

## How some utilities are missing opportunities to extract greater business value from investments in information security\*

### The Global State of Information Security 2007

#### 56%

Percentage of utility respondents who report their organizations does not link security, either through organizational structure or policy, to privacy and/or regulatory compliance.

#### More than 1 out of 3

Number of respondents from utility companies with operations in North American (35%) who say their organization is required to be in compliance with NERC but is not.

#### 52%

Percentage of utility respondents who report their organization has a centralized security information management process.

#### 1:3

Ratio between the number of utility respondents who report their organization maintains an accurate inventory of user data to the number who report they do not.

Complying with regulations ties up a lot of resources in the utilities sector. After all, addressing Sarbanes alone has required enormous commitments. But tackling the battery of regulations—intended, for example, to protect reliability, preserve the environment, or promote structural alignment with various market principles—has also driven utilities to adopt a compliance-centric approach to security and information risk management.

We see some positive implications of this approach. For example, we were pleased to note this year that most utility respondents to the world's largest survey on privacy and information security practices—the Global State of Information Security 2007—say their organization has an overall information security strategy in place (68%); prioritizes information assets according to their risk level at least periodically (63%); and includes legal and regulatory requirements in their security policies (57%). Based on other survey responses, however, we also think utilities are missing opportunities to extract better business value from their investments in security.

- **Writing the rules—but not necessarily making sure that they're followed.** Utilities do a better job than other industries at establishing security policies. They're more likely than the cross-industry average, for example, to ensure that their policies address data protection, disclosure and destruction (65% vs. 53%), incident response (57% vs. 47%), and the appropriate use of the Internet (76% vs. 65%). But only a third or less ensure their policies also address security metrics collection and reporting (29%), enforcement (35%) and classifying the business value of data (28%). Fewer than half (47%) have people dedicated to monitoring employee use of the Internet or other information assets. And only 51% say their organization has measured and reviewed the effectiveness of its security policies and procedures in the past year.
- **Addressing the implications of physical security on information protection is an area of vulnerability.** Although security standards, such as those outlined by NERC CIP 002-009, include requirements for physical access to critical infrastructure assets, there's a lot of work ahead for the sector. While 57% of utilities employ security guards or other physical security measures for information infrastructure, 48% do not conduct personnel background checks. At the same time, half the utility respondents (50%) report their organization addresses physical and information security completely separately – that is, has not yet established any links at an organization or policy level.

## 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 130 respondents from the utilities, 42% were from North America, 26% from Asia, 22% from Europe, and 8% from South America.

To learn more about the survey, or about how PwC helps companies address security and privacy issues, visit: [www.pwc.com/giss2007](http://www.pwc.com/giss2007) or contact:

**Mark Lobel**  
646 471 5731  
[mark.a.lobel@us.pwc.com](mailto:mark.a.lobel@us.pwc.com)

**Brad Bauch**  
713 356 4536  
[brad.bauch@us.pwc.com](mailto:brad.bauch@us.pwc.com)

**David Etheridge**  
415 498 7168  
[david.etheridge@us.pwc.com](mailto:david.etheridge@us.pwc.com)

- **The insider threat is significant.** This year, utility respondents were much more likely than those from other sectors to report that employees represented the most probable source of security incidents (60% vs. 48%). Has the “insider threat” truly increased—or are utility companies simply more aware of the threat? It isn’t clear—though nearly one out of five utility respondents pointed to the abuse of valid user accounts and permissions as the most common method of compromise. What is apparent, however, is that most utilities do not have an effective system in place to provide the right people with the right access to the right assets at the right time. Few utilities dedicate personnel to employee security awareness programs (42%), employ an identity management solution (26%), or engage tiered authentication levels based on user risk classification (34%).
- **Outsourcing processes to third parties doesn’t transfer risk—it often increases it.** One of the often overlooked aspects of compliance—and of sourcing, for that matter—is that ultimate responsibility for protecting sensitive information can rarely be passed on to third-party vendors. So the fact that utilities are more likely than other industries to outsource specific security functions—such as firewall management (33% vs. 25%), data backup (42% vs. 27%) and periodic threat and vulnerability assessments (46% vs. 29%)—is one sign that third-party relationships represent a significant area of risk for utilities. A second sign is the fact that 70% of utility respondents are only “somewhat” or “not at all” confident in third-party security. Yet just over half (57%) require third parties (including outsource vendors) to comply with the organization’s own privacy policies and only 40% have established security baselines for external partners, customers and suppliers.

<b>Security benchmarks: Utilities</b> (Percentage of responses from utilities sector compared to other industries)	<b>Utilities 2007</b>	<b>Oil &amp; Gas 2007</b>	<b>FS 2007</b>	<b>All Industries 2007</b>
Have an overall security strategy	68%	58%	71%	57%
Employ a CISO or CSO	48%	64%	86%	60%
Have a business continuity / disaster recovery plan	60%	60%	71%	51%
Protect data by encrypting it in databases	39%	42%	45%	45%
Ensure security policies include application security segregation-of-duties	57%	66%	68%	53%

© 2007 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. SJ-08-0018-A 08-07 DB



**Business  
Technology  
Leadership**

