

The Global State of Information Security 2005

**What the numbers say:**

**22%**

Percentage of financial executives who report that phishing activities have misappropriated the company's identity and affected the corporate brand.

**3 in every 4**

Percentage of financial services firms (73%) monitoring employee use of the Internet or information assets. This is almost twice the rate reported last year (39%).

**54%**

Percentage of financial services firms that have both measured and reviewed the effectiveness of their security policies and procedures in the past 12 months. (Up from 51% in 2004.)

**50%**

Number of financial services companies that do not have a mechanism in place to report security incidents to customers or business partners.

For the third year in a row, PricewaterhouseCoopers and CIO magazine have teamed up to conduct the world's largest security study. This year, the State of Information Security 2005 reveals how financial services companies continue to lay the foundation for an increasingly strategic approach to information security.

- Financial services firms are setting the pace in security. 57% of executives in financial services report that their organizations have developed an overall security strategy process – compared to 37% of respondents in other industries. And 74% of these industry executives (vs. 56% among others) now engage both business and IT decision makers in addressing security issues – up from 70% in 2004 and 63% in 2003.
- Financial services companies stand out in addressing privacy safeguards. For example, the industry is much more likely than others to encrypt the transmission of data (72% vs. 51%); provide employees with training and awareness of privacy policies (74% vs. 58%); and secure web transactions (75% vs. 54%).
- Events are happening less often. In 2005, more executives (43%) reported zero negative security-related events than did last year's executives (25%), and another 43% claim fewer than 10 events in the past 12 months.
- When events do occur, they take a toll. Although 37% of executives reported no downtime and another 52% experienced system outages for 8 hours or less, financial services companies were more likely than companies in other industries to suffer financial losses (82% vs. 71%), compromises to brand or reputation (80% vs. 64%) and legal actions related to fraud (50% vs. 35%).

## Survey Methodology:

The State of Information Security 2005, a worldwide security survey by PricewaterhouseCoopers and CIO Magazine, was conducted online from March 14 through April 23, 2005. Readers of CIO Magazine, CSO Magazine and clients of PricewaterhouseCoopers from around the globe were invited via email to take the survey. The results discussed in this report are based on the responses of over 8,200 CEOs, CFOs, CIOs, CSOs, vice presidents and directors of IT and information security from 63 countries. The margin of error is 1%.

Of the 1,151 respondents in financial services (14% of survey), 53% were from North America, 25% from Europe, 13% from Asia, 8% from South America, and 2% from the Middle East and Africa. Forty-seven percent reported annual revenues of at least \$500 million.

## Critical areas needing improvement

Leadership in security is a good sign, but it is not clear that financial services companies have achieved a strategic approach to security. Strategy, along with data protection, continue to require attention.

### The alignment gap

An overwhelming majority of financial services executives (93%) report that security policies are aligned with their company's business objectives—understandable, given their work in recent years on developing policies. A lesser majority (77%) believe that security spending is aligned with their business.

### Integration is still elusive

Most financial services executives (55%) report that their organization is not linking security to privacy and/or regulatory compliance, either through organizational structure or policies. And 45% report that their company treats IT and physical security separately.

### Red flags in data protection

Compromise of confidential customer records is an increasingly strategic business risk for many financial services companies, yet most respondents (59%) reported that their company does not include "classifying the value of data" in the organization's security policies. Moreover, 56% reported that their organization does not have an accurate inventory of user data.

<b>Financial services: security benchmarks (Percentage of responses from financial services executives)</b>	<b>2005</b>	<b>2004</b>
Security spending (as % of IT budget)	11.8%	9.9%
Reported no security attacks in past 12 months	43%	25%
Reported from 1 to 9 security attacks in past 12 months	43%	57%
Had privacy audited by third-party	54%	48%
Employs a Chief Information Security Officer (CISO) or Chief Security Officer (CSO)	70%	54%

To learn more about the survey, or about information security services offered by PwC Advisory, visit:

[www.pwc.com/security](http://www.pwc.com/security)

or contact:

Mark Lobel, (646) 471-5731, [mark.a.lobel@us.pwc.com](mailto:mark.a.lobel@us.pwc.com) or  
Jerry Lewis, (214) 754-7425, [jerry.w.lewis@us.pwc.com](mailto:jerry.w.lewis@us.pwc.com).

(\*PricewaterhouseCoopers' refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity.)

© 2005 PricewaterhouseCoopers. All rights reserved. PricewaterhouseCoopers refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity. \*connectedthinking is a trademark of PricewaterhouseCoopers LLP