

Key findings from the 2010 Global State of Information Security Survey®  
Automotive

# Trial by fire\*

## Protected. But under pressure to perform

What global executives expect of information security – In the middle of the world's worst economic downturn in thirty years

October 2009

\*connectedthinking



Business  
Technology  
Leadership



BUSINESS RISK LEADERSHIP

PRICEWATERHOUSECOOPERS 

This year, everything is different.

As in almost every industry, automotive executives are cutting costs. Laying off personnel. And reassessing spending priorities.

Across the enterprise. Across all functions. Including, of course, information security and privacy protection.

Or so we thought it safe to assume. That is, before the results of the 2010 Global Information Security Survey emerged.

What the survey reveals is surprising.

Security budgets appear to be less vulnerable to cost-cutting – as if executives were protecting them. Yet responses also reveal that security is under enormous pressure to “perform”.

This year, moving from 2009 to 2010, may turn out to be a high-stakes “coming of age”. A litmus test for a multi-year investment. In the function itself. And in a new generation of security leaders.

A trial by fire.

# Agenda

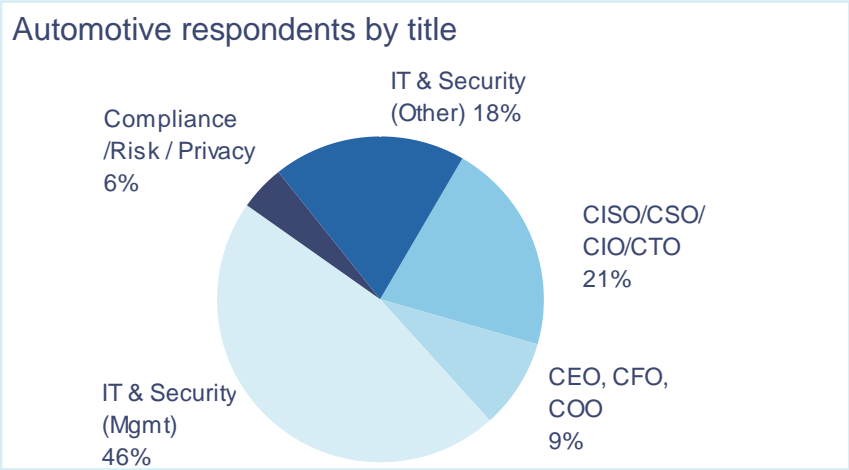
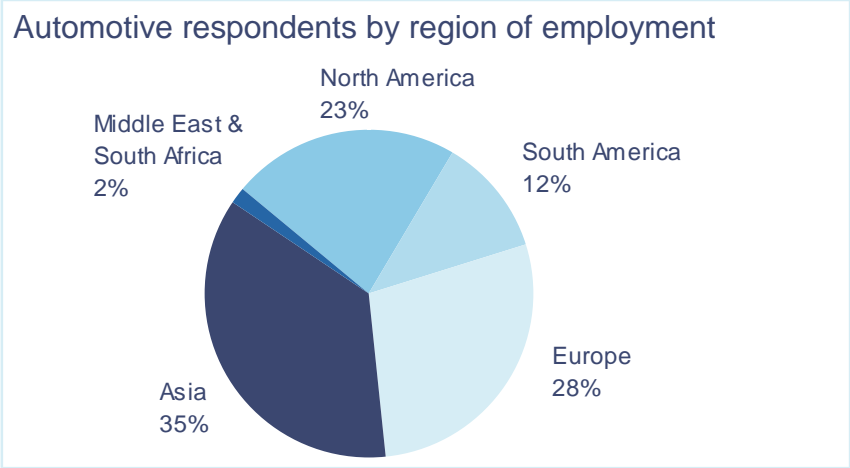
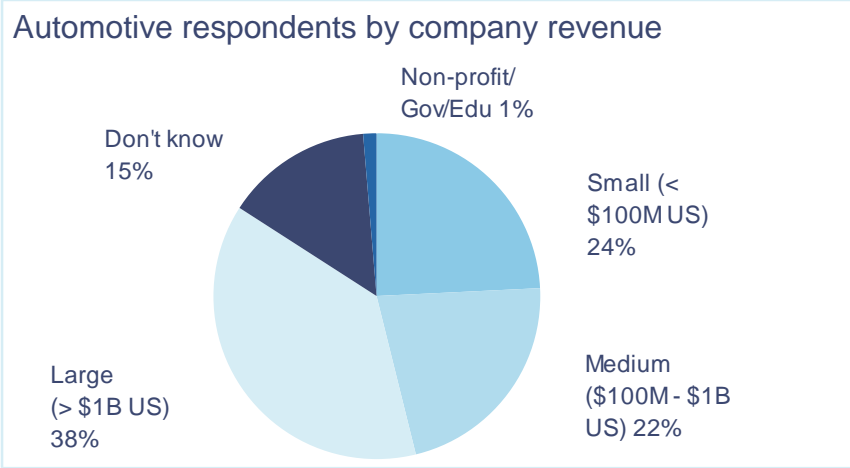
1. Methodology
2. Spending: A decline in growth rate – but a manifestly reluctant one
3. Mounting pressure: Impacts of the economic downturn
4. Breaches: More footsteps and fingerprints – as visibility increases
5. Current state of the arsenal: New gains will be key this year
6. A crucial year: Security at an important threshold
7. What this means for your business

## A worldwide study

The Global State of Information Security 2010, a worldwide study by PricewaterhouseCoopers, CIO Magazine and CSO Magazine, was conducted online from April 22 through June 15, 2009.

