

The global state of information security 2006

**What the numbers say:**

**35%**

Percentage of financial services firms that do not engage both business and IT decision-makers in addressing information security issues.

**1:1**

Ratio of the number of financial services firms that ensure the secure disposal of their technology hardware to the number that do not.

**52%**

Percentage of financial services respondents who report their organization doesn't use patch management tools. However, 24% replied that attackers exploited known application or operating system vulnerabilities.

**56%**

Percentage of financial services firms that do not keep an inventory of third parties using customer data.

Results from the world's largest information security study are in. This year, responses to PricewaterhouseCoopers' and CIO magazine's Global State of Information Security study reveal that, for the third year in a row, financial services companies are spending more of their IT budget on information security, with the majority (55%) expecting spending to increase over the next 12 months. But the survey also reveals that, while financial services firms continue to set many of the highest benchmarks in safeguarding security and privacy, their programs still reflect several critical areas requiring executive attention.

- Strong leadership in security and privacy: Financial services firms are still significantly more likely than companies in other industries to employ a chief information security officer or chief security officer (75% vs. a 43% cross-industry average), have a plan for business continuity and disaster recovery (75% vs. 50%), secure web transactions (74% vs. 53%), and post privacy policies on their internal websites (57% vs. 46%).
- But progress has slowed: Financial services firms have not, however, improved many security capabilities significantly beyond levels they achieved last year. They're no more likely to have established an overall security strategy (57% vs. 57% in 2005) or improved security standards and procedures for handheld and portable devices (40% vs. 40%), the latter despite published and unpublished incidents involving the loss or theft of executive laptops containing sensitive data.
- And responses reveal gaps in awareness: When asked about security-related attacks, more than 3 in 10 respondents were either unaware or uncertain about critical factors affecting their organization's security environment. Thirty percent couldn't estimate the number of security attacks in the last 12 months, 32% didn't know the type of attack, and 32% weren't sure about which class of vulnerabilities had been exploited.

## Survey Methodology:

The State of Information Security 2006, a worldwide security survey by PricewaterhouseCoopers and CIO magazine, was conducted online from April 5 to May 22, 2006. Readers of CIO magazine and 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 7,791 responses from IT and security professionals in 50 countries. Respondent titles included CEO, CFO, CIO, CSO, and vice president, director, and manager of IT and information security. The margin of error is  $\pm 1\%$ .

Of the 772 respondents from companies in the financial services industries (10% of survey), 45% were from North America, 28% from Europe, 14% from Asia, and 12% from South America. Forty percent reported annual revenues of at least \$500 million.

To learn more about the survey, or about the Security and Privacy practice at PwC, visit:  
[www.pwc.com/GISS2006](http://www.pwc.com/GISS2006)

or contact:  
Mark Lobel  
646.471.5731  
[mark.a.lobel@us.pwc.com](mailto:mark.a.lobel@us.pwc.com)

Kurt Gilman  
646.471.8830  
[kurt.gilman@us.pwc.com](mailto:kurt.gilman@us.pwc.com)

## Critical areas needing improvement

### Security user awareness and training

Low awareness responses indicate that financial services companies are not focusing enough on training and education. In fact, only 6 out of 10 conduct security awareness training for employees and only 55% have personnel dedicated to improving employee security awareness.

### Metrics and measurement

Building awareness requires measuring activity and developing a strong set of management metrics that can be used to improve security-related outcomes. But responses reveal that 36% of financial services firms have not measured and reviewed the effectiveness of their information security policies in the past year. Also, most have not established security policies that include security monitoring standards (53%) or security metrics collection and management reporting (71%).

### Access and privilege management

Financial services firms need to improve control over who has access to their systems and information. When asked to identify likely sources and types of attack this year, 55% of financial services executives pointed to either current or former employees and 20% cited the abuse of valid user accounts and permissions. Only 31% of financial services firms have identity management solutions in place and only 37% have tiered authentication levels based on user risk classifications. In addition, 80% of executives in financial services reported that their organization does not revoke access privileges through automated account deprovisioning.

### Data integrity and protection

Among the most crucial security challenges for many financial services firms today is protecting data beyond the datacenter. Companies need to identify where sensitive data resides within the organization and how it flows across infrastructure, peripherals, and portable devices. But while 68% of financial services encrypt data in transmission, less than half (43%) encrypt stored data, and only 42% keep an accurate inventory of user data.

Financial services: security benchmarks (Percentage of responses from financial services sector)	2006	2005	2004
Security spending (as % of IT budget)	16.3%	11.8%	9.9%
Employ a CISO or CSO	75%	70%	54%
Ensure that security policies include procedures with which partners must comply	46%	40%	34%
Use organizational structure or policies to link security with compliance	47%	45%	43%

