

How pharmaceuticals trying to cut costs without compromising compliance are overlooking chances to better manage risks*

The Global State of Information Security 2007

#1

Ranking that pharmaceutical respondents give to regulatory compliance when asked to identify the primary business issue and justification for security spending.

Almost 6 out of 10

Number of pharmaceutical respondents who report their organization does not maintain an accurate inventory of user data.

34%

Percentage of pharmaceutical respondents who say their organization encrypts data on laptops. Sixty-four percent (64%) of payers report the same.

1:1

Approximate ratio between the number of pharmaceutical respondents who report their organization has procedures in place dedicated to protecting intellectual property to the number that do not.

It's a matter of prioritization. As margins shrink, pipelines thin and generic competition heats up, rising cost pressures are forcing pharmaceutical executives to confront difficult choices on which investments in information security will deliver the most valuable impacts to performance and profitability. Not unexpectedly, compliance-related initiatives top the list. This year, the vast majority of pharmaceutical and life sciences respondents to the Global State of Information Security 2007, the world's largest survey on privacy and information security practices, confirm that complying with regulations is the single most important business issue driving security spending (79% vs. 54%, the cross-industry average).

But survey responses also suggest that this heavy focus on compliance is unfolding at the growing expense of another strategic objective: managing critical business risks to assets such as intellectual property, corporate reputations and the data and system integrity so essential to supporting an expanding network of alliances and partnering arrangements. Here are some of the critical areas we believe deserve executive attention.

- **Writing the rules. But not necessarily measuring their impact.** Pharmaceuticals have worked hard over the last 12 months to improve policies. Industry respondents report their organizations are much more likely this year to ensure their policies address risk assessment (56% vs. 39% in 2006), incident response (61% vs. 39%) and application security segregation-of-duties (62% vs. 49%). Most, however, do not audit or monitor user compliance with policies (58%). And while 27% do not classify information data assets according to their risk level, 37% have not measured and reviewed the effectiveness of their policies in the past year.
- **Privacy may be an emerging priority—but it isn't yet fully evident in the numbers.** For a growing number of pharmaceuticals, earning trust from key stakeholders—both inside and outside of the company—is viewed as a strategic differentiator. This year, for example, more companies are requiring employees to certify in writing that they're complying with privacy policies (61% vs. 46%) and posting privacy policies on internal websites (68% vs. 50%). Yet pharmaceuticals are only a step or two ahead of cross-industry averages—in providing employees with training in privacy policies (55% vs. 49%), for example, or auditing privacy standards through third-party assessments (33% vs. 28%). And pharmaceuticals are far less likely than payers to employ a Chief Privacy Officer (22% vs. 53%), encrypt data in transmission (66% vs. 87%) and link security, through either organizational structure or policy, to privacy and regulatory compliance (44% vs. 69%).

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 145 respondents in the pharmaceutical and life sciences sectors (2% of survey), 50% were from North America, 23% from Europe, 17% from Asia, and 8% from South America. Almost half (48%) 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/giss2007 or contact:

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

Pat Roche
973 236 4844
pat.d.roche@us.pwc.com

Mark Simon
973 236 5410
mark.d.simon@us.pwc.com

- **It's even more apparent: the insider threat is significant.** Pharmaceutical respondents reporting that employees represented the most probable source of security incidents increased significantly—from 38% in 2006 to 47%. Has the “insider threat” truly increased—or are companies simply more aware of the threat? It isn't clear. But pharmaceutical respondents were also 2.5 times more likely than payer respondents to cite the abuse of valid user accounts and permissions as the primary method used (25% vs. 10%). In spite of this, very few pharmaceutical respondents say their organization has an identity management solution (25%) or an automated account deprovisioning capability (21%).
- **Aligning security with the business continues to be an elusive endeavor.** IT and security executives are having a hard time communicating the importance of security investments in business terms. Only 20% of pharmaceutical respondents report that their company's spending on information security is “completely aligned” with business objectives. It may have something to do with who is at the table making investment decisions. One out of every two industry respondents says their company does not engage both business and IT decision-makers in addressing information security. Perhaps even more significantly, pharmaceuticals are far less likely than payers (38% vs. 70%) to have their Chief Information Security Officer or equivalent report to the top of the company (CEO, CFO, VP or board).
- **Extending security to third parties is becoming even more crucial.** As efforts to realize tangible value from strategic alliances, joint ventures and other partnering arrangements grow, security can be an enabler of third party alliances and connections and can make doing business with a pharma/life sciences company more attractive. Pharmaceuticals have made clear gains on this front since last year. Many more, for example, have now established security baselines for external partners (48% vs. 33% in 2006). But fully half do not require third parties to comply with their privacy policies and only 23% keep an inventory of all third parties using customer data.

Security benchmarks: Pharmaceutical and Life Sciences

(Percentage of responses from pharmaceutical and life sciences sectors compared to other industries)

	Pharma/ Life Sciences 2007	Health/ Payer 2007	Health/ Provider 2007	Financial Services 2007	All Industries 2007
Have an overall security strategy	58%	79%	61%	71%	57%
Engage both business and IT decision-makers in addressing information security	51%	80%	58%	64%	52%
Ensure that security policies include risk assessment	56%	71%	47%	62%	43%
Have a centralized security information management process	50%	57%	51%	57%	44%
Conduct compliance testing	53%	55%	41%	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**

