

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

# 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

May 25, 2010

\*connectedthinking

PRICEWATERHOUSECOOPERS 

# Agenda

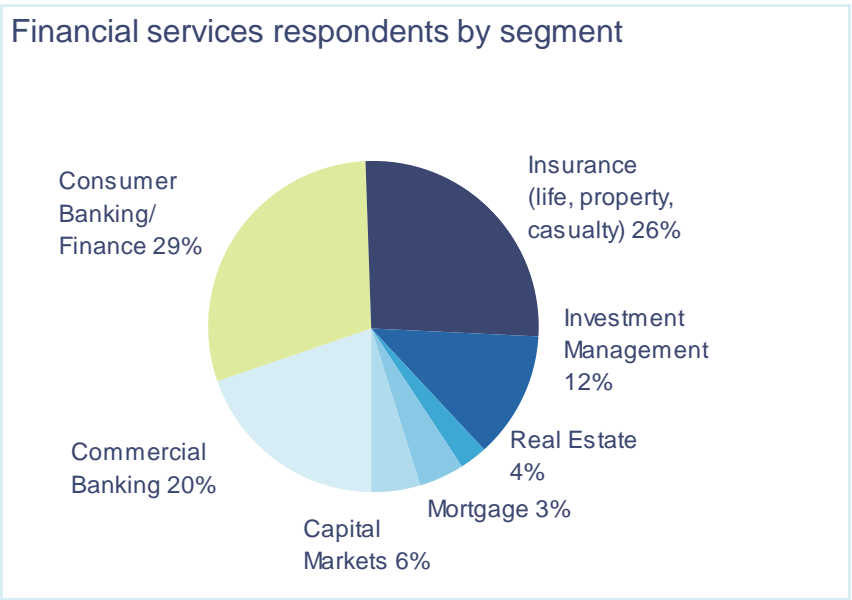
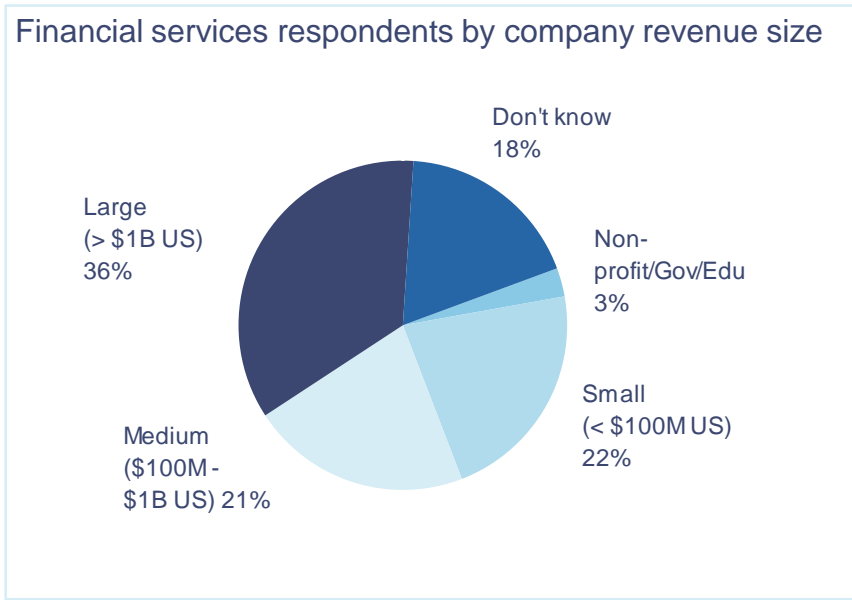
1. Methodology
2. Spending: A decline in growth rate – but a manifestly reluctant one
3. Breaches: More footsteps and fingerprints – as visibility increases
4. Current state of the arsenal: Strong – but also largely static

