Business Risk Management

Does insecure software keep the CEO up at night?

Software Assurance Forum – March 2011

ERNST & YOUNG
Quality In Everything We Do

The Business Case for Software Assurance

The Key Points:

It's cheaper to fix vulnerabilities early on. We'll save money!

We're stuck in an endless cycle of assessments.

The investment now will pay off over time: better software that's easier to maintain.

If software contains vulnerabilities, they'll be exploited!!!

Training will make developers better coders in addition to security-informed.

More secure software + cost savings + better (and happier) developers…

This is a no brainer!

Every executive should make developing and implementing a SDLC a priority.

Why isn't it happening?

Business Risk

- "Business Risk" refers the organization as a whole and is a superset of:
  - Financial Risk - volatility in markets and the real economy
  - Compliance Risk - politics, law, regulation or corporate governance
  - Strategic Risk - customers, competitors, and investors
  - Operational Risk - processes, systems, people and overall value chain of a business

The Top 10 Business Risks of 2010

The CEO's perspective

- EY surveyed 70 industry executives and analysts representing 14 industry sectors asking each interviewee to identify and rank the top business risks for 2010. At least 5 executives or analysts were interviewed in each of the 14 sectors.

1. Regulation and compliance
2. Access to credit
3. Double dip recession
4. Managing talent
5. Emerging markets
6. Cost cutting
7. Non-traditional entrants
8. Radical greening
9. Social responsibility
10. Alliances and transactions
13. **Emerging Technologies**

But…. THE FUD!!!!

Lockheed Martin F-22 Raptor.
Unveiled on April 1997

Chengdu Aircraft Industry Group J-20.
Unveiled January 2011

THE WALL STREET JOURNAL.

Computer Spies Breach Fighter-Jet Project

BusinessWeek

E-SPIONAGE

A BUSINESSWEEK INVESTIGATION

The U.S. military created the Internet. Now the Web may be turning against it. As America fights to protect itself, we uncover startling new instances of cyber spies targeting the government and trace the path of a pernicious attack aimed at defense consultant Booz Allen.

"U.S. defense industry cybersecurity experts have cited 2006—close to the date when the J-20 program would have started—as the point at which they became aware of what was later named the advanced persistent threat (APT), a campaign of cyberintrusion aimed primarily at military and defense industries and characterized by sophisticated infiltration and exfiltration techniques."

--Aviation Week, January 10, 2011

Looking Through a Different Lens

- On March 27th 2007 TJX companies announced they lost 45 million credit card numbers.

NYSE:TJX - Graph from Google Finance

This was the largest breach in US history at the time!

Looking Through a Different Lens

- Largest breach in US history: January 20th, 2009: Heartland payment systems loses 130 million card numbers due to SQL injection:

NYSE:HPY - Graph from Google Finance

Looking Through a Different Lens

- But that was widely publicized as the Citigroup & 7-11 ATM breach… Surely they suffered, right?

Citi:

NYSE:C - Graph from Google Finance

7-11:

TYO:3382- Graph from Google Finance

Looking Through a Different Lens

- What about personal information? Worse press than card numbers? iPad user-agent exploit - 114,000 users affected June 9, 2010

