

How telco providers trying to entice new customers are overlooking security issues that threaten to jostle already fragile new relationships*

The Global State of Information Security 2007

#1

Ranking given by telco respondents to business continuity/disaster recovery (BC/DR) when asked to identify the leading business issues driving their information security spending. Only 50% of telcos have a BC/DR plan in place.

Almost half

Number of telco respondents who don't know how many (47%) or what type of security incidents (48%) their organization has encountered in the past year.

48%

Percentage of telco respondents who say their company's information security policies do not address data protection, disclosure and destruction.

Six out of ten

Number of telco respondents who report their organization does not perform an enterprise risk assessment either annually or semi-annually.

With so many players in the telecommunications space—fixed, mobile, cable and resellers—deploying triple-play (and even quadruple-play) bundles, the fight to attract and retain customers continues to unfold. Telcos that convince their customers to buy and keep more products and services will be the winners—as will be those that exceed their customers' rapidly rising expectations. It's a high-stakes challenge. Preserving the continuity and quality of their services as well as protecting the privacy of customer information will have an increasingly stronger impact on customer loyalty and, by extension, on revenue performance.

So this year, we were pleased to see that the majority of telco respondents to the Global State of Information Security 2007, the world's largest survey on privacy and information security practices, confirm that their organization has an overall information security strategy in place (60%); deploys VPN software (64%); and prioritizes data and information assets according to their risk level at least periodically (76%). But survey responses also make it clear that, while the sector is keeping pace with other industries in addressing security and privacy issues, it isn't doing enough in key areas that significantly impact the telecommunications business model.

- **Infrastructure protection has emerged as a near-term priority.** This year, we note that the telecommunications sector is more likely than others to experience incidents that exploit networks (29% vs. 23%, the cross-industry average) and impact service levels by slowing networks or rendering them unavailable (44% vs. 38%). Telco respondents also report that incidents are more likely to result in alterations to software applications (37% vs. 32%). Among other strategies, stronger policies would help reduce these consequences. Most telco respondents (62%) report that their organization does not ensure that its security policies address security in system development (SDLC). And 42% say their policies do not include application security segregation-of-duty restrictions.
- **Third-party security languishes—even as old competitors morph into valuable allies.** The trend continues. The best value propositions in the industry are often those formed by industry partnerships that extend and complement existing technologies and service offerings. In spite of this, however, we note that most companies in the industry don't keep an accurate inventory of all third parties using customer data (72%). In addition, 70% of telco survey respondents are only "somewhat" or "not at all" confident in third-party security. And, while just over half (57%) require third parties (including outsource vendors) to comply with the organization's own privacy policies, only 48% have established security baselines for external 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 $\pm 1\%$.

This year, of the 675 respondents (9% of survey) from the telecommunications sector, 32% were from Europe, 23% from North America, 28% from Asia, and 13% from South America. Thirty-nine percent (39%) 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, visit: www.pwc.com/giss2007 or contact:

Mark Lobel
646 471 5731
mark.a.lobel@us.pwc.com

Deborah Bothun
213 217 3302
deborah.k.bothun@us.pwc.com

- **As more and more customer information is collected, the probability of a data breach is increasing.** Consumers are increasingly aware of the risks associated with identity theft—and sensitive to how well their service providers are protecting their private information. In spite of this, most telcos do not maintain an accurate inventory either of user data (65%) or of the locations or jurisdictions where this data is stored (68%). At the same time, while two out of three telcos encrypt data in transmission (65%), far fewer encrypt data at rest—in databases (49%), file shares (44%), laptops (45%) and backup tapes (36%). A greater focus on basic privacy protection processes would help. Survey responses indicate that only 41% of telcos require their employees to complete training on privacy policies and procedures. And only 24% employ a Chief Privacy Officer.
- **Aligning security with the business continues to be an elusive endeavor.** IT and security executives are having a hard time communicating the importance of security investments in business terms. Only 26% of telco respondents report that their company's spending on information security is "completely aligned" with business objectives. It may have something to do with who is at the table making investment decisions. One out of every two industry respondents (50%) says their company does not engage both business and IT decision-makers in addressing information security. At the same time, almost as many (47%) report that their organization has not both measured and reviewed the effectiveness of their information security policies and procedures in the past year. But demonstrating better business value for security investments will also have to involve making sure that better risk management is an explicit objective. This year, 68% of telco respondents say their organization's security policies do not include classifying the business value of data.

Security benchmarks: Telecommunications

(Percentage of responses from telecommunications vs. other industries)

	Telecom 2007	Technology 2006	FS 2007	All 2007
Have an overall security strategy	60%	59%	71%	57%
Employ either a CISO or CSO	78%	69%	86%	60%
Dedicate people to monitoring employee use of Internet/Information assets	51%	46%	59%	48%
Centralized security information management	48%	43%	57%	44%
Ensure secure disposal of technology hardware	53%	53%	65%	58%

© 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

