

How retail and consumer companies focused on compliance may be missing opportunities to reduce risk*

The Global State of Information Security 2007

#1

Ranking given to legal/regulatory compliance by R&C respondents when asked to identify how security investments are justified in their organization.

32%

Percentage of R&C respondents who say that security breaches in the past year resulted in alterations to software applications.

8 out of 10

Number of R&C respondents who say their organization does not have mechanisms in place to report incidents to customers.

42%

Percentage of R&C respondents who report that their organization has not measured and reviewed the effectiveness of their security policies and procedures in the past year.

At first glance, the news is good. This year, retail and consumer (R&C) respondents to the world's largest survey on privacy and information security practices, the Global State of Information Security 2007, report some progress—much of it likely driven by efforts to comply with Sarbanes as well as the PCI security standards. Compared to 2006, many more R&C organizations have an overall security strategy (52% vs. 34% in 2006) and a higher percentage this year have their Chief Information Security Officer reporting to the top of the organization—the Board of Directors, CEO, CFO or VP (58% vs. 51%). But complying with SOX and PCI doesn't always mean organizations are more secure. And mechanisms protecting credit card information don't necessarily protect other sensitive data—such as information collected through loyalty programs, customer and employee personal information and employee health information. In fact, a closer examination of survey responses suggests that many R&C companies should expand their focus beyond compliance to address security gaps in the following critical areas.

- **Privacy is high-profile. But not necessarily high priority.** R&C companies have made some gains in protecting privacy. They're much more likely this year than last to require employees to certify in writing that they're complying with privacy policies (52% vs. 34%) and to encrypt data in transmission (60% vs. 45%). But even though the PCI standards also require using encryption to protect stored data—where many data leakage incidents originate—many R&C companies have yet to encrypt sensitive data residing in databases (49%), laptops (52%), and on backup tapes (59%). At the same time, R&C companies are less likely than other sectors to hire a Chief Privacy Officer (14% vs. 22%) and much more likely to report their organization does not yet classify data and information assets according to risk level (42% vs. 30%).
- **Many are spending on technology—but not yet realizing gains from the investment.** Notable this year are much higher adoption rates for technologies such as malicious code detection tools (64% vs. 32%) and user activity monitoring tools (41% vs. 30%). But most industry executives (76%) say spending is either “poorly” or only “somewhat aligned” with business objectives. That may be because R&C companies are not putting the right people at the table: fewer than half (47%) actively engage both business and IT decision-makers in addressing security issues.

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 464 respondents in the retail and consumer industries (6% of survey), 37% were from North America, 23% from Europe, 23% from Asia, and 15% 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

Gerard Verweij
617 530 7015
gerard.verweij@us.pwc.com

Lisa Feigen Dugal
646 471 6916
lisa.feigen.dugal@us.pwc.com

- **The “insider threat” is on the rise.** This year, the percentage of R&C respondents who cite employees as the likely source of attack increased significantly (51% vs. 30%). In addition, 23% say the primary method of breach was the abuse of valid user accounts and permissions. In spite of this, less than one in four respondents say their organization has an automated account deprovisioning capability (21%) or an identity management solution (24%).
- **IT is back in the driver’s seat.** One of the most interesting trends that surfaced this year was a shift in the source of R&C information security funding from functional budgets such as legal, finance and regulatory compliance (23% vs. 49% in 2006) to information technology (74% vs. 46%). Also evident in most other industries, this trend is consistent with the tendency in many organizations to allow business functions to drive spending on technology-based initiatives—at least initially—until they become repeatable capabilities best centralized and maintained by IT.
- **Compliance regulations aside, few R&C companies extend their security practices to third parties.** Many also don’t realize that R&C companies are responsible for the protection of PCI data even when it is processed and stored by third parties such as records management companies, credit card processing organizations, and loyalty management providers. Survey data supports this observation. Slightly more than 1 in 5 (21%) R&C companies keep an inventory of all third parties using their customers’ data. Only 42% require third parties (including outsource vendors) to comply with their privacy policies. And only one in every three R&C companies (33%) ensures that their security policies define the procedures with which partners and suppliers must comply.

Security benchmarks: Retail and consumer sectors (Percentage of responses from R&C sectors vs. all industries)	All 2007	R&C 2007	R&C 2006
Have an overall security strategy	57%	52%	34%
Employ a CISO or CSO	60%	37%	24%
Link security through organizational structure or policy to compliance	42%	37%	23%
Ensure that security policies include enforcement mechanisms	31%	23%	19%
Have vulnerability scanning tools	50%	42%	26%

© 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