

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 266 respondents from the healthcare provider sector, 66% were from North America, 18% from Europe, 9% from Asia and 7% from South America. Thirty percent (30%) reported annual revenues of at least \$500 million.

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 7122
graeme.x.mclellan@nz.pwc.com

Ian Rankin
(03) 374 3041

- **Security and privacy policies and practices are only valuable if they work.** Uncertainty about the business value of compliance investments will be high as long as providers are not checking up to see whether safeguards are actually being followed—or are even working. Most providers (61%), however, do not audit or monitor user compliance with policies and 55% have not measured and reviewed the effectiveness of security policies and procedures in the past year. Many administrators will also need to decide whether internal compliance can be achieved merely through improvements in training and awareness. Though writing rules is perhaps the most cost-effective security practice, two of the elements least likely to be included in health provider security policies include the collection of security metrics (26% vs. 45% reported by payers) and enforcement mechanisms (33% vs. 52% reported by payers).
- **The “insider threat” may actually be growing.** This year, 57% of provider respondents report that employees represented the most probable source of security incidents—a percentage higher than the cross-industry average (48%) and significantly higher than levels reported by payer respondents (36%). Has the “insider threat” truly increased—or are provider organisations simply more aware of the threat? It isn’t clear. But provider respondents identified the primary method of attack as the abuse of valid user accounts and permissions. In spite of this, barely a third of all provider respondents (36%) say their organisation has tiered authentication levels based on user risk classification. Arguably, hospitals, among other providers, face the greatest “insider” challenge. With so many personnel—from doctors to nurses and technicians—logging into common stations, multiple log-on procedures quickly undermine the quality of patient care. In spite of this, only 22% of provider respondents report their organisation has reduced/single sign-on software in place.

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