- PwC's 11<sup>th</sup> year conducting the online survey, 7<sup>th</sup> with CIO and CSO Magazines
- Readers of CIO and CSO Magazines and clients of PwC from 130 countries
- More than 7,200 responses from CEOs, CFOs, CIOs, CSOs, VPs and directors of IT and security
- Over 40 questions on topics related to privacy and information security safeguards
- Thirty-two percent (32%) from companies with revenue of \$500 million+
- Respondents from the automotive industry total 185

# Demographics



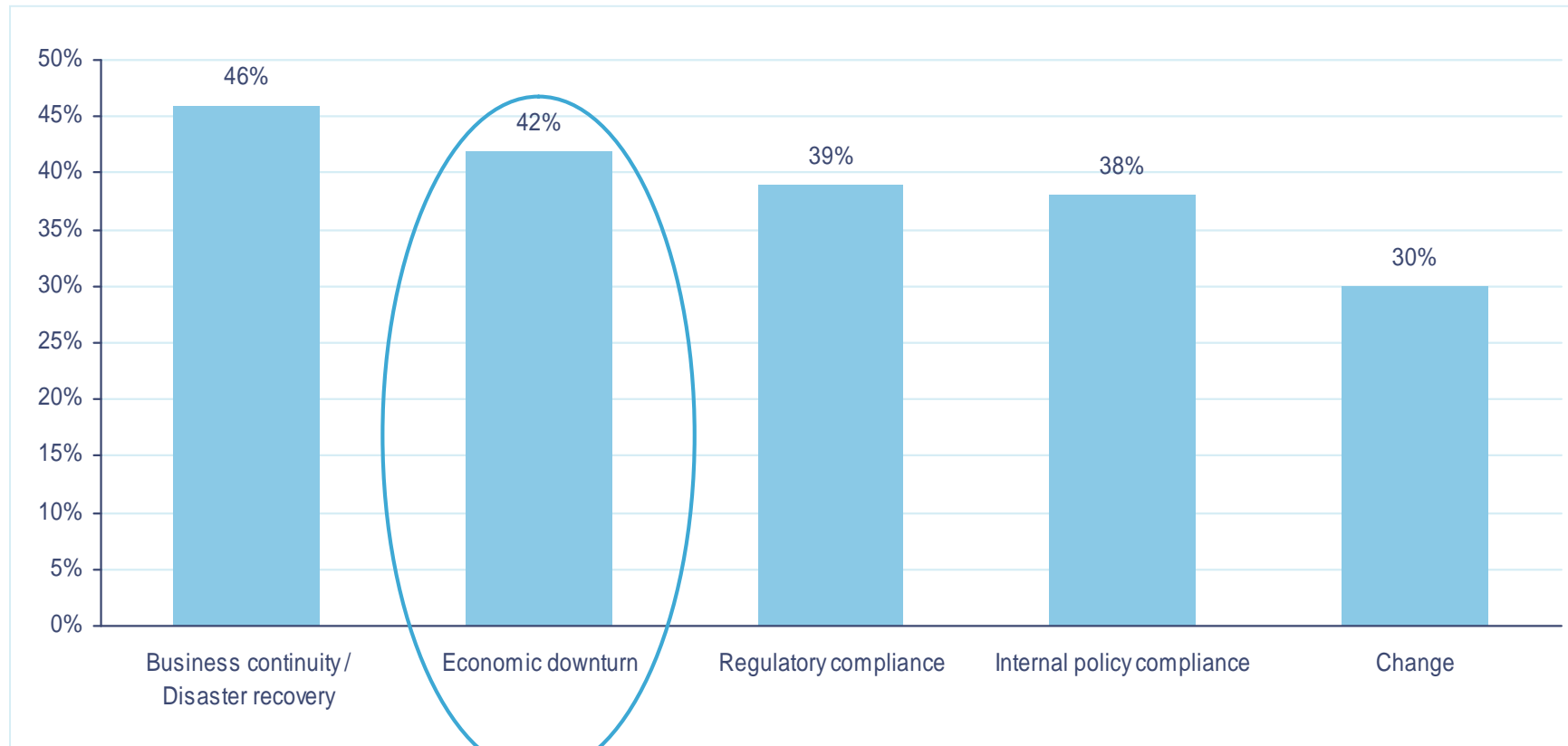
(Numbers reported may not reconcile exactly with raw data due to rounding)

# Agenda

1. Methodology
2. Spending: A decline in growth rate – but a manifestly reluctant one
3. Mounting pressure: Impacts of the economic downturn
4. Breaches: More footsteps and fingerprints – as visibility increases
5. Current state of the arsenal: New gains will be key this year
6. A crucial year: Security at an important threshold
7. What this means for your business

Section 2 – Spending: A decline in growth rate – but a manifestly reluctant one

This year, there’s a new driver of information security spending in the automotive industry – and it’s bigger than almost every other

