

How aerospace and defense companies are seeking better business value from information security*

The Global State of Information Security 2007

6 out of 10

Number of A&D respondents who say their organization's security policies do not include classifying the business value of data.

41%

Percentage of A&D respondents who report their organization conducts an enterprise risk assessment at least semi-annually.

1 out of 2

Number of A&D respondents who say their organization has security standards in place for handheld devices.

46%

Percentage of A&D respondents who say their organization integrates physical security and information security personnel.

Across the aerospace and defense (A&D) industry, information technology systems are under intense pressure to meet high and growing levels of demand for more measurable contributions to business value and performance. For some companies, it's the need to better align Sarbanes Oxley processes with business strategies that's driving demand. For others, it's the ongoing consolidation of stand-alone operations—or executive calls for more effective and efficient security, financial reporting or program management.

So, this year, we are pleased that A&D responses to the world's largest survey on privacy and information security practices—the Global State of Information Security 2007—reveal significant gains made since last year in areas such as establishing an overall information security strategy (67% in 2007 vs. 55% in 2006); engaging processes to protect intellectual property (61% vs. 37%); and linking security, through either organization or policy, to privacy and regulatory compliance (57% vs. 48%). But responses also reveal that, as pressures to reduce risks, improve controls, and carve out better cost efficiencies rise, A&D companies still have significant opportunities to better align their extensive investments in security with their business objectives.

- **Taking advantage of global opportunities will require much better third-party security.** As A&D companies seek to attract more international buyers and leverage a broader global pool of suppliers, they are turning more often to special purpose entities such as joint ventures, partnerships and proxy boards to qualify as suppliers in foreign countries. Yet 63% of A&D survey respondents are only “somewhat” or “not at all” confident in third-party security. Only three out of ten A&D companies keep an accurate inventory of all third parties using customer data and less than half (47%) have established security baselines for external partners, customers and suppliers.
- **As centralization assumes new urgency, some A&D companies are putting IT back in the driver's seat.** One of the most interesting trends this year is a clear shift in the source of A&D information security funding from functional budgets such as legal, finance and regulatory compliance (37% in 2007 vs. 56% in 2006) to information technology (59% vs. 49%). As the drive to centralize funding picks up steam, we also note a comparable shift in performance accountability: A&D companies are much more likely this year than last to have their CISO report to the CIO (51% vs. 32%).

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 171 respondents in the aerospace and defense industries (2% of survey), 48% were from North America, 29% from Europe, 13% from Asia, and 7% from South America. Twenty-six percent (26%) reported annual revenues of at least \$10 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

Donald Christian
703 610 7500
donald.b.christian@us.pwc.com

James Thomas
202 414 1370
james.w.thomas@us.pwc.com

- **A&D organizations are slow to invest in automation that would improve compliance.** A&D companies are certainly investing in technology. This year, responses reveal much higher adoption rates for external threat technologies such as malicious code detection tools (73% vs. 54% in 2006) and vulnerability scanning tools (61% vs. 42%). But much fewer are investing in technologies that would better support regulatory compliance and risk management objectives. Only 39% have implemented identity management solutions to automate controls for access and segregation-of-duties (SoD) requirements. And while most A&D respondents (69%) say their organizations encrypt data in transmission, less than half are protecting data at rest—where so many incidents of data leakage originate: only 44% encrypt data residing in databases and even fewer (34%) encrypt data on removable media.
- **The “insider threat” may actually be growing.** This year, the percentage of A&D respondents reporting that employees represented the most probable source of security incidents increased significantly—from 46% in 2006 to 60%—a ranking that also exceeds the cross-industry average this year (48%). Another 26% of incidents were attributed to former employees. Has the “insider threat” truly increased—or are companies simply more aware of the threat? It isn’t clear. But 45% of A&D 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 automated account deprovisioning capability (27%)—and only 61% conduct employee security awareness training programs.

Security benchmarks: Aerospace and Defense

(Percentage of all A&D sector responses for the last two years compared to the cross-industry average for all companies as well as for those with at least \$25B in revenue)

	A&D 2007	A&D 2006	All 2007	All 2007 (\$25B+)
Have an overall security strategy	67%	55%	57%	77%
Integrate privacy and compliance plans	44%	37%	28%	53%
Encrypt data in transmission	69%	64%	61%	81%
Ensure that security policies address application security segregation-of-duties	65%	49%	53%	78%
Have established a centralized security information management process	55%	53%	44%	66%

© 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