Apple

NASDAQ:AAPL - Graph from Google Finance

AT&T

NYSE:T - Graph from Google Finance

The Curious Case of HFT

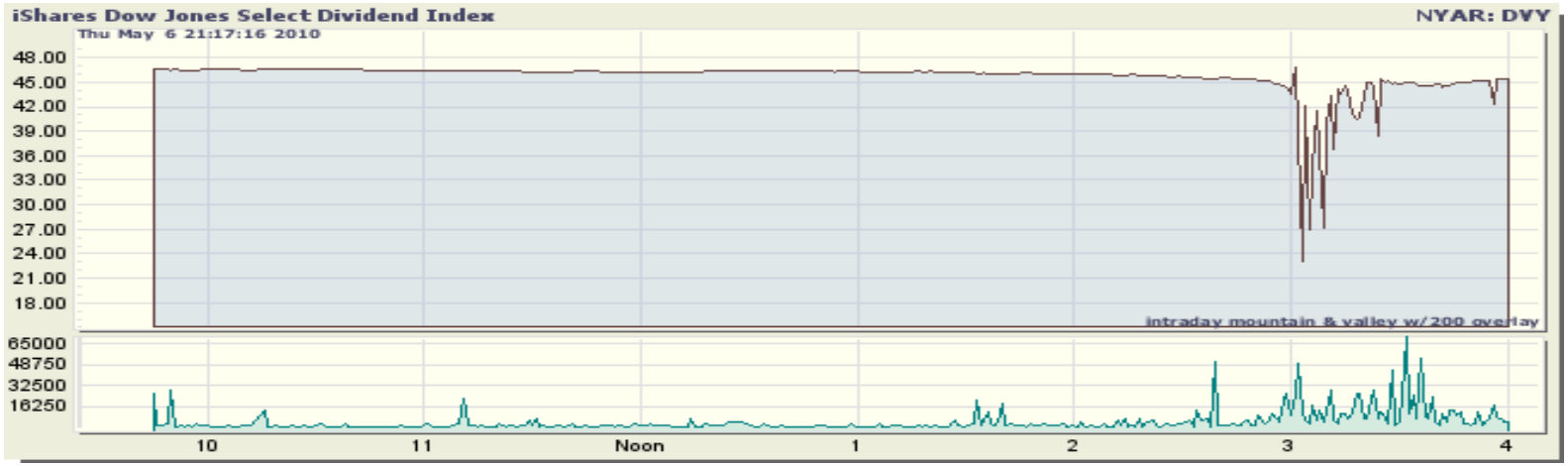
- High frequency trading uses fast computers, sophisticated algorithms and low-latency connections to execute millions of buy and sell orders in short periods.

- The dozen or so players who dominate HFT already represent 60% to 65% of flow in the United States and an estimated 25% to 30% of daily stock trades in London, according to a study conducted by Ernst & Young in 2009

- One system facilitator recently boasted a “round-trip time” — the time it takes to send an order to a venue and confirm the same — of just 16 milliseconds.

The Flash Crash

- On May 6, 2010 the Dow Jones Industrial Average lost 9.2% of its value in a 5-minute period as some 30 S&P 500 Index stocks fell by10% or more



DJIA - Graph from Seekingalpha.com

- A mutual fund complex sold 75,000 E-Mini S&P contracts ($4.1 billion).
- HFT software was configured to "target an execution rate set to 9% of the trading volume calculated over the previous minute, but without regard to price or time."
- HFTs [then] began to quickly buy and then resell contracts to each other—generating a 'hot-potato' volume effect as the same positions were passed rapidly back and forth." The combined sales by the large seller and high-frequency firms quickly drove "the E-mini price down 3% in just four minutes."

Quotes from SEC/CFTC joint report – 5/6/2010

The Flash Crash – Lessons Learned

- The SEC introduces stock-by-stock circuit breaker rules that halt trading in individual stocks if their price moves by more than 10% in a 5-minute period.

- In conjunction with other regulators, the SEC is also considering whether a market-wide circuit breaker could be used to cancel trades in case of significant market instability.

- What's not being fixed?

The HFT Software!!!!

Why not?