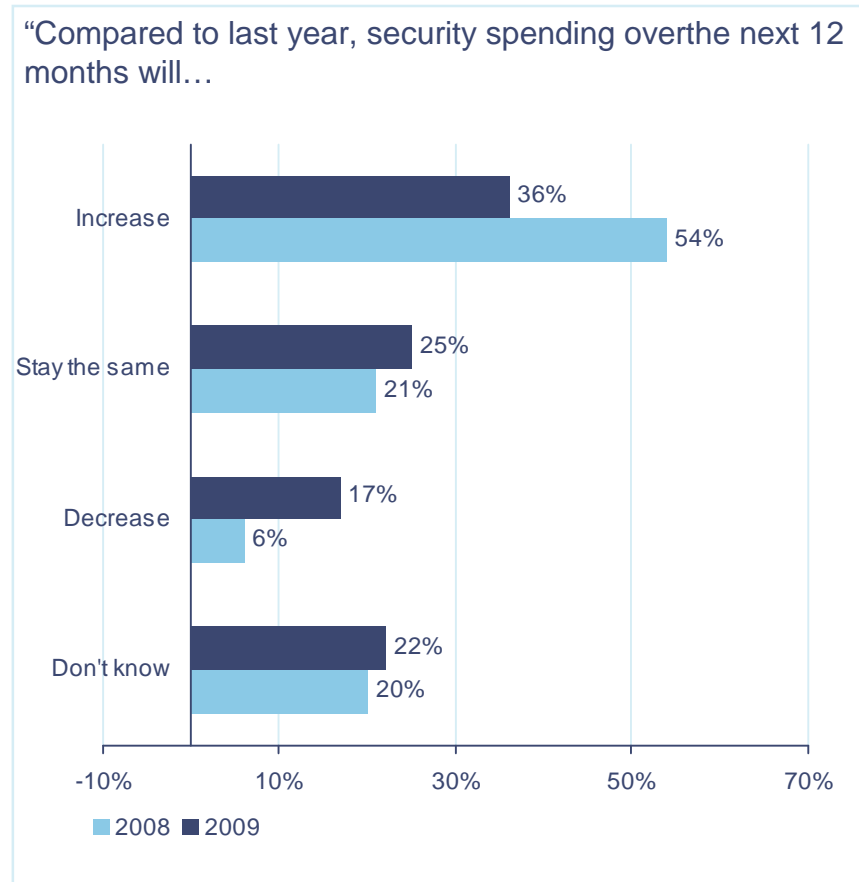


Question 32: “What business issues or factors are driving your information security spending?”  
(Total does not add up to 100%)

## Not surprisingly, spending on security is under pressure

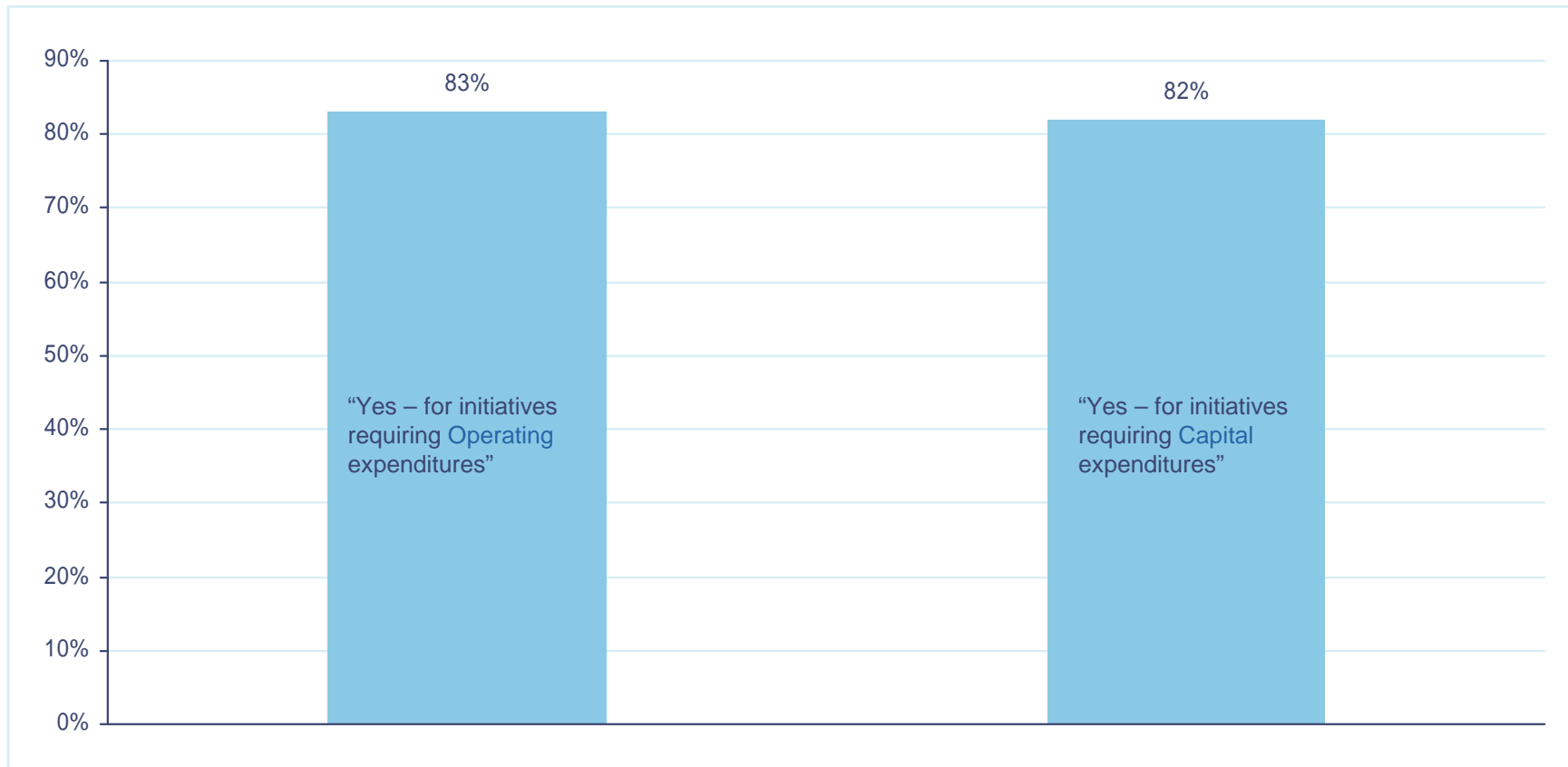
Fewer automotive respondents expect spending to increase this year.