## 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.

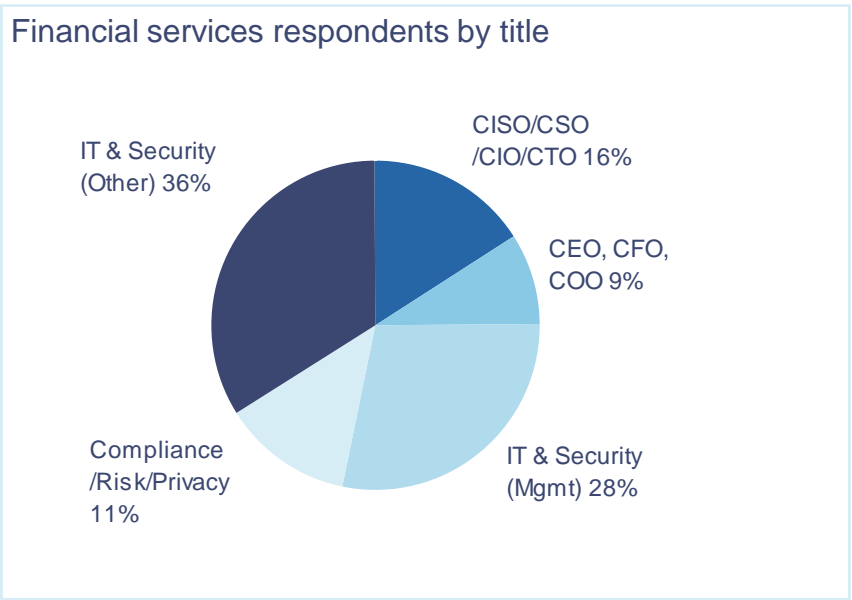
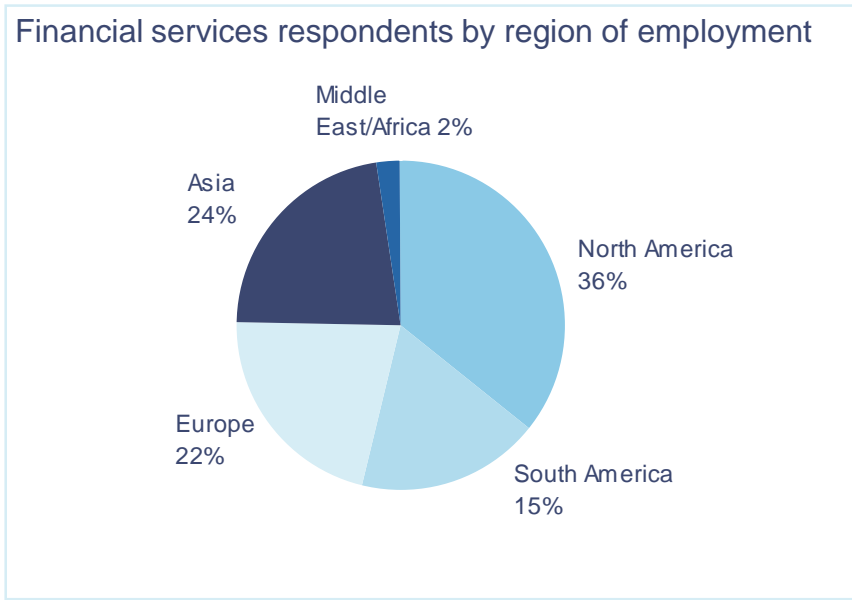
- PwC's 11<sup>th</sup> year conducting the online survey, 7th with CIO and CSO Magazines
- Readers of CIO and CSO Magazines and clients of PwC from 130 countries
- More than 7,200 responses from CEOs, CFOs, CIOs, CSOs, VPs, and directors of IT and security
- Over 40 questions on topics related to privacy and information security safeguards
- Thirty-two percent (32%) from companies with revenue of \$500 million+
- Respondents from financial services industries total 1,165

# Demographics



Numbers do not necessarily add up to 100% due to rounding.

