



## 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 58 respondents from the payer sector, 78% were from North America, 10% from Europe, 3% from Asia, and 3% from South America. Forty-five percent (45%) reported annual revenues of at least \$1 billion.

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

- **Measuring and monitoring are just as important to security as they are to managing outcomes and healthcare costs.** Payer respondents estimate that 82% of their users are in compliance with their information security policies. But 38% also say their organisation does not yet have people dedicated to monitoring employee use of information assets or the Internet. And while 51% report that their organisation doesn't audit or monitor user policy compliance, almost as many (45%) say their company hasn't measured and reviewed the effectiveness of security in the past year.
- **Having a strategy is essential. But it has to translate security investments into business value.** Most sector firms (79%) have a security strategy in place—well above the cross-industry average (57%). But we note an unusually wide spread between the percentage of payer respondents who said their security policies were “completely aligned” with their strategic business objectives (49%) and those who felt the same way about security spending (13%).
- **How much value collaborative arrangements provide will depend in part on whether appropriate security measures are used.** Payers appear significantly more likely than the cross-industry average to outsource some or all of their security (32% vs. 20%)—especially security event monitoring (30% vs. 21% for financial services). And, at least by one measure, the strategy appears to be working: only 8% of payer respondents report incidents that compromised customer records compared to 26% of financial services respondents. But service providers such as consultants and contractors ranked as the second most likely source of a security incident. In spite of this, less than half (40%) of payers do not define security baselines for external partners or vendors and 55% do not keep an accurate inventory of third parties using customer data.

<b>Security benchmarks: Healthcare</b> (Percentage of responses from healthcare vs. other industries)	<b>Health/ Payer 2007</b>	<b>Health/ Provider 2007</b>	<b>Pharma/ Life Sciences 2007</b>	<b>Financial Services 2007</b>	<b>All Industries 2007</b>
Have an overall security strategy	79%	61%	58%	71%	57%
Engage both business and IT decision-makers in addressing information security	80%	58%	51%	64%	52%
Ensure that security policies include risk assessment	71%	47%	56%	62%	43%
Have a centralised security information management process	57%	51%	50%	57%	44%
Conduct compliance testing	55%	41%	53%	59%	40%

© 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**

