

The global state of information security 2006

What the numbers say:

42%

Percentage of pharmaceutical companies that conduct compliance testing—the same number as in last year's survey.

63%

Percentage of pharmaceutical companies that do not keep an accurate inventory of user data.

1:1

Ratio of pharmaceutical companies that have measured and reviewed the effectiveness of their security policies and procedures in the past year to the number that have not.

43%

Percentage of pharmaceutical companies that do not yet have a business continuity or disaster recovery plan.

66%

Percentage of pharmaceutical executives who are either "somewhat" or "not at all" confident in their partners' or suppliers' security.

Results from the world's largest information security study are in. This year, responses to PricewaterhouseCoopers' and CIO magazine's Global State of Information Security study confirm that, for most pharmaceutical, biotech, and biomedical companies, legal and regulatory requirements as well as potential liability continue to be key drivers behind security investments. But survey responses also reveal that, while many companies are posting gains in key areas such as privacy, much of this spending is still reactionary— isolated investments in technologies that are not yet linked to a strategic approach to achieving long-term benefits from an integrated compliance solution.

- Gains in protecting privacy: Pharmaceutical companies are more likely this year than last to encrypt data in transmission (59% vs. 54%), post privacy policies on their external web sites (42% vs. 37%), and secure web transactions (56% vs. 53%).
- Clear signs of new technological capabilities: This year, more organizations report having intrusion-detection systems (48% vs. 44%) and network security tools (59% vs. 55%). They're also more likely to ensure secure disposal of their technology hardware (45% vs. 34%) and use tools for detecting malicious code (38% vs. 31%).
- But strategy and integration are still often overlooked: Getting the best return on these investments often depends on whether they're executed as part of a strategic and comprehensive compliance plan. Pharmaceuticals are taking more of an interest in centralized security information management than they did last year (41% vs. 35%), but most other responses provide little evidence of a strategic approach. Only 46% of pharmaceuticals have an overall security strategy and 73% do not integrate information security safeguards with privacy and compliance plans.

Survey Methodology:

The State of Information Security 2006, a worldwide security survey by PricewaterhouseCoopers and CIO magazine, was conducted online from April 5 to May 22, 2006. Readers of CIO magazine and 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 7,791 responses from IT and security professionals in 50 countries. Respondent titles included CEO, CFO, CIO, CSO, and vice president, director, and manager of IT and information security. The margin of error is $\pm 1\%$.

Of the 216 pharmaceutical, biotech, and biomedical respondents (3% of survey), 38% were from North America, 31% from Europe, 19% from South America, and 13% from Asia. Thirty-seven percent reported annual revenues of at least \$500 million.

To learn more about the survey, or about the Security and Privacy practice at PwC, visit:
www.pwc.com/GISS2006

or contact:
Mark Lobel
646.471.5731
mark.a.lobel@us.pwc.com

Pat Roche
973.236.4844
pat.d.roche@us.pwc.com



Business
Technology
Leadership

Critical areas needing improvement

Protecting data across the entire information lifecycle

Privacy is only one aspect of protecting data across operations, from employee information to clinical trial results and sales and marketing data. Though pharmaceuticals have made gains in encrypting stored data (41% vs. 30% in 2005), the critical challenge today is protecting data beyond the datacenter—within applications, on portable devices, and in emails. But while incidents involving the loss or theft of executive laptops and their stored data continue to occur, only 29% of pharmaceutical companies have security standards or procedures for handheld and portable devices and 30% still do not classify data and information assets according to risk levels.

Controlling access

One of the most effective ways of managing risk to regulated data is by controlling access to structured applications. When asked the likely source of attack this year, 54% of pharmaceutical respondents pointed to either current or former employees. Despite this, 73% of pharmaceutical companies do not yet have an identity management solution. In addition, only 26% use tiered authentication levels based on user risk classification and little more than half (51%) actively monitor and analyze information security intelligence such as vulnerability reports and log files.

Improving oversight of third-party privacy and security practices

Pharmaceuticals also need to improve how they manage information risk when data travels outside of the corporate network. Today only 34% of pharmaceuticals keep an accurate inventory of all third parties using customer data and most (56%) do not yet require third parties (including outsourcing vendors) to comply with their privacy policies.

Pharmaceuticals: security benchmarks (Percentage of responses from pharmaceutical sector)

	2006	2005	2004
Security spending (as % of IT budget)	16.4 %	14.4%	10.6%
Keep inventory of all third parties using customer data	34%	26%	20%
Have a centralized security information management system	41%	31%	31%
Conduct employee background checks	57%	46%	35%
Employ a CISO or chief security officer CSO	52%	41%	30%