But what we find most interesting is that 6 out of 10 (61%) expect spending to either increase or stay the same – in spite of dramatic changes in the global auto industry and the worst economic downturn in decades.



Section 2 – Spending: A decline in growth rate – but a manifestly reluctant one

Is “cancelling, deferring or downsizing security-related initiatives important?” Absolutely – according to more than 8 out of 10 automotive respondents...



Question 11: “To continue meeting your security objectives in the context of these harsher economic realities, how important are the following strategies?” (Respondents who answered “Somewhat Important”, “Important”, “Very Important” or “Top Priority”)

Section 2 – Spending: A decline in growth rate – but a manifestly reluctant one

...but far fewer automotive executives are “acting” on this – and actually “deferring or reducing budgets” for security initiatives.

Has your company deferred security initiatives?	
	Yes
For capital expenditures	49%
For operating expenditures	36%

Has your company reduced budgets for security initiatives?	
	Yes
For capital expenditures	51%
For operating expenditures	49%

Section 2 – Spending: A decline in growth rate – but a manifestly reluctant one

...Among the half or fewer that are taking action, the vast majority are deferring initiatives by less than 12 months or reducing spending by under 20%.

Has your company deferred security initiatives?	Yes	By less than 6 months	By 6 to 12 months	By 1 year or more
For capital expenditures	49%	20%	19%	10%
For operating expenditures	36%	14%	18%	4%

Has your company reduced budgets for security initiatives?	Yes	By under 10%	By 10% to 19%	By 20% or more
For capital expenditures	51%	14%	27%	10%
For operating expenditures	49%	15%	20%	14%

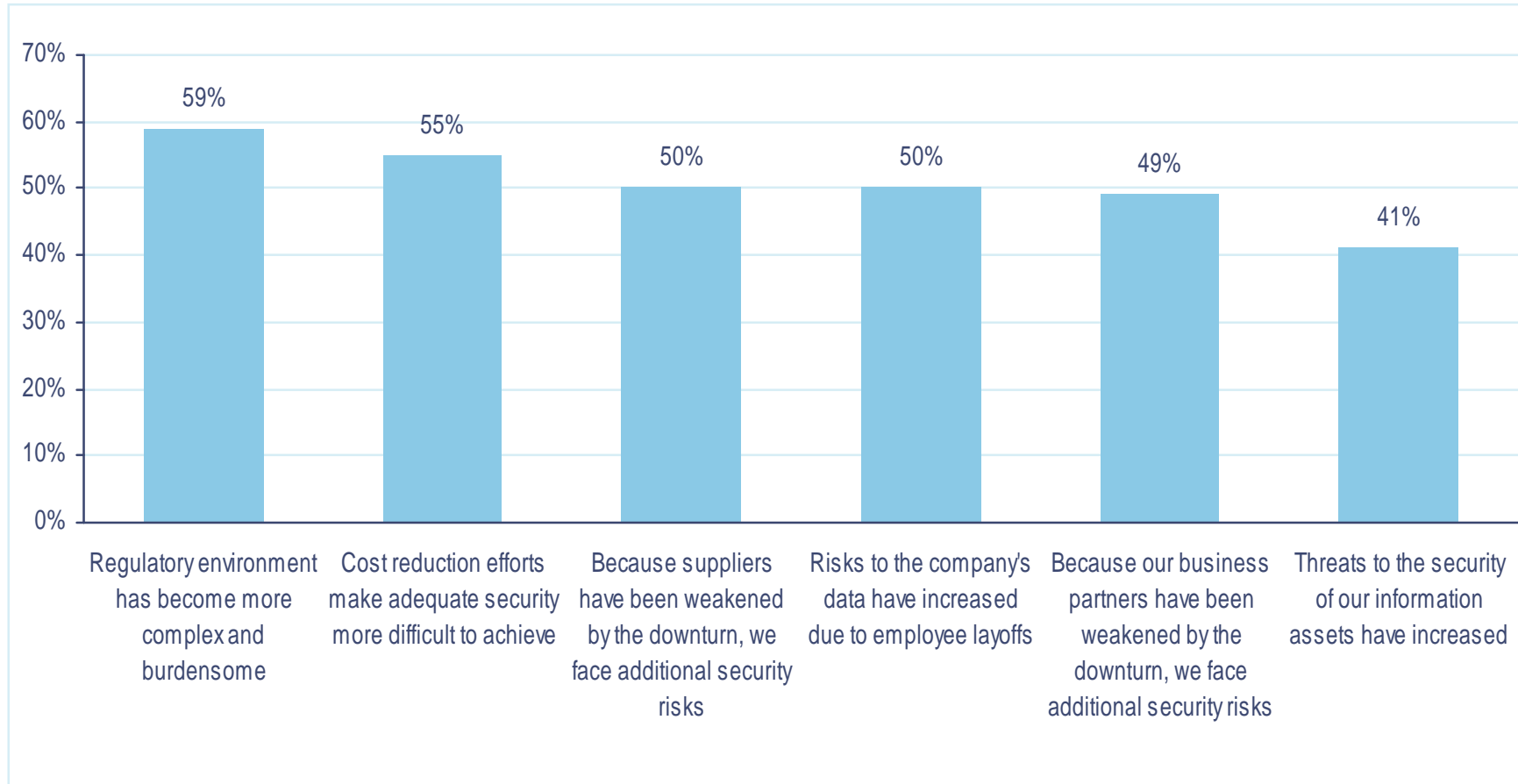
In short, it appears that some automotive executives are reluctant to cut too deeply into security – and may, to some extent, be protecting this investment.

