Socio-organizational Context of IS Security

Carol Hsu

Department of Information Management,
National Taiwan University

Spring 2009

Computer and Information Security

- Information communication technology (ICT) expands the boundary of information exchange, changes how individuals and organizations develop, process and store information

- How can organization protect information
  - Technical problem- certainly!
  - But also a socio-organizational problem

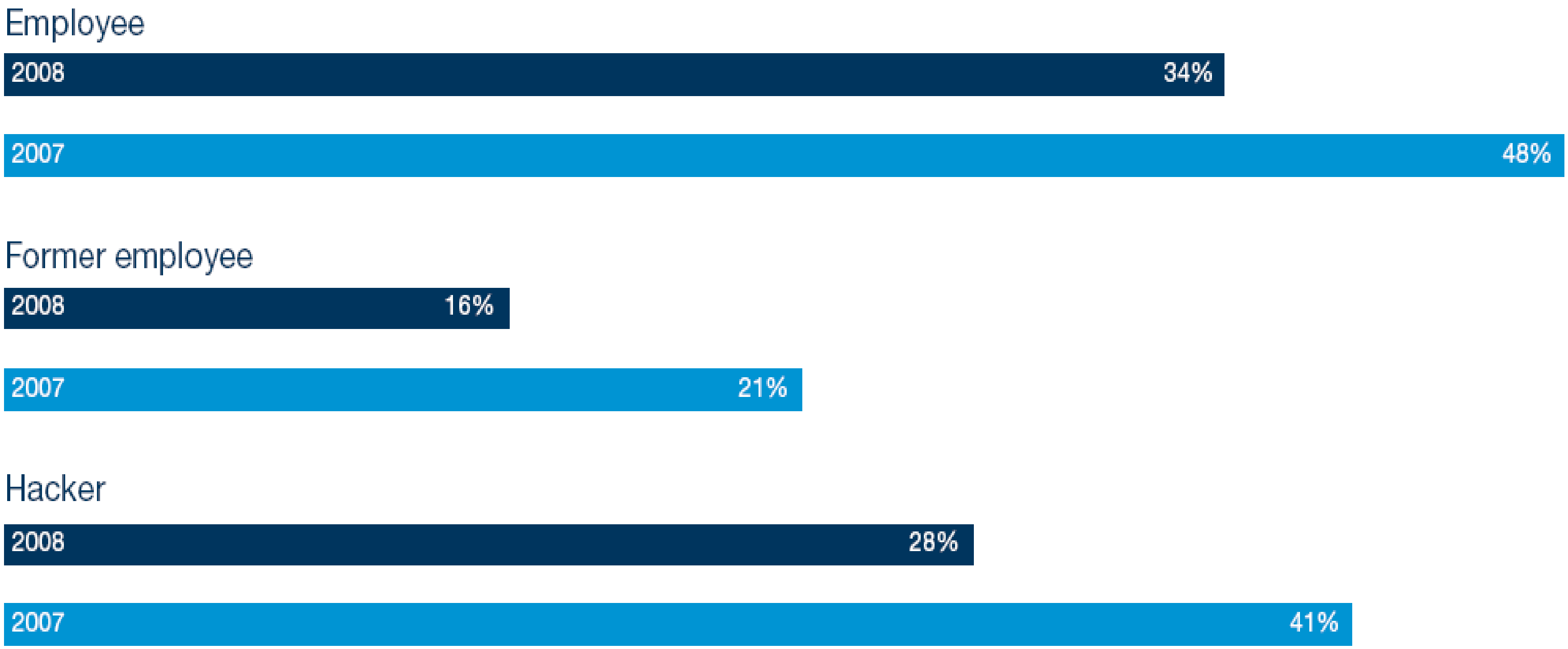
Examples of Industry Risk Events

- Nick Lesson & Barings Bank (1995)
- 11 September (2001)
- SARS (2003)
- Former bank branch manager at Commonwealth Bank stole 19mm of client money over a five year period. (August, 2003)
- Tokyo Stock Exchange (2005)
- Fubon Securities (2005)
- India call centre data leakage (2005)
- Eastern Home Shopping Network (2007)
- Societe Generale (2008)

Problems

- Hacking
- Virus
- Illegal physical access
- Abuse of privileges
- Acts of human errors
- Acts of Gods
- Terrorist attack

Estimated likely source of security incidents



[3]Other likely sources of security incidents cited in 2008 included customers (8%), service providers/contractors (8%), partners/suppliers (7%), terrorists (2%) and foreign governments (2%). Forty two percent (42%) of respondents didn't know. Data does not add up to 100%. Respondents were allowed to indicate multiple factors.

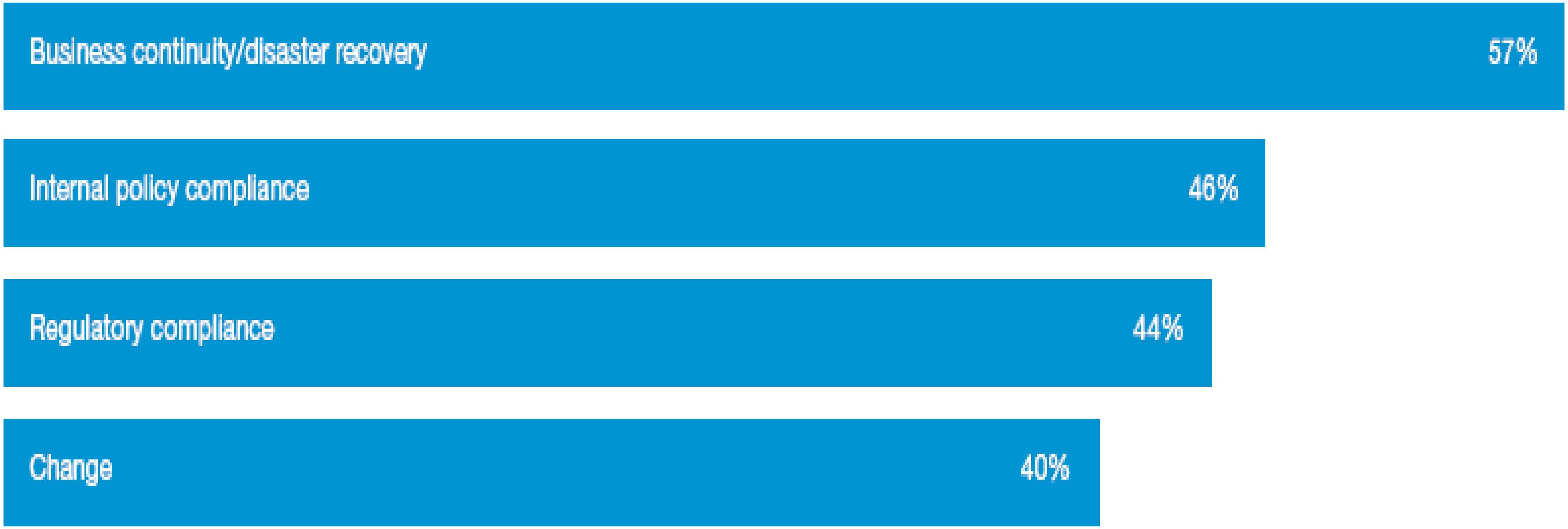
Source: The Global State of Information Security Survey®, 2008

(source: Pricewaterhousecooper)

Rising attention on socio-organizational context of IS security

- Industry practitioners
  - Commercial organizations, consultants, professional development
- Academics
- Regulators

