

The Global State of Information Security 2005

What the numbers say:

87%

Percentage of energy and utility executives confident in the effectiveness of their organization's information security capabilities.

42%

Percentage of energy and utility companies that do not engage both business and IT decision makers in addressing information security.

4 out of 10

The number of energy and utility executives who point to employees as the most likely source of attack.

54%

Percentage of energy and utility companies who address IT and physical security separately.

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 energy and utility companies are making measurable progress in addressing security. Spurred by regulations, such as NERC 1200 and FERC SMD, these industries are also motivated by their important roles in protecting national infrastructure. Some telling indicators:

- Energy and utility companies are more likely than others to have an overall security strategy in place (46% vs. the cross-industry average of 37%).
- They are also more likely to use network security tools (69% vs. 61%), conduct periodic security audits (60% vs. 50%) and actively monitor and analyze security intelligence (61% vs. 53%).

But the study also reveals that energy and utility companies have more work ahead in taking a proactive approach to an expanding portfolio of risks. For example, geopolitical events and high-profile natural disasters around the world have placed new requirements on how the industries protect and secure information.

- Only 50% conduct periodic threat and vulnerability assessments. And only 63% have a business continuity or disaster recovery plan in place.
- Industry executives report that when events occur, they take a toll: 67% report financial losses, 49% cite loss or damage to internal records and 55% report damage to the organization's brand or reputation.

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 442 respondents in the energy and utility industries (5% of survey), 33% were from North America, 33% from Europe, 18% from South America, 12% from Asia, and 4% from the Middle East and Africa. Fifty-seven percent reported annual revenues of at least \$500 million.

Critical areas needing improvement

As energy and utility companies position themselves to address industry trends in consolidation, heightened competition and new models of value creation, strategic security capabilities that lower risk, reduce the cost of compliance and drive performance improvement become even more critical.

Leveraging technology

Energy and utility companies lag in the deployment of core security technologies. Most do not use tools to prevent intrusion (57%) or detect malicious code (63%). And 83% have not implemented an identity management solution – a security initiative proven to reduce costs, support regulatory compliance and improve user productivity.

Risk management

Operating in highly capital-intensive environments, energy and utility companies must live for many years with their investment decisions, including those in IT systems, and guard their huge capital asset inventories. Risk management is therefore essential. In spite of this, almost half (49%) of all energy and utility companies do not conduct periodic risk assessments. And 33% still do not classify data and information assets according to risk levels.

Strengthening security policies

Strong policies are among the first lines of defense in information security. Yet most security policies within energy and utility industries do not address enforcement mechanisms for standards (74%), incident response policies (57%) or application security with respect to segregation of duties (57%).

Energy and utilities: security benchmarks (Percentage of responses from energy and utility executives)	2005	2004
Security spending (as % of IT budget)	8.7%	8.4%
Will increase security budget next year	48%	64%
Reports zero security events in past 12 months	35%	17%
Conducts penetration testing	41%	27%
Employs a Chief Information Security Officer (CISO) or Chief Security Officer (CSO)	46%	35%

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