reported no security incidents in the last 12 months.



Question 17: “Number of security incidents in the past 12 months.”

An inadequate assessment of security incidents can lead to a less-clear understanding of their impact.

Utilities respondents report a low incidence of financial losses from security incidents, yet many do not perform a thorough or consistent appraisal of those losses. For example, only 22% consider damage to brand/reputation and 33% factor in legal defense services.



Question 21: "How was your organization impacted by the security incident?" Question 21C: "What factors are included in your company's calculation of these financial losses?"

Less than half of respondents have security training programs for employees.

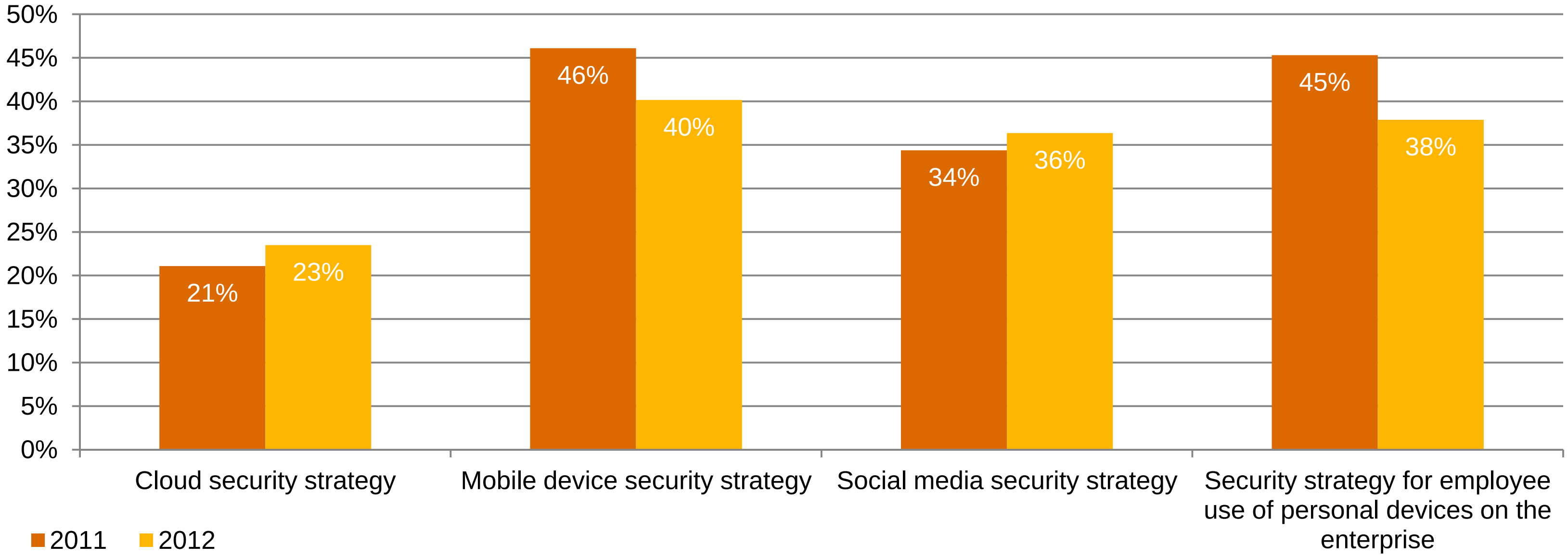
No security program can be effective without adequate training, yet only 48% of utilities respondents have an employee security awareness training program in place. Only one-half have staff dedicated to security awareness.

Information security safeguards	2008	2009	2010	2011	2012
Have employee security awareness training program	49%	62%	51%	51%	48%
Have people dedicated to employee awareness programs	48%	59%	63%	54%	50%

Question 14: “What process information security safeguards does your organization currently have in place?” Question 13: “What information security safeguards related to people does your organization have in place?”

Technology adoption is moving faster than implementation of new security strategies.

Utilities are struggling to implement security strategies for mobility, social media, cloud computing, and use of employee-owned devices. In fact, the numbers still lag adoption of the technologies themselves. We have found, for instance, that 88% of consumers use a personal mobile device for both personal and work purposes.[1]

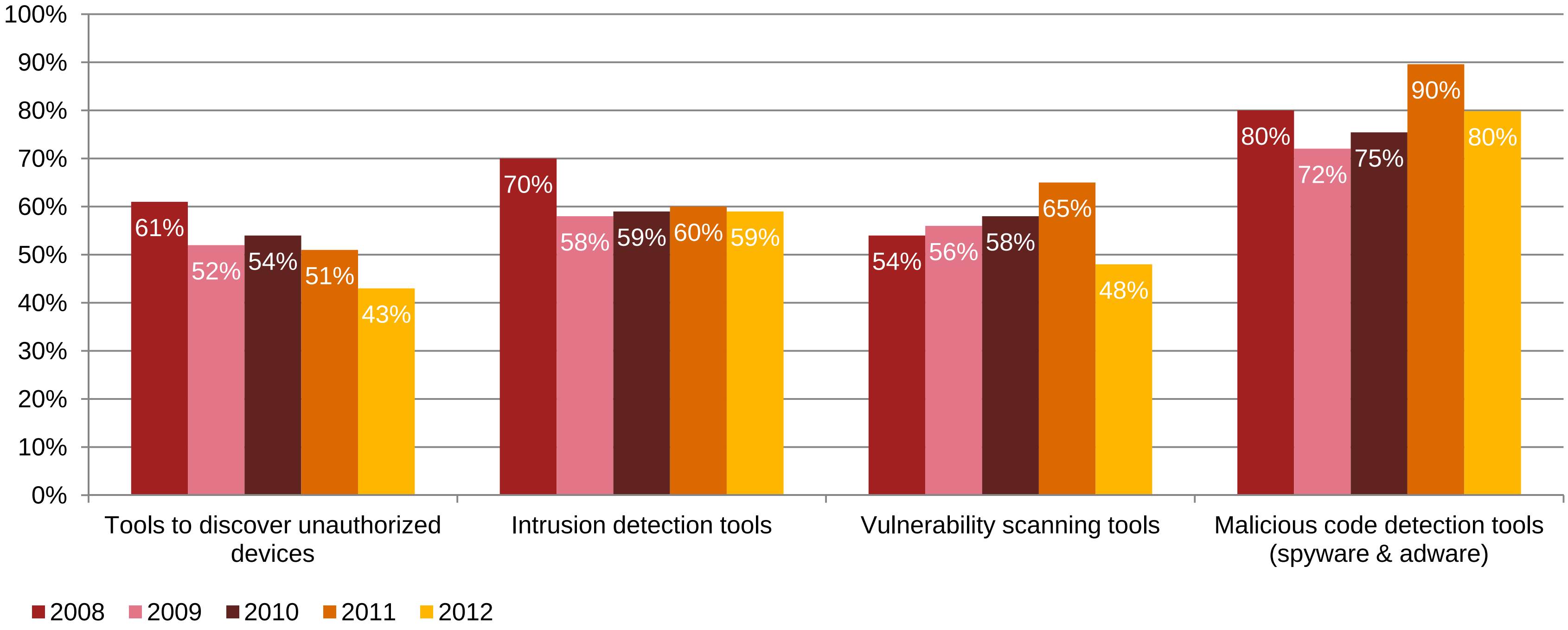


Question 14: "What process information security safeguards does your organization currently have in place?

[1] PwC, Consumer privacy: What are consumers willing to share? July 2012

Use of some key technology safeguards declined over last year.

In some cases, deployment of important information security and privacy tools for incident detection is at a four-year low.



Question 15: “What technology information security safeguards related to detection does your organization have in place?”

Section 4

It’s how you play the game

What keeps security from being what it should be?

52% of utilities respondents continue to perceive top-level leadership as an obstacle to more effective security, although fewer identify CEOs as a stumbling block this year. A lack of vision and a dearth of in-house technical expertise continue to be a concern.

	2011	2012
Leadership – CEO, President, Board, or equivalent	23%	18%
Leadership – CIO or equivalent	18%	21%
Leadership – CISO, CSO, or equivalent	12%	13%
Lack of an actionable vision or understanding	36%	37%
Absence or shortage of in-house technical expertise	26%	28%
Lack of an effective information security strategy	26%	27%
Insufficient capital expenditures	23%	22%

Question 29: “What are the greatest obstacles to improving the overall strategic effectiveness of your organization’s information security function?”

Security leaders don’t always have access to the “top of the house.”

Effective security requires security presence at the executive level. More Chief Security Officers and equivalent senior information security executives are reporting directly to the CEO, although that number remains below 20%. The percentage of Chief Privacy Officers reporting to the CEO increased to 27%.

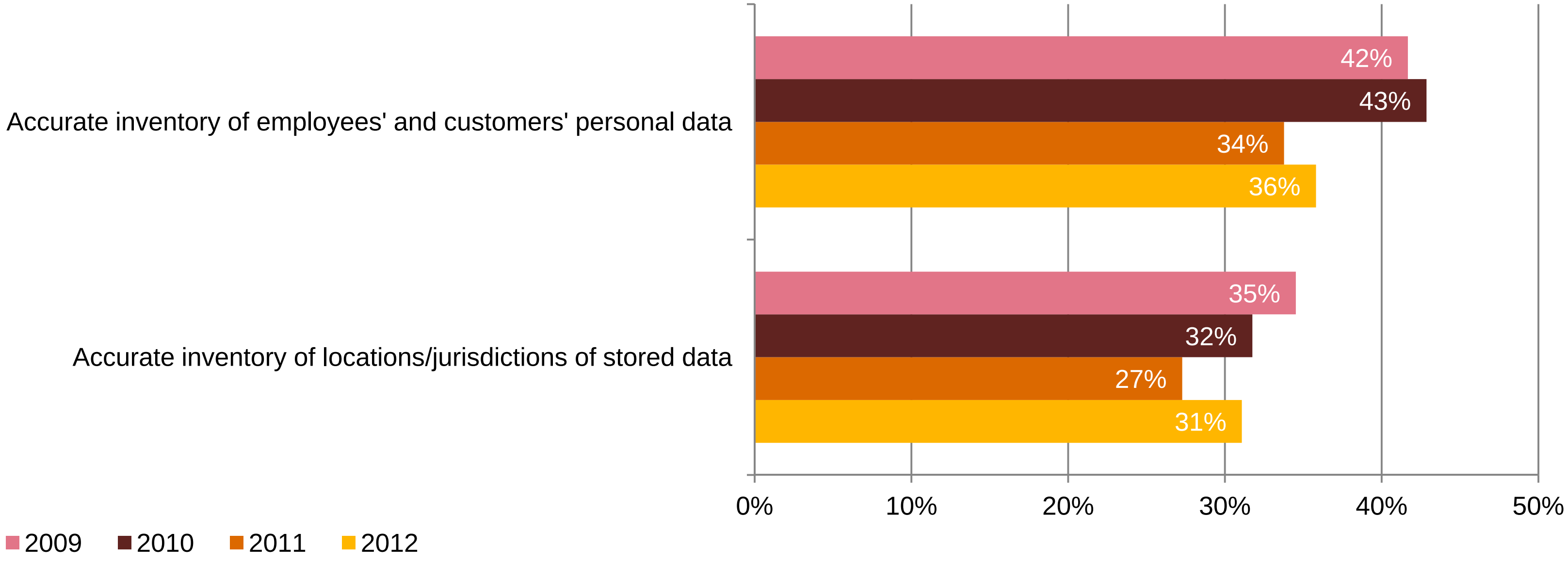
CISO, CSO, or equivalent senior information security executive reports to:	2010	2011	2012
Board of Directors	25%	19%	8%
CEO	40%	15%	17%
CFO	16%	8%	12%

CPO or equivalent senior privacy executive reports to:	2010	2011	2012
Board of Directors	25%	34%	19%
CEO	42%	22%	27%
CFO	18%	25%	8%

Question 13A: “Where / to whom does your CISO, CSO, or equivalent senior information security executive report?” Question 11A: “Where / to whom does your CPO or equivalent senior privacy executive report?”

Utilities respondents know less about their data now than they did three years ago.

While 85% of respondents say protecting customer and employee data is important, far fewer understand what that data entails and where it is stored. This is significant because, increasingly, consumers want to be in control of their personal data and "turn off" the flow of information from companies.[2]



Question 38: "What level of importance does your company place on protecting the following types of information?" Question 11: "Which data privacy safeguards does your organization have in place?"

[2] PwC, Consumer privacy: What are consumers willing to share? July 2012

What you can do to improve your performance.

Information security today is a rapidly evolving game of advanced skill and strategy. As a result, the security models of the past decade are no longer effective.

Effective security requires a new way of thinking. The very survival of the business demands that security leaders understand, prepare for, and quickly respond to security threats.

Businesses seeking to strengthen their security practice must:

- Implement a comprehensive risk-assessment strategy and align security investments with identified risks.
- Understand their organization's information, who wants it, and what tactics adversaries might use to get it.
- Understand that information security requirements – and, indeed, overall strategies for doing business – have reached a turning point.
- Embrace a new way of thinking in which information security is both a means to protect data as well as an opportunity to create value to the business.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
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/giss2013

US Power & Utilities Contacts

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

Jon Stanford
Director
971.544.4325
jon.stanford@us.pwc.com

Michael Echols
Manager
602.364.8043
michael.c.echols@us.pwc.com

The Global State of Information Security® is a registered trademark of International Data Group, Inc.

PwC

www.pwc.com/security

Changing the game

While tight budgets have forestalled updates to security programs, many businesses are confident they're winning the game. But the rules – and the players – have changed.

Public Sector

Key findings from The Global State of Information Security® Survey 2013

September 2012

"You can't succeed in today's elevated threat environment if you don't know the players and you don't know the rules."

– Gary Loveland, Principal, PwC

Information security has always been a high-stakes game. One that demands a smart strategy, the right technology moves, and an unblinking eye on adversaries.

For many businesses, however, it has become a pursuit that is almost impossible to win. That's because the rules have changed, and opponents—old and new—are armed with expert technology skills. As a result, the risks are greater than ever.

Businesses are fighting back by adopting new detection and prevention technologies. At the same time, governments around the world are enacting legislation to combat cyber threats. And regulatory bodies are issuing new guidance on disclosure obligations for cyber incidents.

Yet risks to data security continue to intensify – and show no signs of abating. Those keeping score agree that the bad guys appear to be in the lead.

Nonetheless, many public sector entities believe they are winning. The Global State of Information Security® Survey 2013 shows that most administrators in global public sector organizations are confident in the effectiveness of their information security practices. They believe their strategies are sound and many consider themselves to be leaders in the field.

The odds, however, are not in their favor: Diminished budgets have resulted in degraded security programs, risks are not well understood or properly addressed, and new technologies are being adopted faster than they can be safeguarded.

Given today's elevated threat environment, businesses can no longer afford to play a game of chance. They must prepare to play a new game, one that requires advanced levels of skill and strategy to win.

Agenda

Section 1. Methodology

Section 2. A game of confidence

Section 3. A game of risk

Section 4. It’s how you play the game

Section 1

Methodology

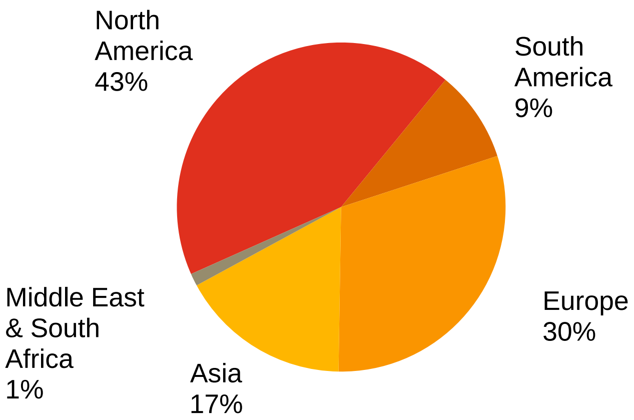
A worldwide study

The Global State of Information Security® Survey 2013, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 1, 2012 to April 15, 2012.

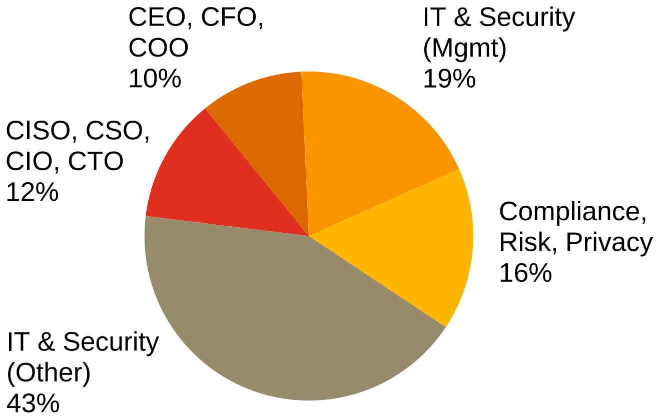
- PwC’s 15th year conducting the online survey, 10th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 128 countries
- More than 9,300 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-three percent (33%) of respondents from companies with revenue of $500 million+
- Survey included 730 respondents from the public sector
- Margin of error less than 1%

Demographics

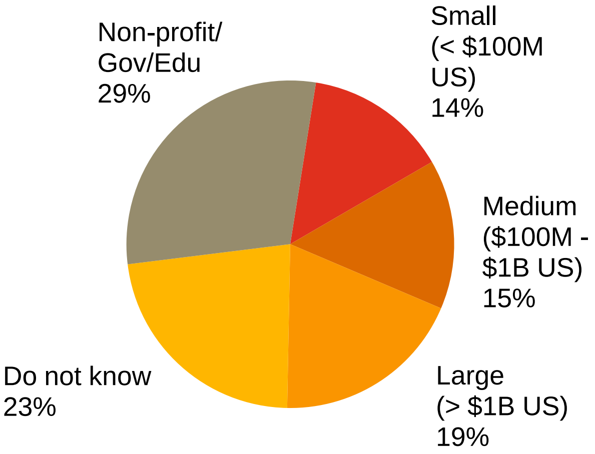
Public sector respondents by region of employment



Public sector respondents by title



Public sector respondents by company revenue size



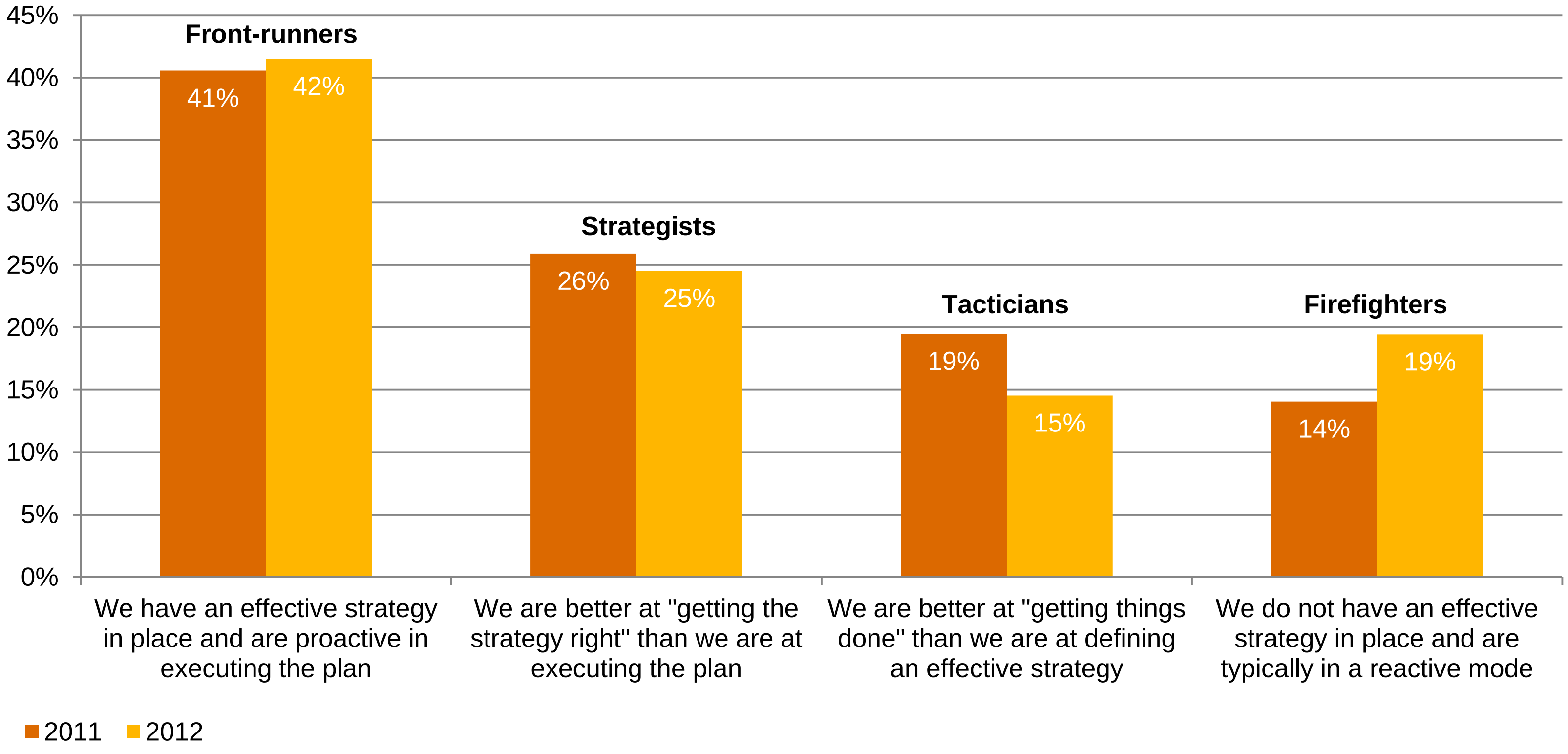
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

A game of confidence

Public sector respondents are confident in their security practices.

42% of respondents say their organization has a strategy in place and is proactive in executing it – exhibiting two distinctive attributes of a leader.



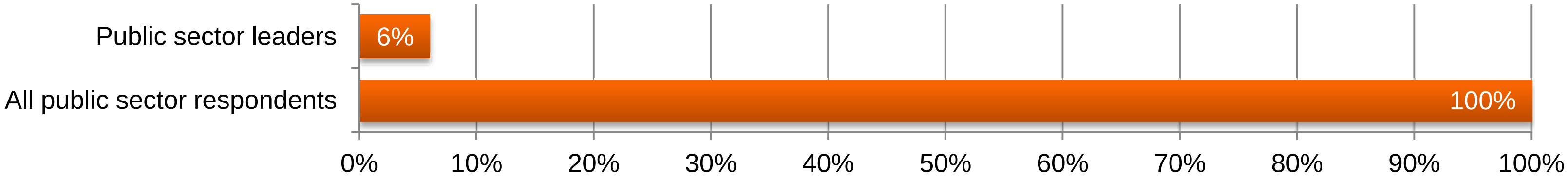
Question 28: "Which category below best characterizes your organization’s approach to protecting information security?"

Does the global public sector perceive itself to be a security leader?

While certain elements of global public sectors' security programs are classified information – and therefore unknown to most survey respondents – we measured respondents' self-appraisal against four generic criteria to define leadership. To qualify, an organization must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the "top of the house" (e.g., to the CEO, CFO, COO, or legal counsel)
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

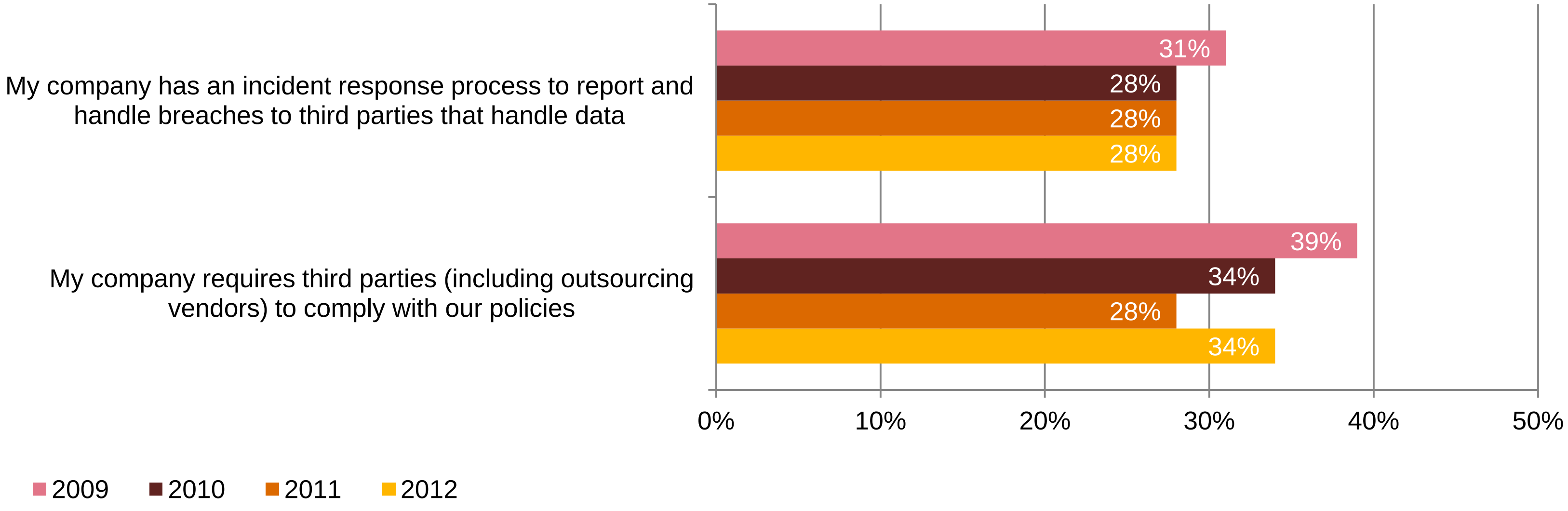
Based on this data, we found that 6% of global public sector respondents rank as leaders.



Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 18: "What types of security incidents (breach or downtime) occurred" and Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

The global public sector should expand its definition of a 'security culture' to include protection from third parties.

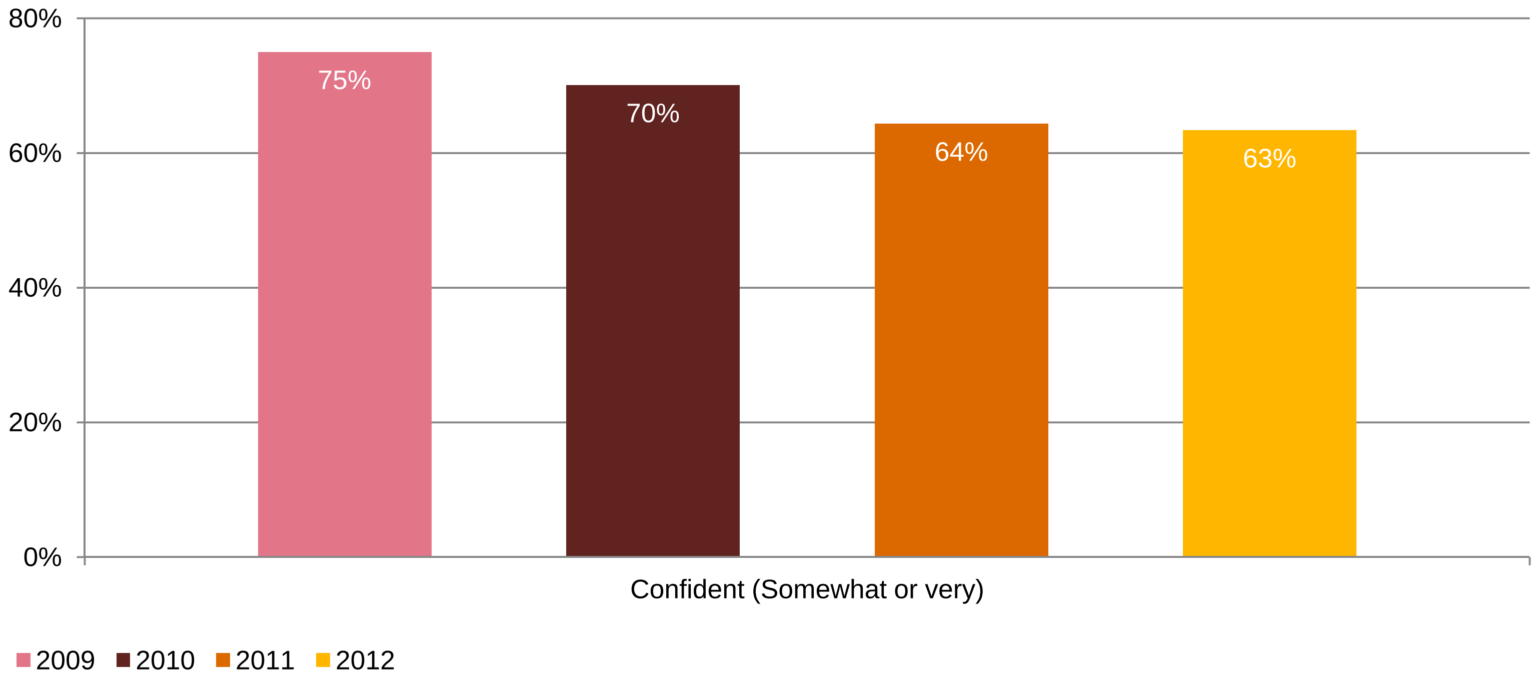
59% of respondents, representing local, state, and national governments, are confident that they have instilled effective security behaviors into their culture. Yet most do not have a process in place to handle third-party breaches, and only 34% require third parties to comply with privacy policies. This suggests a troubling gap in perception – and demonstrates differing security capabilities of governments around the world.



Question 35: "How confident are you that your organization has instilled effective information security behaviors into the organizational culture?"
Question 11: "Which data privacy safeguards does your organization have in place?"

Most respondents say their information security activities are effective, but confidence is eroding.

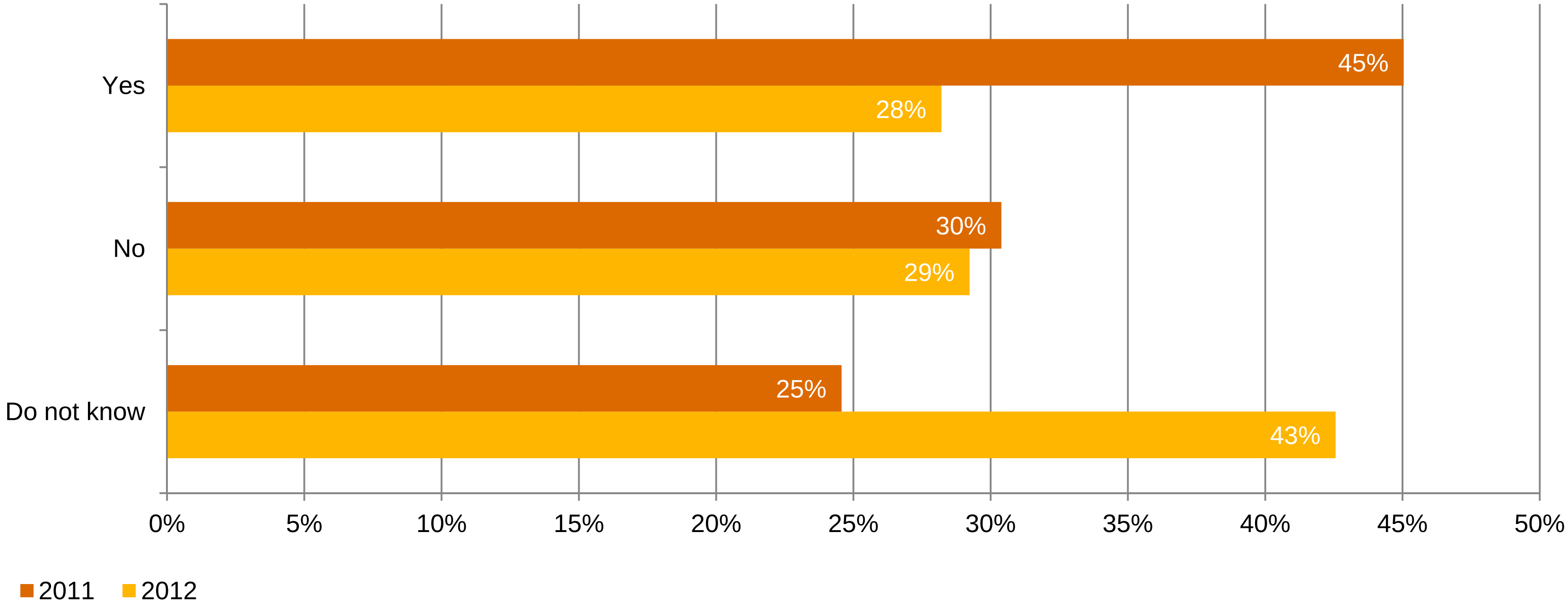
Confidence is a good thing. Although 63% of public sector respondents say they are confident that their company's security activities are effective, they probably don't realize that assurance has dropped since 2009.



Question 41: "How confident are you that your organization's information security activities are effective?"

Creation of ‘cyber commands’ to guard against attacks has stalled.

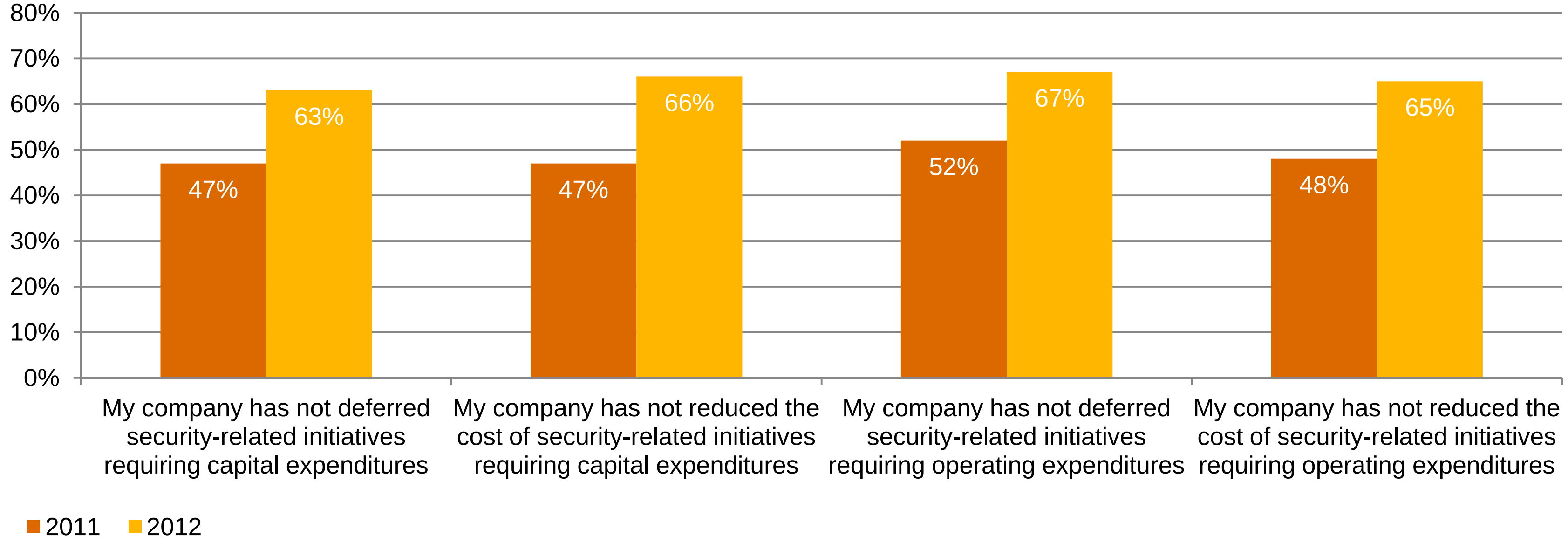
Fewer than one-third of respondents say they are setting up centralized departments to protect public sector IT systems from cyber attacks. That’s a drop of 38% over last year.



(Asked only of Public Sector respondents) Question 3: “Is your organization establishing or does it plan to establish a cyber command department to protect government IT systems from cyber attacks?”

Among public sector respondents, the outlook for security spending over the next 12 months is mixed.

Only 35% of public sector respondents expect security budgets to increase in the year ahead. More encouragingly, respondents report fewer deferrals and fewer budget cutbacks. Compared with last year, for instance, 40% more respondents say their organization had not cut capital spending for security initiatives.



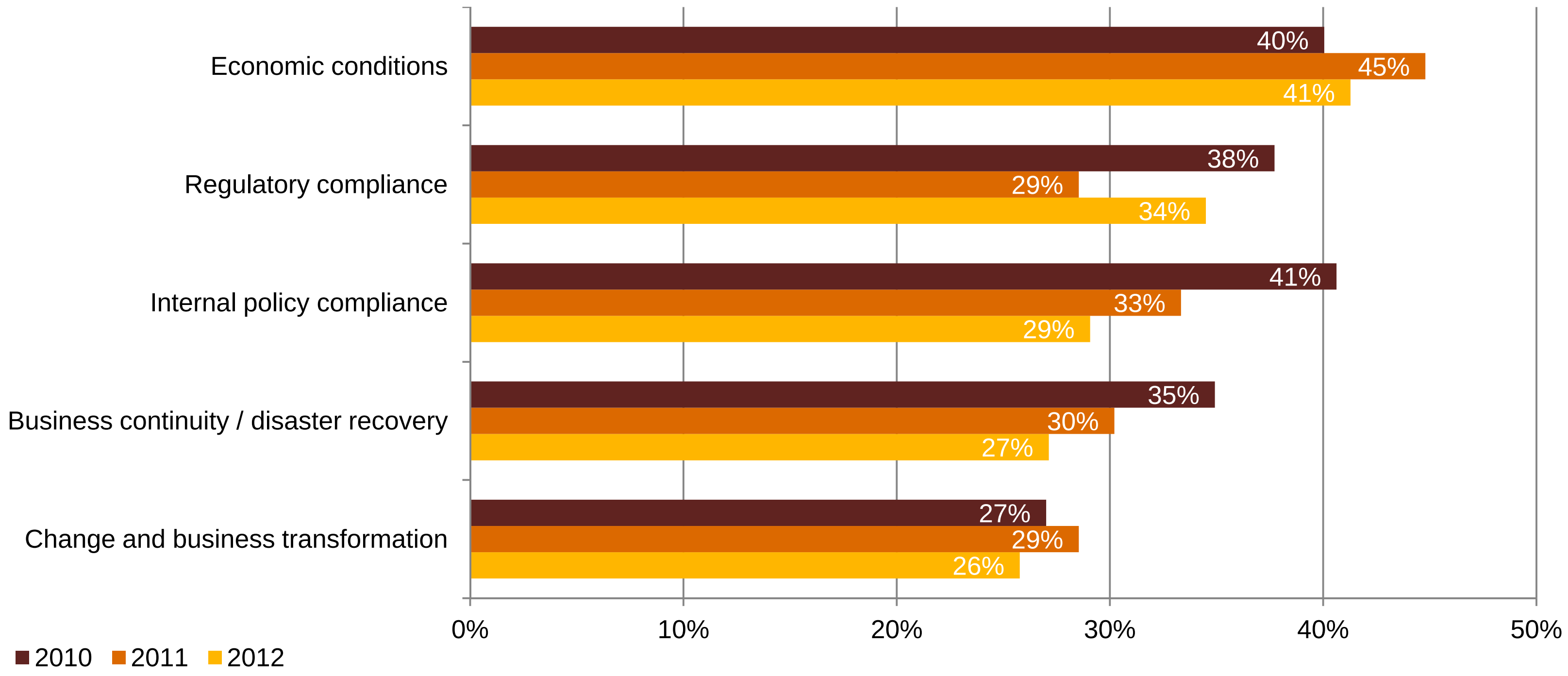
Question 8: “When compared with last year, security spending over the next 12 months will:” Questions 9A and 10A: “Has your company deferred capital and operating security-related initiatives?” Questions 9B and 10B: “Has your company reduced the capital and operating cost of security-related initiatives?”

Section 3

A game of risk

Security budgets are not driven by security needs.

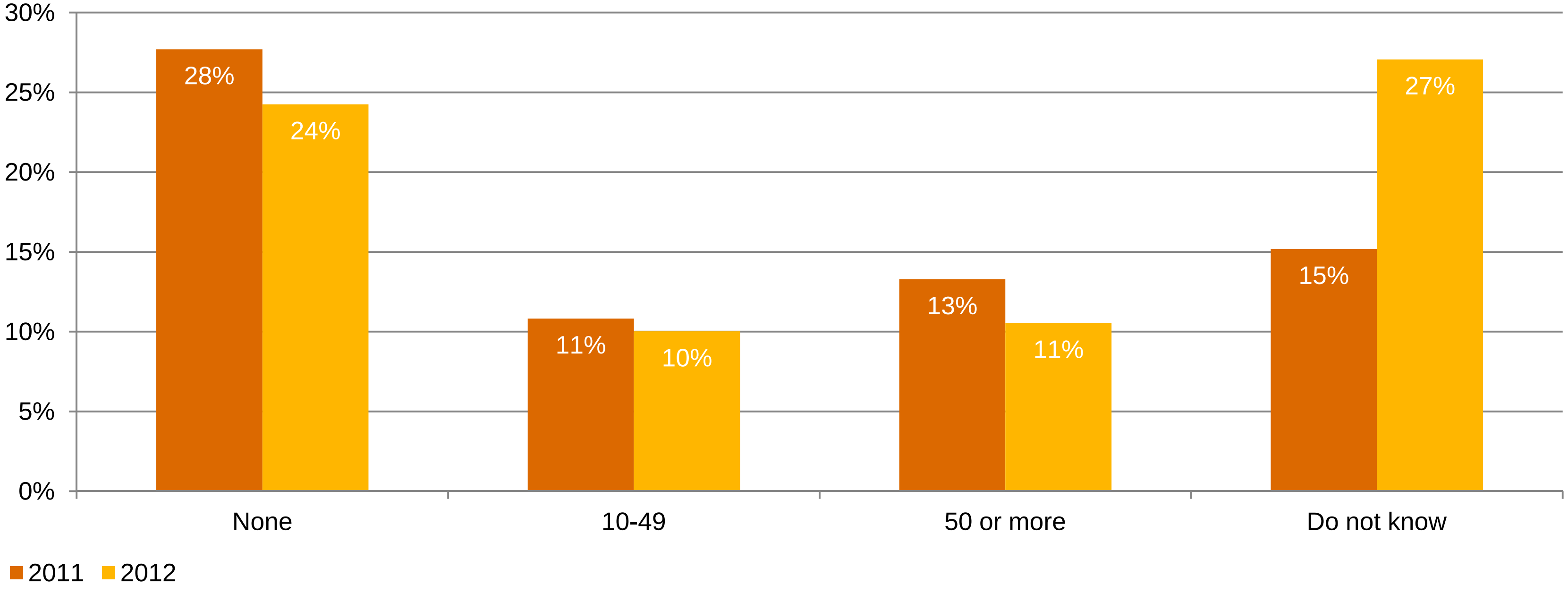
The leading driver of security spending remains economic conditions, cited by 41% of respondents. Compliance – internal and external combined – is cited by 63% of public sector respondents.



Question 37: "What business issues or factors are driving your company's information security spending?" (Not all factors shown.)

Reported security incidents show slight decline as uncertainty rises.

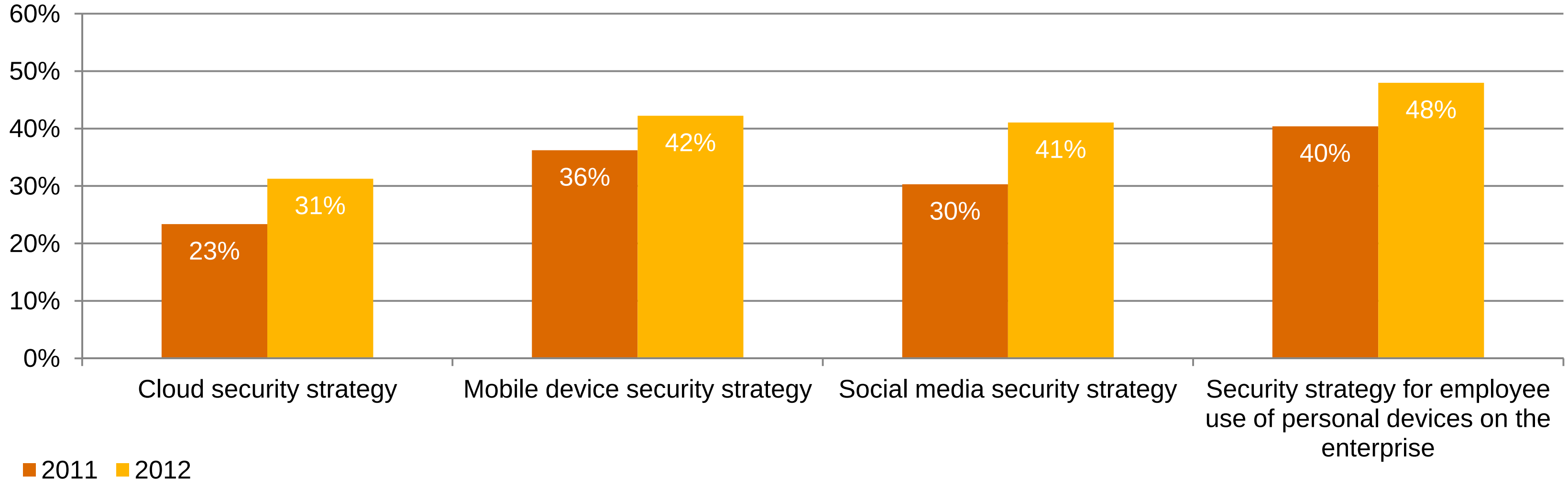
Respondents reporting the most numerous category of security incidents – 50 or more per year – dipped from 2011. Note, however, that the number who do not know the volume of incidents like breaches or downtime almost doubled to 27%.



Question 17: "Number of security incidents in the past 12 months."

Technology adoption is moving faster than security implementation.

As with many private sector industries, public sector entities are struggling to keep pace with the adoption of cloud computing, social networking, mobility, and use of employee-owned devices. These new technologies often are not included in overall security plans even though they are widely used. We have found, for instance, that 88% of consumers use a personal mobile device for both personal and work purposes.[1]

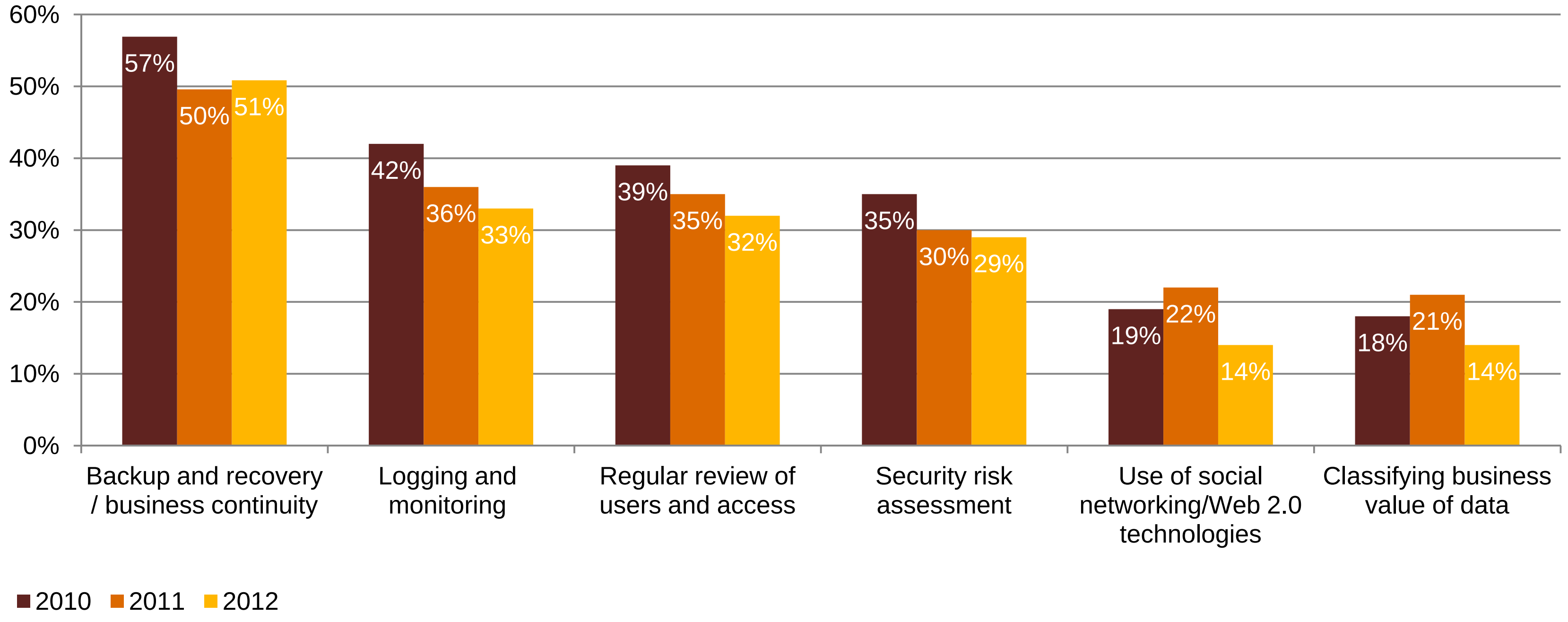


Question 14: “What process information security safeguards does your organization currently have in place?”

[1] PwC, Consumer privacy: What are consumers willing to share? July 2012

Certain security policies are showing signs of degradation.