# Demographics

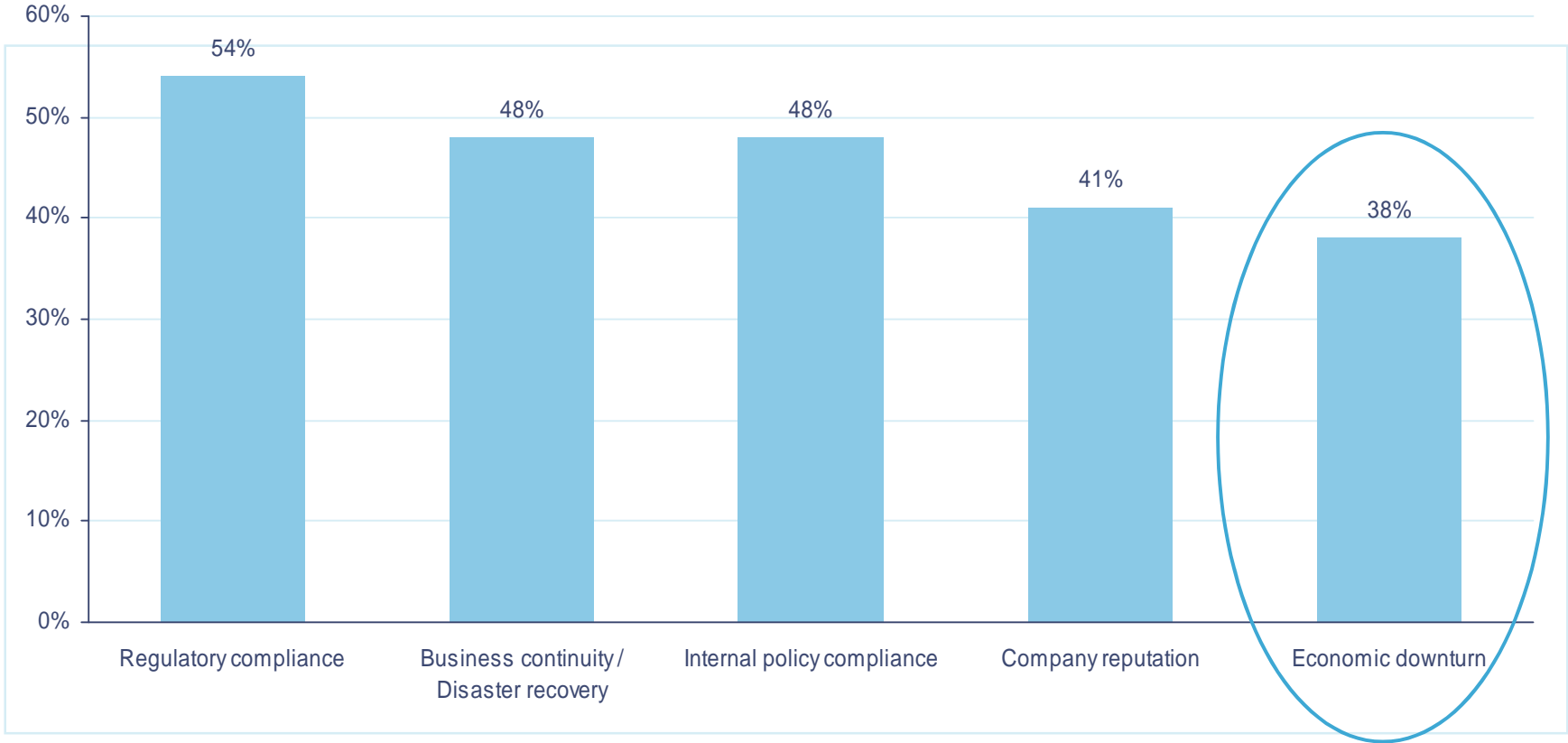


Numbers do not necessarily add up to 100% due to rounding.

# Agenda

1. Methodology
2. Spending: A decline in growth rate – but a manifestly reluctant one
3. Breaches: More footsteps and fingerprints – as visibility increases
4. Current state of the arsenal: Strong – but also largely static

This year, there's a new driver of information security spending in the FS industry – and it's nearly as huge a driver as company reputation



