

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 organisation does not have procedures in place dedicated to protecting intellectual property.

28%

Percentage of E&M respondents who report that their organisation 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 organisation (Board, CEO, CFO or VP). The cross-industry average is significantly higher (72%).

80%

Percentage of E&M respondents who report their organisation 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 organisation 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 organisation's internal website (50% vs. 60%). In addition, although data leakage incidents typically impact data at rest, E&M organisations 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%).