For Commercial Organizations

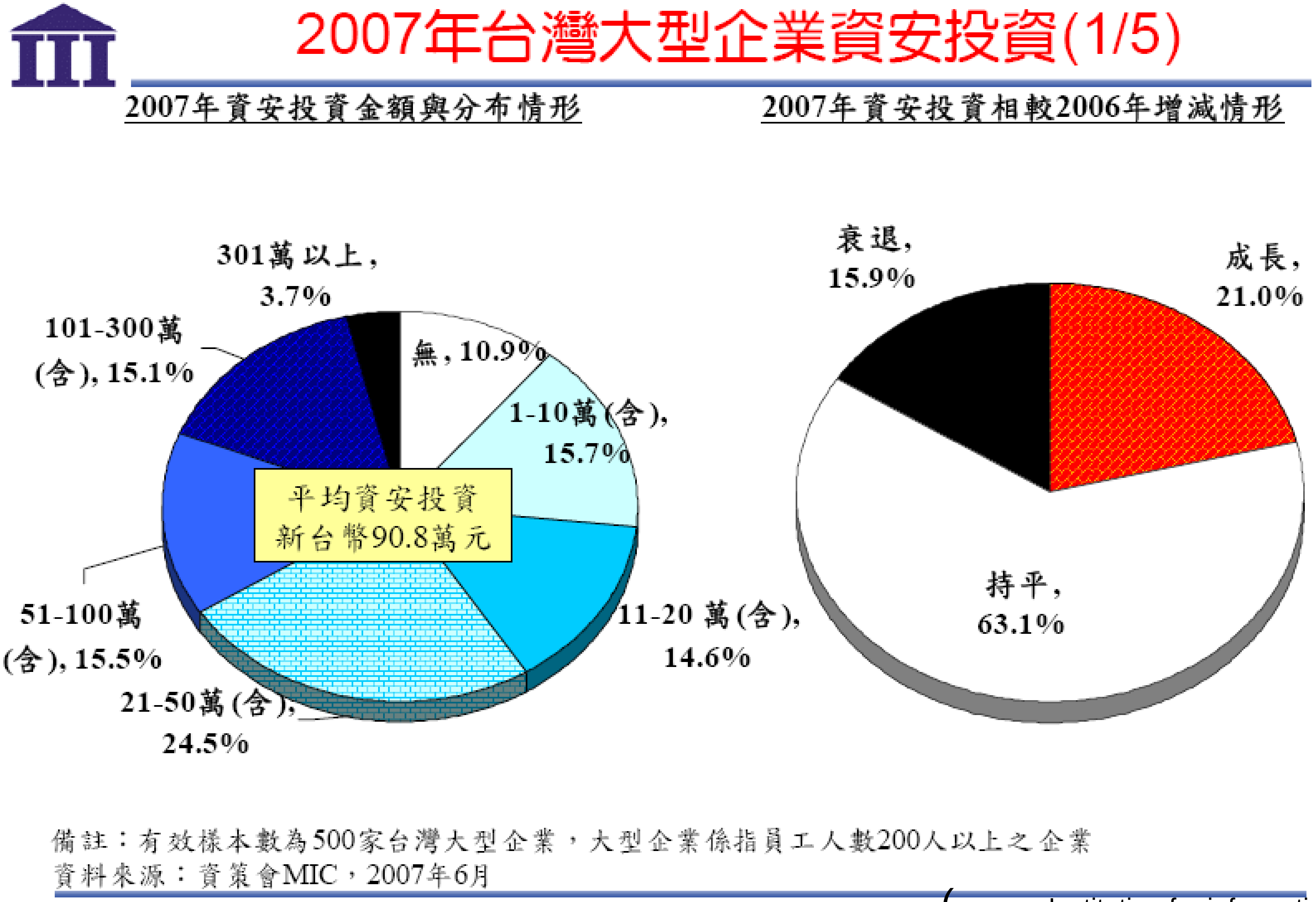


[1]Does not add up to 100%. Respondents were allowed to indicate multiple factors.

Source: The Global State of Information Security Survey®, 2006

(source: Pricewaterhousecooper)

Security Spending in Taiwan



2007年台灣大型企業資安投資(1/5)

2007年資安投資金額與分布情形

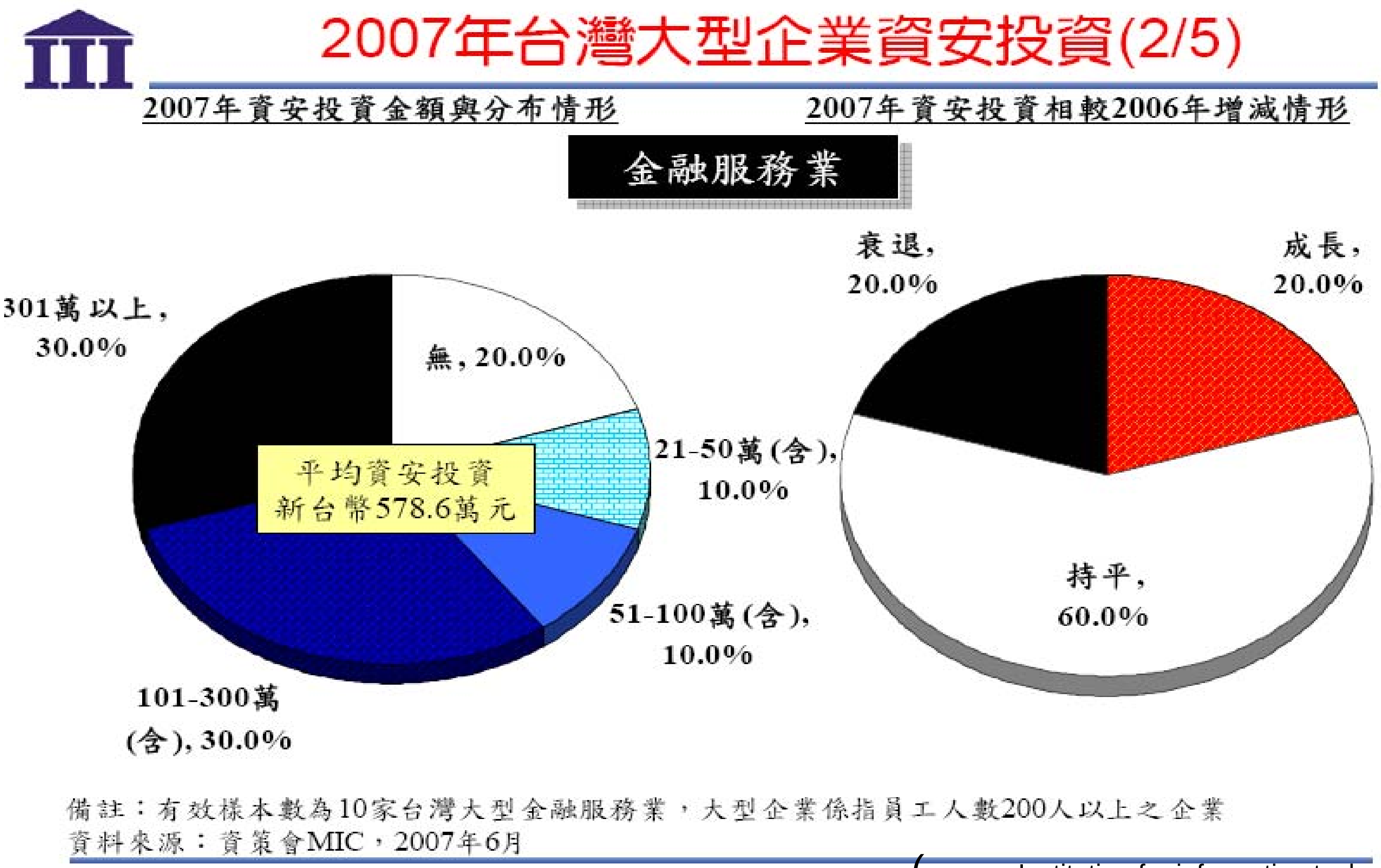
2007年資安投資相較2006年增減情形

備註：有效樣本數為500家台灣大型企業，大型企業係指員工人數200人以上之企業

資料來源：資策會MIC，2007年6月

(source: Institution for information technology)

Security Spending in Taiwan



2007年台灣大型企業資安投資(2/5)

2007年資安投資金額與分布情形

2007年資安投資相較2006年增減情形

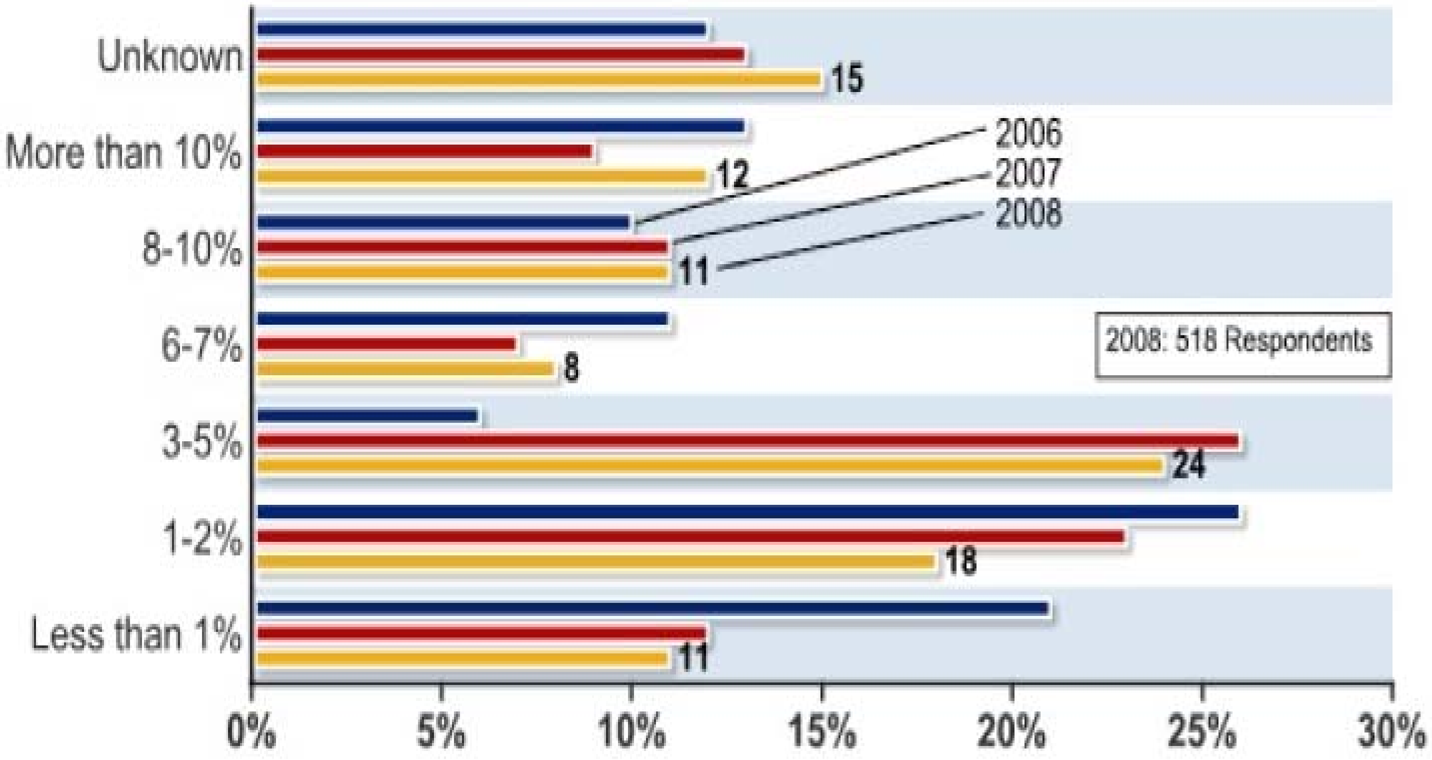
金融服務業

平均資安投資
新台幣578.6萬元

備註：有效樣本數為10家台灣大型金融服務業，大型企業係指員工人數200人以上之企業
資料來源：資策會MIC，2007年6月

(source: Institution for information technology)