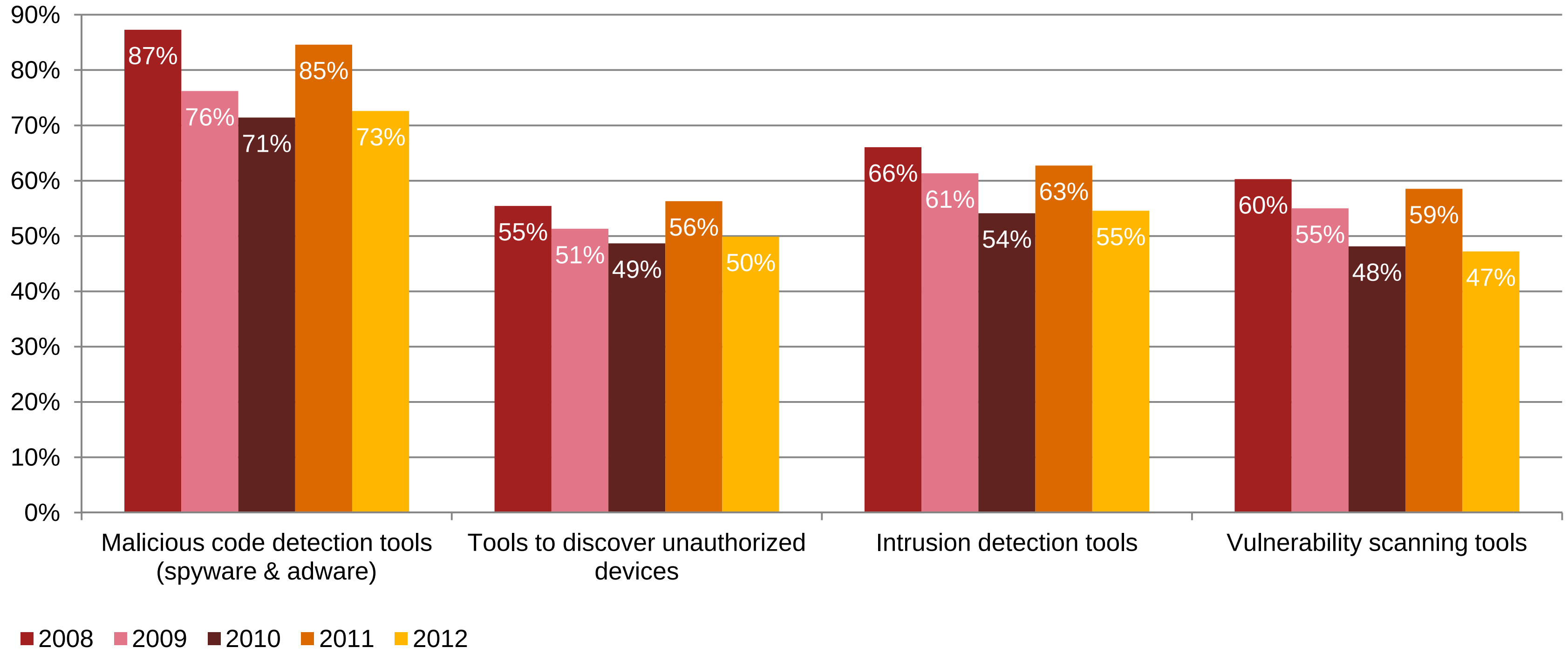
Public sector organizations continue to cut fundamental elements of security from their overall policies.



Question 32: “Which of the following elements, if any, are included in your organization’s security policy?”

Use of key detection technologies resumes a long-term decline after last year's uptick.

The future looked bright last year as many public sector entities stepped up investments in detection safeguards. This year, however, saw a decrease in deployment of important security and privacy tools.



Question 15: "What technology information security safeguards related to detection does your organization have in place?"

Section 4

It’s how you play the game

What keeps security from being what it should be?

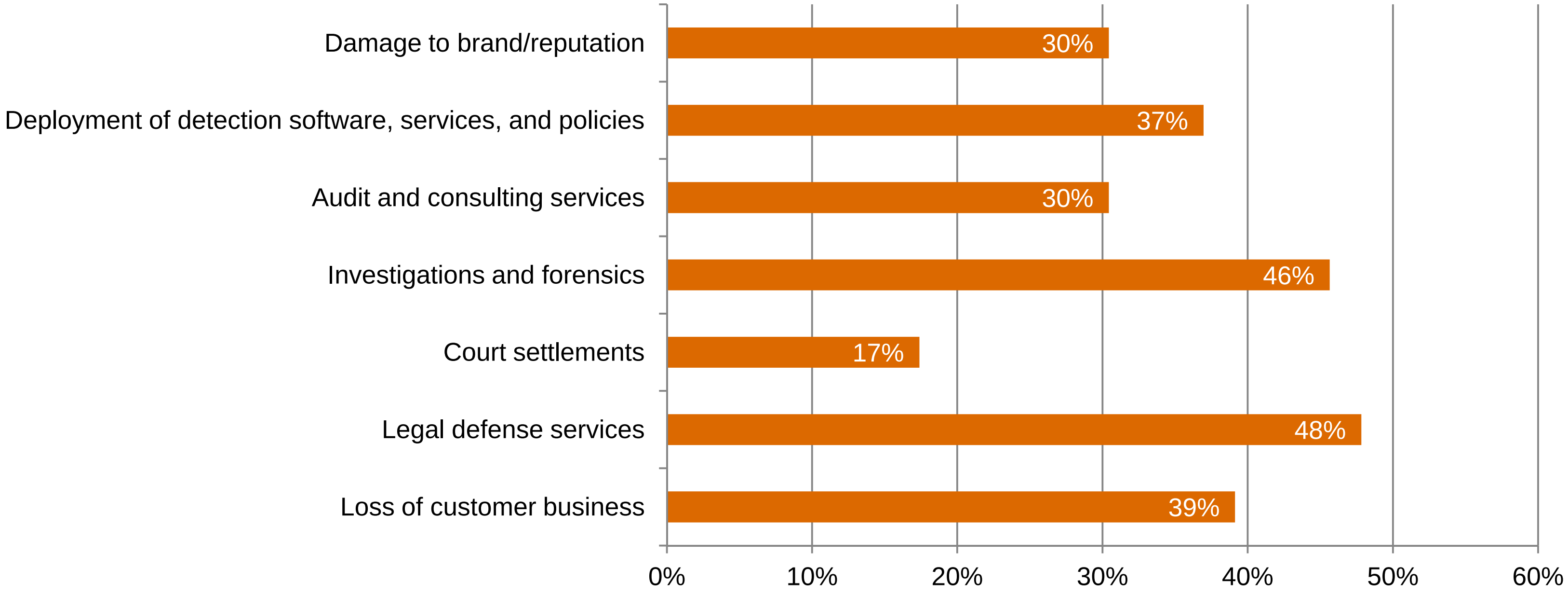
Top leadership is seen as less an obstacle than in the past, although 44% of respondents still point to C-level executives and Boards. But they also cited insufficient funding – for both capital and operating projects – as significant roadblocks to security effectiveness.

	2011	2012
Leadership – CEO, President, Board, or equivalent	25%	20%
Leadership – CIO or equivalent	17%	12%
Leadership – CISO, CSO, or equivalent	15%	12%
Insufficient capital expenditures	28%	28%
Insufficient operating expenditures	21%	28%
Poorly integrated or overly complex IT systems	20%	26%
Absence or shortage of in-house technical expertise	22%	25%

Question 29: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?"

An inadequate assessment of security incidents can lead to a less-clear understanding of their impact.

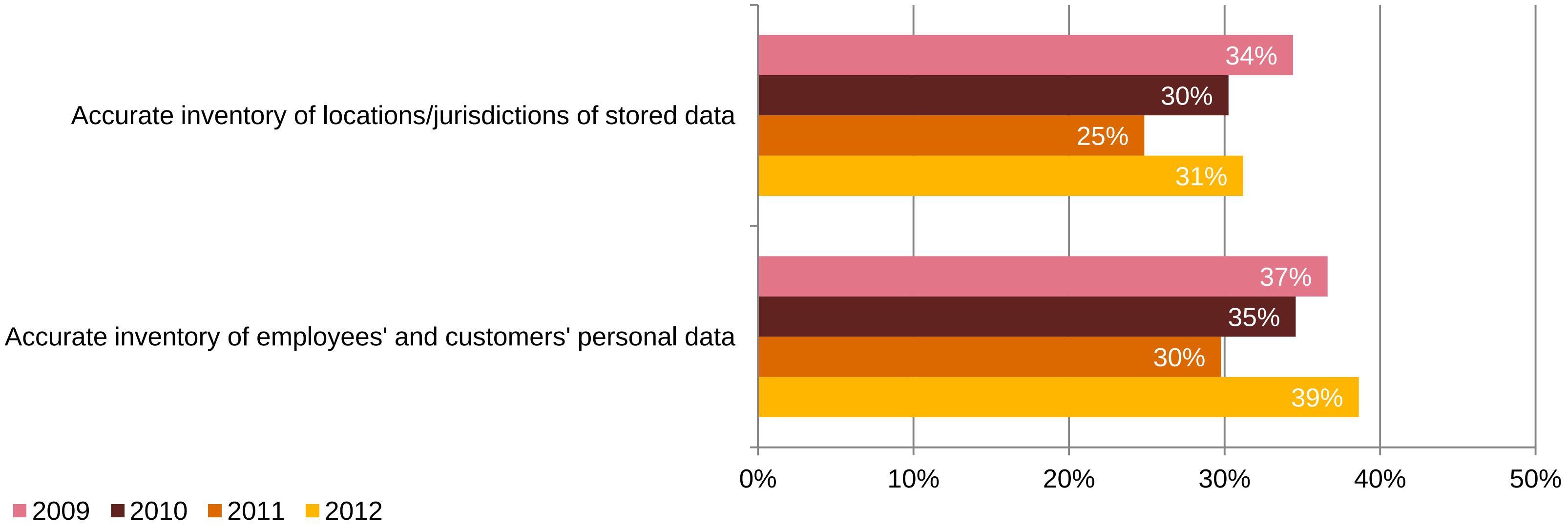
Public sector respondents report a very low incidence of financial losses and other business impacts from security incidents, yet they may not apply thorough or consistent analysis to appraise those costs. For example, only 37% consider the cost of implementing software, services, and policies to mitigate security incidents.



Question 21: “How was your organization impacted by the security incident?” Question 21C: “What factors are included in your company’s calculation of these financial losses?”

Public sector respondents don't know enough about their data and where it resides.

While approximately 75% of respondents say protecting customer and employee data is important, far fewer understand what that data entails and where it is stored. This is significant because, increasingly, consumers want to be in control of their personal data and "turn off" the flow of information from companies.[2]



Question 38: "What level of importance does your company place on protecting the following types of information?" Question 11: "Which data privacy safeguards does your organization have in place?"

[2] PwC, Consumer privacy: What are consumers willing to share? July 2012

What you can do to improve your performance.

Information security today is a rapidly evolving game of advanced skill and strategy. As a result, the security models of the past decade are no longer effective.

Effective security requires a new way of thinking. The very survival of the business demands that security leaders understand, prepare for, and quickly respond to security threats.

Public sector entities seeking to strengthen their security practice must:

- Implement a comprehensive risk-assessment strategy and align security investments with identified risks.
- Understand their organization's information, who wants it, and what tactics adversaries might use to get it.
- Understand that information security requirements – and, indeed, overall strategies for government business – have reached a turning point.
- Embrace a new way of thinking in which information security is both a means to protect data as well as an opportunity to create value to the organization.

For more information, please contact:

US IT Security, Privacy & Risk Contacts – Private Sector

Gary Loveland
Principal
949.437.5380
gary.loveland@us.pwc.com

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

US 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/giss2013

PwC

www.pwc.com/security

Changing the game

While tight budgets have forestalled updates to security programs, many businesses are confident they're winning the game. But the rules – and the players – have changed.

Retail & Consumer

Key findings from The Global State of Information Security® Survey 2013

September 2012

> ***"You can't succeed in today's elevated threat environment if you don't know the players and you don't know the rules."***
>
> ***– Gary Loveland, Principal, PwC***

Information security has always been a high-stakes game. One that demands a smart strategy, the right technology moves, and an unblinking eye on adversaries.

For many businesses, however, it has become a pursuit that is almost impossible to win. That’s because the rules have changed, and opponents—old and new—are armed with expert technology skills. As a result, the risks are greater than ever.

Businesses are fighting back by adopting new detection and prevention technologies. At the same time, governments around the world are enacting legislation to combat cyber threats. And regulatory bodies are issuing new guidance on disclosure obligations for cyber incidents.

Yet risks to data security continue to intensify – and show no signs of abating. Those keeping score agree that the bad guys appear to be in the lead.

Nonetheless, many businesses believe they are winning. The Global State of Information Security® Survey 2013 shows that most executives in the global retail and consumer (R&C) industry are confident in the effectiveness of their information security practices. They believe their strategies are sound and many consider themselves to be leaders in the field.

The odds, however, are not in their favor: Diminished budgets have resulted in degraded security programs, reported security incidents are on the rise, and new technologies are being adopted faster than they can be safeguarded.

Given today's elevated threat environment, businesses can no longer afford to play a game of chance. They must prepare to play a new game, one that requires advanced levels of skill and strategy to win.

Agenda

Section 1. Methodology

Section 2. A game of confidence

Section 3. A game of risk

Section 4. It’s how you play the game

Section 1

Methodology

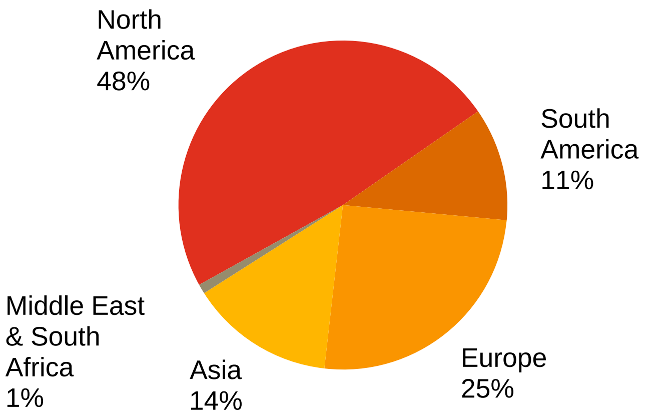
A worldwide study

The Global State of Information Security® Survey 2013, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 1, 2012 to April 15, 2012.

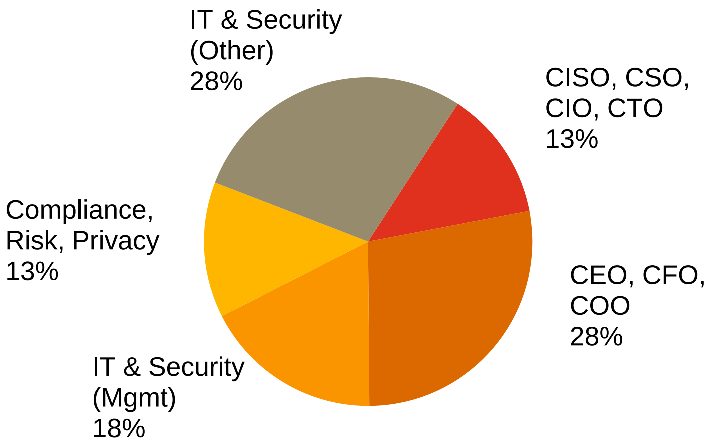
- PwC's 15th year conducting the online survey, 10th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 128 countries
- More than 9,300 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-three percent (33%) of respondents from companies with revenue of $500 million+
- Survey included 1,169 respondents from the R&C industry
- Margin of error less than 1%

Demographics

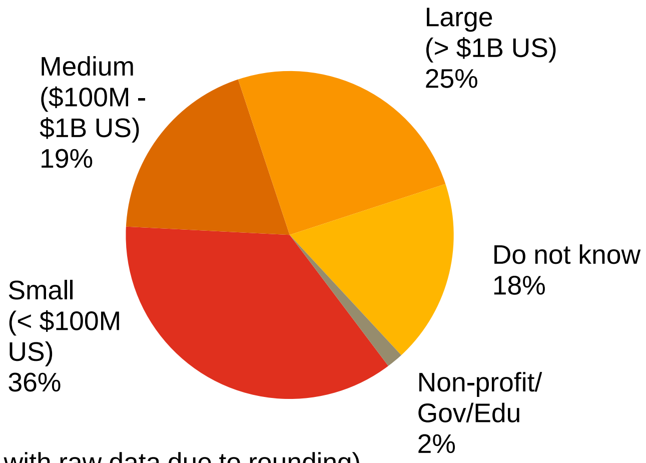
R&C respondents by region of employment



R&C respondents by title



R&C respondents by company revenue size



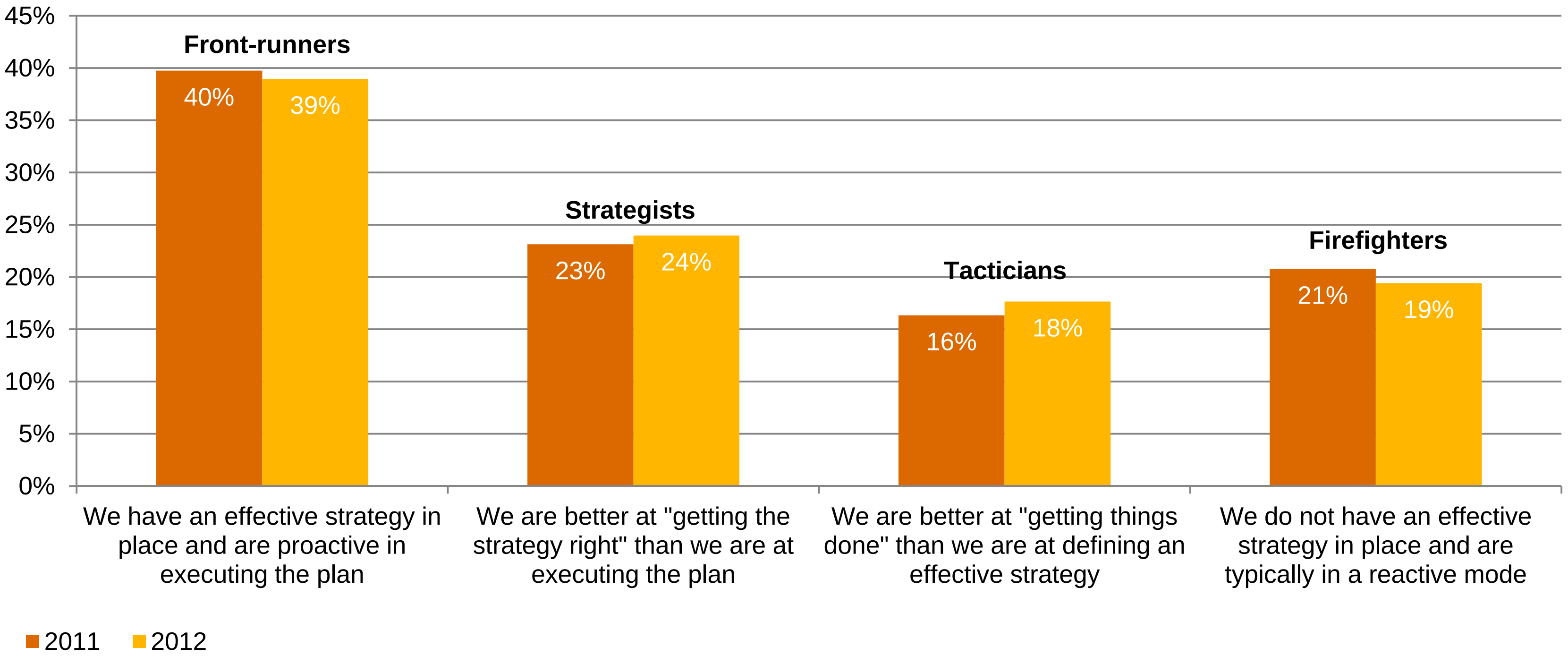
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

A game of confidence

R&C respondents are confident in their security practices.

39% of industry respondents say their organization has a strategy in place and is proactive in executing it – exhibiting two distinctive attributes of a leader.



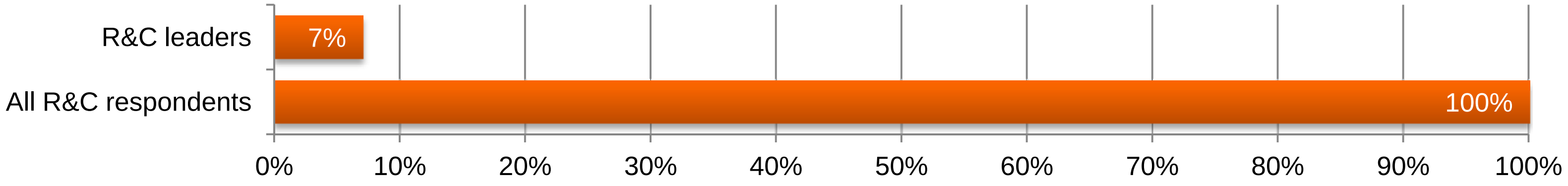
Question 28: "Which category below best characterizes your organization’s approach to protecting information security?"

A reality check on real leaders.

But are they really leaders? We measured R&C respondents' self-appraisal against four key criteria to define leadership. To qualify, organizations must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the "top of the house" (e.g., to the CEO, CFO, COO, or legal counsel)
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

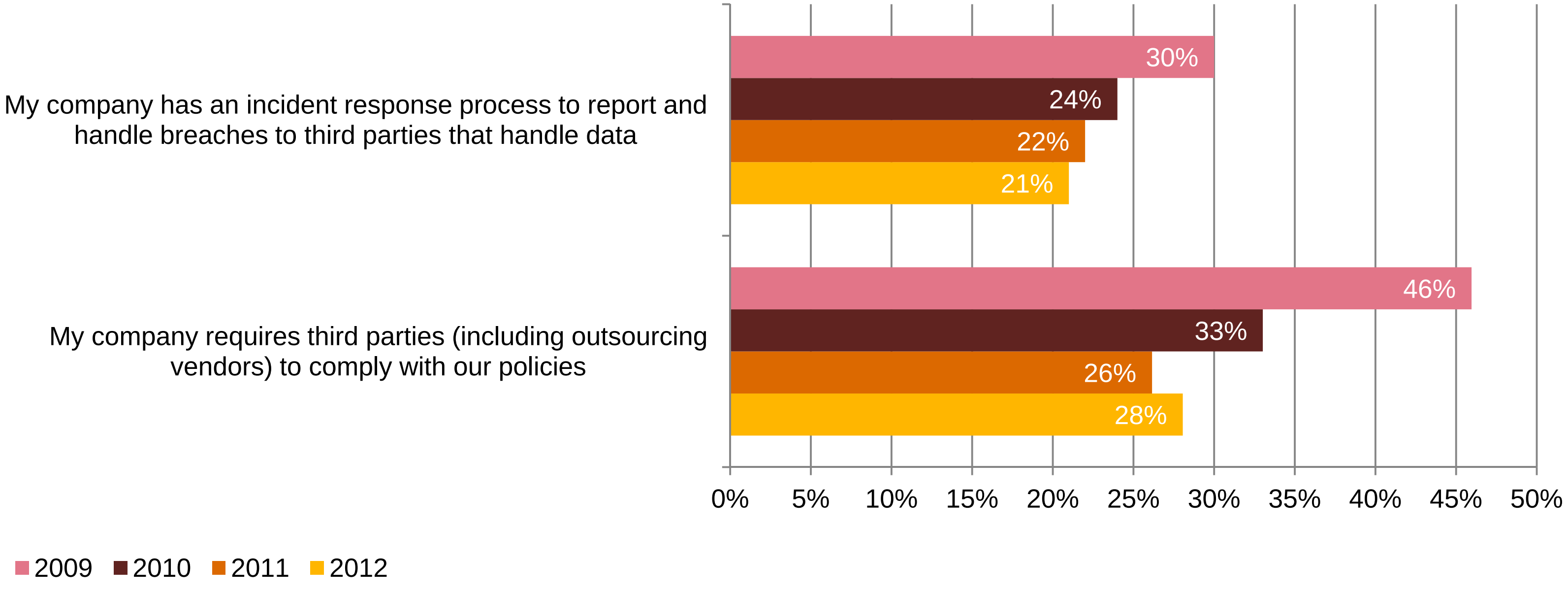
The result? Our analysis found that 7% of R&C respondents rank as leaders.



Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 18: "What types of security incidents (breach or downtime) occurred" and Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Many R&C respondents are over-confident in their organization's security program.

