

The Global State of Information Security 2005

**What the numbers say:**

**81%**

Percentage of public sector respondents confident in the effectiveness of their information security practices. This number is up from 75% in 2004.

**37%**

Percentage of public sector respondents who report that their organization conducts penetration testing. This is up from 27% in 2004.

**3 in every 10**

Number of government organizations that do not have a mechanism in place to report security incidents to constituents or other organizations.

**61%**

Percentage of government organizations that conduct active monitoring of security intelligence. This number is more than twice as high as it was in 2004 (28%).

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 that, on average, public sector organizations in countries around the world aren't just doing a better job than the private sector in addressing information security — they're also making significant year-on-year progress in their own right.

Faced with challenges in securing government computer systems and critical infrastructure, complying with regulations and protecting constituents' private information, government organizations have boosted spending over the past year on information security by 43%. The impacts of this investment are already evident.

- In protecting the privacy of constituent information, public sector entities are more likely than private sector industries to employ a Chief Privacy Officer (20% vs. the cross-industry average of 17%), post privacy policies on internal websites (55% vs. 47%) and provide employees with privacy awareness training (63% vs. 58%).
- Public sector entities are also ahead in establishing core security practices. They're more likely than the private sector to have an overall security strategy in place (44% vs. 37%), integrate IT security with physical security (39% vs. 31%), and conduct periodic security audits (57% vs. 50%).

These efforts appear to be paying off. More government respondents reported no negative security-related events in 2005 (31% vs. 21% in 2004). When events did occur, however, they took a toll: among government responders, 61% report financial losses, 48% cite theft of intellectual property, 44% report loss or damage to internal records and 28% say confidential records were compromised.

## 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 1,241 public sector respondents (15% of survey), 45% were from North America, 23% from Europe, 18% from South America, 12% from Asia, and 1% from the Middle East and Africa.

## Critical areas needing improvement

### Annual measurement and review

Most government entities are required to adhere to specific security requirements – regulations such as Australia’s Federal Privacy Act, the United Kingdom’s Turnbull Report, the EU Data Protection Directive, and the United States Federal Information Security Management Act (FISMA). Common to most of these is the need to conduct annual measurement and review. This is clearly still a challenge for most public entities: government survey responses reveal that 6 out of every 10 entities do not both review and measure the effectiveness of their security practices on an annual basis.

### Policy compliance and spending alignment

On average, public sector respondents believe that 32% of their users are not in compliance with their organization’s security policies. This figure may explain, in part, why public sector entities are more than twice as likely to audit user policy compliance this year (53%) than last (24%). But a gap still exists in spending alignment: while 74% of government respondents report that their security policies are aligned with their organization’s objectives, only 57% agree that spending on security is similarly on target.

### Data protection

For almost any public service organization, data represents a crucial resource – and protecting it a critical responsibility. In spite of this, government respondents indicate that only 28% of public sector entities encrypt stored data, and only 22% keep an accurate inventory of all third parties using customer data. Moreover, one out of every three government organizations still does not classify data and information assets according to their risk level.

<b>Public sector: security benchmarks (Percentage of responses from government respondents)</b>	<b>2005</b>	<b>2004</b>
Security spending (as % of IT budget)	12.6%	8.8%
Organization conducts penetration testing	37%	27%
Reported from 1 to 9 security attacks in past 12 months	49%	55%
Deploys intrusion detection tools	58%	47%
Employs a Chief Information Security Officer (CISO) or Chief Security Officer (CSO)	58%	48%

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