Security Budget



(source: CSI-FBI survey)

Consultants-Annual IS Security Surveys

Consultancy Firms

Professional Development

- Professional certification
  - Certified Information Systems Auditor (CISA)
  - Certified Information Security Manager (CISM)

Professional Development- CISM

1. ***Information Security Governance (23%)***

   Establish and maintain a framework to provide assurance that information security strategies are aligned with the business objectives and consistent with applicable laws and regulations.

2. ***Information Risk Management (22%)***

   Identify and manage information security risks to achieve business objectives.

3. ***Information Security Program Development (17%)***

   Create and maintain a program to implement the information security strategy.

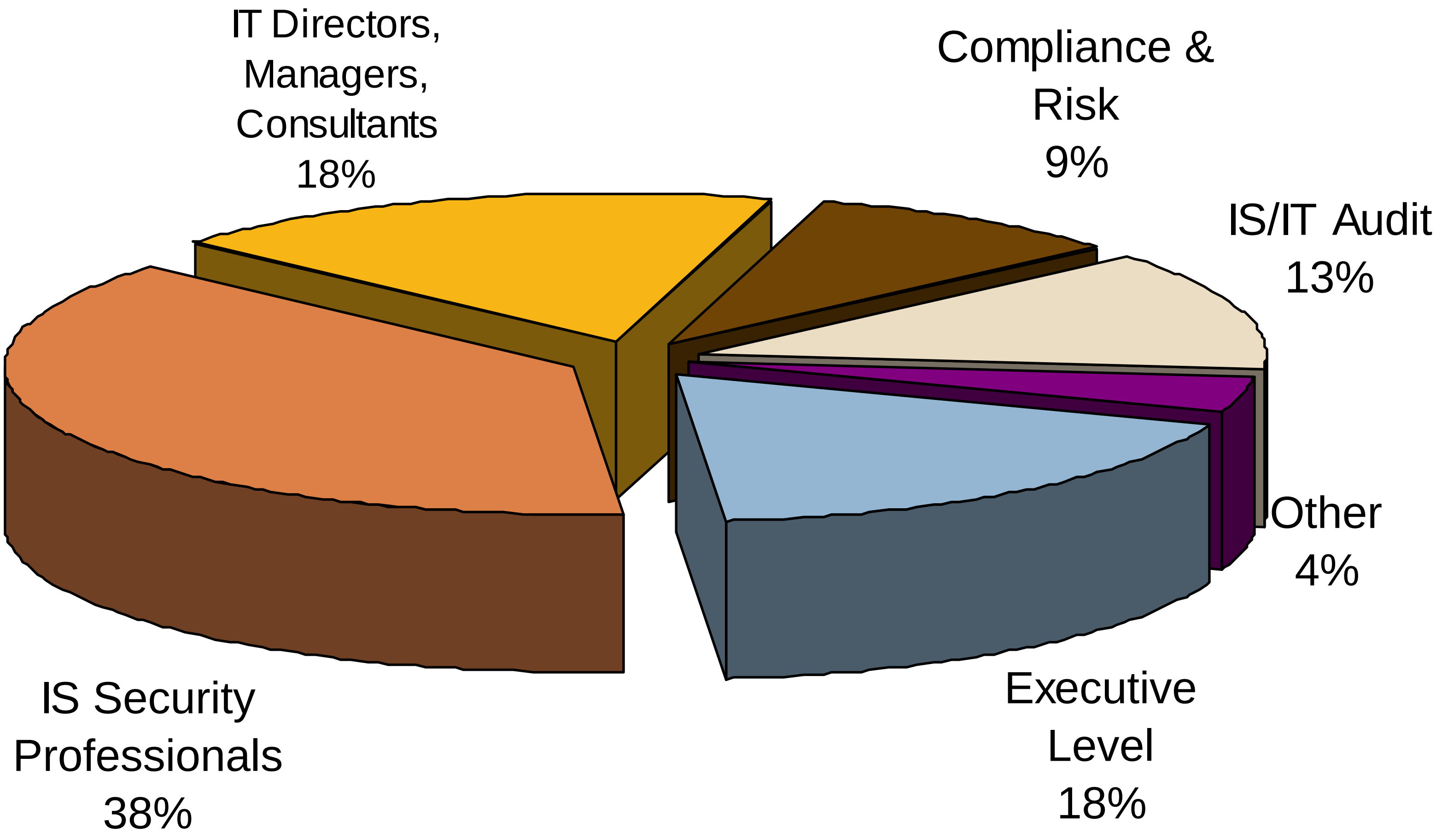
(source: ISACA)

Professional Development- CISM

4. ***Information Security Program Management (24%)***
   Design, develop and manage an information security program to implement the information security governance framework.
5. ***Incident Management and Response (14%)***
   Plan, develop and manage a capability to detect, respond to and recover from information security incidents.

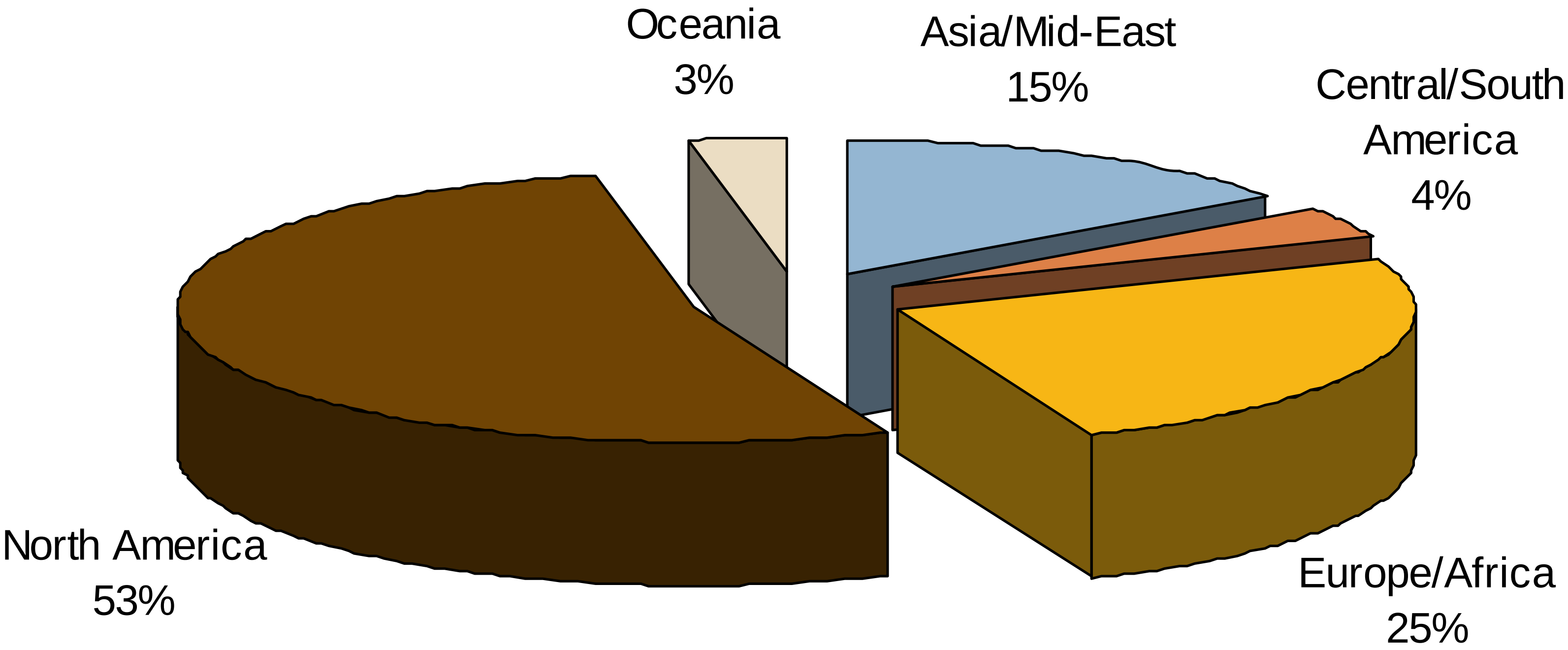
(source: ISACA)

Professional Development- CISM



(source: ISACA)

Professional Development- CISM



(source: ISACA)

Professional Development- CISA

1. ***IS Audit Process – 10%***

   Provide IS audit services in accordance with IS audit standards, guidelines, and best practices to assist the organization in ensuring that its information technology and business systems are protected and controlled.