# Agenda

1. Methodology
2. Spending: A decline in growth rate – but a manifestly reluctant one
3. Mounting pressure: Impacts of the economic downturn
4. Breaches: More footsteps and fingerprints – as visibility increases
5. Current state of the arsenal: New gains will be key this year
6. A crucial year: Security at an important threshold
7. What this means for your business

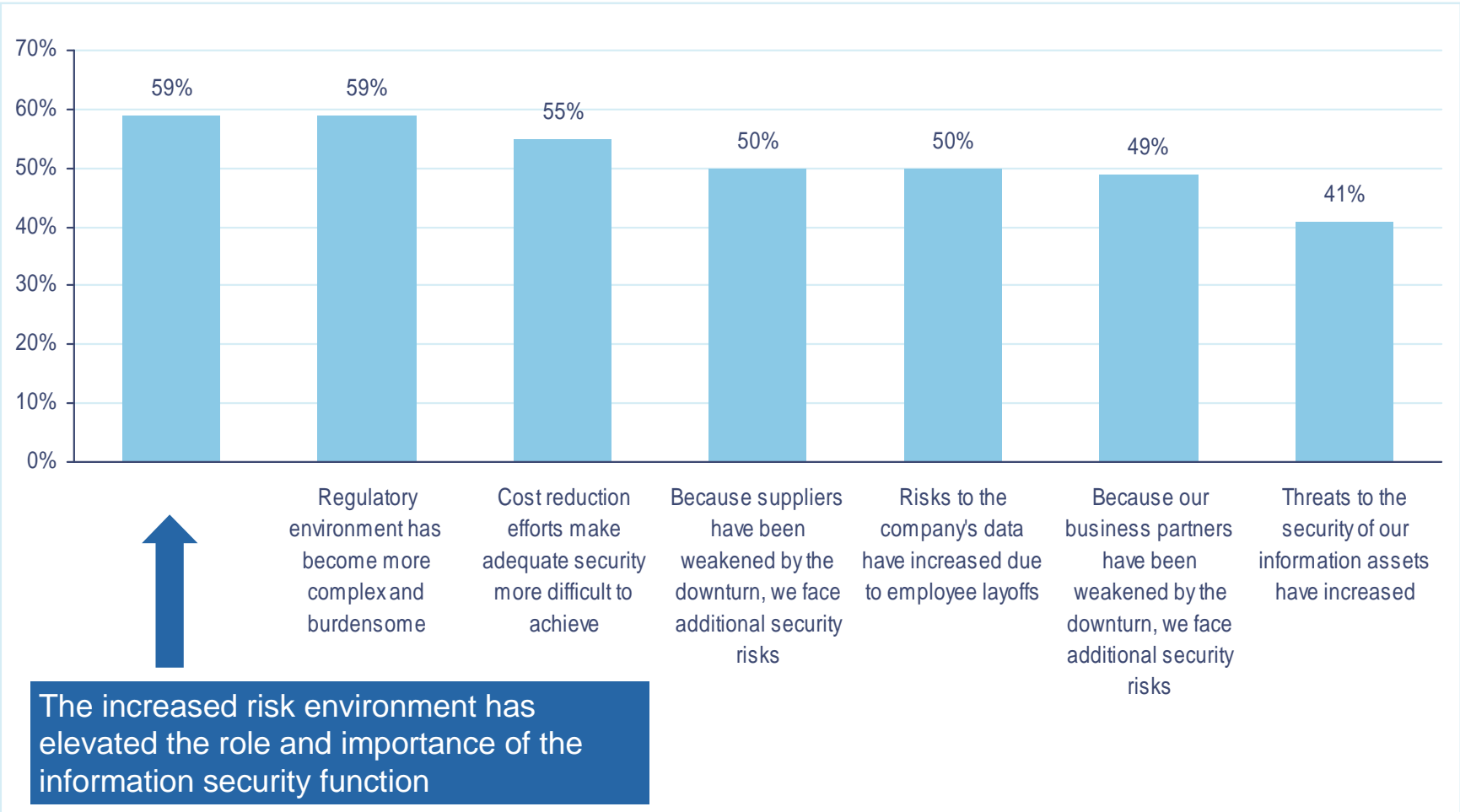
Section 3 – Mounting pressure: Impacts of the downturn

Although given a reprieve, of sorts, from the budget knife, the information security function is under pressure to “perform”



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

# Many auto respondents agree: These impacts are elevating the role and importance of the information security function



Question 10: "What impacts has the current economic downturn had on your company's security function?" (Respondents who answered "Agree" or "Strongly Agree")

# Agenda

1. Methodology
2. Spending: A decline in growth rate – but a manifestly reluctant one
3. Mounting pressure: Impacts of the economic downturn
4. Breaches: More footsteps and fingerprints – as visibility increases
5. Current state of the arsenal: New gains will be key this year
6. A crucial year: Security at an important threshold
7. What this means for your business

## So, given automotive concerns about the higher risks this year, has the number of incidents increased?

Yes. But this is partly – and maybe fully – due to greater visibility into incidents and their causes and impacts (i.e., a multi-year decline in the number of automotive respondents who don't know the answers to key incident-related questions).

Clearly, all the evidence isn't yet on the table. If the downturn-driven, security-related risks that automotive respondents are concerned about were fully reflected here, these numbers – and the ones on the next three slides – would be considerably higher.