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

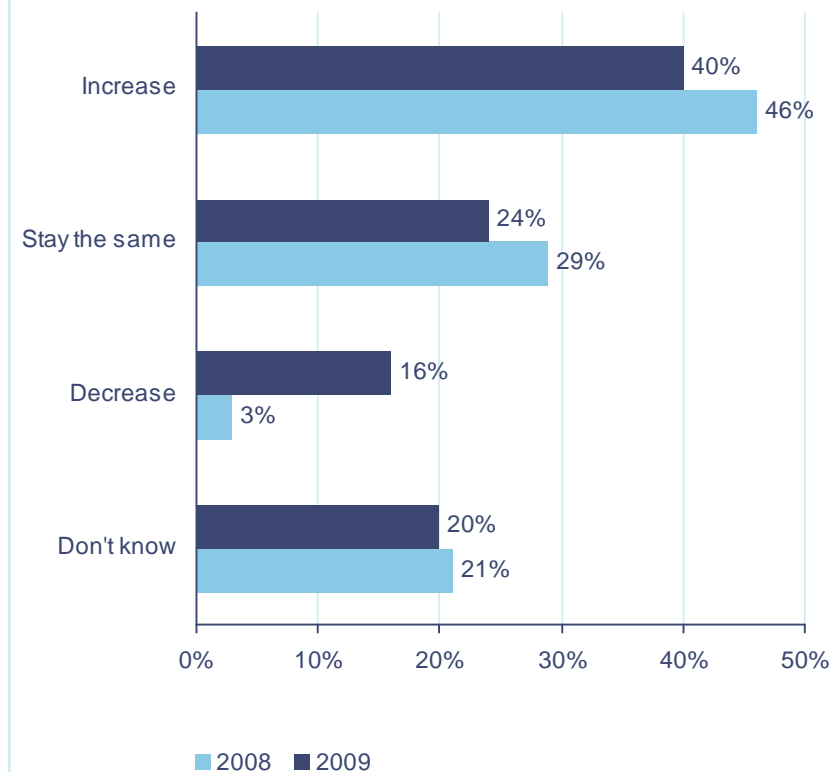
# Not surprisingly, spending on security is under pressure

This year, fewer FS respondents predict spending will increase.

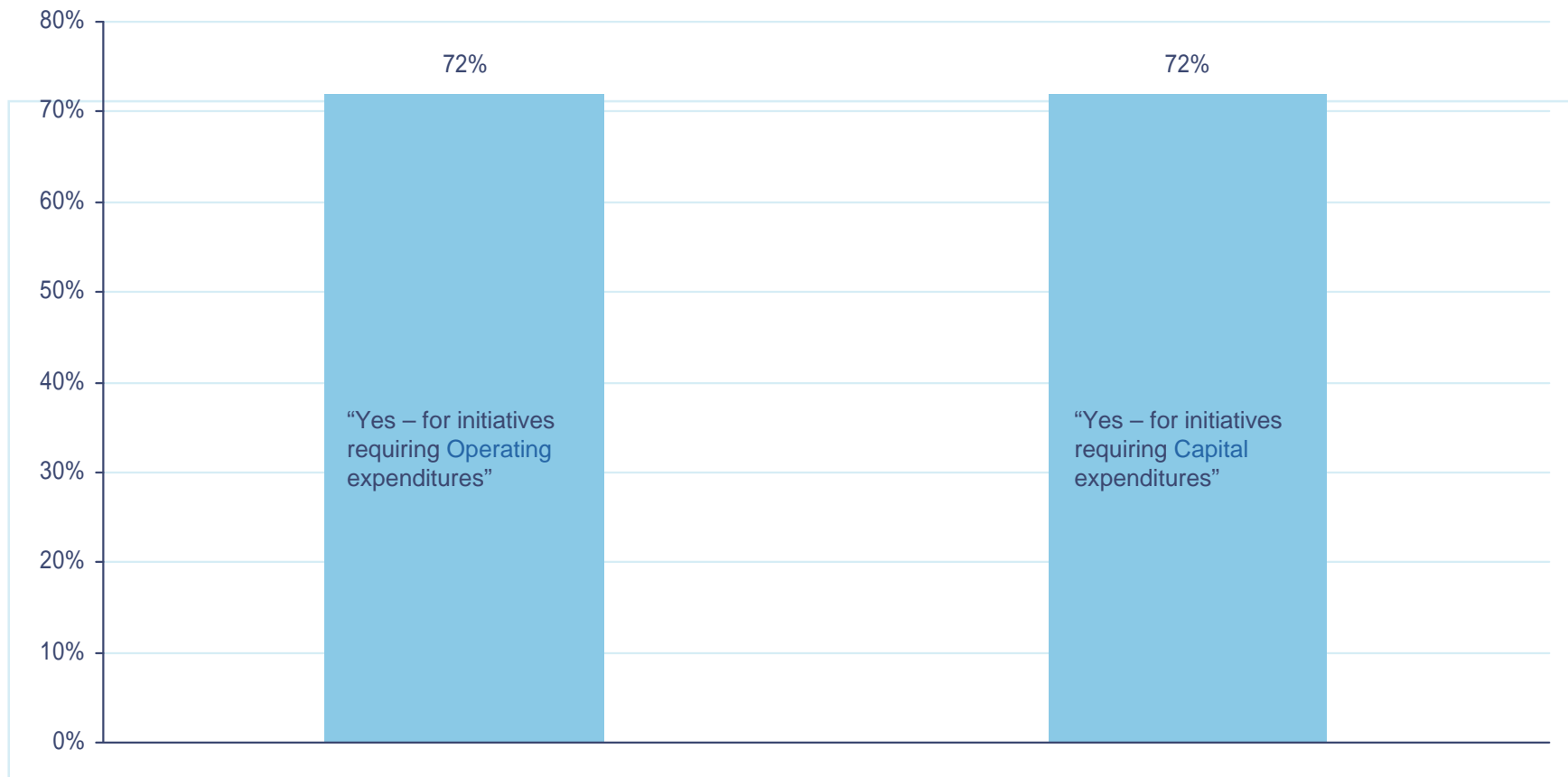
Yet what we find most interesting is that nearly two-thirds (64%) expect spending to either increase or stay the same – in spite of the worst economic downturn in decades.