2. ***IT Governance – 15%***

   Provide assurance that the organization has the structure, policies, accountability, mechanisms, and monitoring practices in place to achieve the requirements of corporate governance of IT.

3. ***Systems and Infrastructure Lifecycle Management – 16%***

   Provide assurance that the management practices for the development/acquisition, testing, implementation, maintenance, and disposal of systems and infrastructure will meet the organization's objectives.

(source: ISACA)

Professional Development- CISA

4. ***IT Service Delivery and Support – 14%***

   Provide assurance that the IT service management practices will ensure the delivery of the level of services required to meet the organization's objectives.

5. ***Protection of Information Assets – 31%***

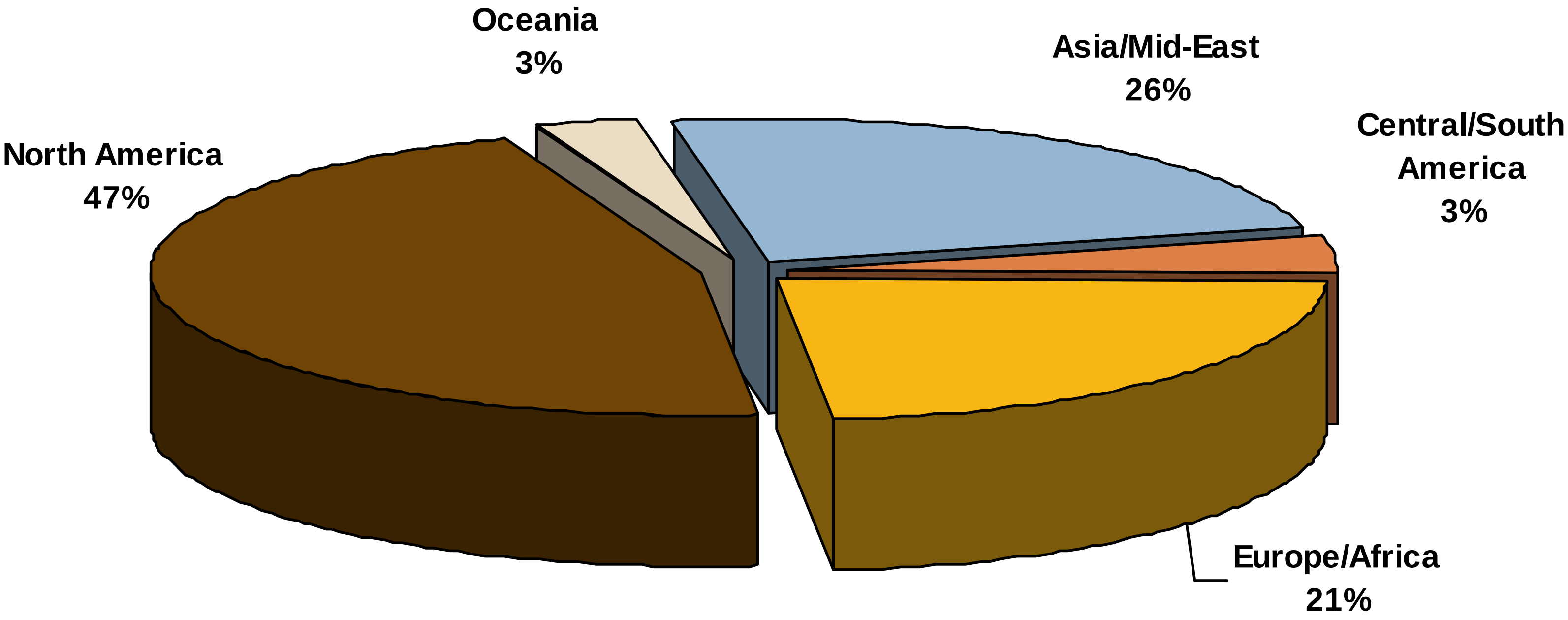
   Provide assurance that the security architecture (policies, standards, procedures, and controls) ensures the confidentiality, integrity, and availability of information assets.

6. ***Business Continuity and Disaster Recovery – 14%***

   Provide assurance that in the event of a disruption the business continuity and disaster recovery processes will ensure the timely resumption of IT services while minimizing the business impact.

(source: ISACA)

Professional Development- CISA



(source: ISACA)

Professional Development-CISA

□ Distribution in Asia (Sept 2007)

□	CISAs	CISMs
Hong Kong	1336	142
Japan	1412	138
Korea	2198	41
China	519	39
Singapore	819	125
Malaysia	187	17
Taiwan	108	23

□ As of Dec. 2008, 163 CISA professionals in Taiwan, 23% growth from Jan. Dec. 。

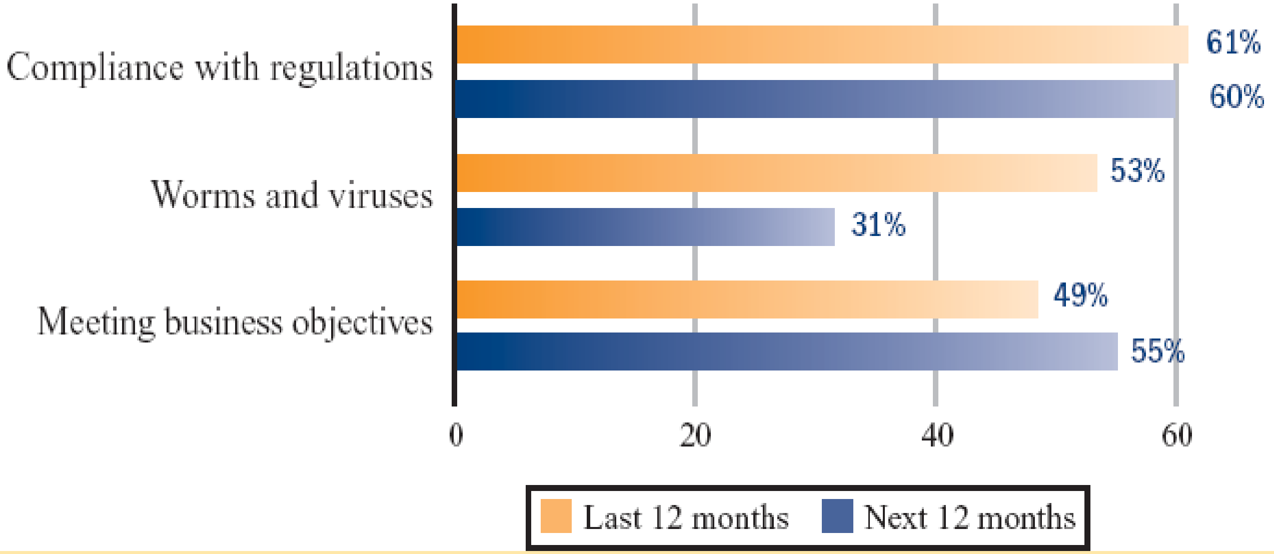
Academics

- MIS Quarterly, special issue on IS security managmeent

- “The increasing number of IS security incidents that organizations have confronted within the last few years suggests that much needs to be done to secure information and knowledge. Interestingly, most of the research on IS security to date has been at the technical level, carried out mostly by computer scientists, mathematicians, and computer engineers (Straub et al. 2008). Comparatively little work has taken a managerial point of view, covering broad organizational and social issues (Dhillon and Backhouse 2001; Straub et al. 2008). Scant work exists examining the *social implications of security technologies*. In addition, increasing interconnections and intercommunications between organizations in products and services value chains *require greater stress on behavioral, analytical, and empirical research in cyber security, privacy, and secure knowledge management*.”

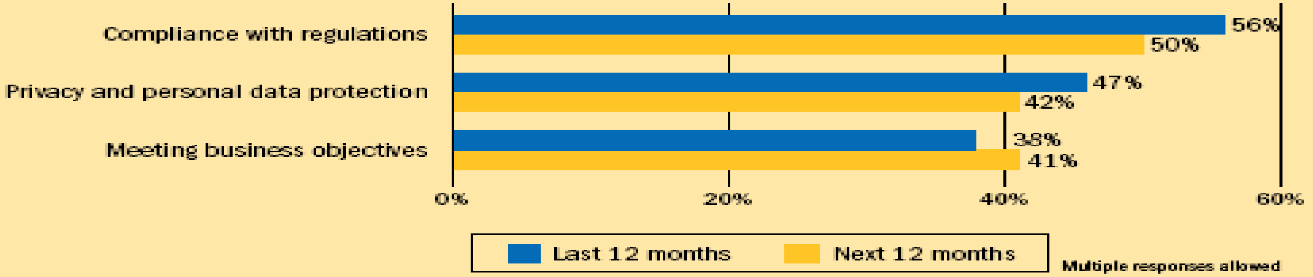
Regulators

- Compliance- E&Y Global Information Security Survey



Compliance is projected to be the primary driver of information security in the next 12 months.