Number of security incidents	2007	2008	2009
No incidents occurred	16%	26%	17%
From 1 to 9 incidents	39%	31%	36%
From 10 to 50 incidents	4%	6%	14%
More than 50 incidents	2%	3%	9%
Don't know	39%	33%	24%

## The new visibility into incidents also extends to types of security incidents – and reveals critical information

Better insights into what types of events are occurring yields two discoveries:

- The impacts to data are actually 90% higher than reported last year.
- And the exploitation of data is now the leading type of incident.

Types of security incidents		2007	2008	2009
#1	Data exploited	19%	13%	25%
	System exploited	15%	15%	23%
	Network exploited	26%	20%	23%
	Device exploited	NA	16%	22%
	Human exploited (Social engineering)	20%	13%	16%
	Application exploited	14%	16%	12%
	Unknown	34%	47%	36%

(Does not add up to 100%)

## Likely sources of incidents

Note that this year, current employees are less likely to be perceived as the source of incidents.

But former employees are twice as likely. We expect that as the year continues to unfold, more incidents will be traced to former employees, in line with the higher risks to security associated with layoffs and terminations.

Likely source of incidents	2008	2009
Current employee	43%	38%
Former employee	13%	27%
Hacker	18%	29%

(Does not add up to 100%)

## Business impacts

While the “full damage report” for 2009 is not yet clear, the first signs aren’t promising. The reported levels for many key business impacts have increased – for example, for financial losses, compromises to brand or reputation and, naturally, loss of shareholder value.

But there are two exceptions – the two business impacts that are the hardest to identify in a timely manner: intellectual property theft and fraud.

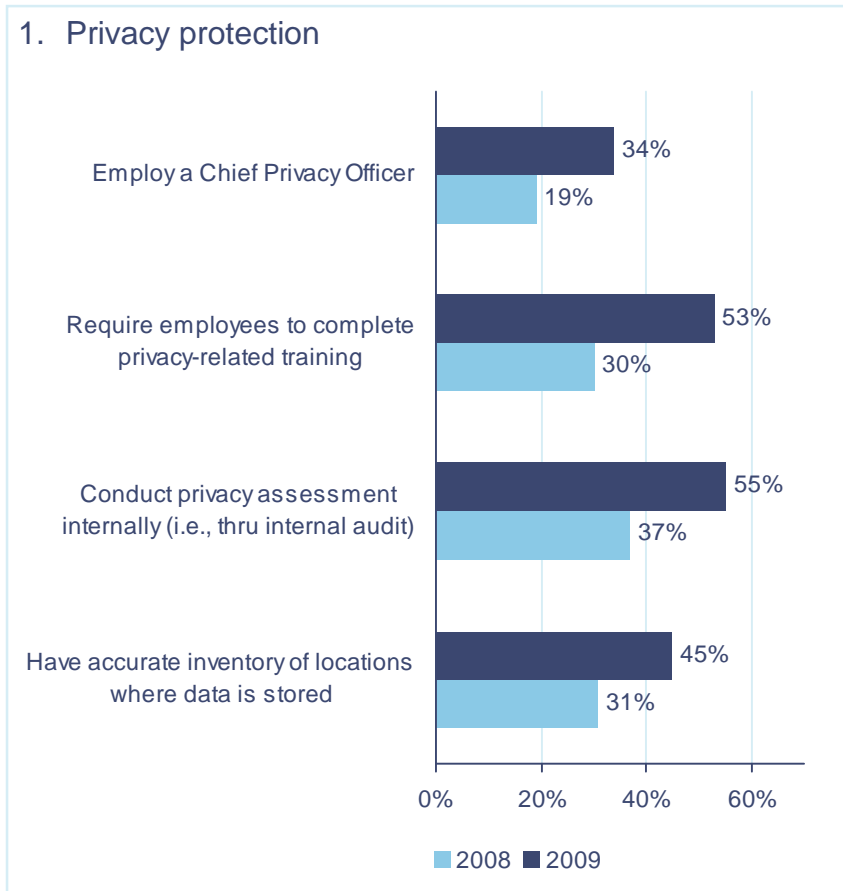
Business impacts	2008	2009
Financial losses	32%	41%
Brand/reputation compromised	8%	36%
Loss of shareholder value	8%	11%
Intellectual property theft	40%	33%
Fraud	32%	9%

(Does not add up to 100%)

