CPA
Practice Advisor

Jun. 12, 2013

Despite broad recognition that cyber threats are more prevalent than ever before, a large number of companies are not adequately prepared to respond to a data breach or IT security crisis, according to findings from the 2013 IT Security and Privacy Survey by global consulting firm Protiviti (www.protiviti.com).

More than two-thirds (68 percent) of respondents in Protiviti’s survey said they have elevated their focus on information security in response to recent press coverage of so-called “cyber warfare.” However, the number of companies that appear inadequately prepared for a crisis is surprisingly high. When asked if their organizations have a formal and documented crisis response plan for use following a data breach or hacking incident, more than one-third reported that either their organizations did not (21 percent) or they did not know (13 percent).

“Cyber security must continue to be a major focus for businesses, especially in light of recent high-profile security breaches,” said Cal Slemp, managing director with Protiviti and global leader of the firm’s IT security and privacy practice. “While we’re seeing a greater number of companies across a wider range of industries devote more attention and resources to improving their approach to data security, there are still a lot of businesses that are susceptible to attacks.”

Data Policy and Retention/Storage Issues

According to the survey results, many companies lack key data policies and are ineffective at managing data through proper retention and storage practices, including the classification of sensitive data. Approximately 22 percent of companies do not have a written information security policy (WISP) and 32 percent lack a data encryption policy. Not having these policies in place is an important consideration when a breach involves information covered by data privacy laws and can expose an

detailed schemes and policies to classify their data, which is key to understanding and securing an organization’s most sensitive information.

CIOs Take a More Strategic Role

Another positive development is that, as data security continues to play a larger role in business operations and the use of so-called big data becomes more integrated with strategic business objectives, CIOs are seeing their responsibilities increase. The survey showed that more CIOs are taking responsibility for data governance strategy, oversight and execution within their organizations. Additionally, companies with documented crisis plans enacted in response to a data breach or hacking incident have now begun to involve their CIOs far more than ever before. In 2012, only 58 percent reported that their CIO was involved in addressing such an incident compared to 72 percent in 2013 (up 14 percent).

“The role of the Chief Information Officer is becoming more prominent in organizations, in part, because of the importance of data, both in terms of advancing the business as well as managing risk,” said Slemp. The reality is that as data continues to evolve as a critically important asset, it must be managed differently, and more effectively than other assets.”

Survey and Benchmarking Tool

The second edition of Protiviti’s IT Security and Privacy Survey gathered insights from 194 information technology executives and professionals at companies with gross annual revenues ranging from less than $100 million to greater than $20 billion. The survey was conducted in the first and second quarters of 2013. Respondents included CIOs, CSOs, IT directors, managers and IT auditors. The survey is available at: www.protiviti.com/ITsecuritysurvey.

IT professionals can also compare their organization’s policies and practices to the

Accounting • Auditing • Firm Management • Security • Small Business • Technology

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.