



## Survey Methodology

The State of Information Security 2007, a worldwide security survey by PricewaterhouseCoopers and CIO Magazine, was conducted online from March 6 to May 4, 2007. Readers of CIO 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 7,200 CEOs, CFOs, CIOs, CSOs, vice presidents and directors of IT and information security from 119 countries. The margin of error is  $\pm 1\%$ .

Of the 902 respondents from the public sector (13% of survey), 46% were from North America, 28% from Europe, 16% from Asia, and 9% from South America.

To learn more about the survey, or about how PwC helps companies address security and privacy issues, contact:

**Philip Whitmore**  
(09) 355 8114  
philip.whitmore@nz.pwc.com

**Graeme McLellan**  
(04) 462 7112  
graeme.x.mclellan@nz.pwc.com

**Ian Rankin**  
(03) 374 3041  
ian.x.rankin@nz.pwc.com

- Another top priority is expanding a compliance-driven focus to better address risk management. Security isn't just about compliance. It's also—and sometimes more importantly—about reducing, mitigating or transferring risks. This year's survey reveals that the alignment of resources to risk levels is a leading-practice strategy that has not yet surfaced in the government sector. One red flag is the fact that, while 29% of public sector respondents report that their organisation's security policies are completely aligned with its objectives, far fewer (15%) say the same thing about their organisation's security spending. But we also note others. Most government organisations (65%), for example, do not conduct an enterprise risk assessment either annually or semi-annually. And only 29% ensure that their security policies include classifying the business value of data.
- Programs to develop a uniform identity credential on a national scale will have to do a better job of addressing the convergence of physical and information security. Unauthorised access to physical facilities and logical IT assets is a global public sector issue. In response to the global threat of terror, public organisations around the world have accelerated their efforts to establish a common credential for employees or contractors requiring physical or logical access to sensitive information systems, secure areas within government facilities and critical sections of the economic infrastructure. In the face of this objective, however, more than half (53%) of all public sector respondents report that their organisation's physical and information security organisations are separate—i.e., that there isn't any linkage or integration across policies or procedures. In addition, only 33% report that physical security and information security are integrated—and report to the same leader.

Security benchmarks: Public Sector (Percentage of responses from public sector vs. financial services sector)	Public Sector 2007	Public Sector 2006	FS 2007
Have an overall security strategy	60%	42%	71%
Employ a CISO or CSO	72%	56%	86%
Have a business continuity / disaster recovery plan in place	55%	55%	71%
Engage in the secure disposal of technology hardware	67%	45%	65%
Ensure security policies include enforcement mechanisms	34%	27%	46%

© 2007 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.



Business  
Technology  
Leadership