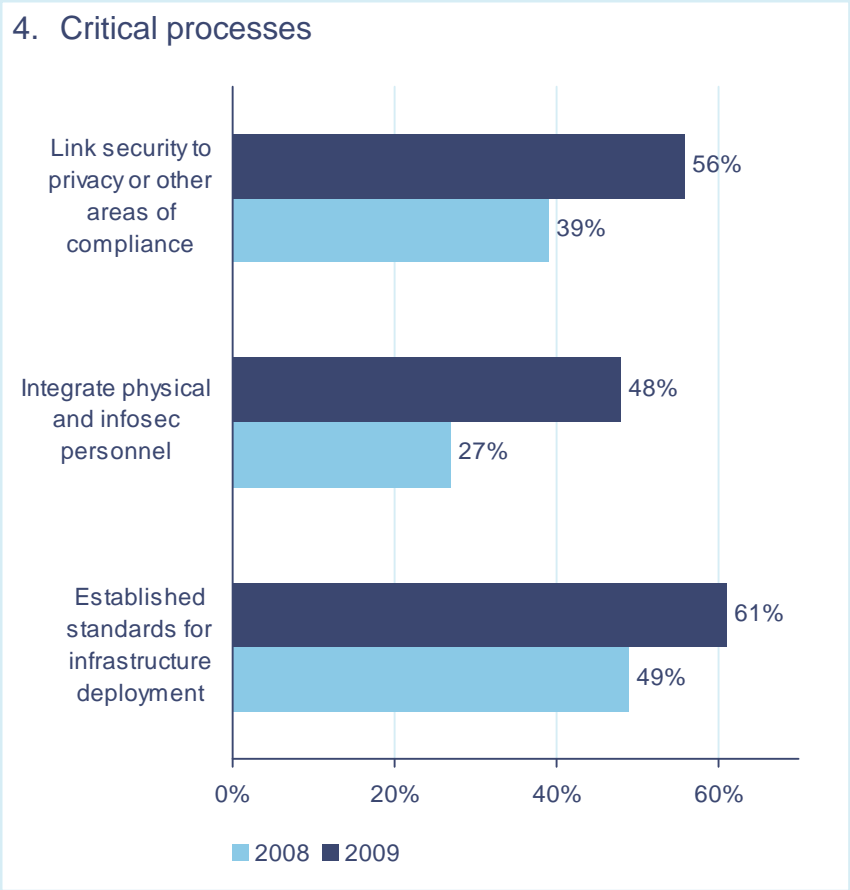
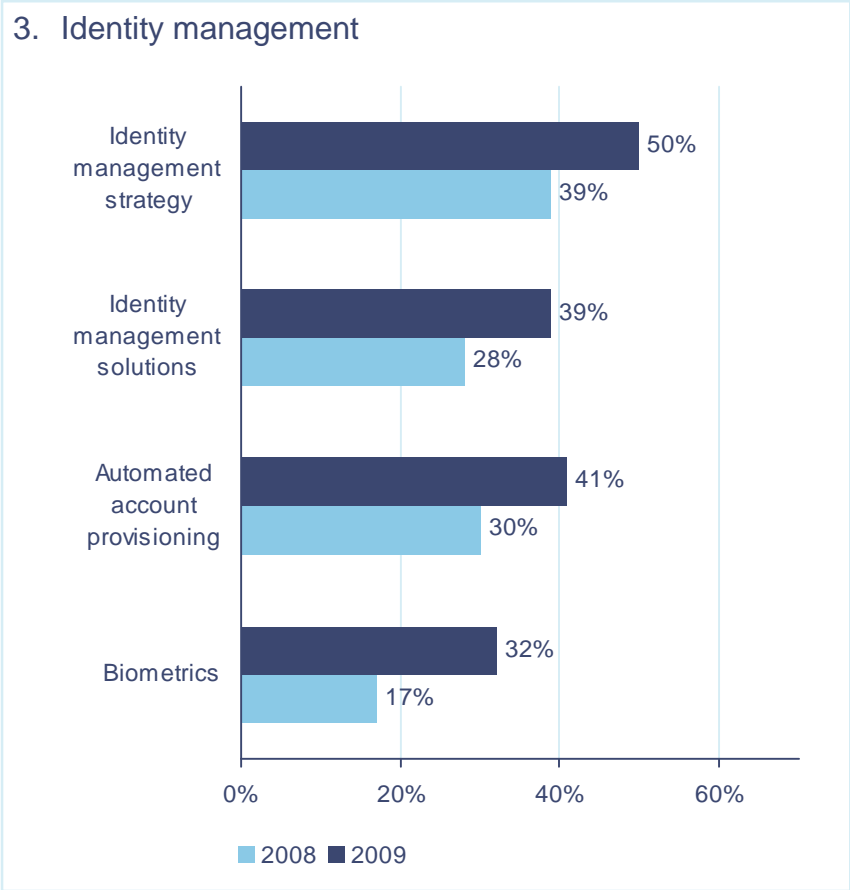
# Agenda

1. Methodology
2. Spending: A decline in growth rate – but a manifestly reluctant one
3. Mounting pressure: Impacts of the economic downturn
4. Breaches: More footsteps and fingerprints – as visibility increases
5. Current state of the arsenal: New gains will be key this year
6. A crucial year: Security at an important threshold
7. What this means for your business

# Survey results reveal that automotive companies have made strong advances in four critical arenas over the last 12 months...



# Each of these areas – privacy, people and training, IdM and critical processes – are just-in-time gains this year



## Advances in other areas are less dramatic

Does this suggest automotive companies are not well positioned to address the unexpected surge in downturn-driven security-related challenges in 2009 – on top of the enormous changes occurring in the industry? Not necessarily.

Progress always unfolds in fits and starts – and a fair view of the readiness of auto companies to address these security-related risks requires acknowledging the gains made over the last several years.

A sampling of capabilities	2006	2007	2008	2009
Overall information security strategy	33%	51%	65%	67%
Intrusion detection tools	36%	49%	57%	59%
Secure disposal of technology hardware	32%	56%	59%	59%
PC access control software	NA	39%	56%	56%
Intrusion prevention tools	29%	47%	59%	60%

# Agenda

1. Methodology
2. Spending: A decline in growth rate – but a manifestly reluctant one
3. Mounting pressure: Impacts of the economic downturn
4. Breaches: More footsteps and fingerprints – as visibility increases
5. Current state of the arsenal: New gains will be key this year
6. A crucial year: Security at an important threshold
7. What this means for your business

## This is a key moment

In short, this year, the automotive information security function – and its leaders – are encountering a powerful combination of factors:

2009

1. The greatest economic turmoil in decades – at a time of enormous industry upheaval
2. High levels of executive concerns about risks – and the impact of the downturn on the company and the supply chain
3. Breach-related evidence that doesn't necessarily reveal the "full picture" of these impacts and downturn-related consequences.
4. A multi-year investment – for better or worse – in the "building blocks" of an effective privacy and information security program that, whether or not it has reached "critical mass", has yet to show a compelling ROI.



