

The global state of information security 2006

What the numbers say:

1 out of 4

Number of technology respondents (25%) that reported their organization needs to be compliant with the EU Data Privacy Directive but is not. Similarly, 22% reported their organization needs to be compliant with Sarbanes-Oxley but is not.

43%

Percentage of technology respondents who reported that their organization informs other companies, organizations, or authorities when an event occurs. This is an enormous increase over last year (16%).

53%

Percentage of technology companies that still don't have a business continuity or disaster recovery plan in place.

1 out of 5

The number of technology companies that do not classify data and information assets according to risk levels.

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 some technology companies are making good progress in building a solid foundation for effective and sustainable security and privacy practices. But, survey responses also reveal that technology companies are still missing opportunities to get the best protection from their technology investments because they're not focusing enough on establishing supporting policies and processes.

- As barriers to security fall, spending gets a boost: Technology respondents report that the three most significant barriers to effective security have started to fall. Compared with last year's study, fewer respondents report that limited budget (51% vs. 59%), limited staff (36% vs. 41%), or limited time (27% vs. 35%) are hindering progress in security. In fact, industry confidence in the effectiveness of information security is higher than it's ever been (87%) and more companies than last year (51% vs. 46%) expect to increase security spending over the next 12 months.
- Gains in building a solid security foundation: Last year, we pointed out that technology companies needed to take a more strategic approach to security. It appears that some have. According to responses in this year's study, technology companies are now more likely to have an overall security strategy (39% vs. 32%). They're also significantly more likely to have measured and reviewed the effectiveness of their information security policies and procedures in the prior 12 months (58% vs. 43%). And with more automated tools available to them, they're also more apt to be proactive in monitoring security intelligence (55% vs. 49%).
- Putting key technologies in place: This year, more technology companies than last year are securing web transactions (58% vs. 53%) and using tools to detect intrusion (53% vs. 46%) or malicious code (42% vs. 32%). Technology companies are also more likely to deploy security for voice-over-IP systems (29% vs. 17%) and for handheld, portable devices such as Blackberries and laptops (28% vs. 23%).

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 1,177 technology respondents (15% of survey), 29% were from Europe, 26% from Asia, 23% from North America, and 20% from South America. Thirty-four percent reported annual revenues of at least \$100 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

Critical areas needing improvement

Leveraging people, policies, and procedures to strengthen privacy

We were surprised again this year to see that technology companies have made few recent advances in these areas—especially with respect to protecting privacy. Many have made little or no headway in posting privacy policies on their external web sites (39% vs. 39%) or providing employees with privacy training (56% vs. 55%). Only 25% have integrated privacy and compliance plans and only 56% engage both business and IT decision-makers in addressing security issues.

Improving data protection

For many technology companies, one of the most crucial upcoming challenges will be doing a better job at protecting data across the information lifecycle. Most technology respondents (70%) admit that their security policies don't address classifying the value of data and 47% report that their organization doesn't have policies governing data protection, disclosure, and destruction. In addition, only 52% of technology respondents report that their organization encrypts data in transmission and only 41% say they encrypt data in storage.

Extending security and privacy to third parties

Survey results indicate that 75% of technology companies outsource some component of their information security capabilities. Many of these capabilities, such as help desk and call center operations, require third-party access to customer data. Despite this, 61% of this group admitted that they were either "not at all" or only "somewhat" confident in their outsource vendor's security. We think good security housekeeping begins at home, but only 34% of technology companies keep an inventory of all third parties using their customer data. Even fewer (33%) require third parties (including outsourcing vendors) to comply with their privacy policies.

Technology: security benchmarks (Percentage of responses from technology sector)	2006	2005	2004
Security spending (as % of IT budget)	22.6%	16.6%	13.5%
Do not classify information assets according to level of risk	20%	28%	27%
Report that IT and physical security are separate	19%	41%	43%
Keep inventory of all third parties using customer data	34%	27%	17%
Employ a CISO or CSO	41%	36%	31%

