

How privacy is assuming new urgency as entertainment and media companies evolve toward closer relationships with consumers*

The Global State of Information Security 2007

Almost 7 out of 10

Number of E&M respondents who report their organization does not have procedures in place dedicated to protecting intellectual property.

28%

Percentage of E&M respondents who report that their organization requires third parties (including outsource vendors) to comply with privacy policies. The cross-industry average is 41%.

Less than half

Number of E&M respondents (46%) who say their company's CISO or equivalent reports to the top of the organization (Board, CEO, CFO or VP). The cross-industry average is significantly higher (72%).

80%

Percentage of E&M respondents who report their organization does not have security standards or procedures in place for handheld or portable devices such as flash drives or external drives.

As entertainment and media (E&M) sector companies continue to embrace new business models and digital distribution channels, they are also focused on securing the safety of the sector's single most important asset, digital content. And, since many are evolving toward closer relationships with consumers and partners, protecting privacy is becoming an increasingly urgent priority.

So this year we were pleased that 43% of E&M respondents to the Global State of Information Security 2007, the world's largest survey on privacy and information security practices, now say their organization has a security strategy—a clear improvement over last year's reported level (30%). However, the cross-industry average for having a strategy is much higher (57%) and E&M security practices tend to lag behind companies in other industries. While there is some good news, E&M companies are encountering expanding risks—to intellectual property (IP), digital assets, and reputations—and protecting future performance will require sustained focus in several critical areas.

- **Protecting privacy is an emerging imperative**—At the top of the list is the need to protect sensitive customer information. Today, however, E&M companies are less likely than those in other industries to employ a Chief Privacy Officer (14% vs. 22%), keep an accurate inventory of where they store user data internally (28% vs. 33%) and provide employees with training on privacy policy and practices (38% vs. 49%). This gap also extends to practices that require little investment—such as requiring employees to certify in writing that they are complying with privacy policies (42% vs. 53%) and posting privacy policies on the organization's internal website (50% vs. 60%). In addition, although data leakage incidents typically impact data at rest, E&M organizations lag behind other industries in using encryption to protect laptops (33% vs. 42%), file shares (29% vs. 36%) and backup tapes (30% vs. 38%).
- **The “insider” threat may be growing**—This year, E&M respondents are more than twice as likely to consider employees as the probable source of an attack (44% vs. 21% in 2006). Another 18% consider former employees the probable culprits and 22% say the primary method of breach was the abuse of valid user accounts and permissions. In spite of this, most E&M companies do not have an automated account deprovisioning capability (84%). And more than half do not ensure that security policies define the appropriate use of email (54%) or conduct personnel background checks (57%).

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 ±1%.

Of the 232 respondents in the entertainment and media industries (3% of survey), 36% were from North America, 25% from Europe, 23% from Asia, and 15% from South America. Thirty percent (30%) reported annual revenues of at least \$500 million.

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

Dana McIlwain
646 471 3305
dana.mcilwain@us.pwc.com

- **Application and system security needs attention**—One of the frontlines of defense in preventing content piracy and protecting intellectual property is securing applications and systems. This year, however, E&M respondents were much more likely to report that security attacks exploited known application or operating system vulnerabilities (53% vs. 41%)—a rate significantly higher than this year’s cross-industry average (35%). And almost 4 in 10 reported that the attack altered software applications. How can E&M companies begin closing this gap? By improving basic policies and practices. Survey responses reveal that the E&M sectors lag behind other sectors in applying user passwords (68% vs. 80%), using application firewalls (57% vs. 62%) and ensuring that their security policies address segregation-of-duty conflicts at the application level (46% vs. 58%). In addition, only 29% have security policies for Security in System Development (SDLC).
- **Securing data beyond the network is critical**—Extracting value from new E&M business models and monetizing digital content is increasingly difficult without sharing data with partners and suppliers. Yet most E&M companies (84%) do not have an inventory of all third parties using customer data. And only one out of three (36%) have established security baselines for partners, customers and suppliers.
- **Preparing for major disruptive events**—When asked to identify which business issues or factors are driving information security spending, E&M respondents overwhelmingly selected business continuity and disaster recovery (60%)—over other factors such as compliance with regulations (41%) or internal policies (45%). In spite of this, only 37% reported that their organization has a business continuity or disaster recovery plan in place.

Security benchmarks: Entertainment and media sectors (Percentage of responses from E&M sectors vs. all industries)	All 2007	E&M 2007	E&M 2006	E&M 2005
Have an overall security strategy	57%	43%	30%	31%
Employ a CISO or CSO	60%	46%	41%	19%
Link security through organizational structure or policy to compliance	42%	29%	24%	21%
Ensure that security policies include user security awareness training	43%	31%	25%	23%
Use secure browsers	55%	49%	35%	28%

© 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