Top three drivers that most significantly impacted or will significantly impact organizations' information security practices



Multiple responses allowed

Regulation

- Sarbanes-Oxley Act 2002 (SOX)
- Basel II
- Data Protection Act

Information Systems Security Management & Governance

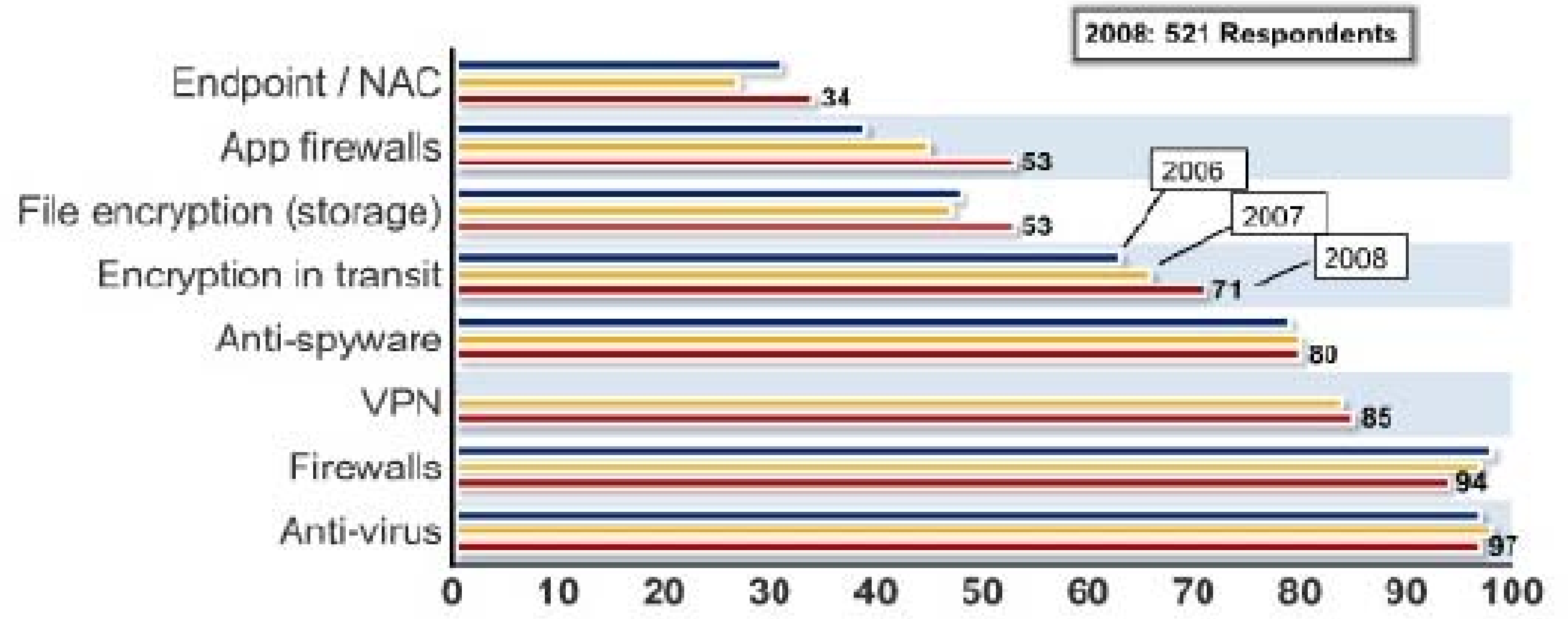
A Secured Organization…

- Technical
- Formal
- Informal

- Appropriate Security Technology
- Appropriate Security Policy
- Appropriate Education and Awareness Program

Technical Approach

Figure 16: Security Technologies Used



(Source: 2008 CSI/FBI Computer Security Survey)

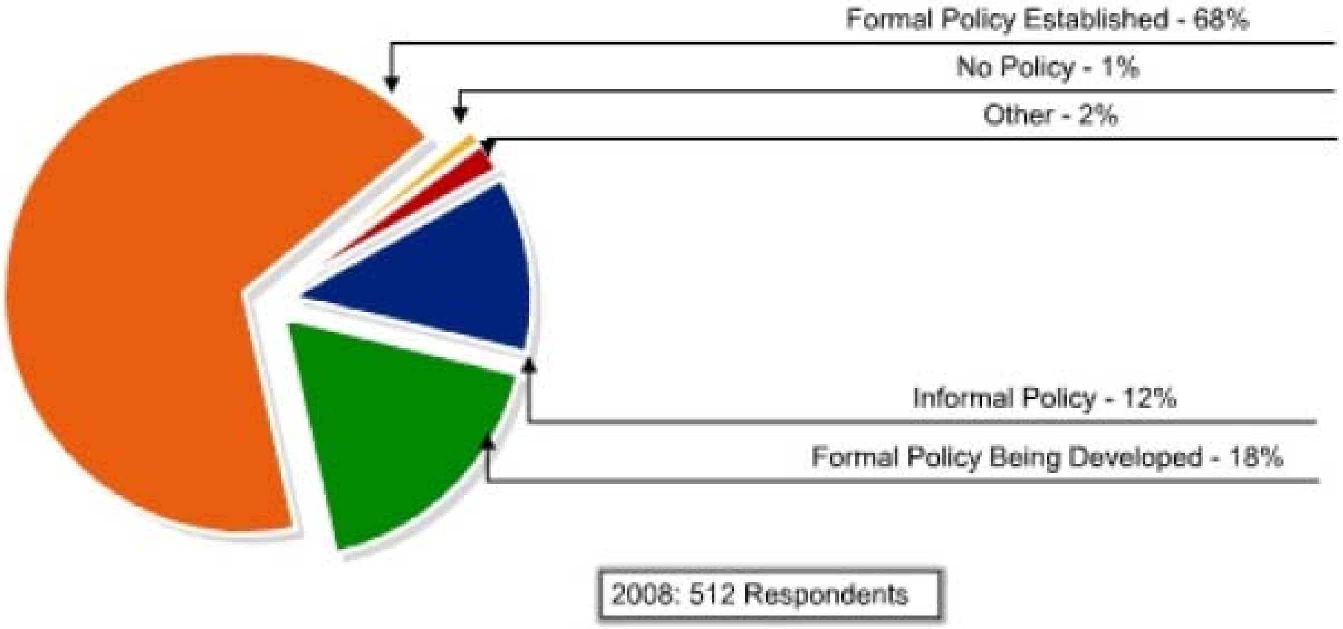
Formal Approach

- ISO/IEC 17799

- Security policy
- Management Committee
- Audit
- Risk management

Formal Approach

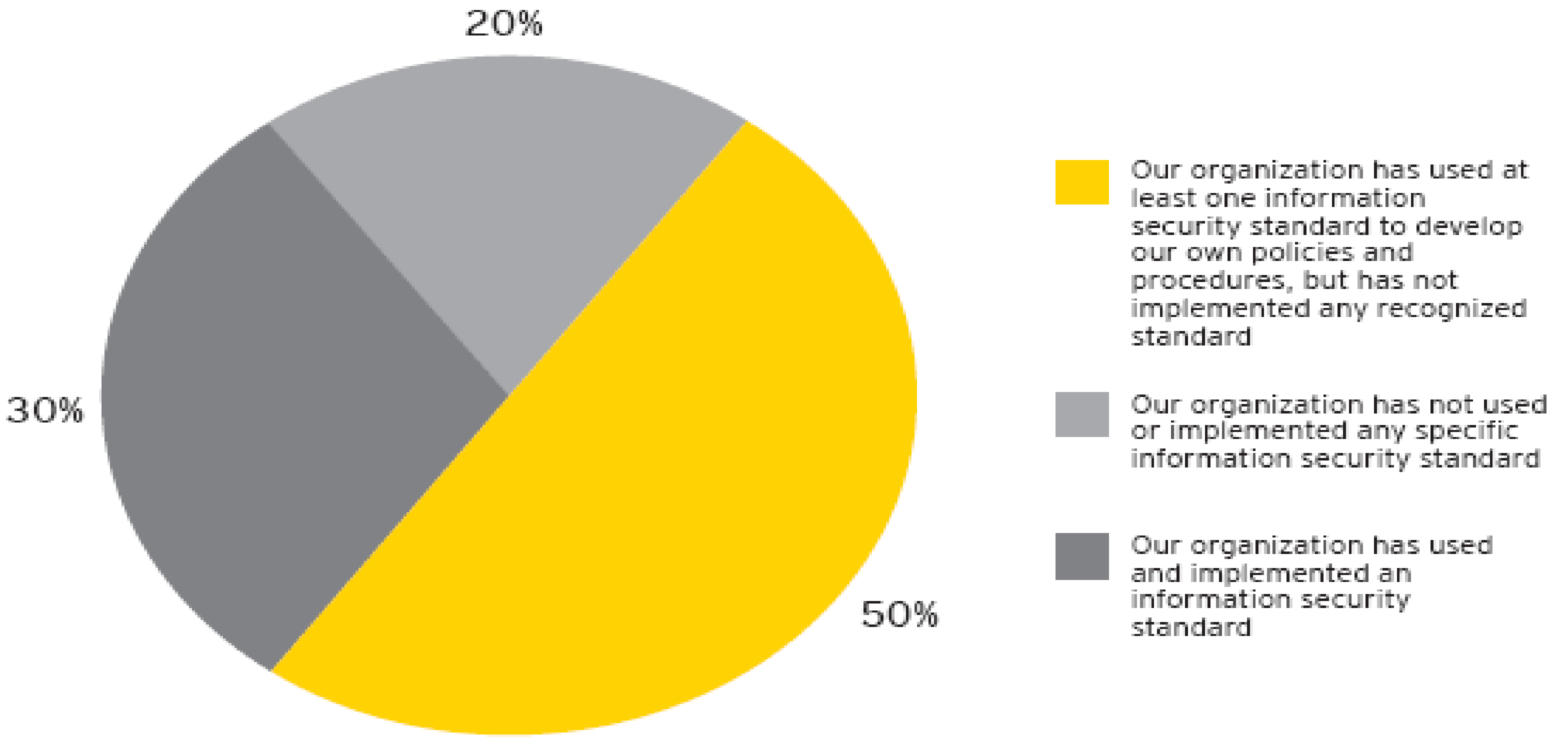
Figure 22: Information Security Policy w/n Your Organization



(Source: 2008 CSI/FBI Computer Security Survey)

Formal Approach

Which of the following statements best describes your organization's use of information security standards (e.g., ISO/IEC 27002:2005)?



