protiviti®
Risk & Business Consulting.
Internal Audit.

MEDIA RELEASE

24 July 2013

Companies not prepared for cyber threats

CIOs are assuming more strategic roles based on evolving risks and opportunities

Despite broad recognition that **cyber threats** are **more prevalent than ever**, a large number of companies are not adequately prepared to respond to a data breach or IT security crisis, the Protiviti's *2013 IT Security and Privacy Survey* has found.

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 organisations 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 organisations 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 Protiviti managing director Mark Harrison. "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 organization to significant legal liability.

Companies also lack clarity on what constitutes data as sensitive, confidential or public, with only 63 percent of respondents reporting that their organisations have a system for properly classifying data. "The findings suggest many companies are either ineffective in securing the most important data or attempting to secure all data instead of focusing resources on data that presents the greatest risk, if exposed through a breach," said Mr Harrison. However, he added that in a positive development, there was year-over-year growth in the percentage of companies putting into place detailed schemes and policies to classify their data, which is key to understanding and securing an organisation'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."

About the survey

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.

Webinar and Podcast Explore Survey Results

A complimentary webinar discussing the survey results will be held XXXXXXXXXXXXXXXXXX

About Protiviti

Protiviti (www.protiviti.com.au) is a global consulting and internal audit firm composed of experts specialising in risk and advisory services. The firm helps clients solve problems in finance, operations, technology, litigation and governance, risk and compliance. Protiviti's highly trained, results-oriented professionals serve clients in, Asia-Pacific, the Americas, Europe and the Middle East and provide a unique perspective on a wide range of critical business issues.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

# # #

Protiviti is not a law firm and is not licensed or registered as a public accounting firm. The company does not issue opinions on financial statements or offer attestation services.