

What the numbers say:

53%

Percentage of technology companies that engage both business and IT decision makers in addressing information security issues.

No. 1

Ranking given to “intrusion detection systems” by technology executives asked to rank how their organization learned about security events.

52%

Number of technology companies that do not yet employ intrusion detection monitoring.

43%

Percentage of technology companies that have both measured and reviewed the effectiveness of their information security policies in the past year.

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 that although the security practices of technology industries still lag behind those in other sectors, larger security budgets than last year give technology companies a fresh opportunity to address important areas of vulnerability.

- In information security, technology companies are less likely to have an overall security strategy in place (32% vs. the cross-industry average of 37%), have a business continuity or disaster recovery plan (48% vs. 55%) or conduct periodic security audits (44% vs. 50%).
- Surprisingly, some of the clearest deficits are in technology. Although technology companies are more likely to deploy personal firewalls (46% vs. 41%), they’re less likely to back up data (79% vs. 84%), deploy patch management tools (30% vs. 35%) and engage role-based access controls (25% vs. 29%).
- When negative security-related events occur, they take a toll. Impacts reported include financial losses (71%), losses or damages to internal records (49%) and unauthorized changes to operating systems (33%) and software applications (24%).
- Survey responses from executives suggest that technology companies are aware of, and willing to close, some of their vulnerability gaps. This year, technology companies are spending, on average, 22% more on security than they did in 2004.

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 1,713 technology respondents (21% of survey), 35% were from Europe, 26% from North America, 18% from South America, 18% from Asia, and 3% from the Middle East and Africa. Forty-three percent reported annual revenues of at least \$100 million.

Critical areas needing improvement

Strategy and centralization

To stay abreast of current challenges, such as those emerging from convergence, technology companies seeking to redefine themselves as integrated end-to-end providers need to make information security a major priority. Survey responses point to several critical areas:

Leveraging technology and automation

Improving security depends, in part, on deploying core technologies and taking advantage of the benefits provided by automated solutions. This is an area requiring attention from technology companies: most, for example, don't use network security tools (76%), deploy malicious code detection tools (83%) or engage identity management solutions (87%).

Protecting intellectual property

Safeguarding intellectual property (IP) is critical for many technology companies—especially given industry trends in outsourcing and off-shoring, mergers and acquisitions and the transfer and sharing of proprietary technology across global supply chains. However, 42% of technology executives reported that security incidents within the past 12 months had resulted in intellectual property (IP) theft. And most technology companies still don't employ tools to discover unauthorized devices (78%), ensure the secure disposal of technology hardware (68%) or ensure that their security policies address data protection, disclosure and destruction (59%).

Giving security policies real muscle

For security policies to be effective, ground rules are essential. Yet only a minority of the technology organizations surveyed ensure that their security policies address the following critical areas: application security with respect to segregation of duties (36%), incident response policy (28%) and an enforcement mechanism for standards (19%). And only four in ten technology companies (41%) audit or monitor user compliance with security policies.

Technology: security benchmarks (Percentage of responses from technology executives)	2005	2004
Security spending (as % of IT budget)	16.6%	13.5%
Plans to increase budget next year	46%	66%
Does not classify information assets according to level of risk	28%	27%
IT and physical security are separate	41%	43%
Employs a Chief Information Security Officer (CISO) or Chief Security Officer (CSO)	36%	31%

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