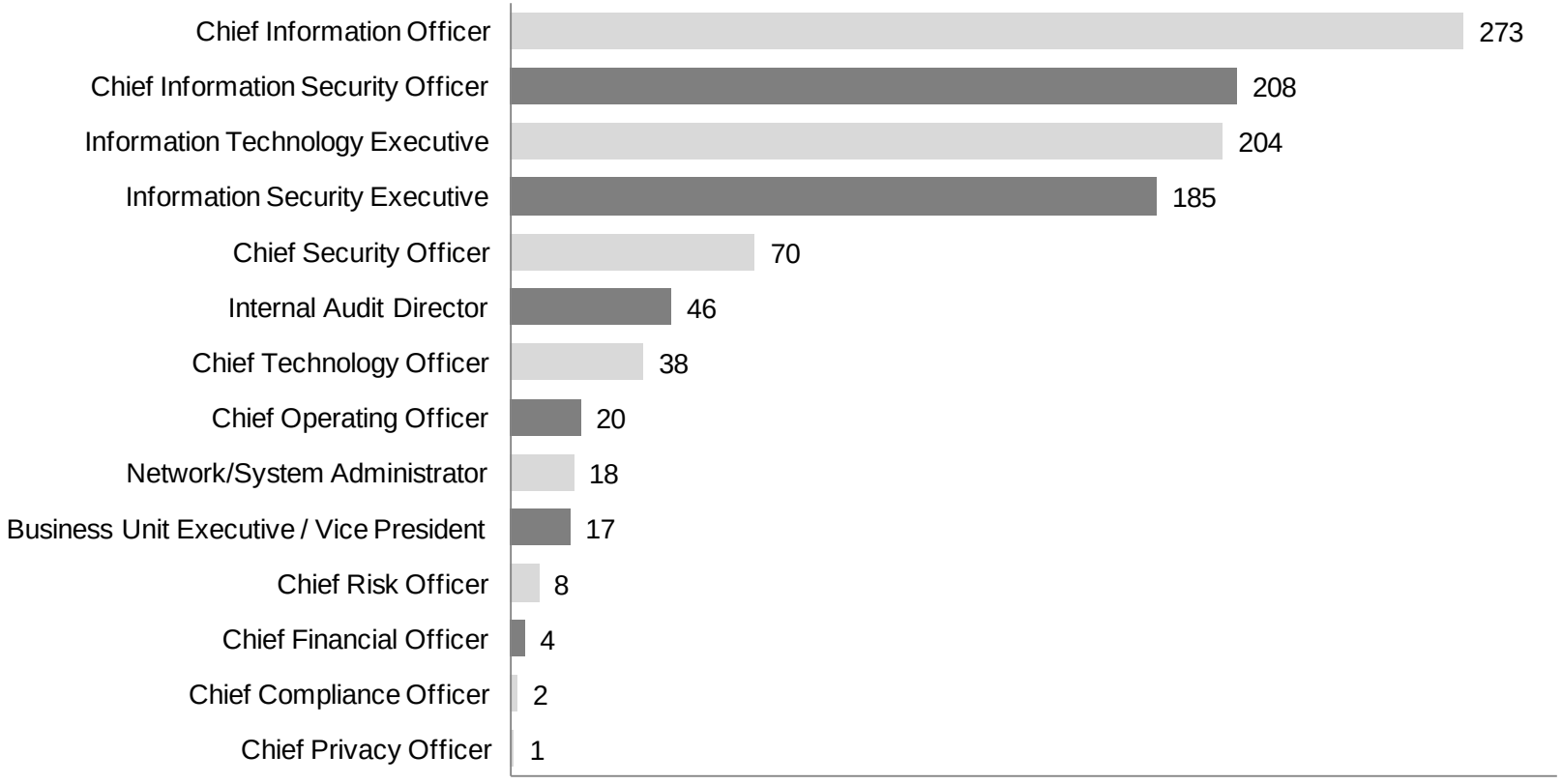
Precious milliseconds…

No Blips on the Executive Risk Radar

- If the perceived risk doesn't justify an investment, it won't be made.
  - Impact is too small to affect the company
  - Probability of occurrence is too small
  - Another risk has higher priority (cost-cutting)
- These priorities trickle-down to us!

Global Information Security Survey

- EY's 13th annual GISS was conducted from 1 June to 31 July 2010 with 1,598 organizations in 56 countries and across all major industries participating.