🟨 Our organization has used at least one information security standard to develop our own policies and procedures, but has not implemented any recognized standard

⬜ Our organization has not used or implemented any specific information security standard

⬛ Our organization has used and implemented an information security standard

(Source: 2008 E&Y Global Security Survey)

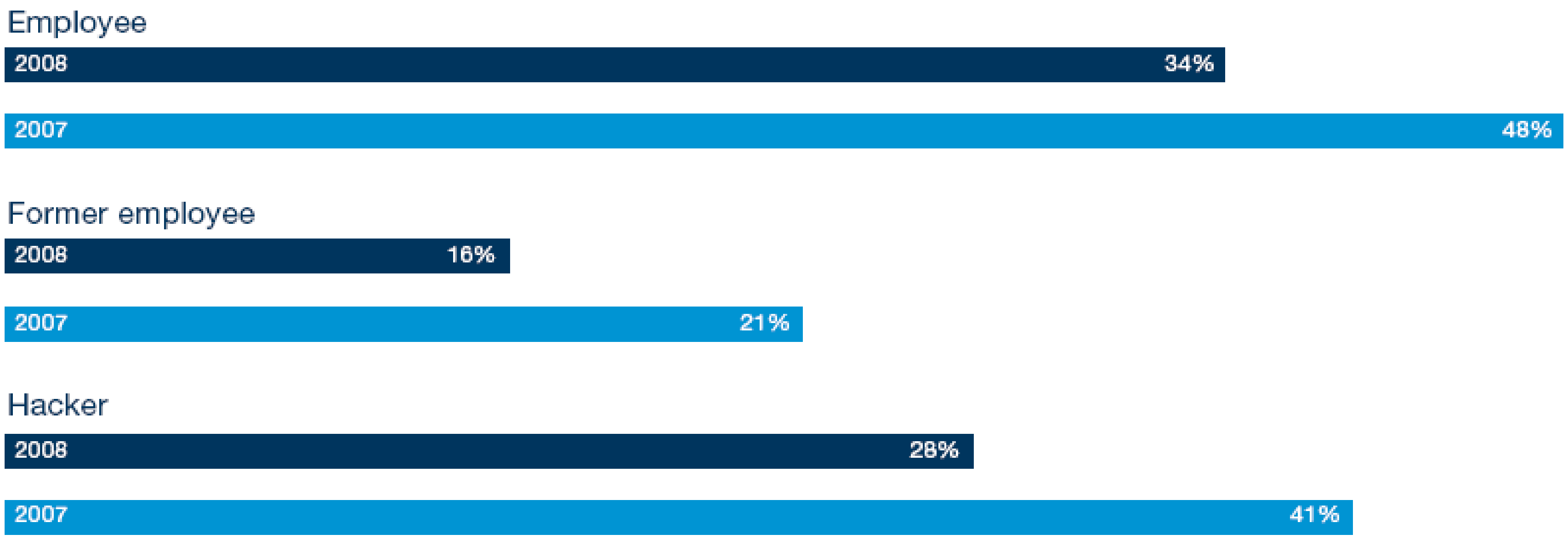
Informal Approach

- Social engineering
- Security awareness programme
- Security culture

Creation of Human Firewall!

Informal Approach

Figure 9: Estimated likely source of security incidents over the last 12 months[3]

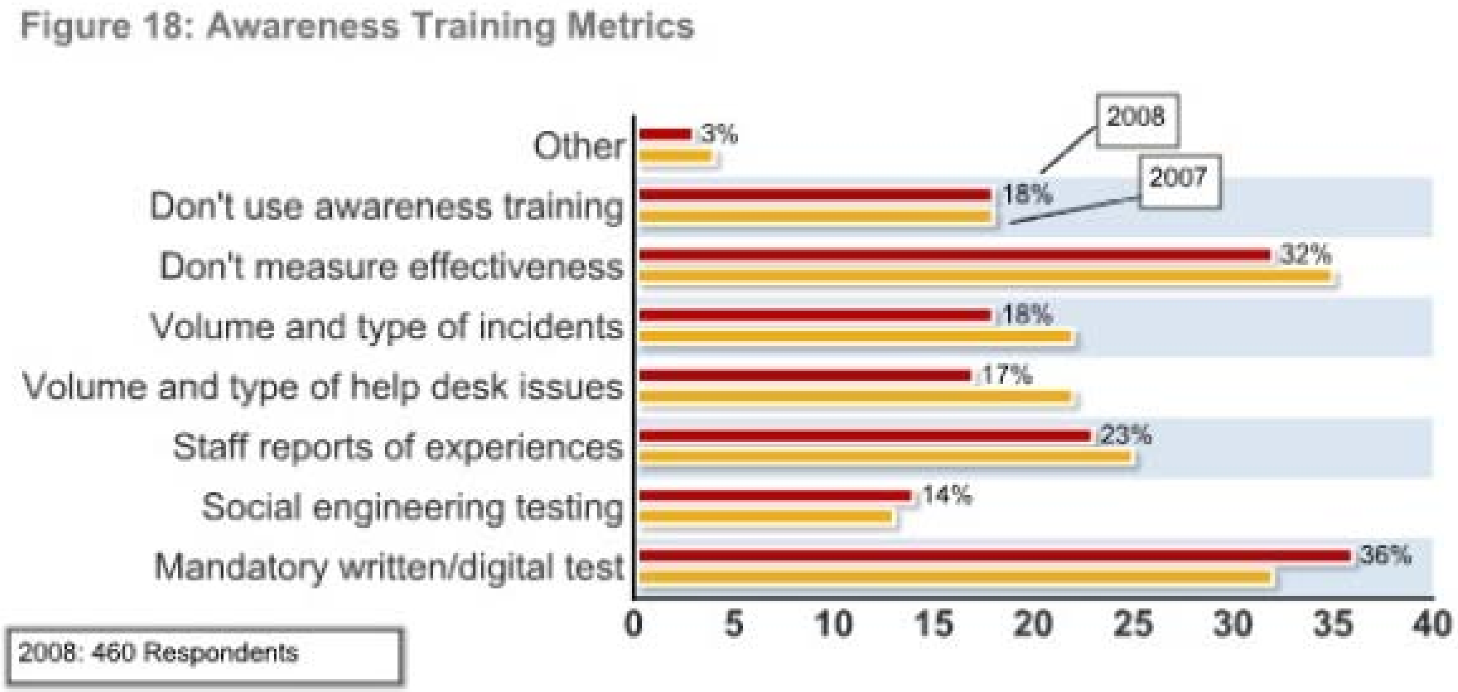


[3]Other likely sources of security incidents cited in 2008 included customers (8%), service providers/contractors (8%), partners/suppliers (7%), terrorists (2%) and foreign governments (2%). Forty two percent (42%) of respondents didn't know. Data does not add up to 100%. Respondents were allowed to indicate multiple factors.

