

How globalisation is rapidly spurring financial services firms to raise the bar in information security and privacy*

The Global State of Information Security 2007

44%

Percentage of financial services respondents who said their company has mechanisms in place to report security incidents out to customers or business partners.

43%

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

59%

Percentage of financial services respondents who say their company's information security policies do not include classifying the business value of data.

50%

Percentage of financial services respondents who report their organisation performs an enterprise risk assessment either annually or semi-annually.

New opportunities often change benchmarking thresholds for core capabilities. And so it is in the financial services industry—which many believe has been defining best practices in protecting privacy and securing information for years. As global initiatives open doors to new channels for enhanced performance and shareholder value, many financial services firms are also assuming greater risks. Globalisation is making it harder to centrally control and manage processes, policies and risks. And the web of collaborative arrangements continues to widen. As a result, it's getting harder to safeguard the sensitive information that supports building stronger relationships in a global marketplace. With increasing frequency, highly publicized data security breaches and concerns about identity theft are threatening to undermine trust, a cornerstone of the industry.

So this year we were pleased that 71% of the financial services respondents to the Global State of Information Security 2007—the world's largest survey on privacy and information security practices—now say their organisation has a security strategy in place. This is a watershed gain over last year's reported level (57%). But keeping up with a shifting set of risks, opportunities and regulatory requirements globally will require expanding capabilities in several crucial areas.

- **As the global regulatory environment becomes more complex, gains in protecting data privacy have slowed.** Progress has flattened out in key areas as privacy governance issues continue to challenge executives. Financial services firms may be more likely this year to employ a Chief Privacy Officer (33% vs. 25% last year) and require employees to certify in writing that they are complying with privacy policies (65% vs. 56%) but firms are less likely to review their privacy policies annually (56% vs. 61%) and provide employees with privacy-related training (58% vs. 69%).
- **The “insider threat” may actually be growing.** Industry respondents reporting that employees represented the most probable source of security incidents increased significantly—from 34% in 2006 to 51%—a ranking that places employees ahead of hackers for the first time in this survey. Has the “insider threat” truly increased—or are companies simply more aware of the threat? It isn't clear. But 38% of financial services respondents identified the primary method of security incidents as either the abuse of valid user accounts and permissions or “social engineering”. In spite of this, few respondents say their organization has tiered authentication levels based on user risk classification (38%) or an automated account deprovisioning capability (27%).

