

How energy firms seeking M&A synergies or more efficient operations are missing opportunities to turn security investments into business value*

The Global State of Information Security 2007

#1

Ranking given by energy respondents to business continuity/disaster recovery (BC/DR) when asked to identify the leading business issues driving their information security spending.

40%

Percentage of energy companies that do not have a BC/DR plan in place.

Less than half

Number of energy respondents who report their organisation engages a centralised security information management process – a powerful means of controlling and reducing security costs.

62%

Percentage of energy respondents who report their organisation does not conduct a periodic risk assessment at least annually or semi-annually.

The scale of today's energy companies dwarfs that of companies in other industries. After all, feeding the world's growing demand for affordable and reliable access to energy sources requires greater capital, larger workforces and better technology. But as consolidations reshape segments of the industry and geopolitical risks threaten margins in some areas, energy executives are under pressure to improve the efficiency of global operations that are increasingly larger and more complex. One important facet of this challenge is reducing unexpected impacts to performance by ensuring the adequacy of information security programs.

So this year we were pleased that most energy respondents to the world's largest survey on privacy and information security practices—the Global State of Information Security 2007—now report that their organisation employs either a CISO or a CSO (64%); has an overall security strategy in place (58%); and links security, through organisational structure or policy, to privacy or regulatory compliance (53%). A closer examination of survey results, however, reveals that oil and gas companies are missing key opportunities to improve the business value of their investments in information security.

- **As capital requirements increase, executives need to ensure that investments are being made in the right areas.** Three out of four energy respondents (75%) report that their organisation's information security spending is only "somewhat" or "poorly" aligned with business objectives. But getting better business value from security requires knowing where the greatest risks are. Yet 62% of energy companies do not conduct an enterprise risk assessment either annually or semi-annually. And only half (51%) ensure that their security policies address risk assessment.
- **Benefiting from collaboration will require moving beyond recognising the risks posed by third-party security to addressing them.** Extracting business value from an expanding global footprint will be increasingly difficult without improving data sharing with joint venture partners and suppliers. Yet energy companies are two or three times more likely than those in other industries to see partners (29% vs. 8%) or service providers (24% vs. 11%) as the probable source of an incident. In spite of this, 78% of energy companies do not keep an inventory of all third parties using customer data. And only one out of every two energy companies (50%) has established security baselines for partners, customers and suppliers.

Survey Methodology

The State of Information Security 2007, a worldwide security survey by PricewaterhouseCoopers and CIO Magazine, was conducted online from March 6 to May 4, 2007. Readers of CIO 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 7,200 CEOs, CFOs, CIOs, CSOs, vice presidents and directors of IT and information security from 119 countries. The margin of error is $\pm 1\%$.

Of the 103 respondents from the oil and gas industry, 41% were from North America, 21% from Europe, 18% from South America, and 14% from Asia. Thirty-six percent (36%) reported annual revenues of at least \$1 billion.

To learn more about the survey, or about how PwC helps companies address security and privacy issues, contact:

Philip Whitmore
(09) 355 8114
philip.whitmore@nz.pwc.com

Graeme McLellan
(04) 462 7112
graeme.x.mclellan@nz.pwc.com

Ian Rankin
(03) 374 3041
ian.x.rankin@nz.pwc.com

- The “insider threat” may actually be growing. Energy respondents are much more likely than those in other industries to report that employees represented the most probable source of security incidents (60% vs. 48%). Has the “insider threat” truly increased—or are companies simply more aware of the threat? It isn’t clear. But when asked to identify the primary method used, 24% of energy respondents pointed to the abuse of valid user accounts and permissions and 27% cited “social engineering”. In spite of this, very few respondents say their organisation has tiered authentication levels based on user risk classification (30%) or an automated account deprovisioning capability (24%)—and less than half conduct employee training programs to increase security awareness (45%).
- Measurement and monitoring: Rules are only effective if they’re followed. Across industries, the security policies least likely to be written include those that address enforcement and metrics. Energy company policies, however, stand out. Oil- and gas-related entities are significantly more likely than those in other sectors to ensure their policies address enforcement mechanisms or standards (43% vs. 31%) and security metrics collection and reporting (42% vs. 28%). But less than half (49%) of energy respondents report that their organisation has both measured and reviewed the effectiveness of its information security policies and procedures in the past year. And while energy respondents estimate that, on average, 68% of their users comply with corporate security policies, 62% say their organisation does not actually audit or monitor this compliance.

Security benchmarks: Energy

(Percentage of responses from the oil and gas sectors compared to other industries)

	Energy 2007	FS 2007	All 2007
Have an overall security strategy	58%	71%	57%
Employ both business and IT decision-makers in addressing security	60%	64%	52%
Ensure that security policies include risk assessment	51%	62%	43%
Cite incidents resulting in loss or damage to internal records	30%	14%	18%
Report that the CISO reports to the CEO	7%	28%	32%

© 2007 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.



Business
Technology
Leadership

