

The global state of information security 2006

What the numbers say:

1 out of 4

Number of energy and utility respondents that say lack of support or limited support from executive management represents a leading barrier to good security measures in their organization.

56%

Percentage of energy and utility companies that have a business continuity and disaster recovery plan in place.

38%

Percentage of energy and utility respondents that say their organization needs to be in compliance with various state and local privacy regulations and is not. Significant percentages of energy and utility entities also need to be in compliance with the EU Data Privacy Directive (23%) and the Sarbanes-Oxley Act (31%), but are not.

6 out of 10

Number of energy and utility companies that do not integrate physical and information security personnel.

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 reveal that energy and utility companies worldwide are spending 12.9% of their IT budgets on information security—more than they spent in 2004 (8.4%) but considerably less than what companies in other industries are currently investing (17.3%).

Despite this spending gap, energy and utility companies appear to be doing a better job of building up their security programs, at least on a capability-specific basis. But survey responses also reveal critical deficiencies in addressing security, compliance, and privacy from a strategic approach.

- **Securing systems and infrastructure:** Energy and utility companies are more likely than those in other industries to use a centralized security information management process (46% vs. 34%), secure web transactions (60% vs. 53%), and conduct training programs to improve employee security awareness (47% vs. 39%). But they're only marginally better at ensuring the secure disposal of technology hardware (40% vs. 38%) and they're less likely than others to have measured and reviewed security in the past year (45% vs. 47%).
- **Controlling access:** Although 53% of energy and utility respondents point to current or former employees as the likely source of attack, their organizations are not much more likely than firms in other industries to conduct personnel background checks (52% vs. 51%), employ identity management systems (24% vs. 20%), or use tiered authentication based on user risk classifications (22% vs. 22%). Access-related risks to industry firms may actually increase when employees leave, since 81% of energy and utility organizations do not automate account deprovisioning.
- **Measuring impact:** Security incidents are occurring more often. Only 28% of energy and utility respondents reported encountering none this year, down from 35% in 2005. And when events did occur, they took a toll: More than 36% of respondents reported that software or operating system files had been altered. Other impacts cited included compromising of customer or employee records (20%), financial losses (19%), and impacts to the organization's brand or reputation (13%).

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 265 respondents in the energy and utility industries (3% of survey), 34% were from North America, 28% from Europe, 25% from South America, and 13% from Asia. Forty-four 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

Brad Bauch
713.356.4536
brad.bauch@us.pwc.com

Critical areas needing improvement

Engaging a strategic approach

As regulatory change, geopolitical events, and natural disasters complicate the risk environment, energy and utility companies need to take a strategic approach to integrating security, compliance, and risk management capabilities. Today, however, only 39% have an overall security strategy in place and 43% do not actively engage both business and IT decision-makers in addressing information security issues. In addition, only 30% use organizational structure or policy to link security to privacy or regulatory compliance and even fewer (22%) engage business processes that integrate privacy and other compliance programs.

Improving data protection

Another critical priority is the need to protect private employee and customer information. Yet 62% of energy and utility companies do not maintain an accurate inventory of user data and most do not encrypt stored data (74%) or data in transmission (54%). Only 52% address data protection, disclosure, and destruction in their security policies, and 30% still do not classify data and information assets according to risk levels.

Extending security practices to partners, vendors, and other third parties

Energy and utility firms worldwide often rely extensively on close collaboration with partners, vendors, or suppliers in connection with production sharing contracts, mergers, acquisitions, or strategic alliances. Most (73%), however, have not yet established security baselines for external suppliers and vendors. Moreover, only 42% require third parties (including outsource vendors) to comply with their privacy policies, and 72% do not keep an accurate inventory of all third parties using customer data.

Energy and utilities: security benchmarks (Percentage of responses from the energy and utilities sectors)

	2006	2005	2004
Security spending (as % of IT budget)	12.9%	8.7%	8.4%
Rely on a centralized security information management process	46%	40%	36%
Keep an inventory of all third parties using customer data	28%	24%	16%
Employ a CISO or CSO	53%	46%	35%

© 2006 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. *connectedthinking is a trademark of PricewaterhouseCoopers LLP.