Or perhaps because of it.

“Compared to last year, security spending over the next 12 months will...”



# Is “cancelling, deferring or downsizing security-related initiatives important?” Absolutely – according to 7 in 10 FS 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”)

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

Has your company deferred security initiatives?	Yes
For capital expenditures	44%
For operating expenditures	41%

Has your company reduced budgets for security initiatives?	Yes
For capital expenditures	48%
For operating expenditures	47%

...And among the fewer than half that are taking action, most are taking the least dramatic response – either by deferring initiatives by less than 6 months or reducing spending by under 10%.

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	44%	22%	14%	8%
For operating expenditures	41%	23%	13%	5%

Has your company reduced budgets for security initiatives?	Yes	By under 10%	By 10% to 19%	By 20% or more
For capital expenditures	48%	18%	17%	13%
For operating expenditures	47%	19%	16%	12%

In short, it appears that some FS executives are reluctant to cut too deeply into security – and may, to some extent, be protecting the security function.

# Agenda

1. Methodology
2. Spending: A decline in growth rate – but a manifestly reluctant one
3. Breaches: More footsteps and fingerprints – as visibility increases
4. Current state of the arsenal: Strong – but also largely static

# So, given FS 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 FS respondents who don't know the answers to key incident-related questions).

Perhaps all the evidence isn't yet on the table. If the downturn-driven, security-related risks that FS 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	21%	23%	17%
1 to 9 incidents	23%	27%	36%
10 to 50 incidents	6%	7%	10%
50 or more incidents	4%	6%	5%
Don't know	45%	38%	32%

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

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

- The impacts to data are actually 50% higher than reported last year.
- And the exploitation of data is now the leading type of attack.

Types of security incidents	2007	2008	2009
#1 Data exploited	18%	15%	23%
Network exploited	17%	19%	22%
System exploited	13%	10%	18%
Application exploited	12%	14%	17%
Device exploited	NA	13%	16%
Human exploited (Social engineering)	21%	18%	16%
Unknown	49%	44%	35%

(Does not add up to 100%)

## Likely sources of incidents

Little change from last year – which may suggest that the true impacts of the downturn had not yet emerged at the time of the survey (April 22 to June 15, 2009).

We expect, however, 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	32%	33%
Former employee	14%	16%
Hacker	29%	27%
Unknown	45%	37%

(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. Reported levels for many key business impacts are up: financial losses, IP theft, compromises to brand or reputation and, naturally, loss of shareholder value.

With the glaring exception of one – the business impact that’s one of the hardest to identify in a timely manner: fraud.

Business impacts	2008	2009
Financial losses	43%	50%
Intellectual property theft	17%	23%
Brand/reputation compromised	28%	32%
Loss of shareholder value	8%	12%
Fraud	32%	19%

(Does not add up to 100%)

# Breach Case Studies

- Breach Sources
  - Customer Phishing Attacks
  - Internal Employee Malware
  - Web Application Security Exploits
  - Accidental Data Leakage
- Breach Actions
  - Targeting 401k Accounts – initiating 401K loans or withdraws for retirement ages
  - Targeting Cash Value Life Insurance Accounts – loads/withdraws
  - Used information for identity theft

The technical sophistication of attacks continues to increase as skillful resources in Asia and Eastern Europe have been and continue to be attracted by lucrative returns from recent cyber attacks. Ninety-five percent of records compromised are the result of attacks involving advanced skills, significant customization, and/or extensive resources. Additionally, organized criminal groups account for 91 percent of records compromised.<sup>1</sup>

<sup>1</sup>Source: 2009 Data Breach Investigations Report (Verizon Business RISK Team)

# Agenda

1. Methodology
2. Spending: A decline in growth rate – but a manifestly reluctant one
3. Breaches: More footsteps and fingerprints – as visibility increases
4. Current state of the arsenal: Strong – but also largely static

## If you look hard enough at this year's FS survey responses – and long enough – you'll find a few gains.

Has the FS industry advanced its security and privacy capabilities in the past year? In some areas, yes. Such as security leadership, risk assessment, data security, third-party security and physical security.