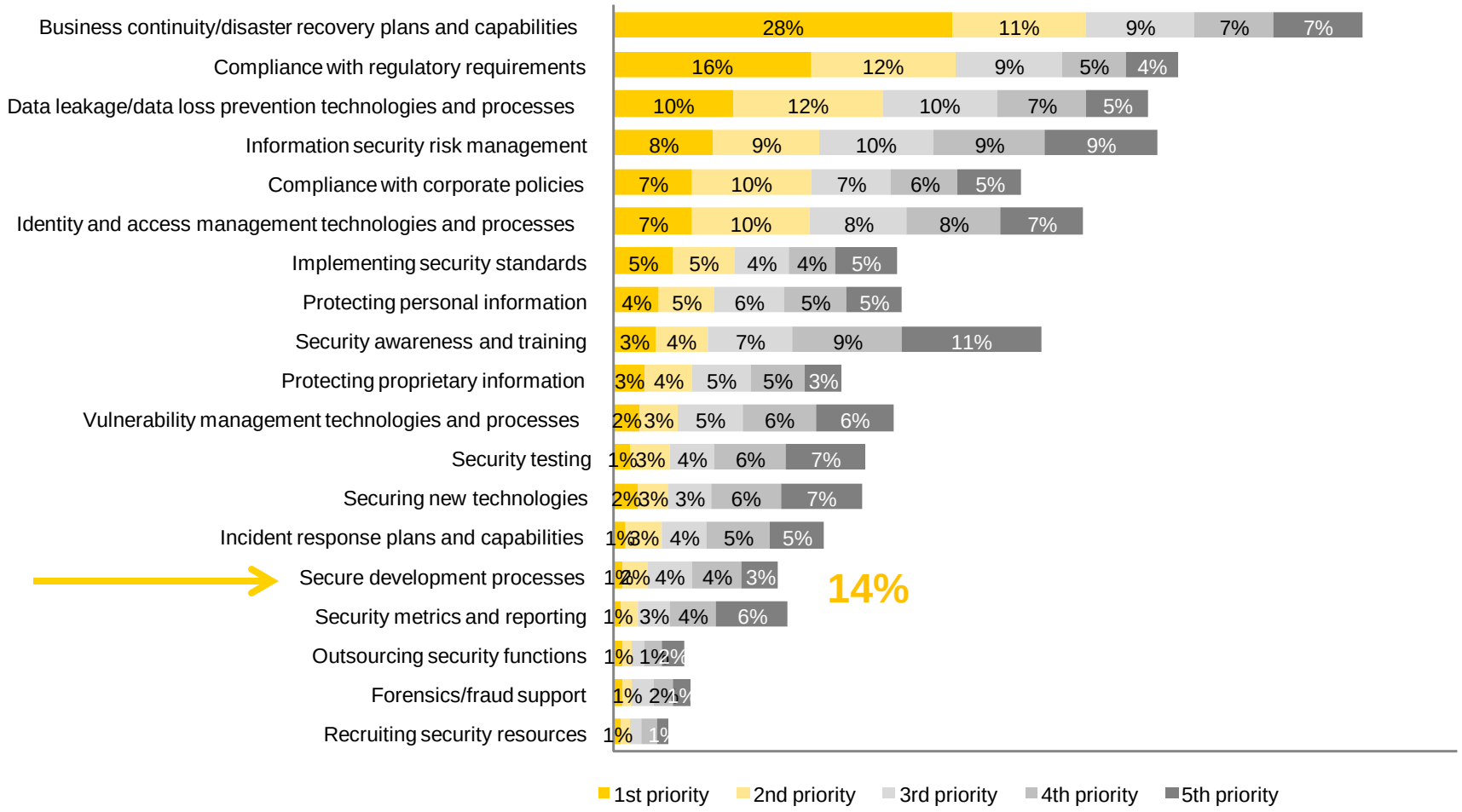


Shown: number of participants

Note: 504 participants with other titles

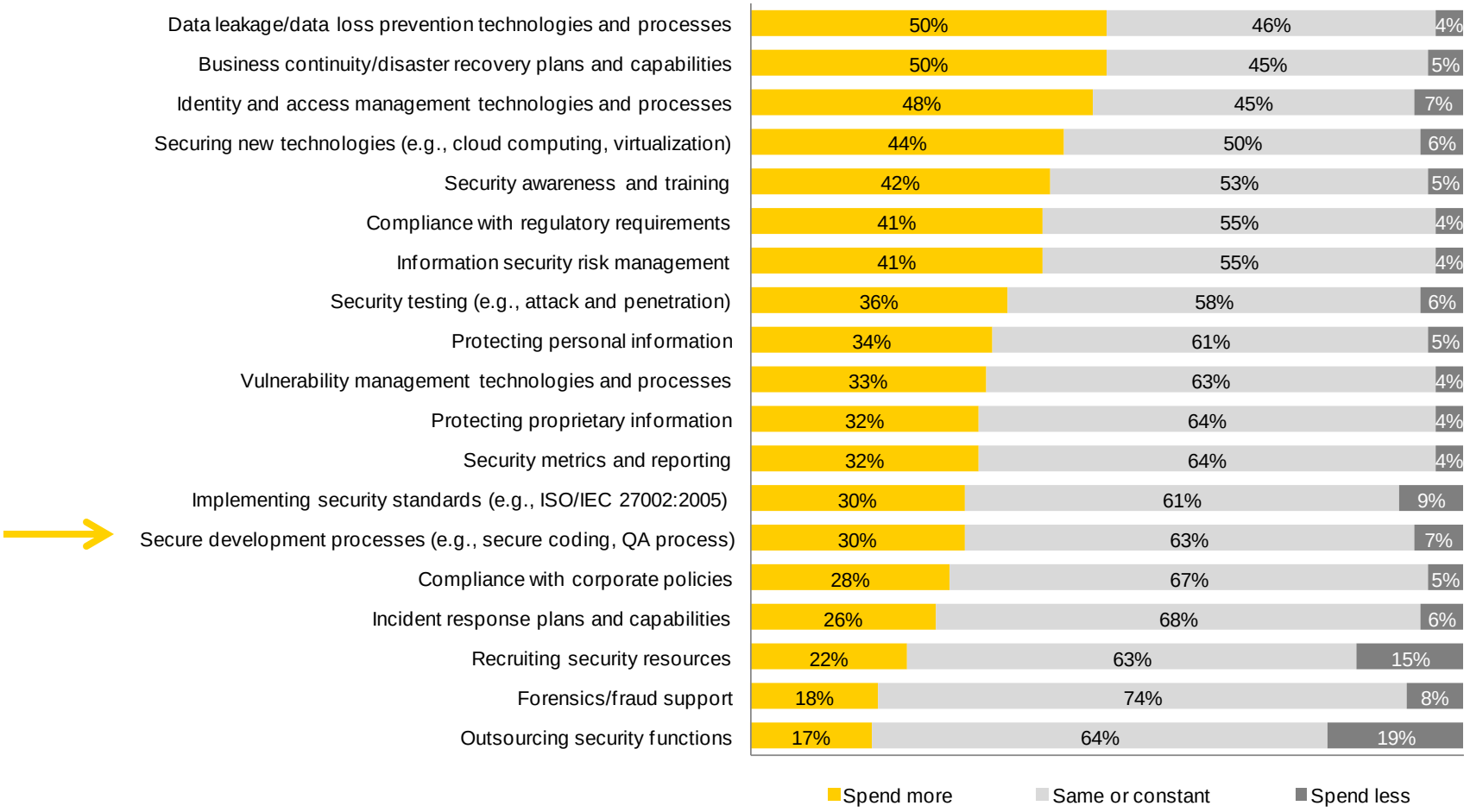
Global Information Security Survey

Please indicate your top five security priorities for the coming 12 months from the following list:



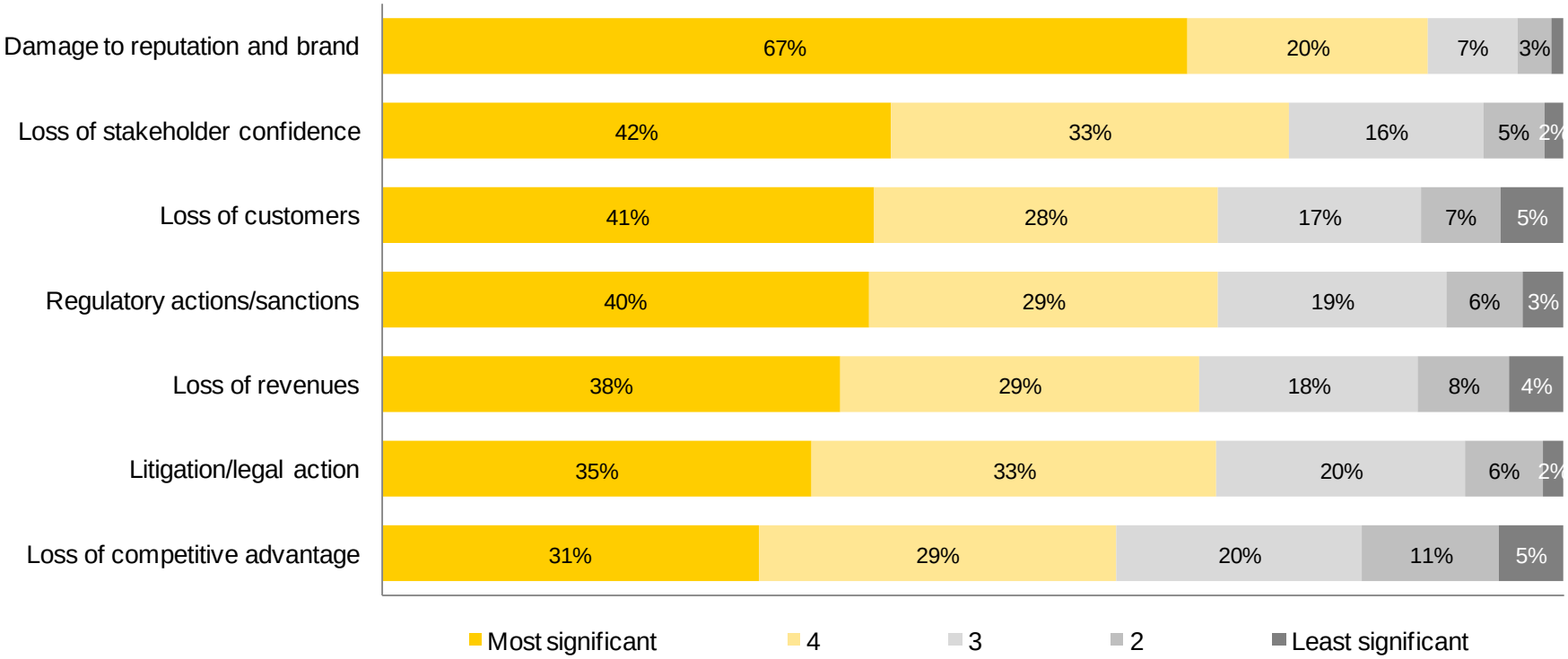
Global Information Security Survey

Compared to the previous year, does your organization plan to spend more, less or relatively the same amount over the next year for the following activities?



Global Information Security Survey

What is the level of significance for each of the following consequences if your organization's customer information is lost or stolen?



Our Arguments Countered

Financial advantages + some fringe benefits

Security Individual	C-Level Perception
It's cheaper to fix vulnerabilities early on. We'll save money!	Development will take longer. Application performance will be affected.
We're stuck in an endless cycle of assessments.	If we had an SDLC we'd stop testing? Doubtful.
The investment now will pay off over time: better software that's easier to maintain.	How long to realize savings? Gadgets mitigate risk. Development must be fast.
If software contains vulnerabilities, they'll be exploited!!!	Fallout from that is insignificant. The probability of occurrence is small.
Training will make developers better coders in addition to security-informed.	Developers can't be bothered. Let them code, they're already very good.

Let the developers do their jobs! Stop pushing security down their throats, it's ineffective. – Caleb Sima at RSA 2011

Summary

- Executives don't appreciate the age-old arguments. Their tolerance for and understanding of risk is different than ours.
- That does NOT mean they're right and we're wrong. Nor does it mean software assurance is a BAD idea.

  It means we're framing our arguments ineffectively!
- Currently, security is seen as a TAX. It needs to be seen as an enabler! Haven't we been making this business case for a while, too?

