

The global state of information security 2006

What the numbers say:

46%

Percentage of infocomm respondents who report their organization actively engages both business and IT decision-makers in addressing information security issues.

1 out of 4

Number of infocomm respondents who report that attacks resulted in denial of service.

#1

Ranking that infocomm respondents gave to intrusion-detection systems when asked to identify how their organization learned of a negative security incident. Only 51% of infocomm companies have such a system in place.

More than 7 of 10

Number of infocomm organizations that have not yet established security baselines for external vendors.

75%

Percentage of infocomm respondents who are not very confident in their partners' or suppliers' security (including that of their outsource vendors).

Results from the world's largest information security study are in. This year, responses to PricewaterhouseCoopers' and CIO magazine's Global State of Information Security study reveal that companies within the cable, Internet, and telecommunications sectors worldwide are spending a considerably larger portion of their IT budget on security than firms in other industries (23% vs. a 17.3% cross-industry average).

This fact, by itself, isn't news to industry insiders. The convergence of voice, video, and data that promises potentially enormous gains in shareholder value also requires competing in new markets, deploying unfamiliar technologies, and assuming the expanded portfolio of risks associated with a new and open business model. Surprisingly, though, the survey also reveals that despite this investment, infocomm companies are not doing a better job than companies in other industries at putting in place the basic building blocks of a sustainable security and privacy foundation.

- **Securing systems and infrastructure:** Infocomm companies are clearly more likely than firms in other industries to implement security for new technologies, such as voice-over-IP (27% vs. 18%) and web services (37% vs. 31%). But they're no more likely to have an overall security strategy in place (37% vs. 37%) or engage in periodic risk assessments (42% vs. 42%). And they're less likely to have a plan for business continuity and disaster recovery in effect (46% vs. 50%).
- **Protecting privacy:** Infocomm companies are also more likely than other organizations to encrypt stored data (39% vs. 33%) and post privacy policies on their internal websites (52% vs. 46%). But they lag in ensuring that security policies are reviewed at least once a year (40% vs. 43%) and that an accurate inventory of user data is kept (34% vs. 36%).
- **Assessing the risks:** This year, security incidents are occurring more often: Only 17% of companies in these sectors report no such incidents—half the rate reported in this survey last year (34%) and notably lower than this year's cross-industry average (27%). And when events did occur, they tended to have more impact than in other industries. Sector respondents were significantly more likely to report financial losses (25% vs. 19%) and negative impacts to their organization's brands and reputation (23% vs. 15%).

Survey Methodology:

The State of Information Security 2006, a worldwide security survey by PricewaterhouseCoopers and CIO magazine, was conducted online from April 5 to May 22, 2006. Readers of CIO magazine and CSO 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 7,791 responses from IT and security professionals in 50 countries. Respondent titles included CEO, CFO, CIO, CSO, and vice president, director, and manager of IT and information security. The margin of error is $\pm 1\%$.

Of the 626 respondents from the cable, Internet, and telecommunications industries (8% of survey), 36% were from Europe, 29% from South America, 17% from Asia, and 16% from North America. Thirty-four percent reported annual revenues of at least \$100 million.

To learn more about the survey, or about the Security and Privacy practice at PwC, visit:
www.pwc.com/GISS2006

or contact:
Mark Lobel
646.471.5731
mark.a.lobel@us.pwc.com

Rik Boren
314.206.8899
rik.boren@us.pwc.com

Critical areas needing improvement

Given that security is crucial to extending advanced services successfully and sustainably to customers through new content-delivery technologies and new models of value creation, we believe the following areas, in particular, require executive attention.

Preventing service disruptions by protecting the network

Survey results point to clear deficits in network security. Most infocomm companies (73%) do not use patch management tools, even though, when asked how attacks occurred, 43% of respondents pointed to exploitation of a known application or operating system vulnerability. Only 67% deploy application firewalls and even fewer (60%) use network security tools.

Securing content and data across the entire information lifecycle

At the heart of the emerging new business models is the assumption that content and other forms of data can be protected—not just within the application but across the entire information lifecycle. Forty-six percent of infocomm organizations, however, do not address data protection, disclosure, and destruction in their security policies. Moreover, 24% do not classify data and information assets according to risk levels, and 53% do not encrypt data in transmission.

Ensuring third-party privacy and security practices

Today it's almost impossible to deliver telecom services to customers and value to shareholders without collaboration with third parties. However, only 26% of infocomm companies keep an accurate inventory of all third parties using customer data and most (67%) do not yet require third parties (including outsourcing vendors) to comply with their privacy policies. In addition, while incidents involving the loss or theft of executive laptops and their stored data continue to occur, 73% of infocomm organizations do not yet have security standards or procedures for handheld and portable devices.

InfoComm: security benchmarks

(Percentage of infocomm sector responses compared to other industries)

	All	InfoComm	Financial services
Have overall security strategy	37%	37%	57%
Conduct security awareness training for employees	39%	40%	60%
Have a business continuity/disaster recovery plan	50%	46%	75%
Employs a CISO or CSO	43%	59%	75%