	2008	2009
Employ a CISO	45%	51%
Employ a CSO	38%	45%
Conduct risk assessments via third party	41%	51%
Have accurate inventory of locations where data is stored	36%	48%
Have incident response process to report breaches and coordinate with third parties handling data	44%	52%
Have a data loss prevention (DLP) capability in place	33%	46%
Integrate physical security and information security personnel	37%	55%

But the most striking finding among FS responses is that – across all major security domains – *the “chalk lines” have essentially not moved.*

For the first time in the 12-year history of this survey, the majority of metrics we use to track advances in security-related capabilities – across all major security domains, including strategy, structure, people, process and technology – have, by and large, for the financial services industry, not improved.

FS security-related capabilities in 2009: A representative sampling	2008	2009
Overall information security strategy	75%	74%
Conduct threat and vulnerability assessments	59%	59%
Have people dedicated to monitoring employee use of Internet	64%	64%
Encrypt removable media	45%	46%
Have tools to discover unauthorized devices	56%	58%
Use wireless handheld device security	50%	49%
Have established security baselines for external partners/suppliers	59%	61%
Require employees to complete training on privacy policies/practices	61%	61%

## Why?

Global trends are never the result of one factor. One key reason for this “freezing” in the data is the shift in this year’s answer pool.

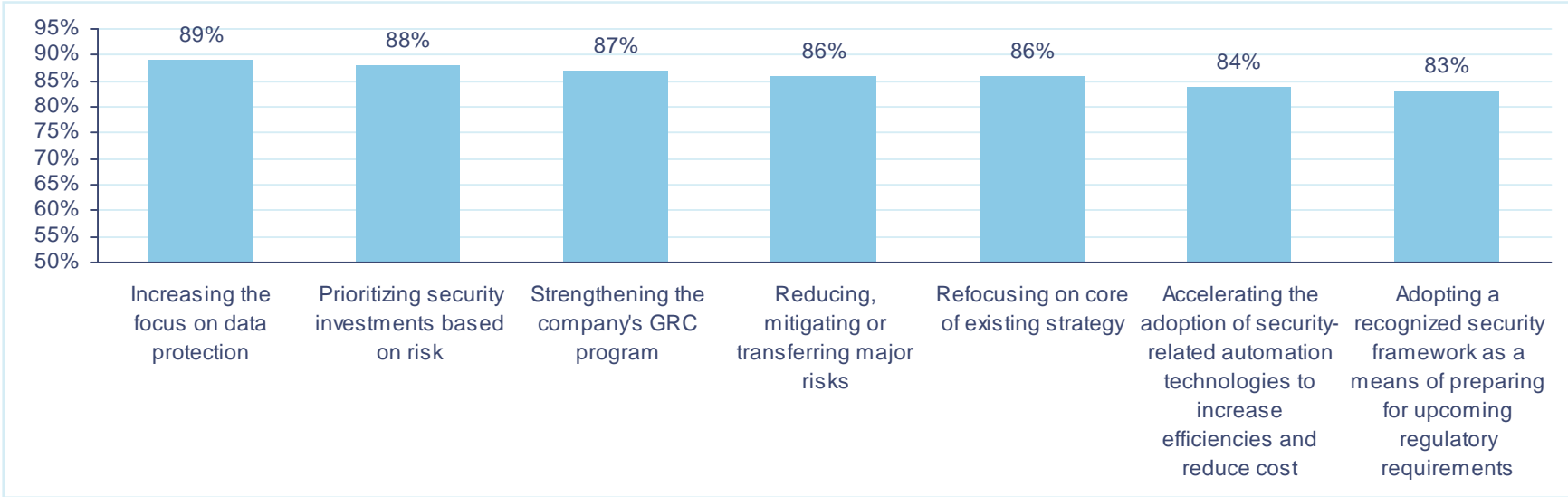
- There was a 12-point (from 48% to 36%) decline in the number of respondents employed in North America – a decline offset by 6-point increases from those employed in South America and Asia. In regional response comparisons, South America’s security capabilities tend to lag behind those in other regions of the world, while Asia’s are currently on a par with North America.)