Source: The Global State of Information Security Survey®, 2008

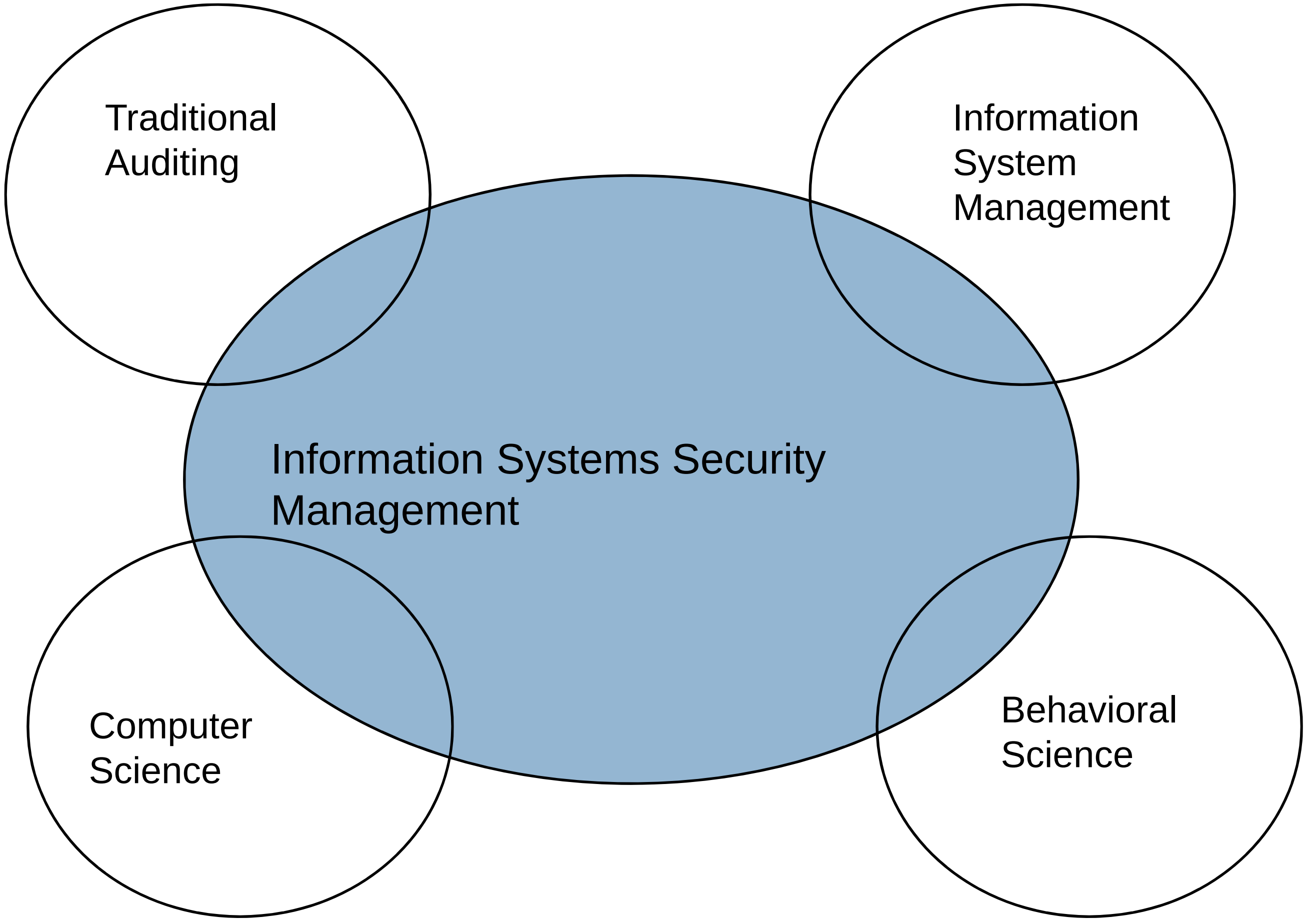
(source: Pricewaterhousecooper)

Informal Approach



(Source: 2008 CSI/FBI Computer Security Survey)

Information Security Management: Multi-discipline knowledge



Traditional Auditing

Information System Management

Information Systems Security Management

Computer Science

Behavioral Science

Source:Weber,1999

Information Security Management: Multi-discipline knowledge

- □ *Traditional Auditing*
  - Internal Control Principle
- □ *Computer Science*
  - Security Technology

- □ *Information Systems Management*
  - Information System Design
- □ *Behavioral Science*

  - *Organizational Behavior*

BUT……….

WHERE IS THE ECONOMIC/BUSINESS VALUE OF SECURITY?!?!

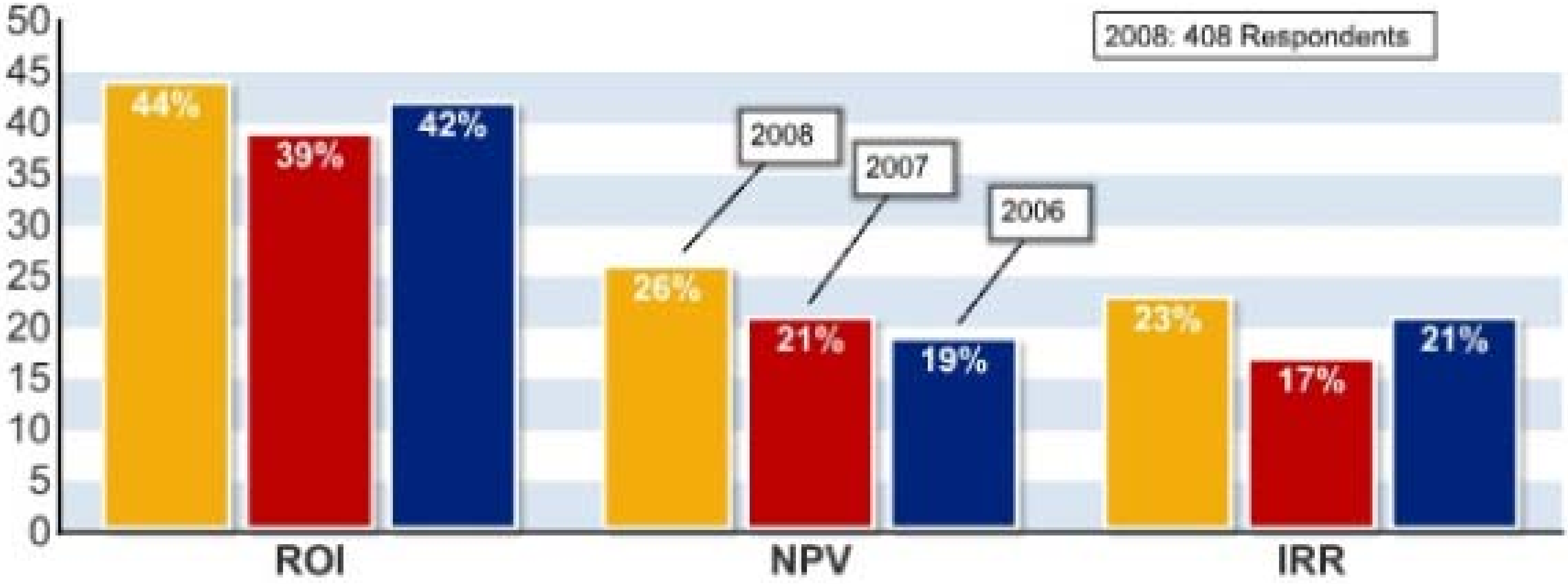
Security also comes with cost

" Security is *not an isolated good*, but just one component of a complicated transaction. It costs money, but it also it in intangibles: time, convenience, flexibility, or privacy"

Schneier, beyond Fear, 2003

Business Justification

Figure 7: Percentage Using ROI, NPV, and IRR Metrics



(Source: 2008 CSI/FBI Computer Security Survey)