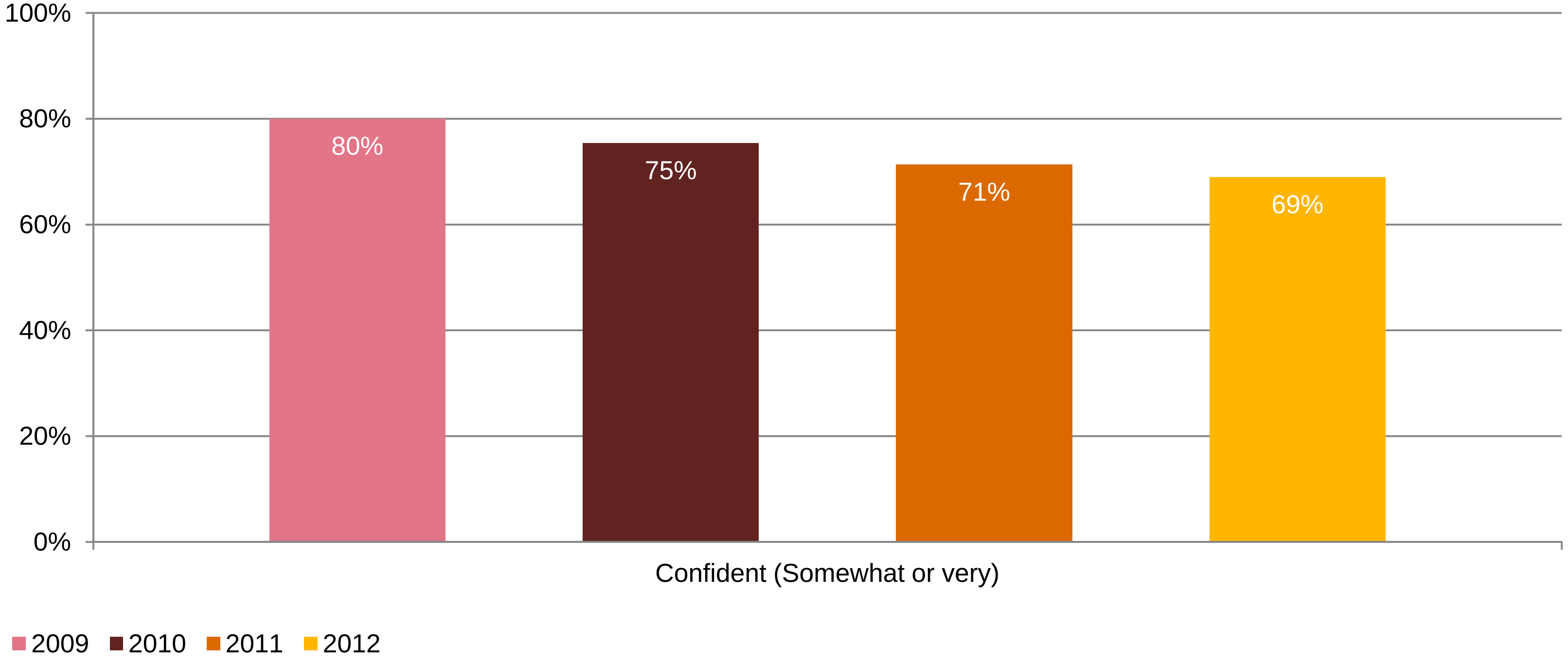
64% of respondents are confident that they have instilled effective security behaviors into their organization's culture, yet most do not have a process in place to handle third-party breaches. What's more, only 28% require third parties to comply with their security policies. This suggests a troubling gap in perception.



Question 35: "How confident are you that your organization has instilled effective information security behaviors into the organizational culture?"
Question 11: "Which data privacy safeguards does your organization have in place?"

Most respondents say their information security activities are effective, but this confidence is eroding.

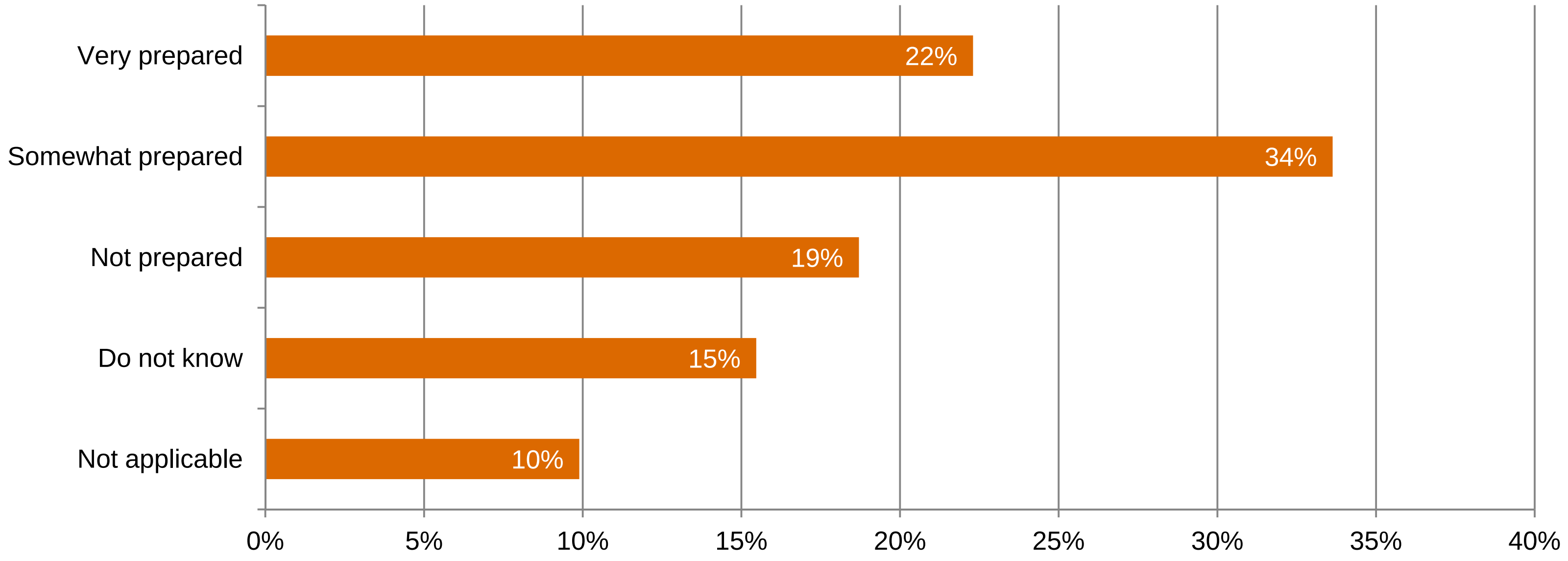
Confidence is a good thing. Although 69% of R&C respondents say they are confident that their company's security activities are effective, they may not realize that assurance has dropped considerably since 2009.



Question 41: "How confident are you that your organization's information security activities are effective?"

Many R&C respondents are unsure how to handle sensitive data in the cloud.

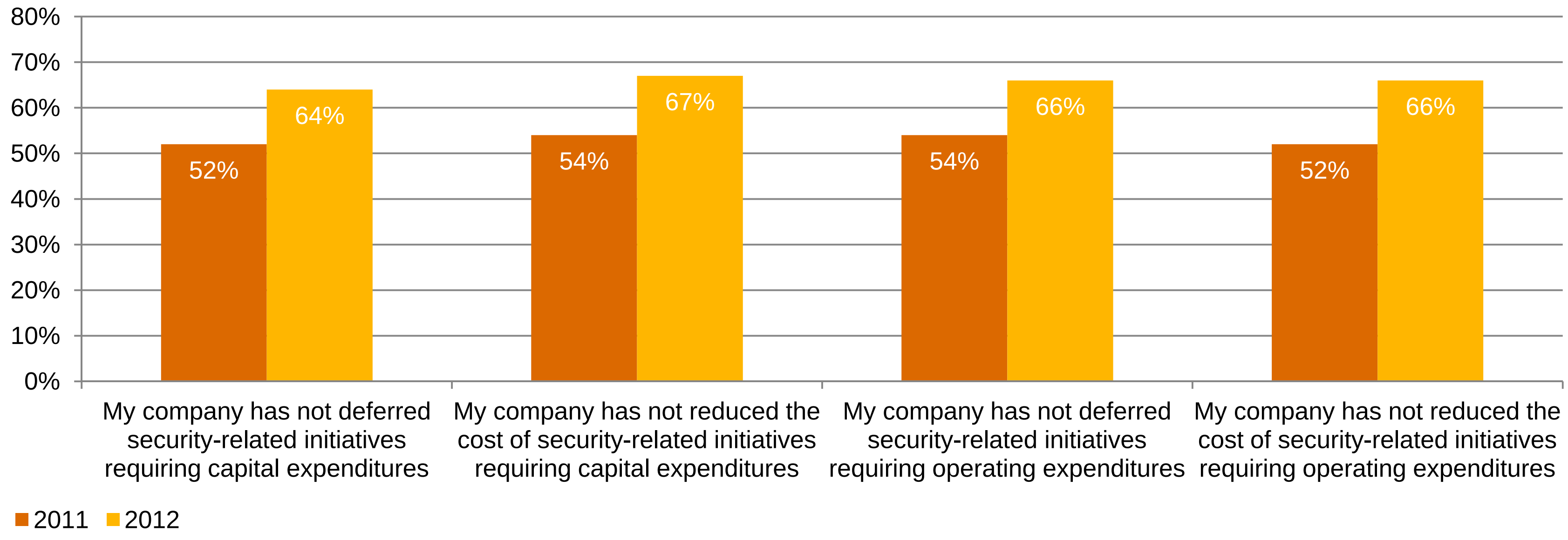
As cloud computing moves from hype to mainstream, many respondents are grappling with protection of sensitive data in the cloud or other third-party environments. Their biggest concern? Ensuring compliance with data security regulations.



(Asked only of R&C respondents) Question 1: “How prepared is your organization to handle sensitive data protection in the cloud and/or in third-party environments over the next 12 to 18 months?” Question 2 (R&C): “What potential issues does your organization face regarding third-party cloud environments?”

Among R&C respondents, the outlook for security spending over the next 12 months is mixed.

Fewer than half – 40% – of R&C respondents expect security budgets to increase in the year ahead. More encouragingly, respondents report fewer deferrals and fewer budget cutbacks for security initiatives. Compared with last year, for instance, 24% more respondents say they have not cut capital expenditures for security programs.



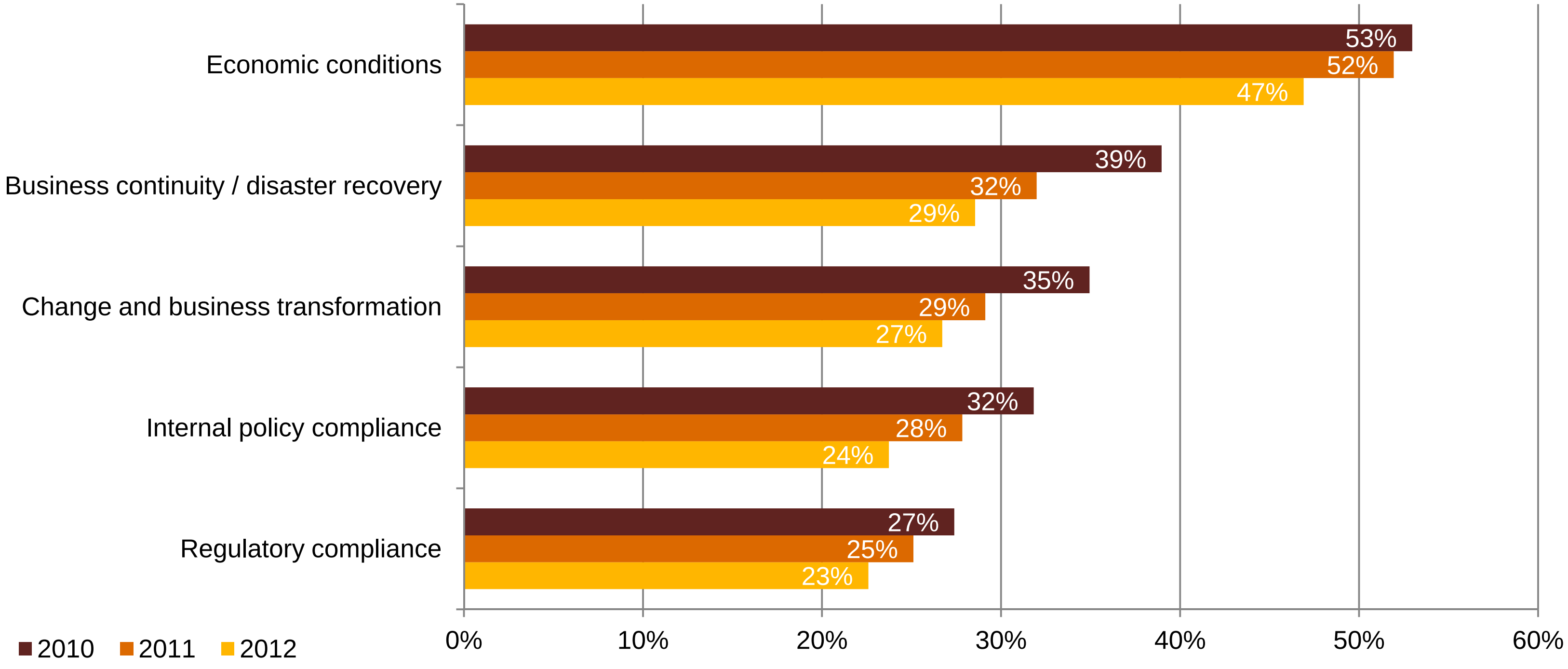
Question 8: "When compared with last year, security spending over the next 12 months will:" Questions 9A and 10A: "Has your company deferred capital and operating security-related initiatives?" Questions 9B and 10B: "Has your company reduced the capital and operating cost of security-related initiatives?"

Section 3

A game of risk

Security budgets are not driven by security needs.

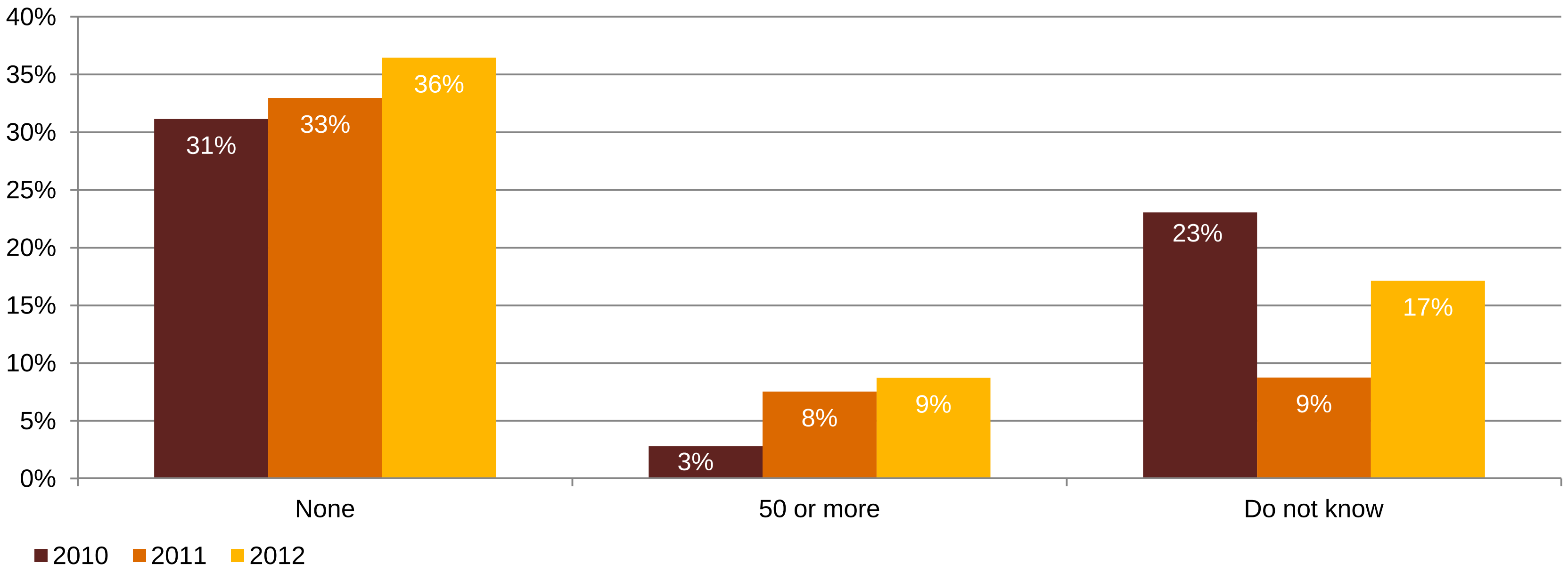
The leading driver of security spending is – by far – economic conditions, cited by 47% of respondents. That's a risky way to set priorities. Business continuity/disaster recovery is the top security-specific response, at 29%.



Question 37: "What business issues or factors are driving your company's information security spending?" (Not all factors shown.)

Reported security incidents appear to be leveling off after a big rise – but that may not tell the whole story.

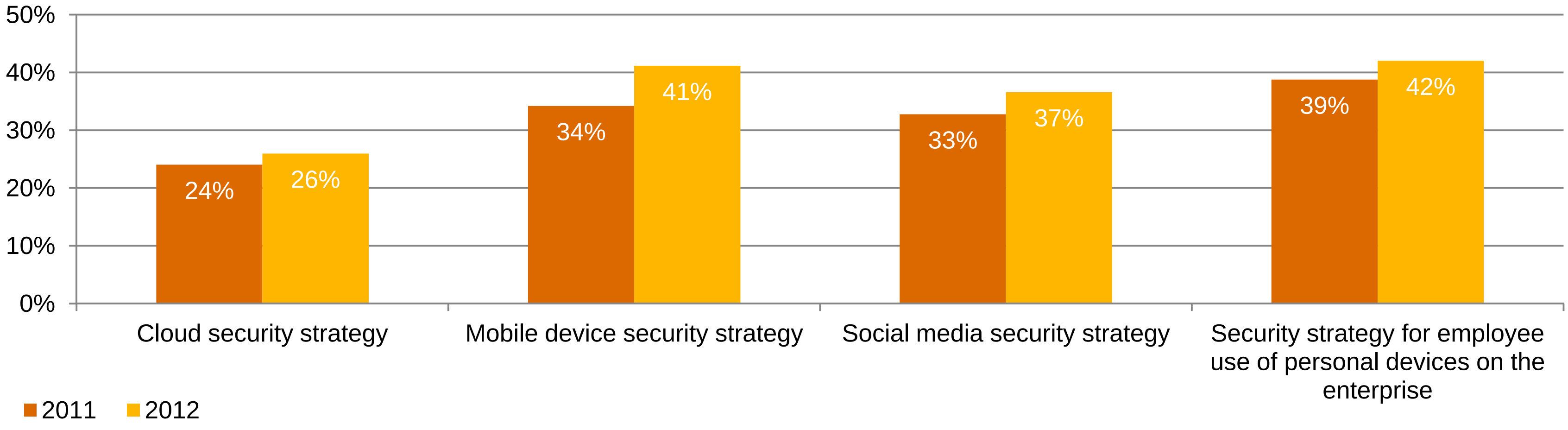
The number of respondents reporting 50 or more security incidents per year has leveled off – a good sign. But the frequency of respondents who did not know how many security incidents they had experienced almost doubled, suggesting ineffective security practices.



Question 17: “Number of security incidents in the past 12 months.”

Technology adoption is moving faster than security implementation.

As with many industries, R&C companies are struggling to keep pace with the adoption of cloud computing, social networking, mobility, and use of employee-owned devices. Though widely used, these technologies are often not included in overall security plans. We have found, for instance, that 88% of consumers use a personal mobile device for both personal and work purposes.[1]

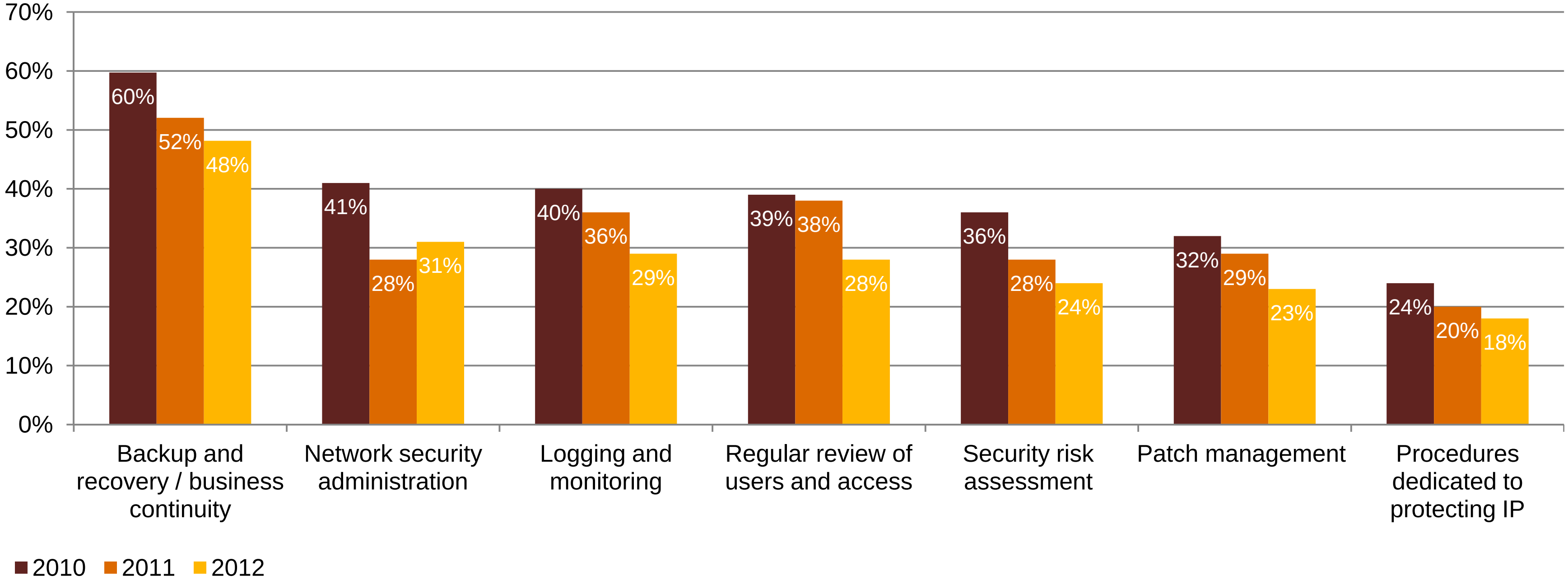


Question 14: “What process information security safeguards does your organization currently have in place?”

[1] PwC, Consumer privacy: What are consumers willing to share? July 2012

Security policies have grown less robust and inclusive.

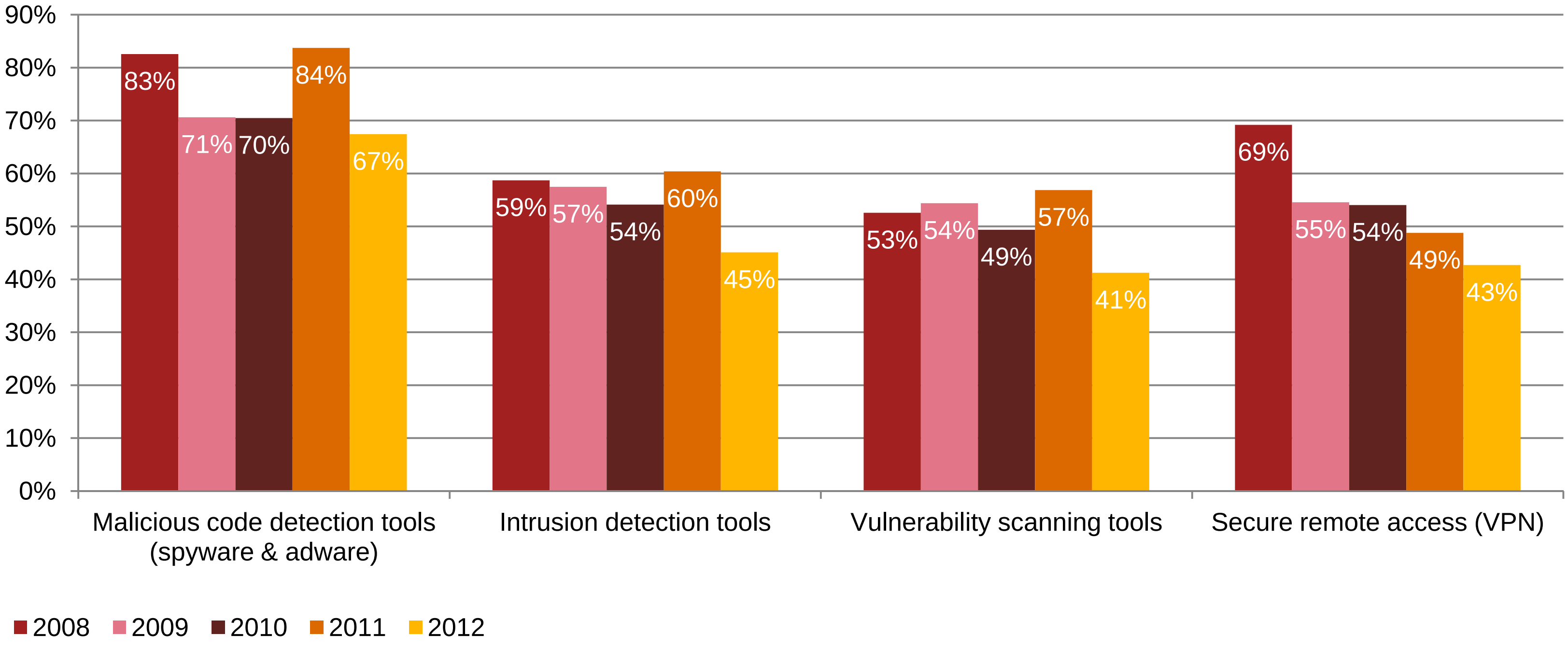
Many companies are omitting fundamental elements of security from their overall policies. The result? An incomplete framework of policies, procedures, and guidelines that hinders the organization's ability to mitigate risks.



Question 32: "Which of the following elements, if any, are included in your organization's security policy?"

After an uptick last year, use of some key technology safeguards has declined.

The future looked bright last year as many R&C firms stepped up investments in detection safeguards. This year, however, respondents report a decrease in deployment of important security and privacy tools.



Question 15: “What technology information security safeguards related to detection does your organization have in place?”

Section 4

It's how you play the game

What keeps security from being what it should be?