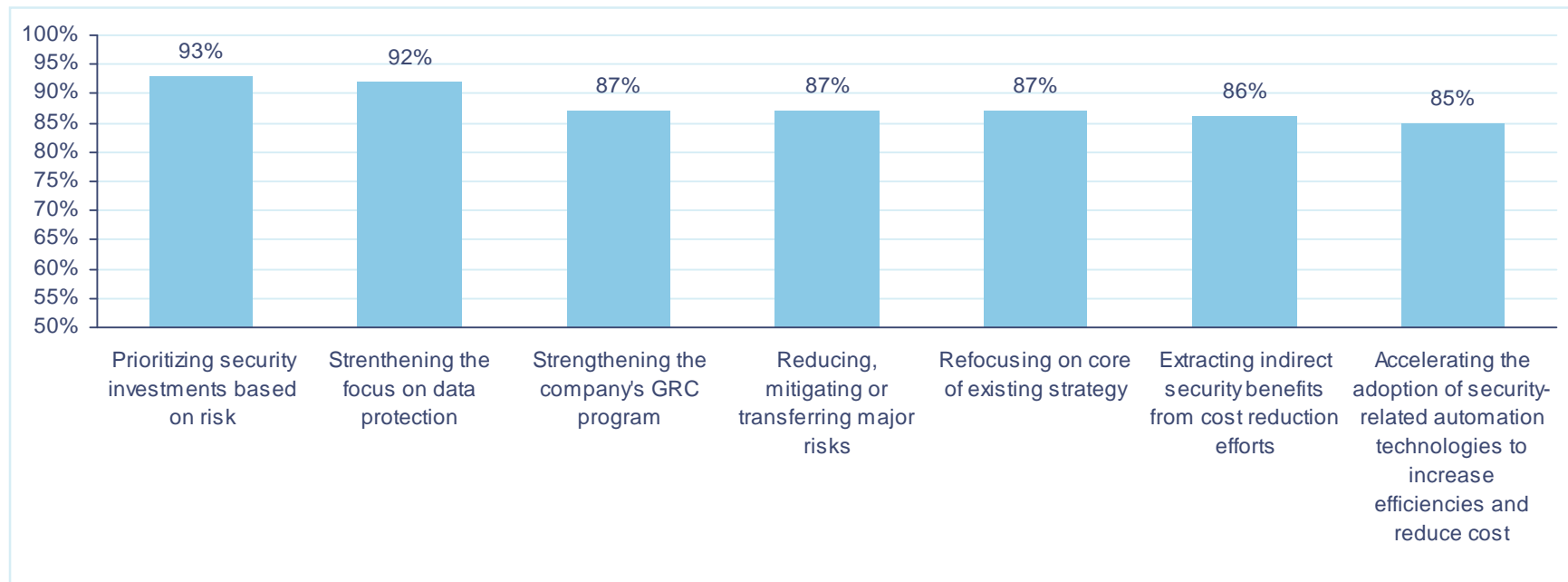
Enormous pressure (and opportunity) to deliver concrete, measurable business value – *now*, not just later.

# Agenda

1. Methodology
2. Spending: A decline in growth rate – but a manifestly reluctant one
3. Mounting pressure: Impacts of the economic downturn
4. Breaches: More footsteps and fingerprints – as visibility increases
5. Current state of the arsenal: New gains will be key this year
6. A crucial year: Security at an important threshold
7. What this means for your business

## So how are automotive executives trying to tighten the alignment of security’s contribution with the business?

They’re looking hardest at – and placing their highest expectations on – initiatives that (1) address the big risks first, (2) safeguard the underlying data, (3) pull this portfolio of multi-year investments together (strategy), (4) reduce cost, and (5) increase efficiency.



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

## After years in the limelight, data protection is now in the spotlight at – arguably – the most critical time

While data protection capabilities are uneven – not just across the industry, but within many companies as well – advances in the past year are worth noting.

- **Data Loss Prevention (DLP):** Industry respondents who say their organization has a DLP capability leapt this year – from 25% to 39%. In addition, 79% consider pursuing more complete configuration of DLP tools to be “important” – which suggests the adoption rate will spike again this year.
- **Classification:** The industry also continues to make steady advances in prioritizing data and information assets according to their risk level – from 17% in 2008 to 31% today.
- **Protection, disclosure and destruction:** To protect data, however, you also have to have a clear “rule book”. This year’s responses reveal that only 1 out of every 2 automotive respondents say that their organization’s security policies address the protection, disclosure and destruction of data.

## The crucial importance of a having a clear strategy

- In order to prioritize security investments, especially in today's economy, IT and security leaders must follow a principles-based approach to managing risk and reward in order to secure investments.
- It is not enough to justify security investments merely as a defensive response to uncertainty in the business environment or the threat of regulation.
- Instead, decision-makers must align security with drivers that are reshaping the auto business – drivers such as rapid innovation and the embrace of new business models.
- Linking risk and reward requires a clear strategy.
- If your security leaders understand the greatest sources of value creation across the organization, assign clear accountability for risk management and performance management, and are able to quantify the rewards associated with the risks, your information security function will play a critical role in determining how your company will weather the challenges ahead.

© 2009 PricewaterhouseCoopers LLP. All rights reserved. "PricewaterhouseCoopers" refers to PricewaterhouseCoopers LLP, a Delaware limited liability partnership, or, as the context requires, the PricewaterhouseCoopers global network or other member firms of the network, each of which is a separate and independent legal entity. \*connectedthinking is trademark of PricewaterhouseCoopers LLP (US).

