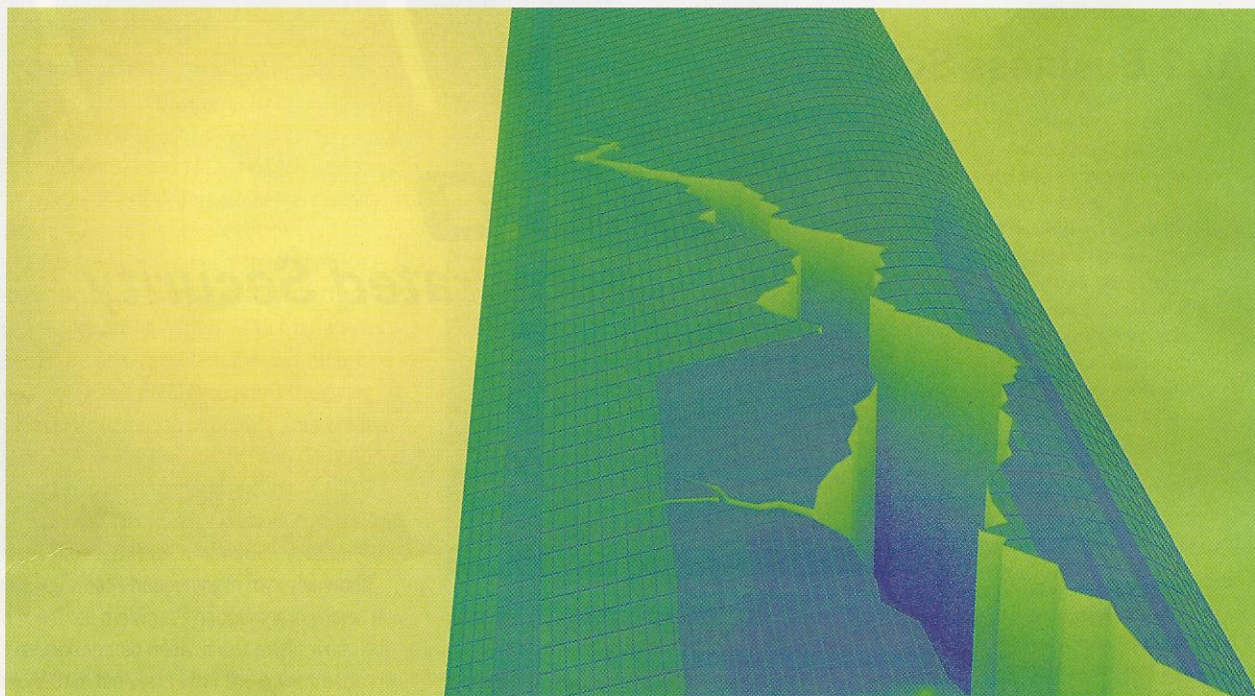


# tech

TOOLS SYSTEMS NETWORKS DATA PRIVACY



## Half Measures Can be Fatal

It's only a matter of time before you suffer a breach. What's your incident-response plan? BY GEORGE V. HULME

ROUGHLY \$60 BILLION WILL BE INVESTED in IT security products and services this year, according to the market research firm Gartner. That's up from \$55 billion last year, with growth expected through at least 2016, when security spending is anticipated to hit a staggering \$86 billion annually.

That's no small sum, and leads observers to ask whether organizations are getting value for their money. With more than 560 million records exposed in 3,438 data breaches since 2005, according to the Privacy Rights Clearinghouse, the only honest answer can be along the lines of "not really."

According to the tenth annual Global Information Security Survey (GISS), conducted by PricewaterhouseCoopers in partnership with CSO, many of the 12,052 business and technology execs surveyed reported that their organizations fell victim to a wide variety of breaches. Those breaches included data exfiltration, mobile attacks, application breaches, network breaches, successful social engineering attacks, and lost or stolen removable storage devices. "One of the things I try convince clients is that while they may not be able to prevent certain breaches, they can certainly learn to respond to breaches more proactive-

ly," says Dave Shackleford, CTO and senior vice president of research at IANS.

With roughly 70 percent of respondents to our survey admitting to having suffered a breach in the past 12 months, it's amazing so few companies heed Shackleford's advice. Of our respondents, only 27 percent have an incident-response process that covers reporting breaches to third parties that handle data. Only 24 percent of respondents have an incident-response plan in place as part of their larger security policy. And even when a company has an incident-response plan, key personnel are often unaware of it.

CSO Staff