

What the numbers say:

1 in every 3

Number of healthcare providers that employ a chief privacy officer (CPO). This rate (35%) is twice as high as the cross-industry average (17%).

No. 1

Ranking that healthcare providers gave to intrusion detection systems when listing how their organization learned of security attacks.

38%

Percentage of healthcare providers that are not in compliance with HIPAA but need to be.

39%

Percentage of healthcare providers that employ compliance testing.

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 how healthcare providers are starting to build on the security capabilities they previously established to achieve compliance with HIPAA.

- Working toward compliance with HIPAA's security rule and other regulations has been a grueling and resource-intensive effort—an achievement based, in some cases, on an unsustainable level of expenditure. Thus, we find healthcare providers spending less on security this year than the cross-industry average (10.5% of IT budget vs. the 13.2% reported by others). Only a slight majority of healthcare respondents (52%) anticipate an increase in spending in 2005 (vs. 62% in 2004 and 67% in 2003).
- This massive buildup of the past two years has helped position healthcare providers as leaders in privacy practices. Healthcare providers are far more likely than companies in other industries, for example, to increase employee awareness of privacy policies (71% vs. 51%); review privacy policies at least once a year (59% vs. 45%); and encrypt data transmitted (58% vs. 51%).
- The compliance effort has helped the industry get ahead in security. Healthcare providers are more likely to engage personnel in monitoring employee use of the Internet or information assets (67% vs. 59%); prepare business continuity and disaster recovery plans (63% vs. 55%); and develop internal security communication procedures for employees (60% vs. 52%).
- Some goals are yet to be realized. While 33% of healthcare respondents report no negative security-related events in the prior 12 months, 77% report financial losses, 63% cite impacts to their organization's brand or reputation, and 29% indicate that 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 658 respondents in healthcare (8% of survey), 59% were from North America, 24% from Europe, 9% from South America, 8% from Asia, and 1% from the Middle East and Africa. Thirty-one percent reported annual revenues of at least \$500 million.

Critical areas needing improvement

Strategy and centralization

Only 44% of healthcare executives report engaging an overall information security strategy process, and fewer still (41%) say they use a centralized security management process. Developing new capabilities in these areas will be critical as healthcare providers look beyond complying with the HIPAA security rule to achieving economies of scale with respect to security and the elimination of duplicative efforts and documentation.

The alignment gap

Although 80% of healthcare executives believe that their organization's security policies are aligned with business objectives, a smaller majority (63%) believe that security spending is similarly aligned. Insight into this difference might be found in the 38% of healthcare responders (vs. 47% in 2004) who report that their organization does not yet actively engage both business and IT decision makers in addressing security.

Handling protected health information (PHI)

Many healthcare providers are discovering that the majority of the data in their systems is protected health information. From bills to prescriptions to family medical history accounts and more, this is data that must be guarded. Unlike other industries that see value in classifying data according to risk levels, healthcare providers are more likely to want to protect it all. For many providers, this will be a challenge: survey responses indicate that only 37% keep an accurate inventory of user data, and only 30% encrypt stored data. Moreover, nearly 3 out of 10 report that when security events have occurred, internal records were lost or damaged.

Healthcare: security benchmarks (Percentage of responses from healthcare executives)	2005	2004
Security spending (as % of IT budget)	10.5%	10.1%
Reported from 1 to 9 security attacks in past 12 months	53%	56%
Employs intrusion detection tools	52%	42%
Had privacy audited by third-party	34%	31%
IT and physical security are separate	54%	57%

To learn more about the survey, or about information security services offered by PwC Advisory, visit:
www.pwc.com/security

or contact:

Mark Lobel, (646) 471-5731, mark.a.lobel@us.pwc.com or
Jerry Lewis, (214) 754-7425, 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