  Software assurance is an enabler of cost savings!
- We're going in circles…

The Way Forward

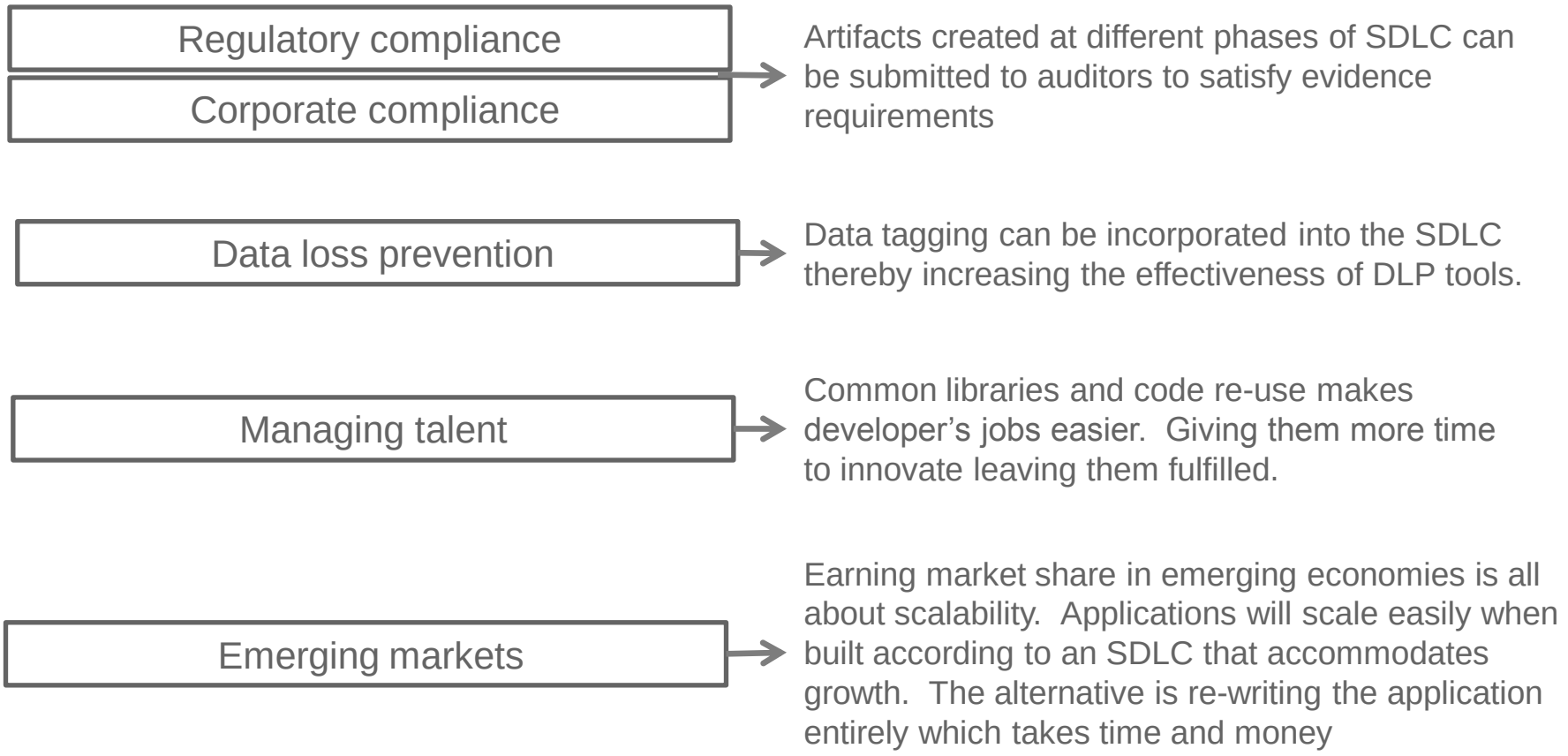
- Security IS an enabler, but for executive buy-in it needs to *enable the executive's priorities*:

Top 5 priorities revisited:

	CEO	CIO / CISO / IT Executive
1:	Regulatory compliance	Business continuity / Disaster recovery
2:	Access to credit	Regulatory compliance
3:	Slow economic recovery	Data loss prevention
4:	Managing talent	Information Security Risk Management
5:	Emerging markets	Corporate compliance

Some Ideas

The business case for software assurance doesn't need to include security… it just needs to address executive priorities. Security can be a value-add, not the main motivation.



Thank You

Joshua.Stabiner@ey.com

ERNST & YOUNG
Quality In Everything We Do