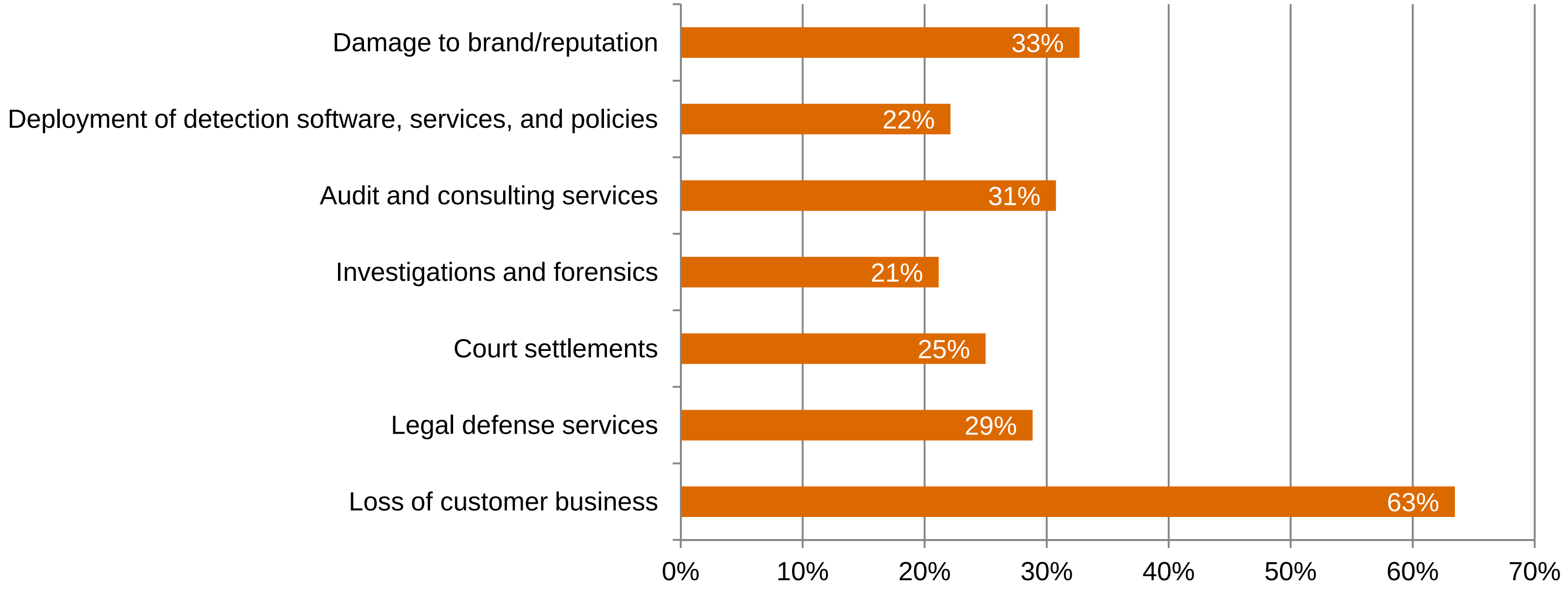
Lack of capital funding was the most-cited single inhibitor to security this year. Top-level leadership is also perceived to be an obstacle to effective security, according to 47% of respondents.

	2011	2012
Leadership – CEO, President, Board, or equivalent	23%	23%
Leadership – CIO or equivalent	15%	11%
Leadership – CISO, CSO, or equivalent	16%	13%
Insufficient capital expenditures	29%	25%
Lack of an actionable vision or understanding	24%	23%
Lack of an effective information security strategy	23%	22%

Question 29: “What are the greatest obstacles to improving the overall strategic effectiveness of your organization’s information security function?”

An inadequate assessment of security incidents can lead to a less-clear understanding of their impact.

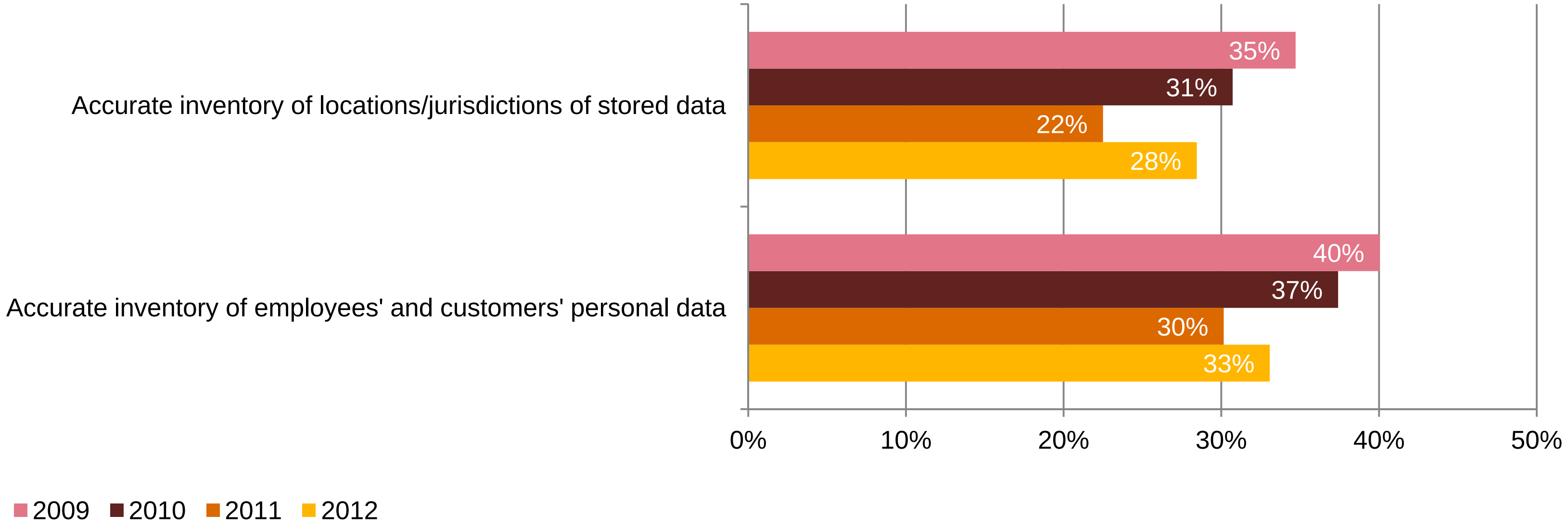
R&C respondents report a lower incidence of financial loss from security incidents, yet many do not apply a thorough or consistent analysis to appraise those costs. For example, only 21% consider the cost of investigations and forensics, while 33% factor in damage to brand/reputation.



Question 21: “How was your organization impacted by the security incident?” Question 21C: “What factors are included in your company’s calculation of these financial losses?”

R&C respondents know less about their data now than they did three years ago.

While approximately 80% of respondents say protecting customer and employee data is important, far fewer understand what that data entails and where it is stored. This is significant because organizations must know where data resides in order to effectively protect it. What's more, consumers increasingly want to control their personal data.[2]



Question 38: "What level of importance does your company place on protecting the following types of information?" Question 11: "Which data privacy safeguards does your organization have in place?"

[2] PwC, Consumer privacy: What are consumers willing to share? July 2012

What you can do to improve your performance.

Information security today is a rapidly evolving game of advanced skill and strategy. As a result, the security models of the past decade are no longer effective.

Effective security requires a new way of thinking. The very survival of the business demands that security leaders understand, prepare for, and quickly respond to security threats.

Businesses seeking to strengthen their security practice must:

- Implement a comprehensive risk-assessment strategy and align security investments with identified risks.
- Understand their organization's information, who wants it, and what tactics adversaries might use to get it.
- Understand that information security requirements – and, indeed, overall strategies for doing business – have reached a turning point.
- Embrace a new way of thinking in which information security is both a means to protect data as well as an opportunity to create value to the business.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
949.437.5380
gary.loveland@us.pwc.com

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

US Retail & Consumer Contacts

Lisa Dugal
Principal
646.471.6916
lisa.feigen.dugal@us.pwc.com

Pieter Penning
Principal
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/giss2013

The Global State of Information Security® is a registered trademark of International Data Group, Inc.

PwC

www.pwc.com/security

Changing the game

While tight budgets have forestalled updates to security programs, many businesses are confident they're winning the game. But the rules – and the players – have changed.

Technology

Key findings from The Global State of Information Security® Survey 2013

September 2012

> ***"You can't succeed in today's elevated threat environment if you don't know the players and you don't know the rules."***
>
> ***– Gary Loveland, Principal, PwC***

Information security has always been a high-stakes game. One that demands a smart strategy, the right technology moves, and an unblinking eye on adversaries.

For many businesses, however, it has become a pursuit that is almost impossible to win. That's because the rules have changed, and opponents—old and new—are armed with expert technology skills. As a result, the risks are greater than ever.

Businesses are fighting back by adopting new detection and prevention technologies. At the same time, governments around the world are enacting legislation to combat cyber threats. And regulatory bodies are issuing new guidance on disclosure obligations for cyber incidents.

Yet risks to data security continue to intensify – and show no signs of abating. Those keeping score agree that the bad guys appear to be in the lead.

Nonetheless, many businesses believe they are winning. The Global State of Information Security® Survey 2013 shows that most executives in the global technology industry are confident in the effectiveness of their information security practices. They believe their strategies are sound and many consider themselves to be leaders in the field.

The odds, however, are not in their favor: Diminished budgets have resulted in degraded security programs, reported security incidents are on the rise, and new technologies are being adopted faster than they can be safeguarded.

Given today's elevated threat environment, businesses can no longer afford to play a game of chance. They must prepare to play a new game, one that requires advanced levels of skill and strategy to win.

Agenda

Section 1. Methodology

Section 2. A game of confidence

Section 3. A game of risk

Section 4. It’s how you play the game

Section 1

Methodology

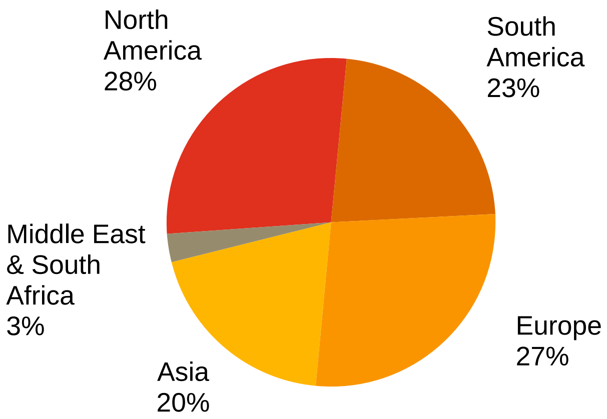
A worldwide study

The Global State of Information Security® Survey 2013, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 1, 2012 to April 15, 2012.

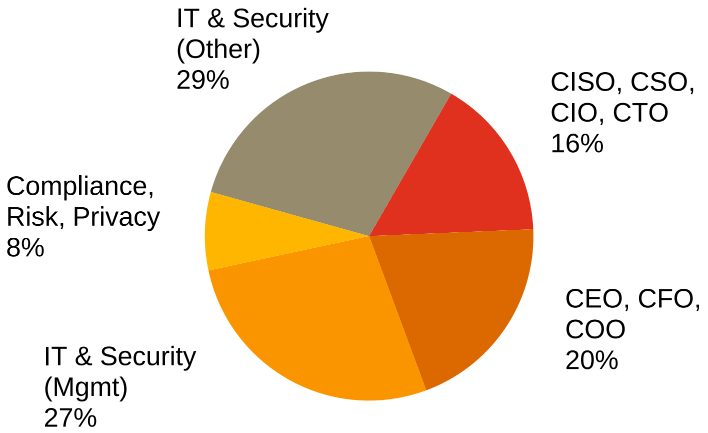
- PwC's 15th year conducting the online survey, 10th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 128 countries
- More than 9,300 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-three percent (33%) of respondents from companies with revenue of $500 million+
- Survey included 1,469 respondents from the technology industry
- Margin of error less than 1%

Demographics

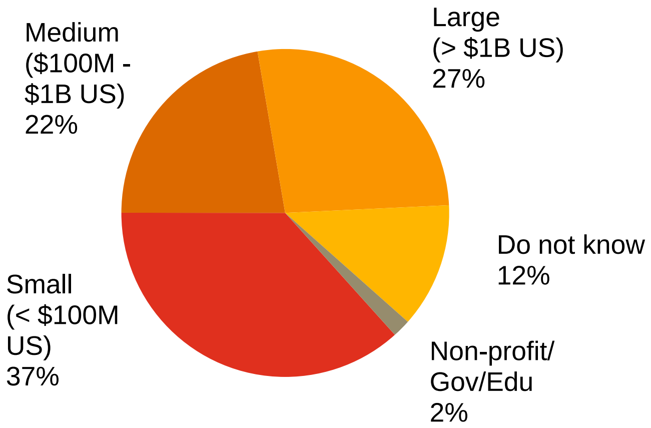
Technology respondents by region of employment



Technology respondents by title



Technology respondents by company revenue size



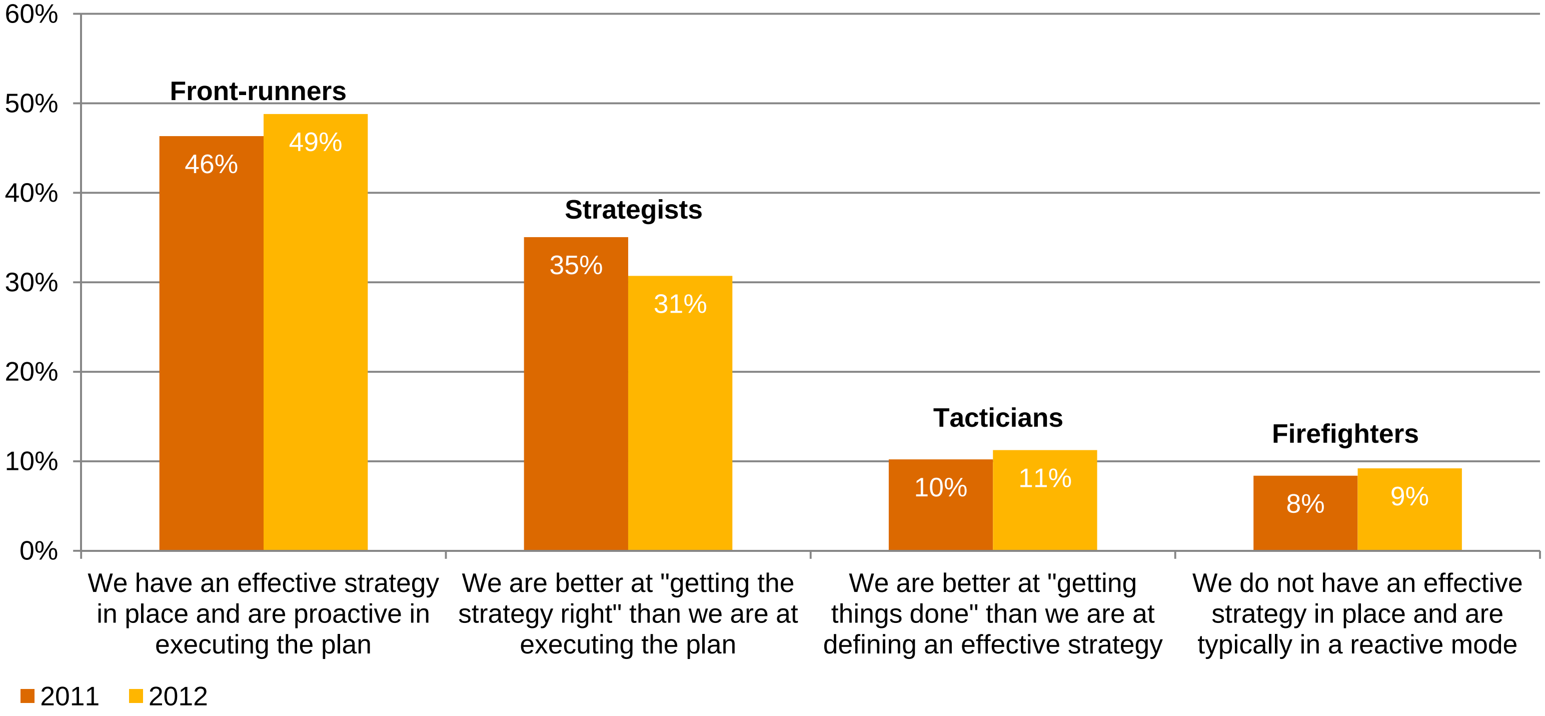
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

A game of confidence

Technology respondents are confident in their security practices.

49% of technology respondents say their organization has a strategy in place and is proactive in executing it – exhibiting two distinctive attributes of a leader.



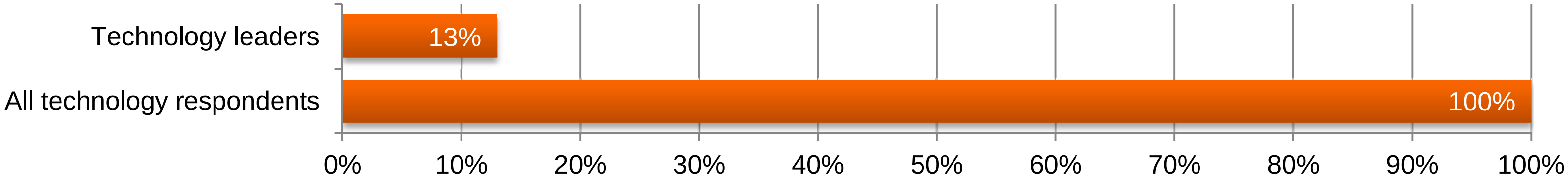
Question 28: "Which category below best characterizes your organization's approach to protecting information security?"

A reality check on real leaders.

But are they really leaders? We measured technology respondents' self-appraisal against four key criteria to define leadership. To qualify, organizations must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the "top of the house" (e.g., to the CEO, CFO, COO, or legal counsel)
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

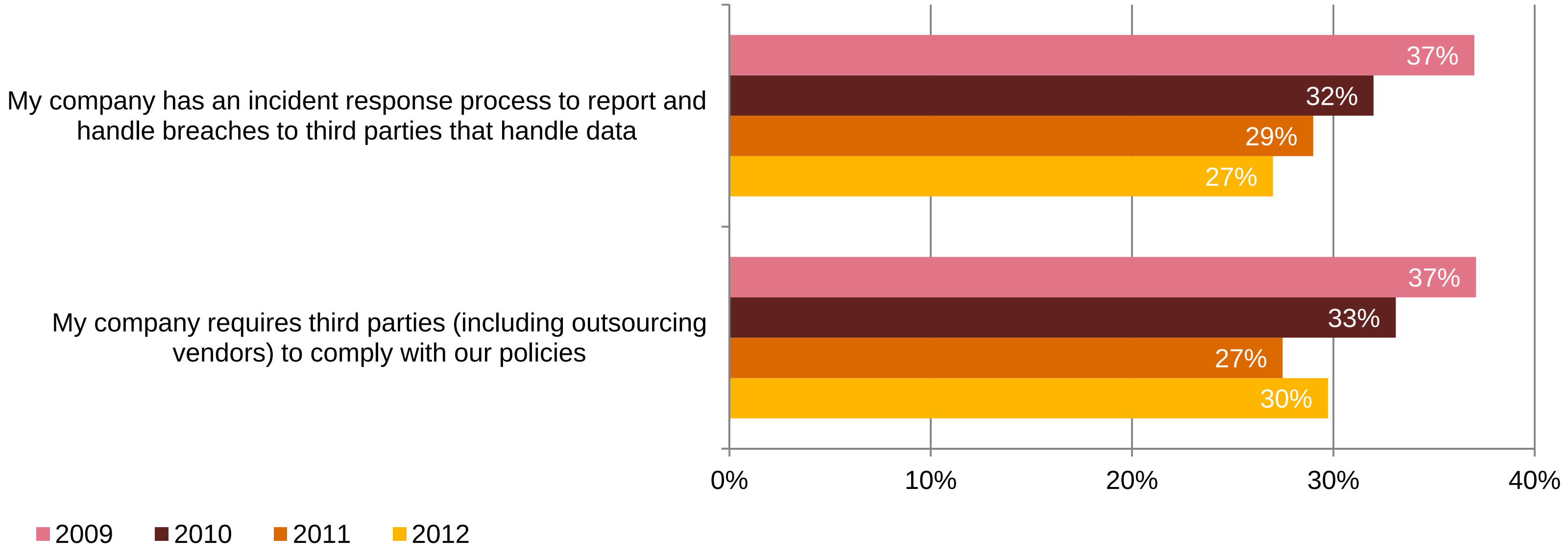
The result? Our analysis found that 13% of technology respondents rank as leaders.



Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 18: "What types of security incidents (breach or downtime) occurred" and Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Many technology respondents are over-confident in their organization’s security program.

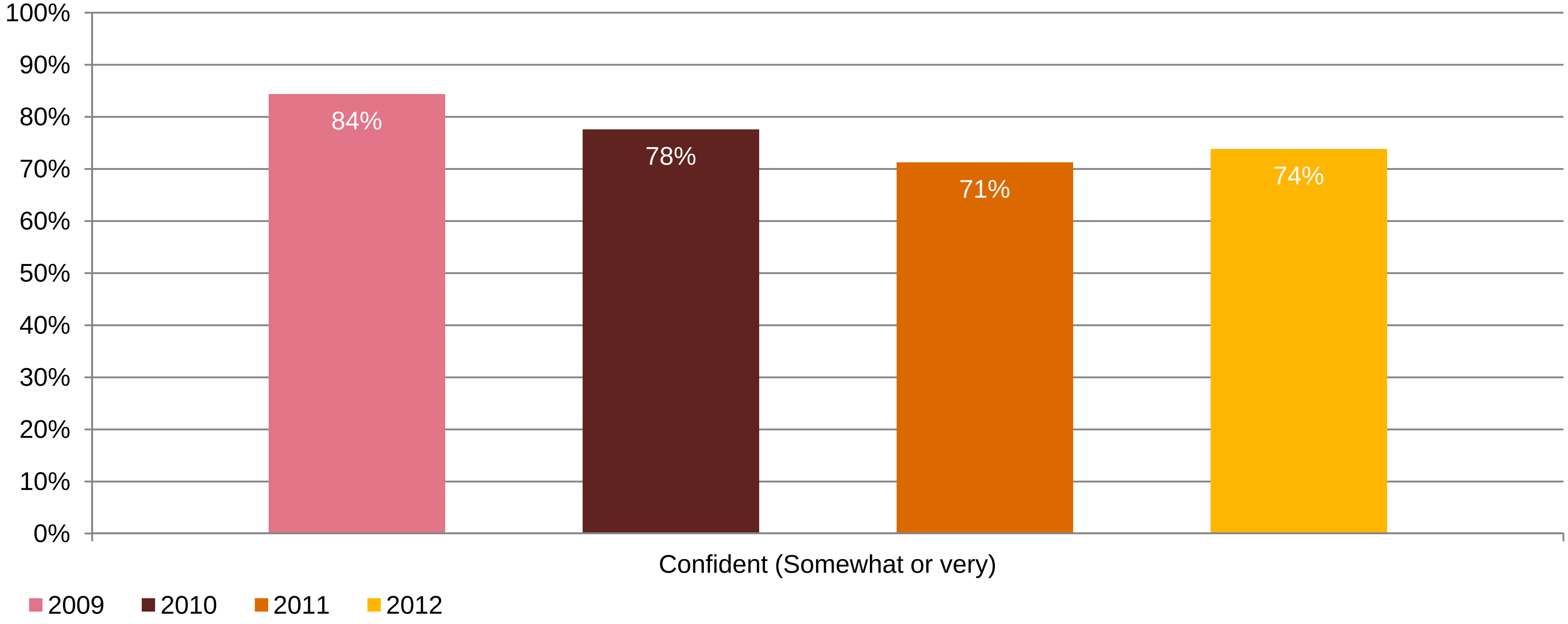
74% of respondents are confident that they have instilled effective security behaviors into their organization’s culture, yet many do not have a process in place to handle third-party breaches. What’s more, only 30% require third parties to comply with privacy policies. This suggests a troubling gap in perception.



Question 35: “How confident are you that your organization has instilled effective information security behaviors into the organizational culture?”
Question 11: “Which data privacy safeguards does your organization have in place?”

Most respondents say their information security activities are effective, but confidence has eroded.

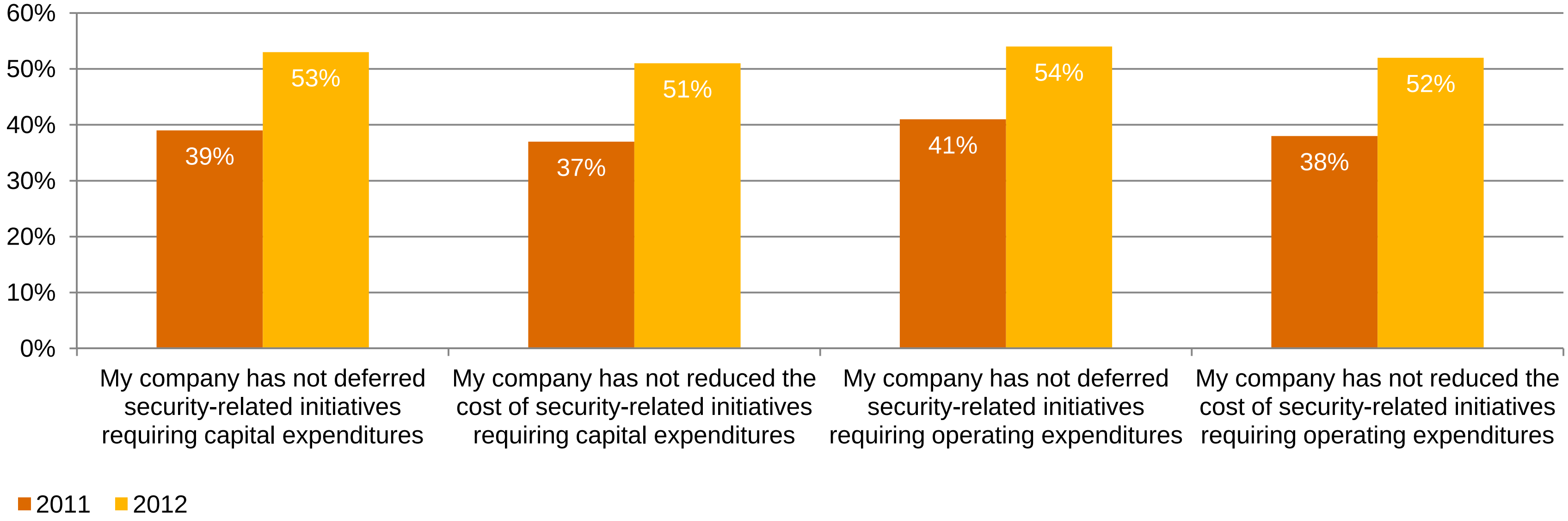
Confidence is a good thing. Although three-quarters of technology respondents are confident that their company's security activities are effective, they probably don't realize that assurance has dropped since 2009.



