

How payers setting the benchmarks for so many security and privacy practices are confronting a few strategic gaps in their approach*

The Global State of Information Security 2007

31%

Percentage of payer respondents whose organizations do not link security, either through organizational structure or policy, to privacy and/or regulatory compliance.

Almost 100%

Percentage of payer respondents (97%) who say their company employs either a CISO or a CSO. Eighty-six percent (86%) of other financial services sectors report the same.

57%

Percentage of payer respondents who report their organization conducts a periodic risk assessment. Among financial services respondents, 70% report the same.

1:1

Ratio between the number of payer respondents who report their organization has security standards in place for hand-held/portable devices and the number who report they do not.

More heavily regulated than companies in almost any other industry, payers have now jostled financial services firms aside as leaders in establishing high-water marks for a widening range of security and privacy practices. And the leads are often commanding. Consider the results of the world's largest survey on privacy and information security practices, the Global State of Information Security 2007. Payer responses reveal that sector firms are far more likely than financial services organizations—which rely just as critically on digital assets—to employ a Chief Privacy Officer (53% vs. 33%), encrypt data in transmission (87% vs. 75%), and have a business continuity or disaster recovery plan in place (83% vs. 71%).

But being the best at security isn't the point. Well beyond compliance, security has a crucial contribution to make to a complex array of sector challenges—not just to controlling costs and building efficiencies—but also to protecting profitability and competitive differentiation. In this sense, the benchmarks the sector should apply to itself aren't those that define a leadership position. It should be the few lingering—but often enormously strategic—gaps that could undermine performance objectives. Here are the ones we believe deserve the most critical attention.

- **Compliance-driven gains in security do not extend deeply enough to core data protection capabilities.** It isn't just the growing importance of electronic health records or the need to share information through health information networks. It's also consumerism—and rising expectations for Web-enabled access to, for example, provider cost and quality or customized benefit statements. Yet payers are actually less likely than financial services organizations to encrypt data at rest in databases (47% vs. 51%), files shares (30% vs. 35%), and backup tapes (28% vs. 44%). And more than 6 out of 10 do not keep an accurate inventory either of user data or locations and jurisdictions where this data is stored.
- **With so much at stake—from system integrity to corporate reputation—internal compliance shouldn't be discretionary.** In general, payers do an excellent job of defining the policies they expect to be carried out across expanding global enterprises. They're much more likely than financial services organizations to ensure that security policies address compliance with legal and regulatory requirements (83% vs. 65%) and application security segregation-of-duties (86% vs. 68%). But most do not address the need to collect security metrics (55%) or classify the business value of data (57%). And only one of every two payers includes enforcement mechanisms or standards in their policies.

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, visit: www.pwc.com/gjss2007 or contact:

Mark Lobel
646 471 5731
mark.a.lobel@us.pwc.com

Rik Boren
314 206 8899
rik.boren@us.pwc.com

Paul Veronneau
860 241 7586
paul.veronneau@us.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 organization does not yet have people dedicated to monitoring employee use of information assets or the Internet. And while 51% report that their organization 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.

Security benchmarks: Healthcare (Percentage of responses from healthcare vs. other industries)	Health/ Payer 2007	Health/ Provider 2007	Pharma/ Life Sciences 2007	Financial Services 2007	All Industries 2007
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 centralized security information management process	57%	51%	50%	57%	44%
Conduct compliance testing	55%	41%	53%	59%	40%

© 2007 PricewaterhouseCoopers LLP. All rights reserved. “PricewaterhouseCoopers” refers to PricewaterhouseCoopers LLP (a Delaware limited liability partnership) or, as the context requires, the PricewaterhouseCoopers global network or other member firms of the network, each of which is a separate and independent legal entity. SJ-08-0018-A 08-07 DB



**Business
Technology
Leadership**