But a second likely reason is impossible to ignore.

It’s hard to avoid the conclusion that the economic “freight train” has impacted FS companies more than those in any other industry – and largely stopped the global financial services industry’s multi-year investment in security capabilities effectively, if temporarily this year, “in its tracks”.

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

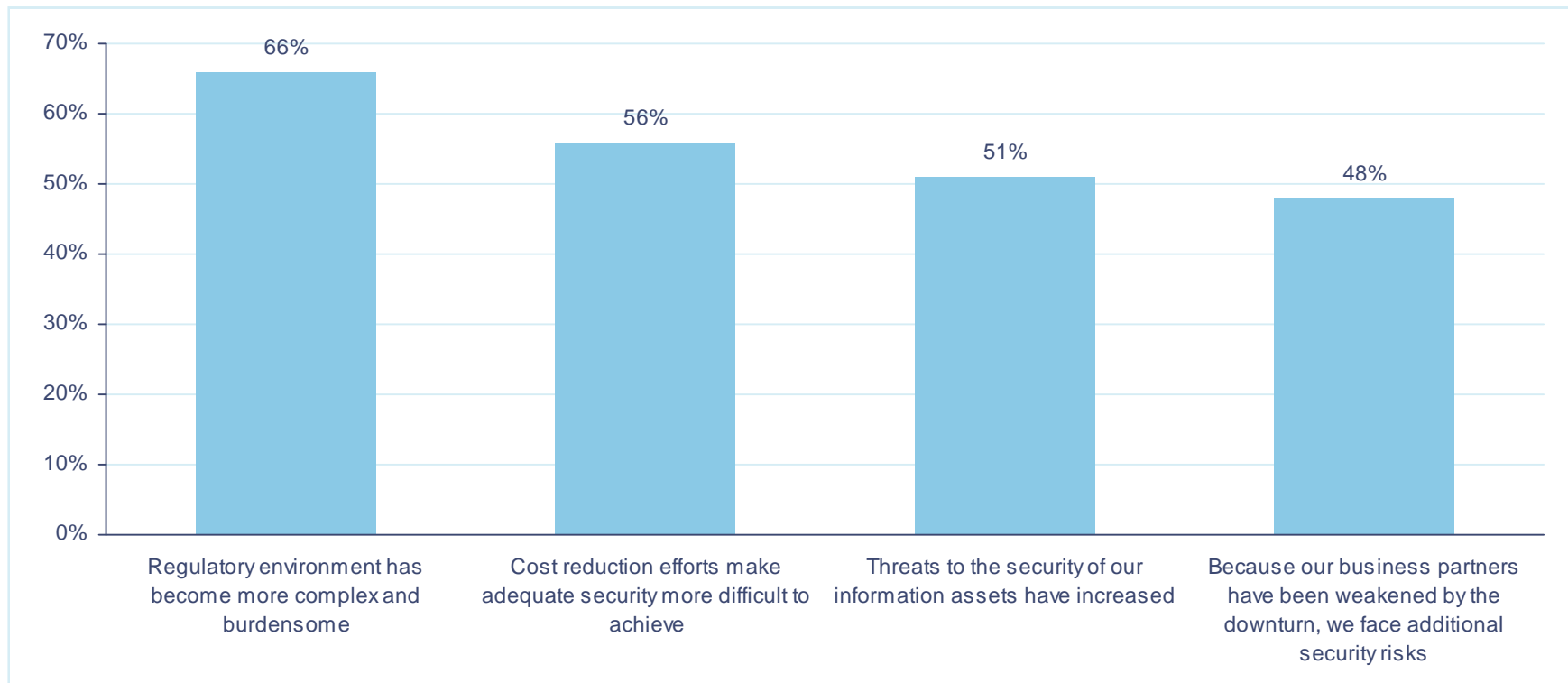
They’re looking hardest at – and placing their highest expectations on – initiatives that (1) pull this portfolio of multi-year investments together (strategy and integration); (2) address the big risks first; (3) reduce cost and increase efficiency; and (4) manage the security-related impacts of regulation. But across all of these priorities – the single most important one is increasing the protection of data.