Question 41: "How confident are you that your organization's information security activities are effective?"

Technology respondents are optimistic about security spending over the next 12 months.

57% of technology respondents expect security budgets to increase in the year ahead. Also encouraging: Respondents report fewer deferrals and fewer budget cutbacks for security initiatives. Compared with last year, for instance, 38% more respondents say they had not cut capital spending for security programs.



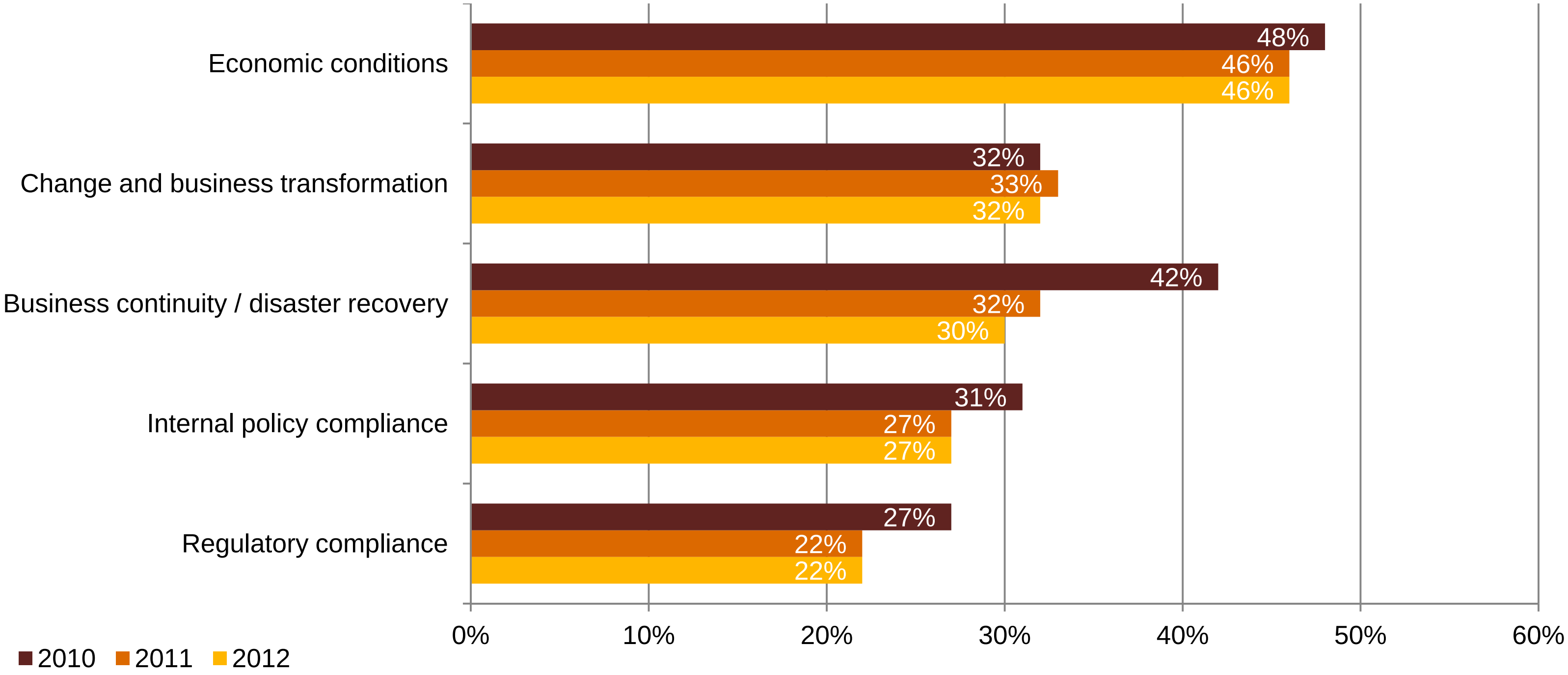
Question 8: “When compared with last year, security spending over the next 12 months will:” Questions 9A and 10A: “Has your company deferred capital and operating security-related initiatives?” Questions 9B and 10B: “Has your company reduced the capital and operating cost of security-related initiatives?”

Section 3

A game of risk

Security budgets are not driven by security needs.

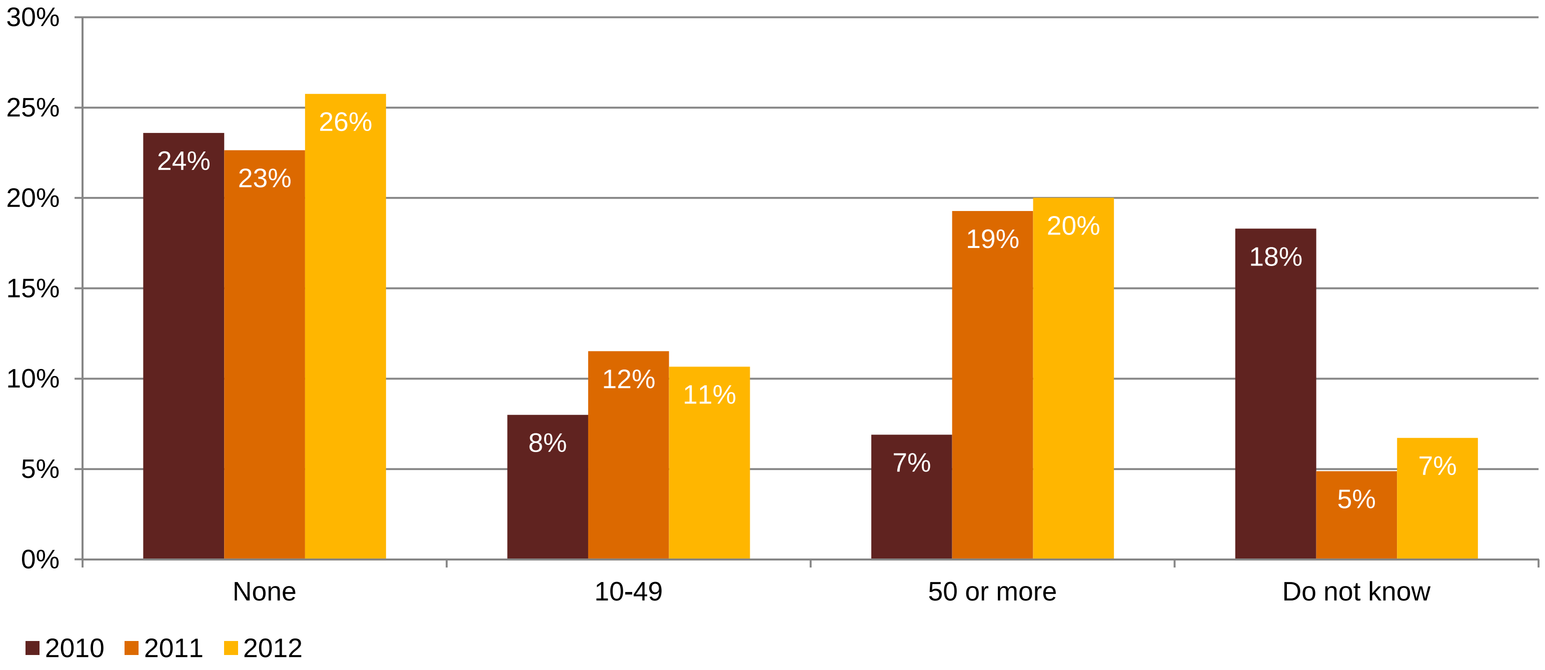
Economic conditions rank as the leading driver of security spending for technology respondents, at 46%, followed by change and business transformation. Business continuity/disaster recovery is the highest-rated security-specific response.



Question 37: “What business issues or factors are driving your company's information security spending?” (Not all factors shown.)

Reported security incidents are leveling off after a sharp uptrend.

20% of technology respondents report 50 or more security incidents in the last 12 months, up a tick over 2011 and a sharp increase over previous years. On the upside, only 7% report that they do not know the number of incidents.



Question 17: "Number of security incidents in the past 12 months."

Less than half of respondents have security training programs for employees.

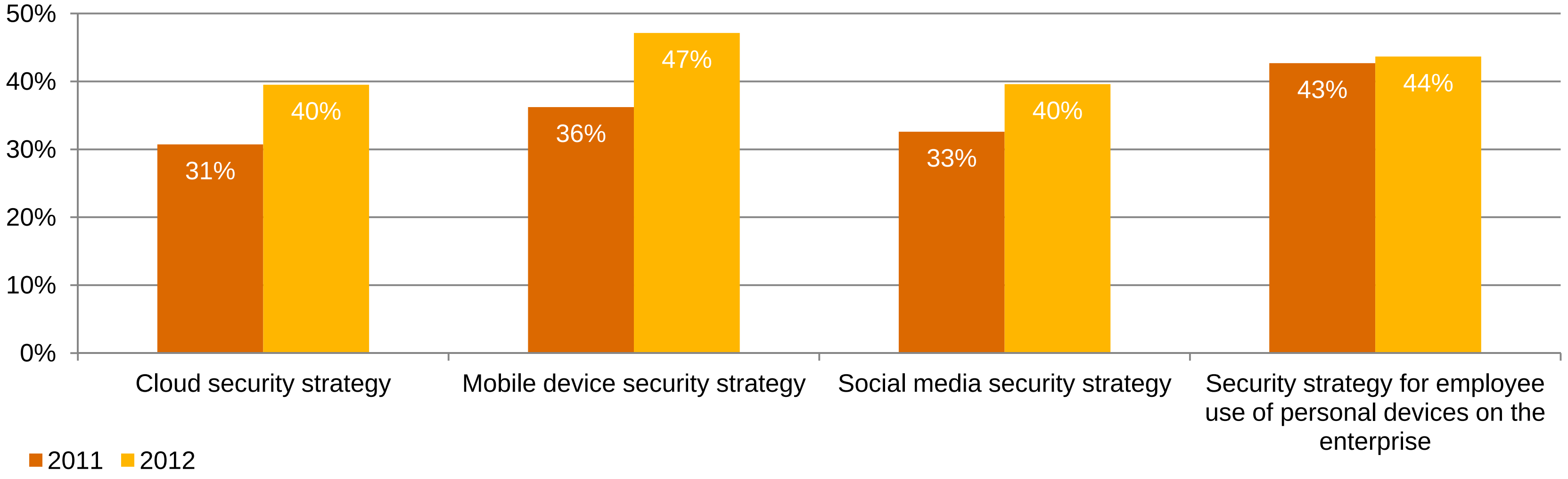
No security program can be effective without adequate training, yet only 47% of technology respondents have an employee security awareness training program in place.

Information security safeguards	2009	2010	2011	2012
Have employee security awareness training program	54%	47%	43%	47%
Have people dedicated to employee awareness programs	58%	57%	49%	49%

Question 14: “What process information security safeguards does your organization currently have in place?” Question 13: “What information security safeguards related to people does your organization have in place?”

Technology adoption is moving faster than security implementation.

As with many industries, technology companies are struggling to keep pace with the adoption of cloud computing, social networking, mobility, and use of personal devices. These new technologies often are not included in overall security plans even though they are widely used. In a recent survey, for instance, we found that 88% of consumers use a personal mobile device for both personal and work purposes.[1]

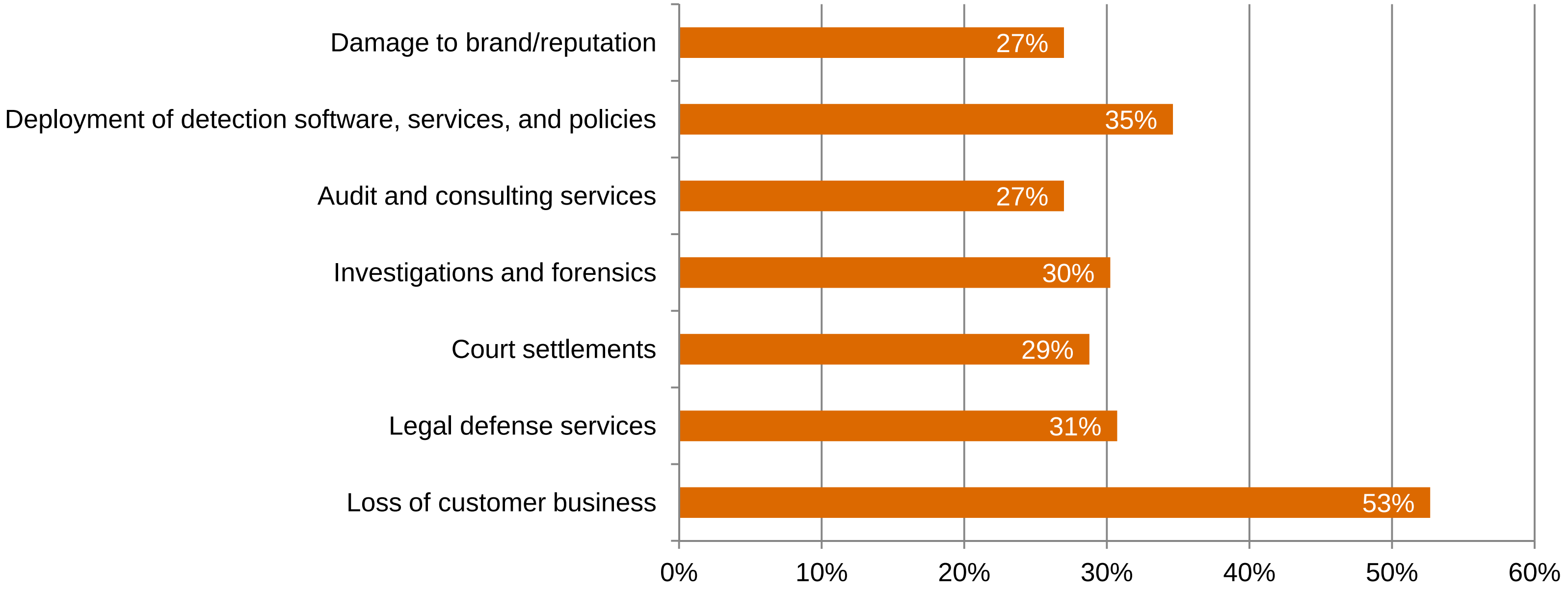


Question 14: “What process information security safeguards does your organization currently have in place?”

[1] PwC, Consumer privacy: What are consumers willing to share? July 2012

An inadequate assessment of security incidents can lead to a less-clear understanding of their impact.

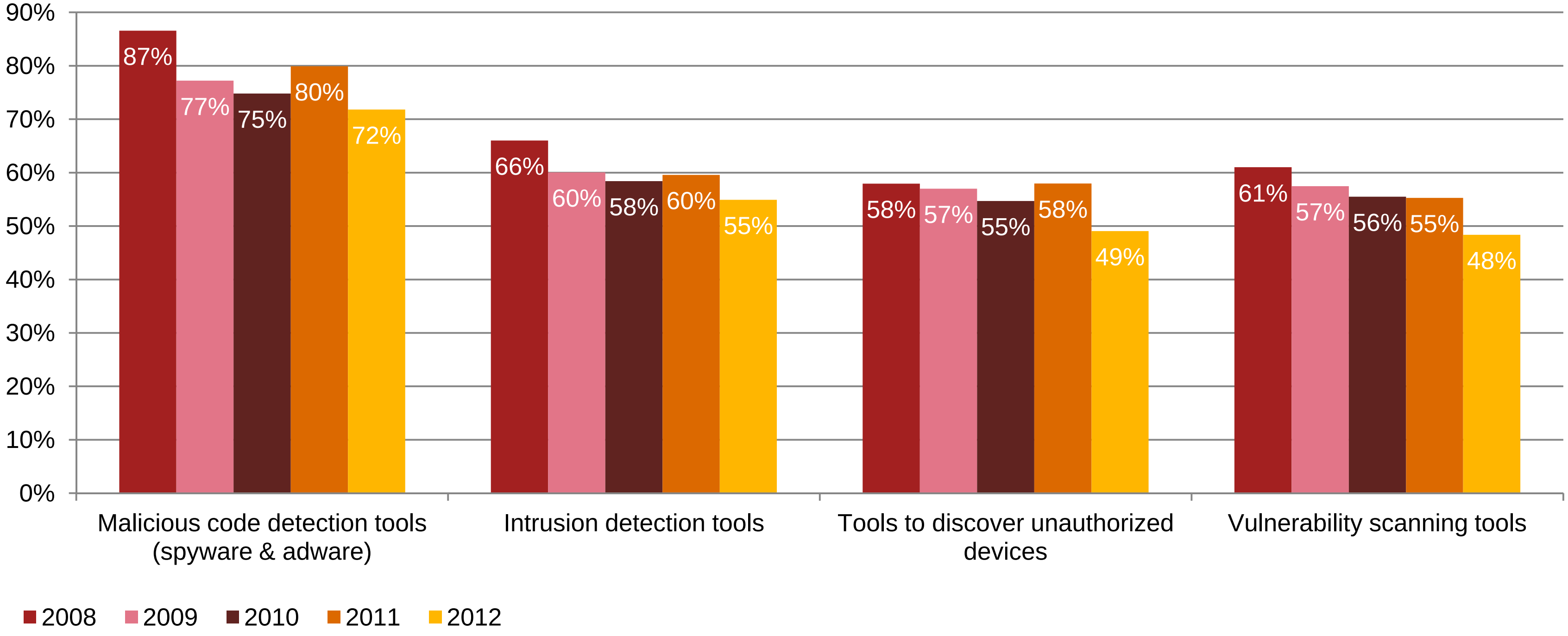
Technology respondents report a lower incidence of monetary losses from security incidents compared with last year, yet their assessments may be inaccurate due to incomplete appraisals. For example, only 27% consider damage to brand/reputation, while 30% factor in investigations and forensics.



Question 21: "How was your organization impacted by the security incident?" Question 21C: "What factors are included in your company's calculation of these financial losses?"

Use of some key technology safeguards resumed a long-term decline after last year's uptick.

The future looked bright last year as many technology firms stepped up investments in detection safeguards. This year, however, saw a decrease in deployment of important security and privacy tools.



Question 15: "What technology information security safeguards related to detection does your organization have in place?"

Section 4

It’s how you play the game

What keeps security from being what it should be?

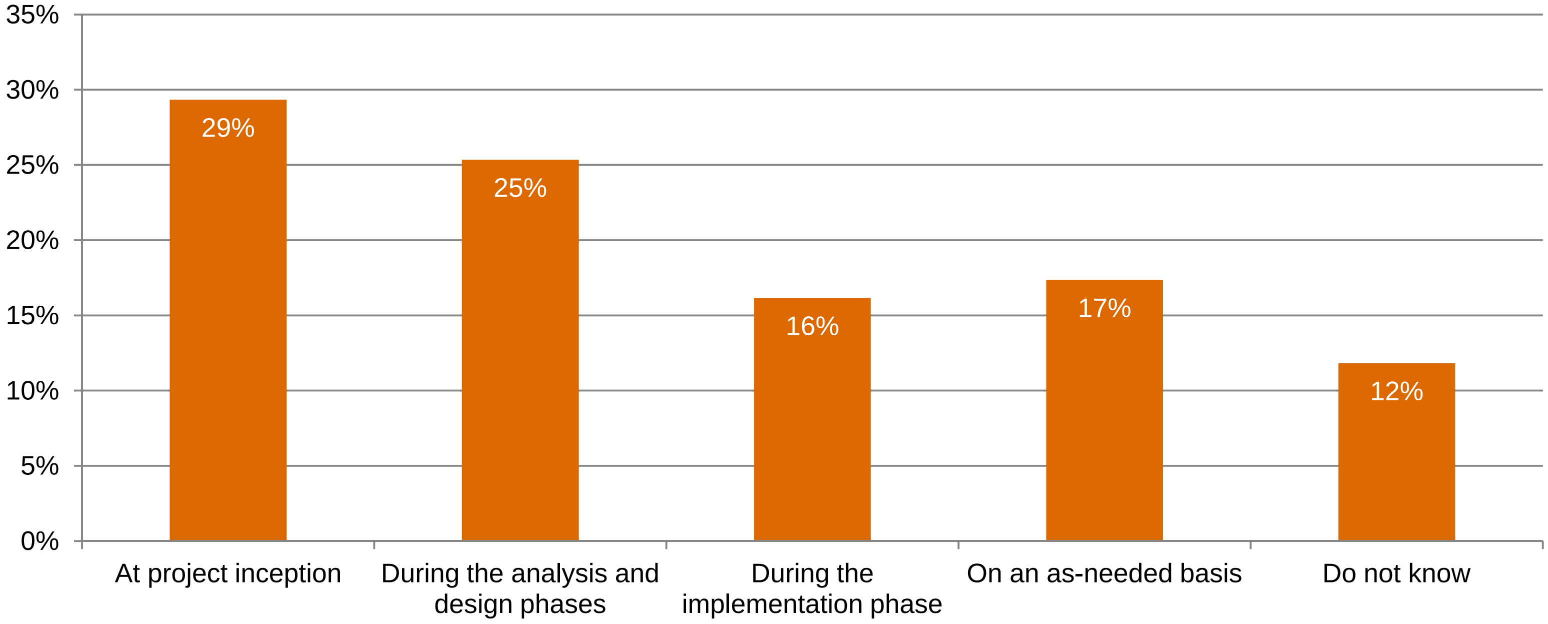
Top-level leadership is perceived to be an obstacle to effective security, with executives and Boards cited by 67% of technology respondents. Other top concerns include insufficient capital expenditures and lack of an actionable vision.

	2011	2012
Leadership – CEO, President, Board, or equivalent	25%	25%
Leadership – CIO or equivalent	24%	21%
Leadership – CISO, CSO, or equivalent	25%	21%
Insufficient capital expenditures	25%	25%
Lack of actionable vision or understanding	29%	24%
Lack of an effective information security strategy	29%	23%

Question 29: “What are the greatest obstacles to improving the overall strategic effectiveness of your organization’s information security function?”

Security is not always baked into major projects from the beginning.

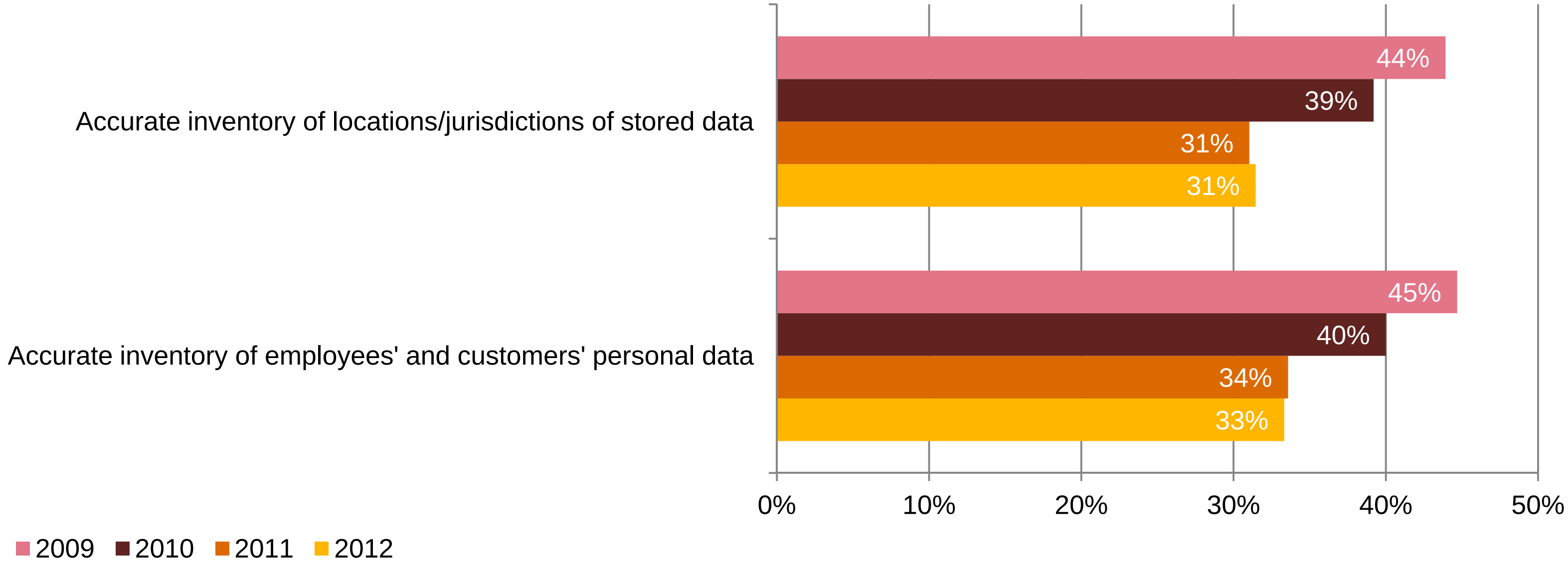
Any project should include security from the very beginning. Yet one-third of technology respondents involve security only during the implementation phase or on an as-needed basis. For many, security seems to be an afterthought.