Alignment Issue

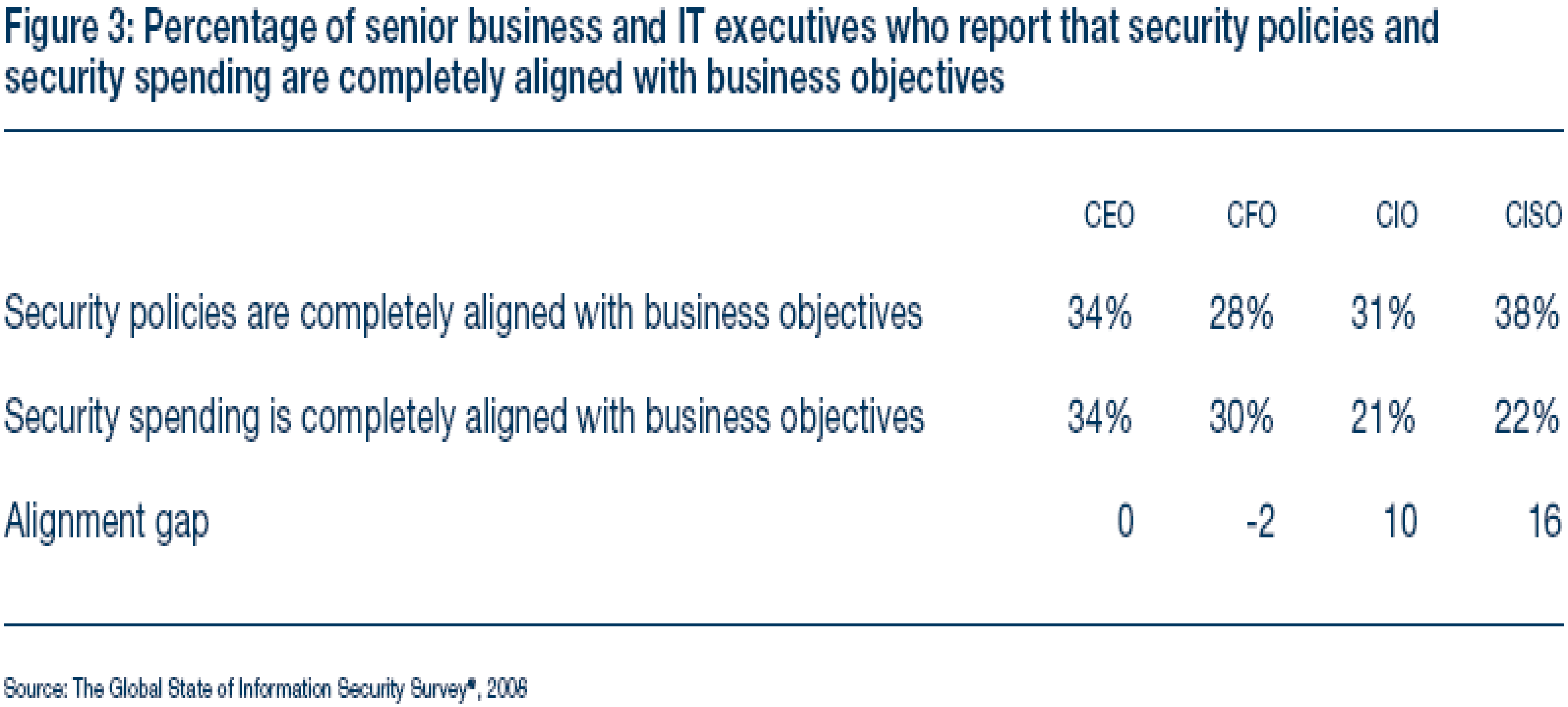
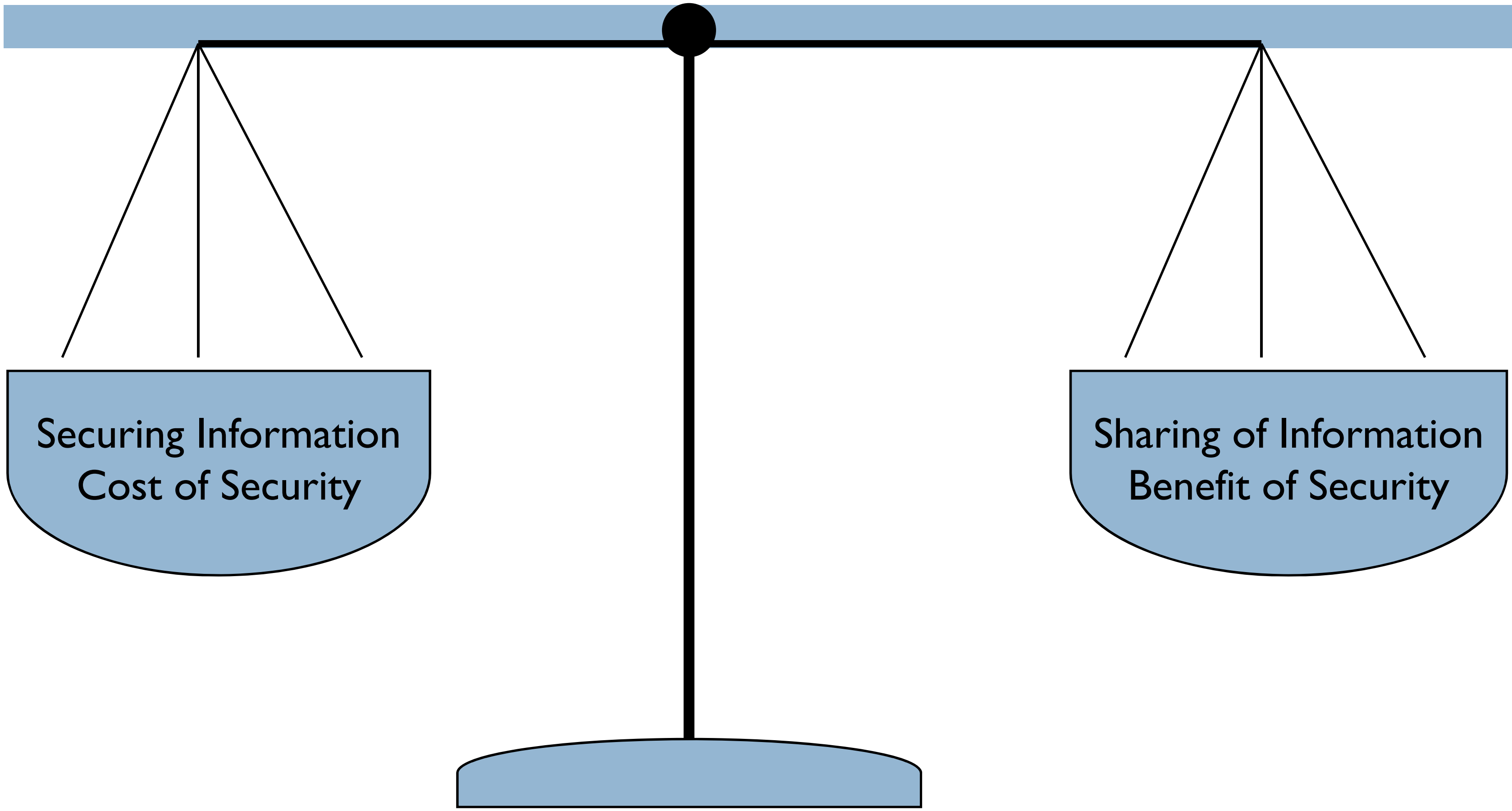


Figure 3: Percentage of senior business and IT executives who report that security policies and security spending are completely aligned with business objectives

	CEO	CFO	CIO	CISO
Security policies are completely aligned with business objectives	34%	28%	31%	38%
Security spending is completely aligned with business objectives	34%	30%	21%	22%
Alignment gap	0	-2	10	16

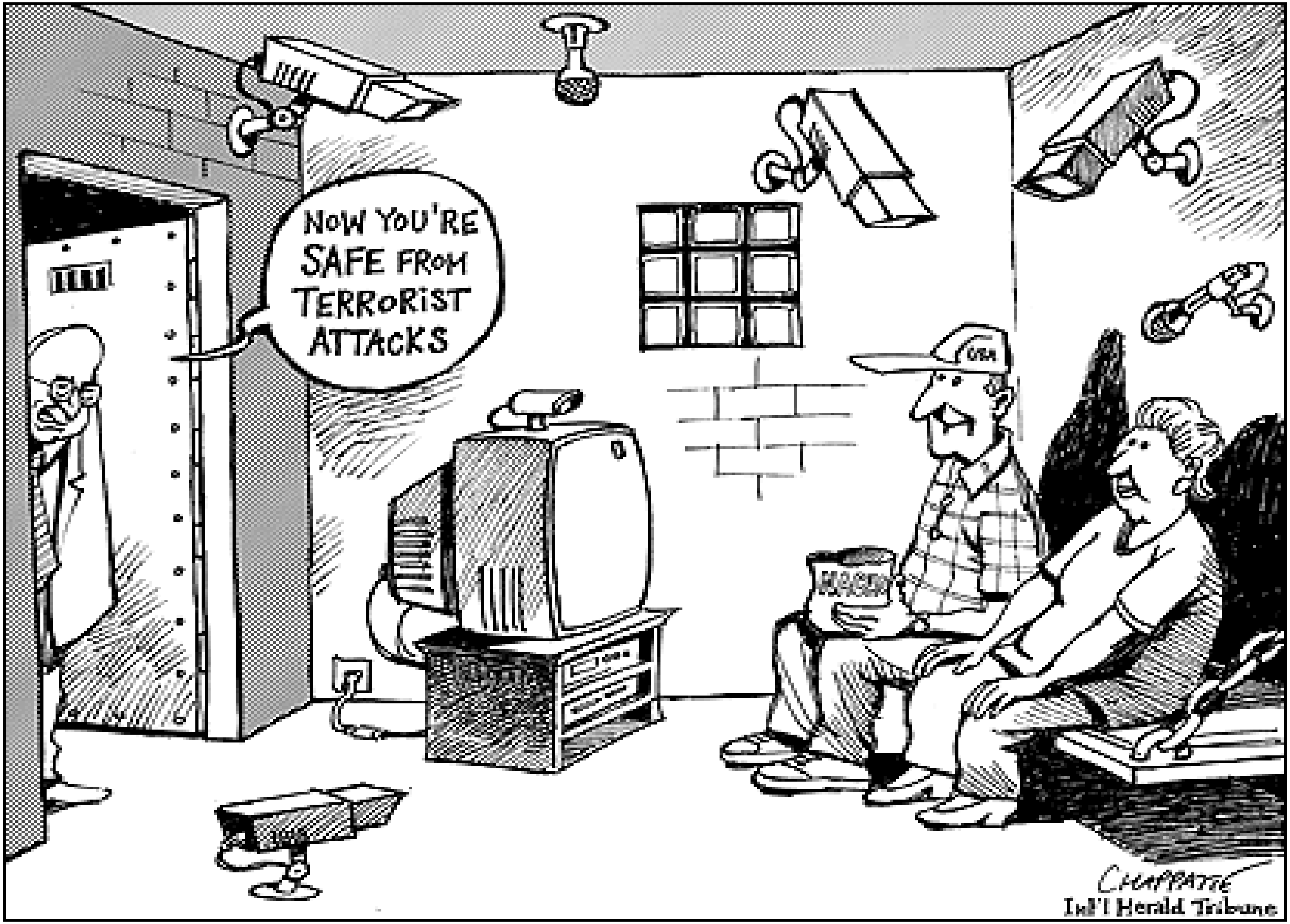
Source: The Global State of Information Security Survey®, 2006

So..What Information Security is about…



Securing Information
Cost of Security

Sharing of Information
Benefit of Security


NOW YOU'RE SAFE FROM TERRORIST ATTACKS
USA
CHAPPATTE
Int'l Herald Tribune