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%)

# New and evolving regulatory requirements

FS institutions are struggling with their response to new and evolving regulatory requirements (ex. Red Flags rule; MA 201; PCI). They are treating new requirements as one-off projects, resulting in increased cost of compliance. FS institutions should approach their response more strategically, leveraging other corporate initiatives such as compliance, privacy or security



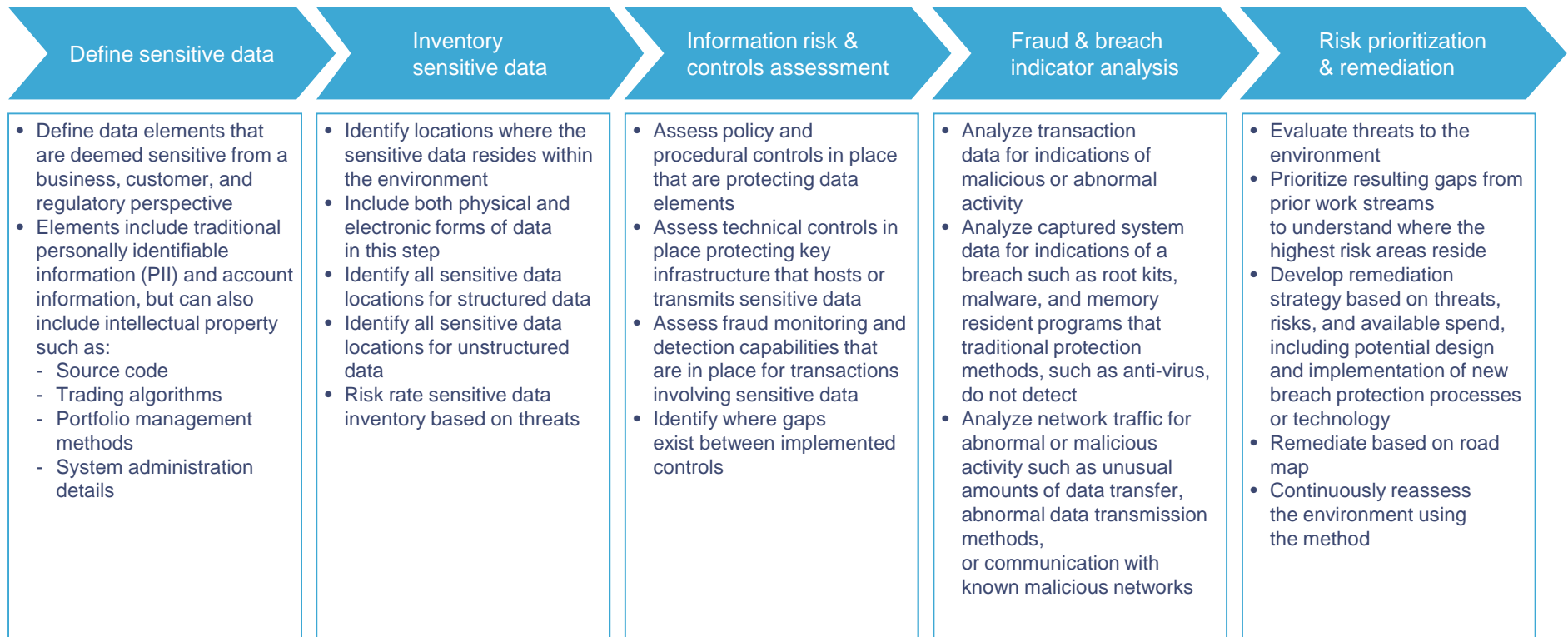
# Most Common Security Initiatives

- Adaptive Authentication & Authorization – risk based
- Data Protection
  - Inventory
  - Classification
  - DLP Technology
- Tighter integration of security into SDLC
- Re-alignment of regulatory compliance efforts:
  - Red Flag Law
  - State Breach Notification
  - HIPAA / HiTech
  - GLBA
  - SOX
- Identity & Access Management

# Framework for action

Approach focuses on identifying and preventing breaches and protecting sensitive data.

Traditionally, financial services companies have focused on performing risk and controls assessments on base technology infrastructure, but not combining those efforts with a detailed data inventory and a transaction and breach indicator analysis.



© 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).