Question 30: “When does information security become involved in major projects?”

Technology respondents know less about their data now than they did three years ago.

While approximately 90% of respondents say protecting employee and customer data is important, far fewer understand what that data entails and where it is stored. This is significant because, increasingly, consumers want to be in control of their personal data and "turn off" the flow of information from companies.[2]



Question 38: "What level of importance does your company place on protecting the following types of information?" Question 11: "Which data privacy safeguards does your organization have in place?"

[2] PwC, Consumer privacy: What are consumers willing to share? July 2012

What you can do to improve your performance.

Information security today is a rapidly evolving game of advanced skill and strategy. As a result, the security models of the past decade are no longer effective.

Effective security requires a new way of thinking. The very survival of the business demands that security leaders understand, prepare for, and quickly respond to security threats.

Businesses seeking to strengthen their security practice must:

- Implement a comprehensive risk-assessment strategy and align security investments with identified risks.
- Understand their organization's information, who wants it, and what tactics adversaries might use to get it.
- Understand that information security requirements – and, indeed, overall strategies for doing business – have reached a turning point.
- Embrace a new way of thinking in which information security is both a means to protect data as well as an opportunity to create value to the business.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
949.437.5380
gary.loveland@us.pwc.com

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

US 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/giss2013

PwC

www.pwc.com/security

Changing the game

While tight budgets have forestalled updates to security programs, many businesses are confident they're winning the game. But the rules – and the players – have changed.

Telecommunications

Key findings from The Global State of Information Security® Survey 2013

September 2012

"You can't succeed in today's elevated threat environment if you don't know the players and you don't know the rules."

- Gary Loveland, Principal, PwC

Information security has always been a high-stakes game. One that demands a smart strategy, the right technology moves, and an unblinking eye on adversaries.

For many businesses, however, it has become a pursuit that is almost impossible to win. That's because the rules have changed, and opponents—old and new—are armed with expert technology skills. As a result, the risks are greater than ever.

Businesses are fighting back by adopting new detection and prevention technologies. At the same time, governments around the world are enacting legislation to combat cyber threats. And regulatory bodies are issuing new guidance on disclosure obligations for cyber incidents.

Yet risks to data security continue to intensify – and show no signs of abating. Those keeping score agree that the bad guys appear to be in the lead.

Nonetheless, many businesses believe they are winning. The Global State of Information Security® Survey 2013 shows that most executives in the global telecommunications industry are confident in the effectiveness of their information security practices. They believe their strategies are sound and many consider themselves to be leaders in the field.

The odds, however, are not in their favor: Diminished budgets have resulted in degraded security programs, reported security incidents are on the rise, and new technologies are being adopted faster than they can be safeguarded.

Given today's elevated threat environment, businesses can no longer afford to play a game of chance. They must prepare to play a new game, one that requires advanced levels of skill and strategy to win.

Agenda

Section 1. Methodology

Section 2. A game of confidence

Section 3. A game of risk

Section 4. It’s how you play the game

Section 1

Methodology

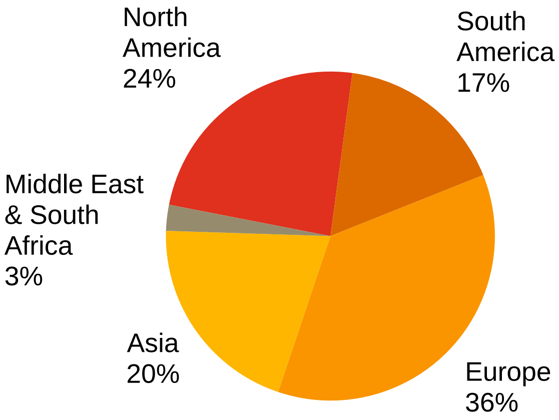
A worldwide study

The Global State of Information Security® Survey 2013, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 1, 2012 to April 15, 2012.

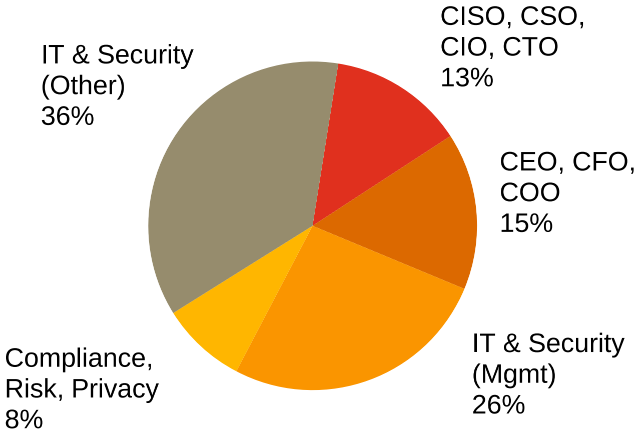
- PwC’s 15th year conducting the online survey, 10th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 128 countries
- More than 9,300 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-three percent (33%) of respondents from companies with revenue of $500 million+
- Survey included 511 respondents from the telecommunications industry
- Margin of error less than 1%

Demographics

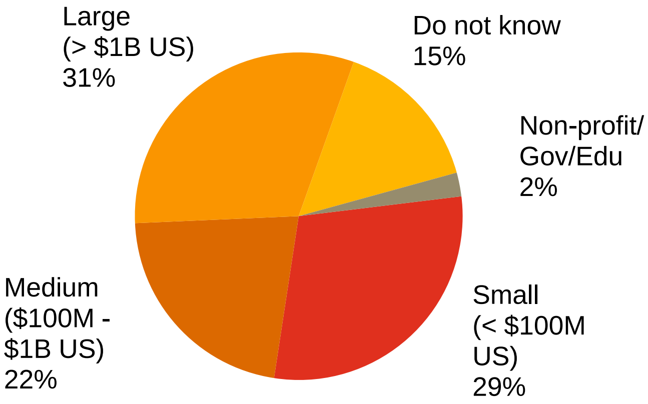
Telecom respondents by region of employment



Telecom respondents by title



Telecom respondents by company revenue size



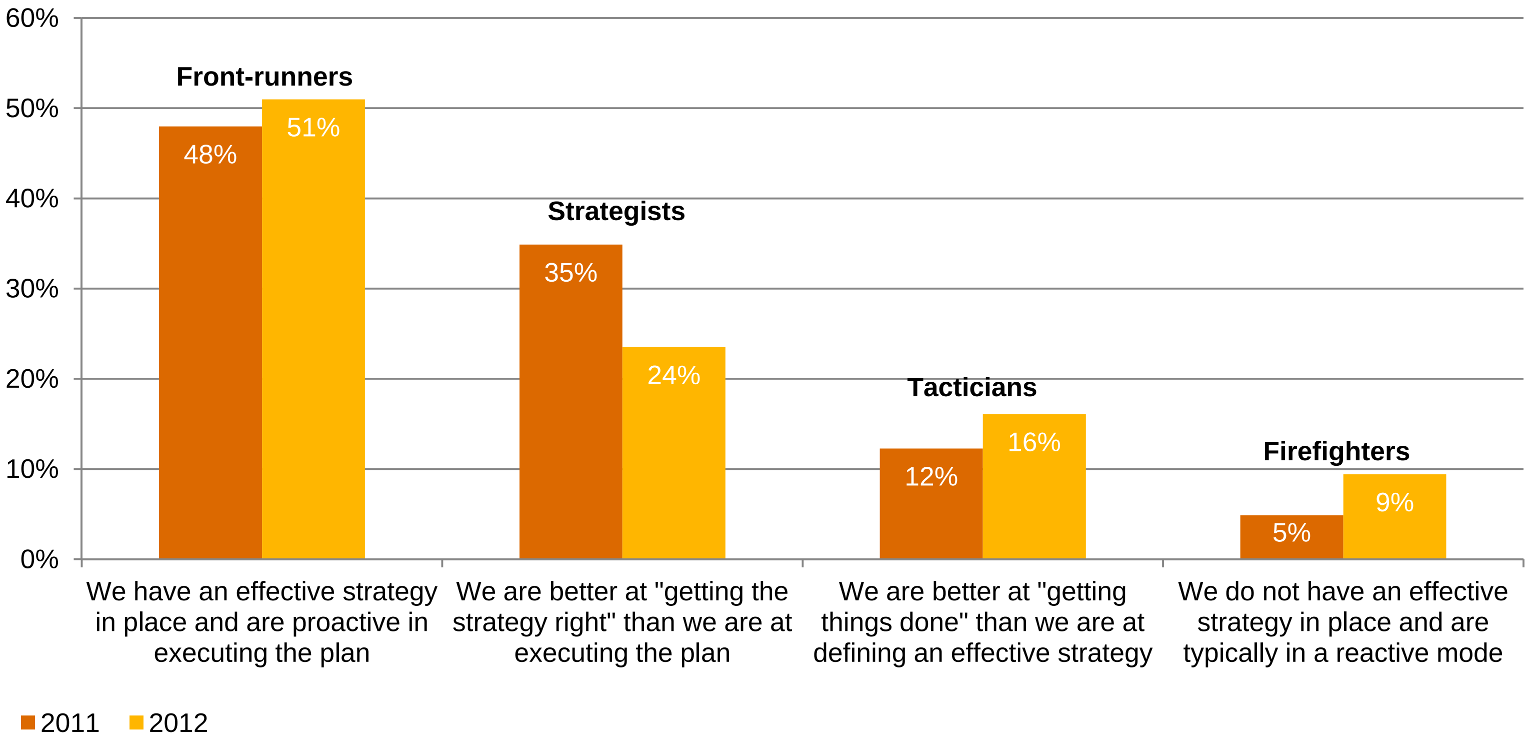
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

A game of confidence

Telecom respondents are confident in their security practices.

51% of telecom respondents say their organization has a strategy in place and is proactive in executing it – exhibiting two distinctive attributes of a leader.



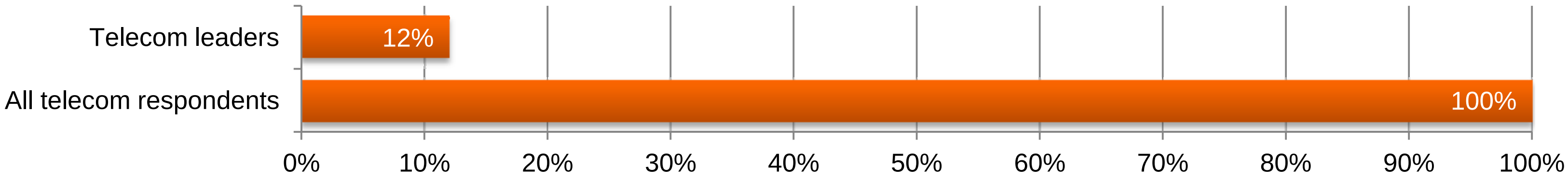
Question 28: "Which category below best characterizes your organization's approach to protecting information security?"

A reality check on real leaders.

But are they really leaders? We measured telecom respondents' self-appraisal against four key criteria to define leadership. To qualify, organizations must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the "top of the house" (e.g., to the CEO, CFO, COO, or legal counsel)
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

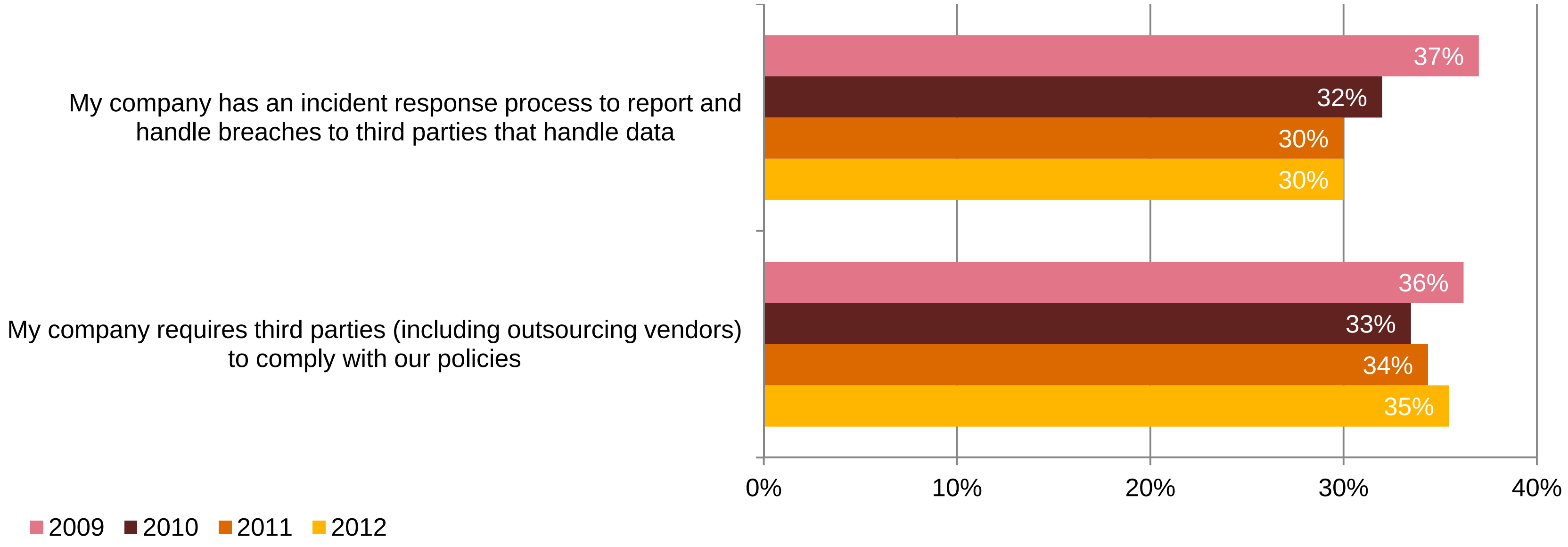
The result? Our analysis found that 12% of telecom respondents rank as leaders.



Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 18: "What types of security incidents (breach or downtime) occurred" and Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Many telecom respondents are over-confident in their organization's security program.

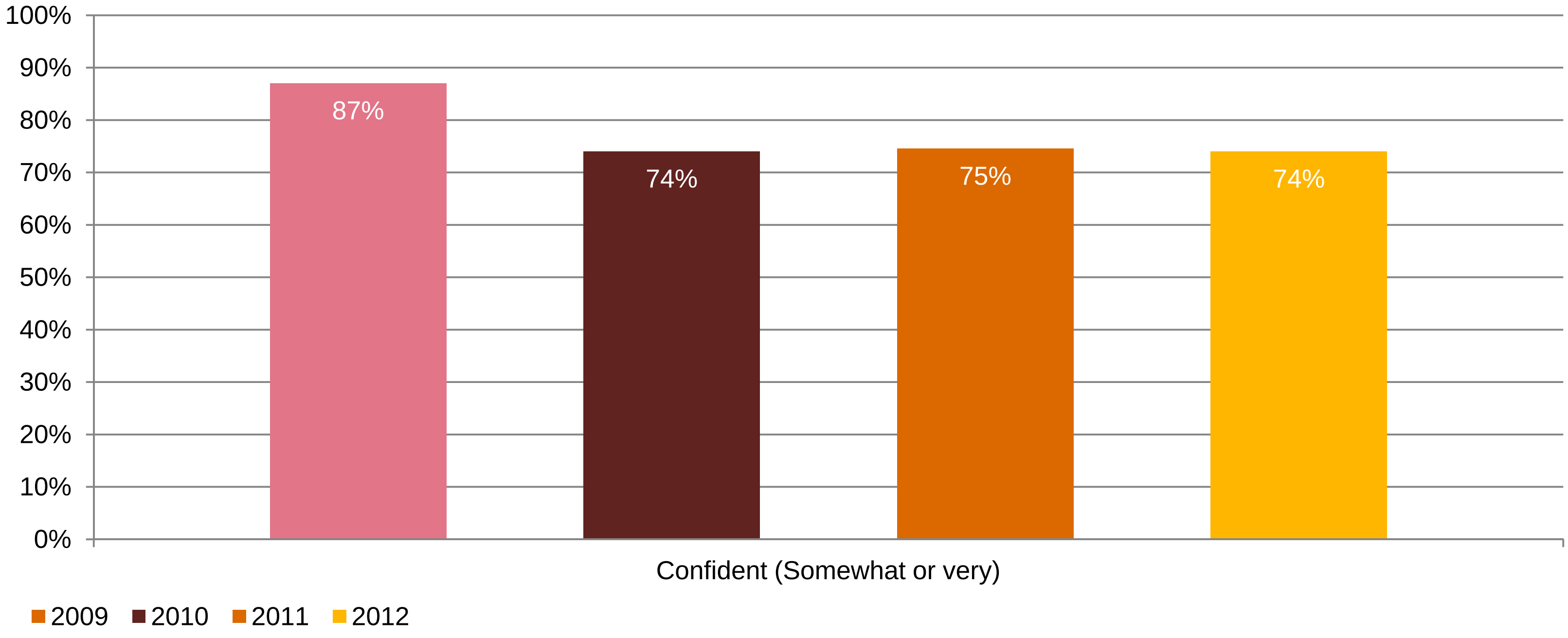
70% of respondents are confident that they have instilled effective security behaviors into their organization's culture, yet most do not have a process in place to handle third-party breaches. What's more, only 35% require third parties to comply with privacy policies. This suggests a troubling gap in perception.



Question 35: "How confident are you that your organization has instilled effective information security behaviors into the organizational culture?"
Question 11: "Which data privacy safeguards does your organization have in place?"

Most respondents say their information security activities are effective, but confidence is eroding.

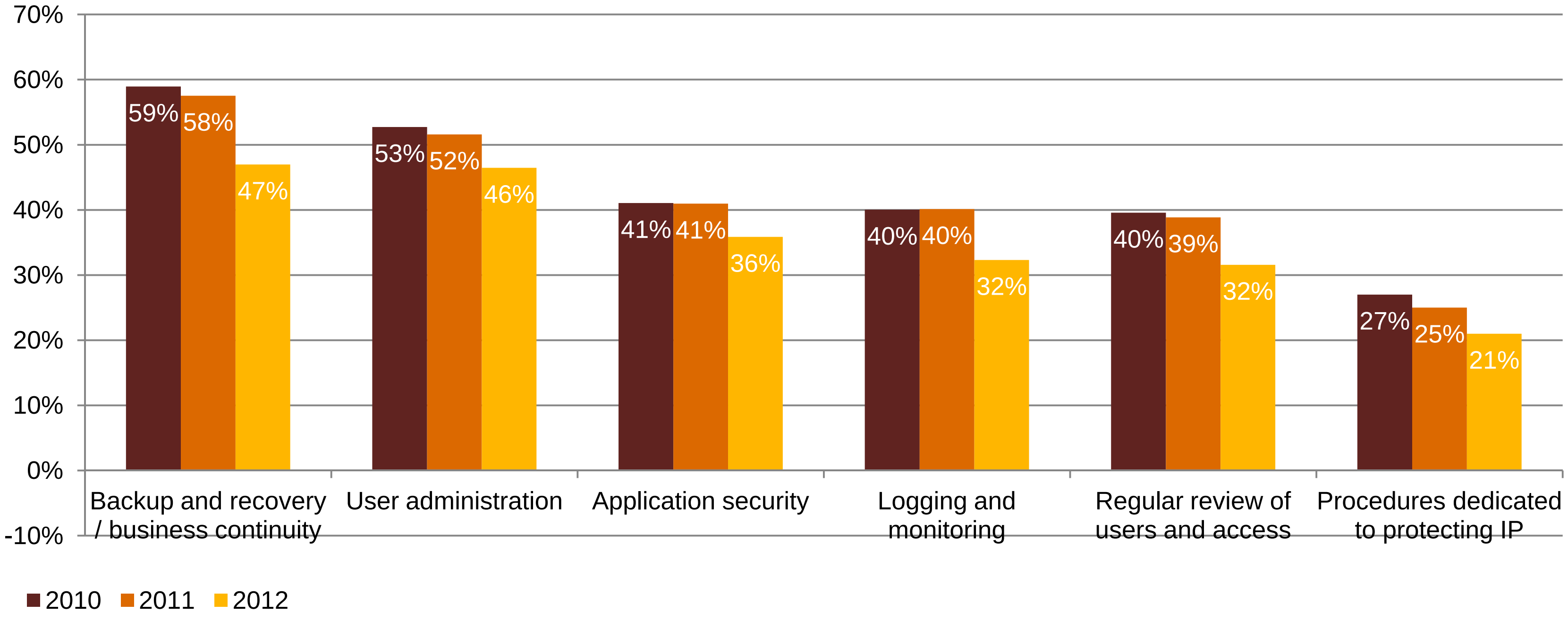
Confidence is a good thing. A strong 74% of telecom respondents say they are confident that their company's security activities are effective, but many may not realize that assurance has dropped since 2009.



Question 41: “How confident are you that your organization's information security activities are effective?”

Security policies have weakened over time.

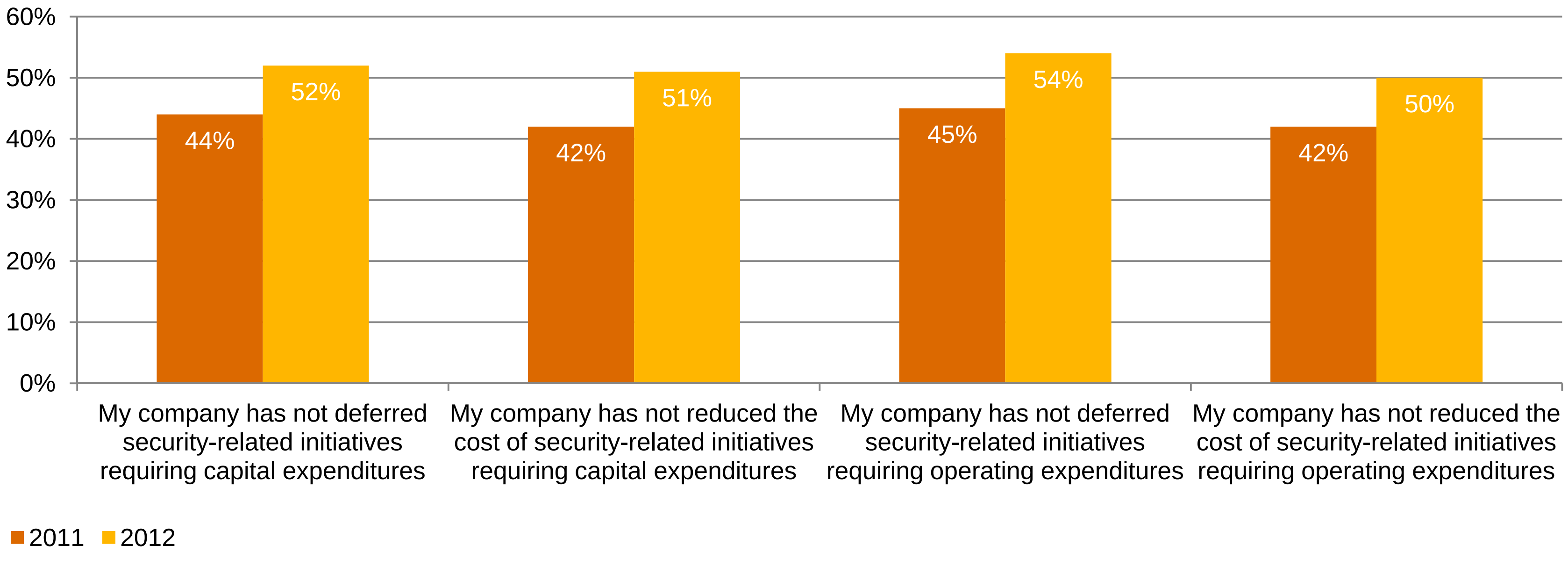
Some key elements of security policies show substantial degradation from earlier highs.



Question 32: "Which of the following elements, if any, are included in your organization’s security policy?"

Telecom respondents are optimistic about security spending over the next 12 months.

51% of telecom respondents expect security budgets to increase in the year ahead. More encouragingly, respondents report fewer deferrals and fewer budget cutbacks for security initiatives. Compared with last year, for instance, 21% more respondents say they had not cut capital expenditures for security programs.



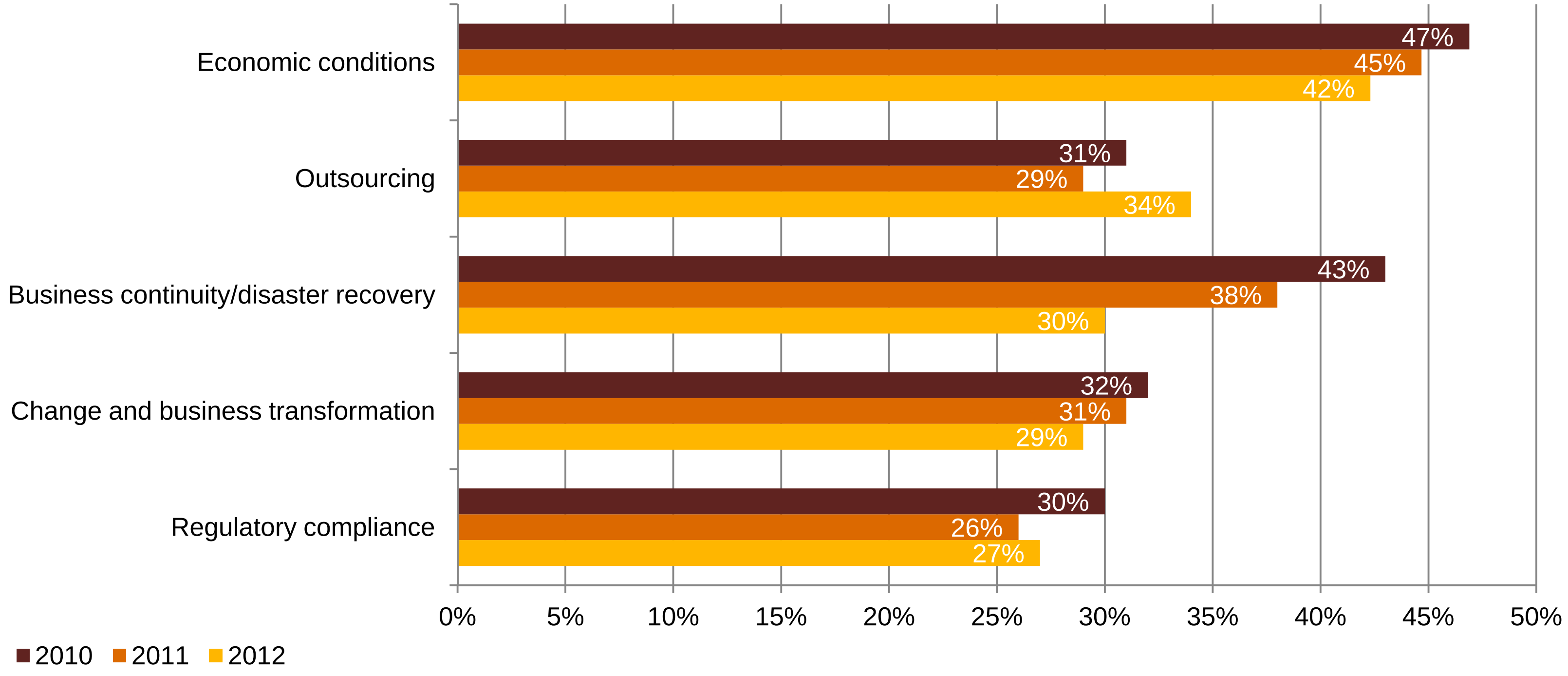
Question 8: “When compared with last year, security spending over the next 12 months will:” Questions 9A and 10A: “Has your company deferred capital and operating security-related initiatives?” Questions 9B and 10B: “Has your company reduced the capital and operating costs of security-related initiatives?”

Section 3

A game of risk

Security budgets are not driven by security needs.

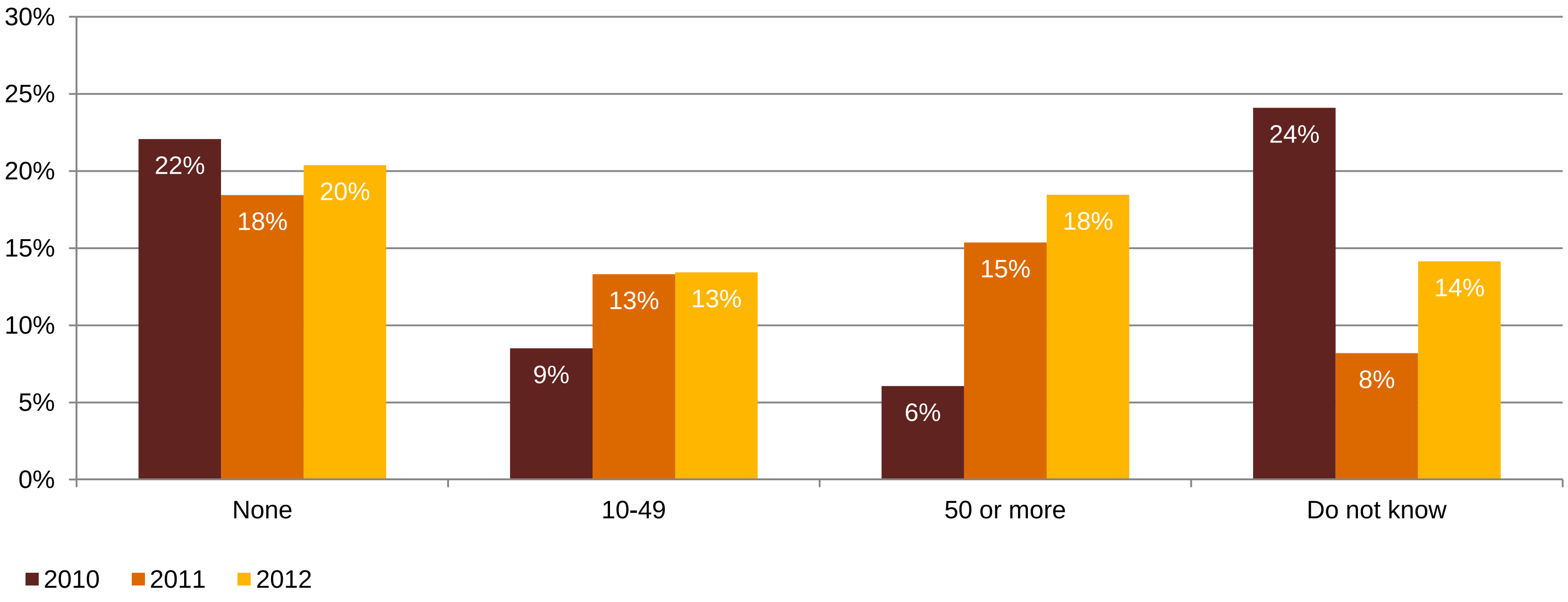
Economic conditions rank as the most-cited driver of security spending for telecom respondents, continuing a multi-year trend. At 42%, it's a risky way to set priorities. Business continuity/disaster recovery is the largest security-specific response.



Question 37: "What business issues or factors are driving your company's information security spending?" (Not all factors shown.)

Reported security incidents are on the rise.

The number of respondents reporting the most numerous category of security incidents – 50 or more per year – jumped 20% over 2011 and 200% over 2010. Also up: The number of respondents who do not know the number of incidents, an uncertainty that suggests ineffective security practices.



Question 17: “Number of security incidents in the past 12 months.”

Only half of respondents have security training programs for employees.

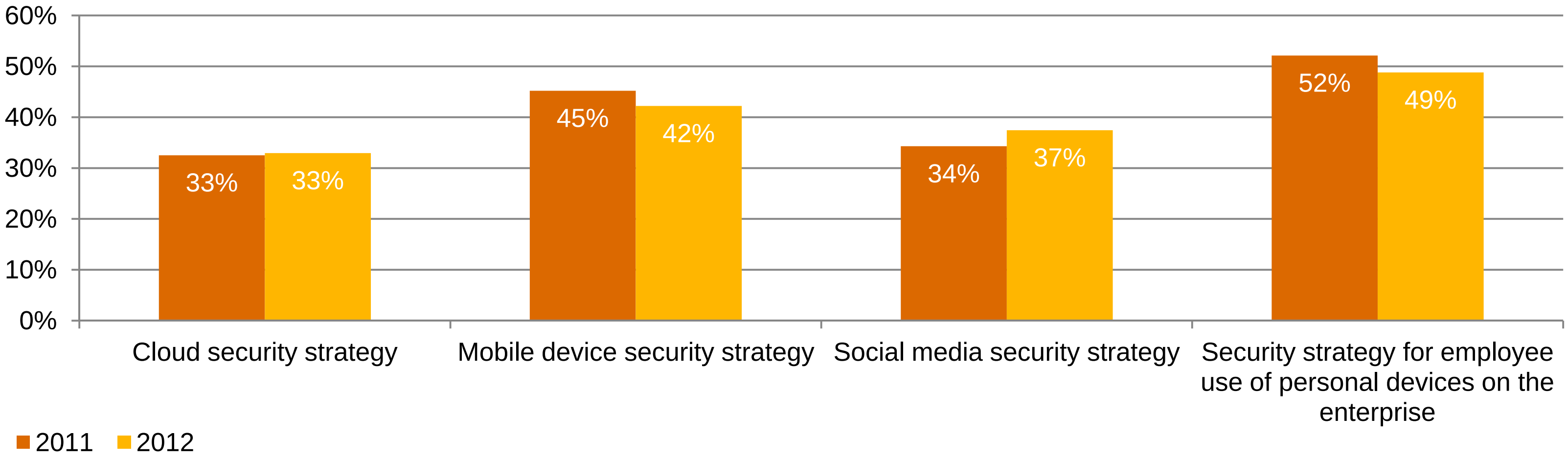
No security program can be effective without adequate training, yet only 50% of telecom respondents have an employee security awareness training program. Staff dedicated to security awareness and training are in place at 55% of companies.

Information security safeguards	2009	2010	2011	2012
Have employee security awareness training program	52%	48%	48%	50%
Have people dedicated to employee awareness programs	61%	58%	58%	55%

Question 14: “What process information security safeguards does your organization currently have in place?” Question 13: “What information security safeguards related to people does your organization have in place?”

Technology adoption is moving faster than security implementation.

As with many industries, telecom companies are struggling to keep pace with the adoption of cloud computing, social networking, user mobility, and employee-owned devices in the workplace. But the numbers still lag adoption of the technologies themselves. A recent PwC survey found, for instance, that 88% of consumers use a personal mobile device for both personal and work purposes.[1]

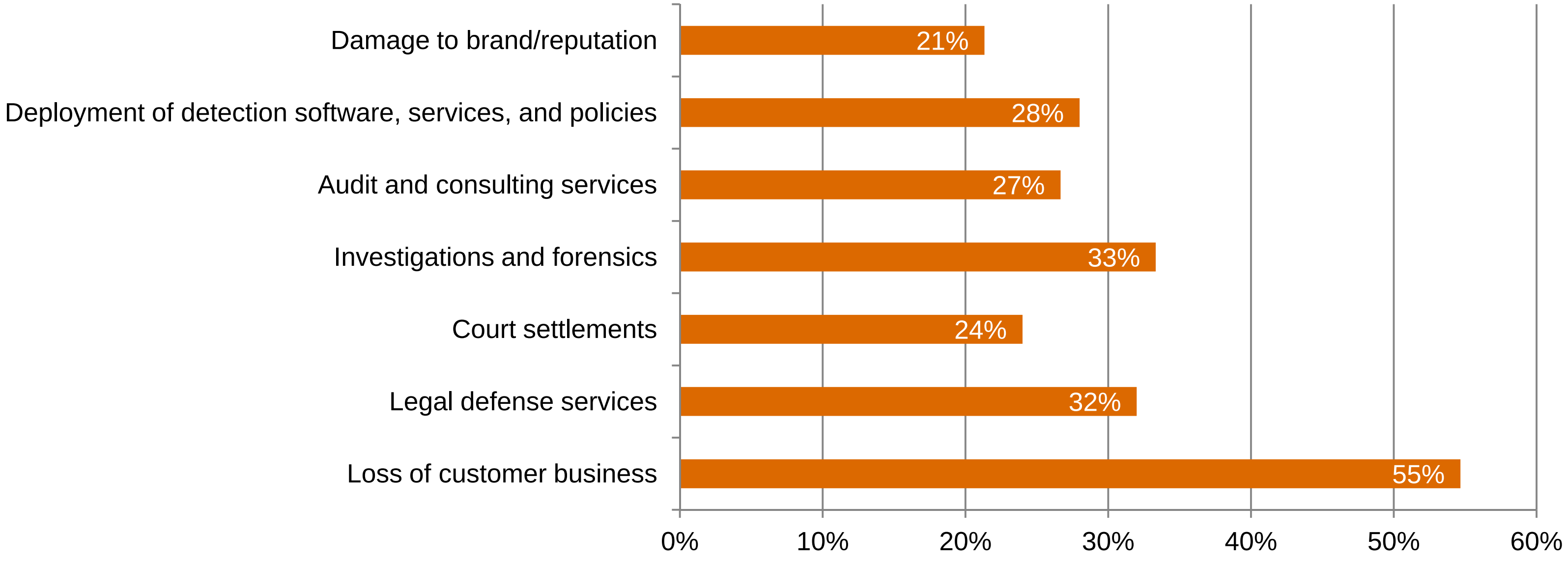


Question 14: "What process information security safeguards does your organization currently have in place?"

[1] PwC, Consumer privacy: What are consumers willing to share? July 2012

An inadequate assessment of security incidents can lead to a less-clear understanding of their impact.

Telecom respondents report a lower incidence of financial losses from security incidents than last year, yet many do not apply thorough or consistent analysis to appraise those losses. Consider customer business: Our consumer survey found that 61% of respondents would stop using a company's products or services after a breach.[2]

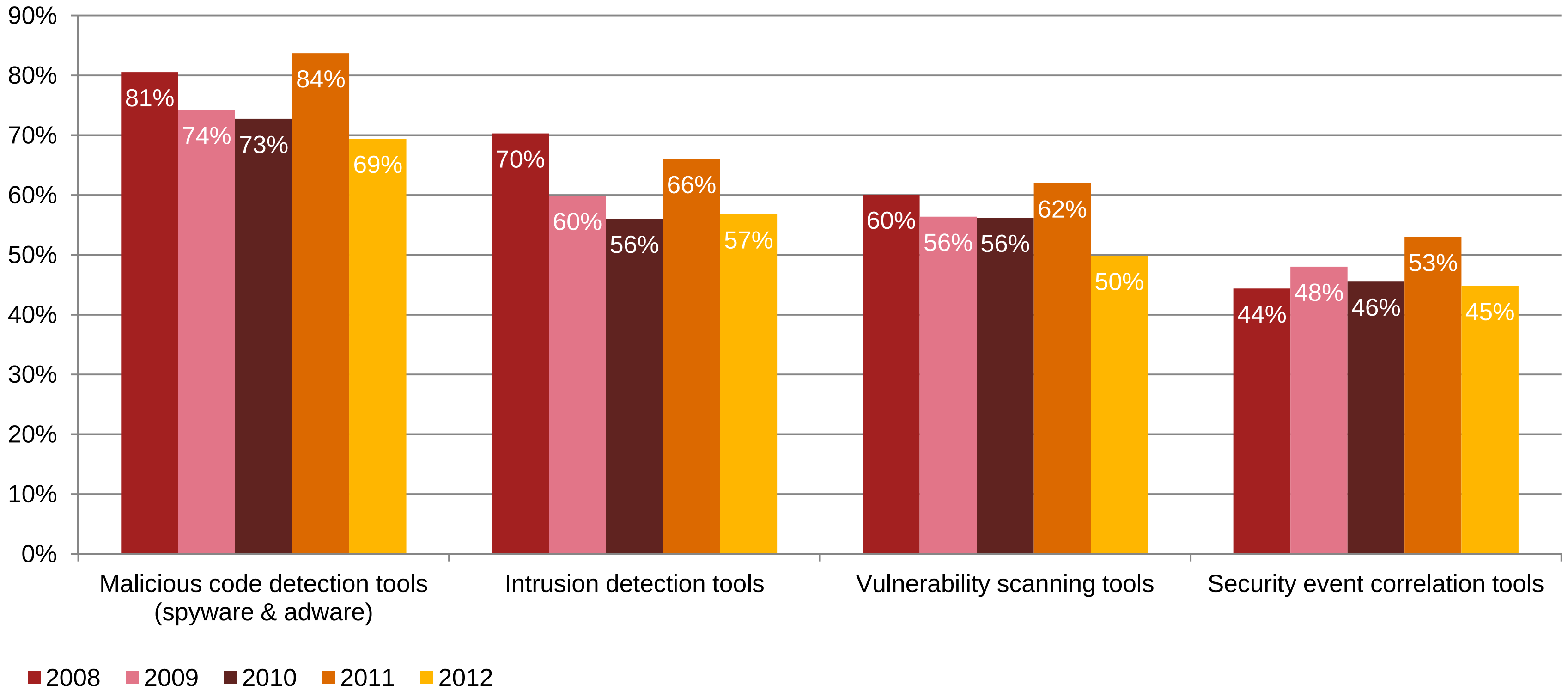


Question 21: "How was your organization impacted by the security incident?" Question 21C: "What factors are included in your company's calculation of these financial losses?"

[2] PwC, Consumer privacy: What are consumers willing to share? July 2012

Use of some key technology safeguards resumed a long-term decline after last year's uptick.

Deployment of important security and privacy tools for incident detection has atrophied over time.



Question 15: "What technology information security safeguards related to detection does your organization have in place?"

Section 4

It’s how you play the game

What keeps security from being what it should be?

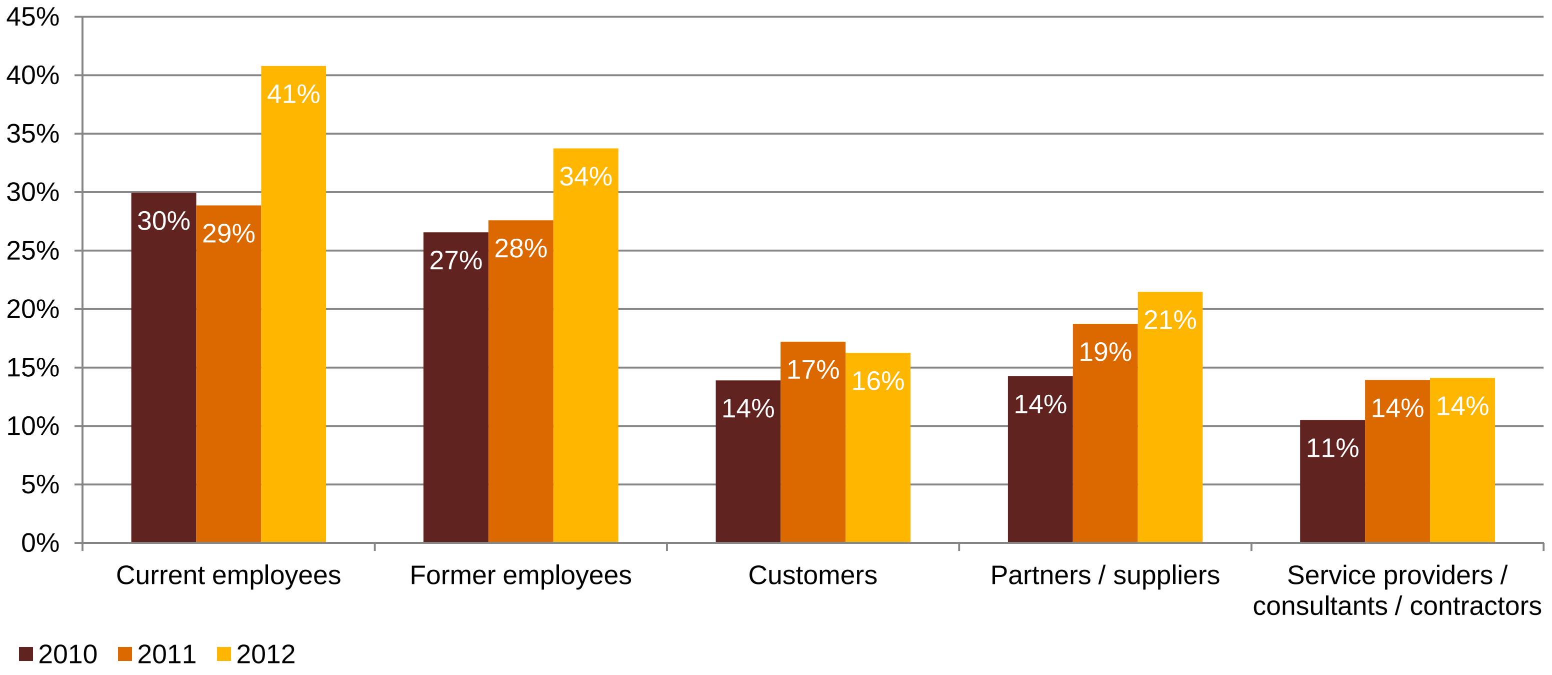
Company leadership is seen as less an obstacle than in the past, although 55% of respondents still point to C-level executives and Boards. Insufficient funding (both capital and operational) continues to be a top concern.

	2011	2012
Leadership – CEO, President, Board, or equivalent	25%	21%
Leadership – CIO or equivalent	21%	18%
Leadership – CISO, CSO, or equivalent	24%	16%
Insufficient capital expenditures	28%	27%
Lack of an actionable vision or understanding	30%	24%
Lack of an effective information security strategy	27%	23%
Insufficient operating expenditures	21%	22%

Question 29: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?"

Threats from insiders – current and former employees – have increased.

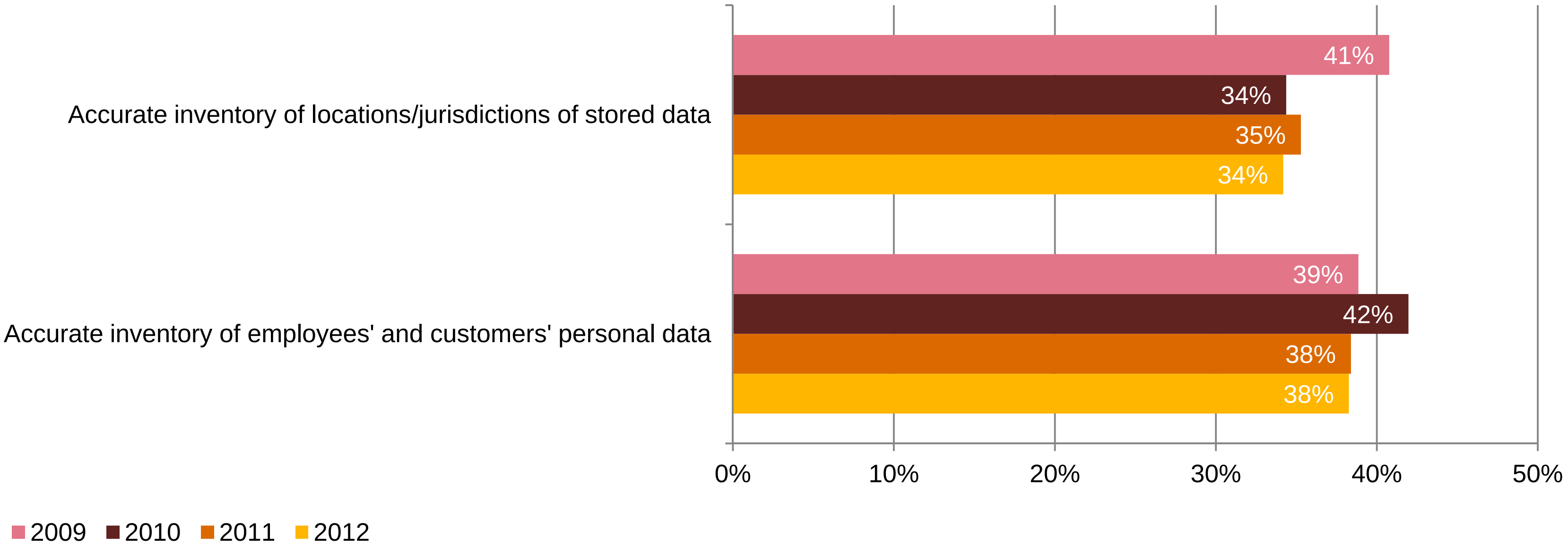
Security incidents attributed to current employees are at the highest level in years, as are those attributed to former workers. On the other hand, 23% of this year's respondents point the finger at competitors.



Question 20: "Estimated likely source of incidents."

Telecom respondents know less about their data now than they did three years ago.

While more than 80% of respondents say protecting customer and employee data is important, far fewer understand what that data entails and where it is stored. This is significant because, increasingly, consumers want to be in control of their personal data and "turn off" the flow of information from companies.[3]



Question 38: "What level of importance does your company place on protecting the following types of information?" Question 11: "Which data privacy safeguards does your organization have in place?"

[3] PwC, Consumer privacy: What are consumers willing to share? July 2012

What you can do to improve your performance.

Information security today is a rapidly evolving game of advanced skill and strategy. As a result, the security models of the past decade are no longer effective.

Effective security requires a new way of thinking. The very survival of the business demands that security leaders understand, prepare for, and quickly respond to security threats.

Businesses seeking to strengthen their security practice must:

- Implement a comprehensive risk-assessment strategy and align security investments with identified risks.
- Understand their organization's information, who wants it, and what tactics adversaries might use to get it.
- Understand that information security requirements – and, indeed, overall strategies for doing business – have reached a turning point.
- Embrace a new way of thinking in which information security is both a means to protect data as well as an opportunity to create value to the business.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
949.437.5380
gary.loveland@us.pwc.com

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

US Telecommunications Contacts

Deborah Bothun
Principal
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/giss2013

PwC