News release

Date 13 October 2014

Contact Pavol Adamec, Director, PwC
Tel.: +421 2 59350 042
pavol.adamec@sk.pwc.com

Zuzana Sehnalová, Marketing & Communications Leader, PwC
Tel.: +421 2 59350 133
Mobile: +421 911 357 151
zuzana.sehnalova@sk.pwc.com

Cybersecurity Incidents More Frequent and Costly, but Budgets Decline, Says PwC, *CIO* and *CSO* Global State of Information Security® Survey 2015

Impact extends to C-suite and boardroom, insider incidents and high-profile crimes increasing

Bratislava, New York, NY and Framingham, MA, 13 October 2014 -- The number of reported information security incidents around the world rose 48 percent to 42.8 million, the equivalent of 117,339 attacks per day in 2013, according to *The Global State of Information Security® Survey 2015,* released in September by PwC, in conjunction with *CIO* and *CSO* magazines. Detected security incidents have increased 66 percent year-over-year since 2009, the survey data indicates.

"It's not surprising that reported security breach incidents and the associated financial impact continue to rise year-over-year," said David Burg, PwC's Global and US Advisory Cybersecurity Leader. "However, the actual magnitude of these breaches is much higher when considering the nature of detection and reporting of these incidents."

As security incidents become more frequent, the associated costs of managing and mitigating breaches are also increasing. Globally, the estimated reported average financial loss from cybersecurity incidents was $2.7 million – a 34 percent increase over 2013. Big losses have been more common this year as organizations reporting financial hits in excess of $20 million nearly doubled.

But despite elevated concerns, the survey found that global information security budgets actually decreased four percent compared with 2013. Security spending as a percentage of IT budget has remained stalled at 4 percent or less for the past five years.

"Strategic security spending demands that businesses identify and invest in cybersecurity practices that are most relevant to today's advanced attacks," explained Mark Lobel, PwC Advisory principal focused on information security. "It's critical to fund processes that fully integrate predictive, preventive, detective and incident-response capabilities to minimize the impact of these incidents."

Organizations of all sizes and industries are aware of the serious risks involved with cybersecurity; however, larger companies detect more incidents. Large organizations – with gross annual revenues of $1 billion or more – detected 44 percent more incidents this year. Medium-sized organizations – with revenues of $100 million to $1 billion – witnessed a 64 percent increase in the number of incidents detected. And while risk has become universal, the survey found that financial losses also vary widely by organizational size.

"Large companies have been more likely targets for threat actors since they offer more valuable information, and thus detect more incidents," said Bob Bragdon, publisher of *CSO*. "However, as large companies implement more effective security measures, threat actors are increasing their assaults on middle-tier companies. Unfortunately, these organizations may not yet have security practices in place to match the efficiency of large companies."

Insiders have become the most-cited culprits of cybercrime – but in many cases, they unwittingly compromise data through loss of mobile devices or targeted phishing schemes. Respondents said incidents caused by current employees increased 10 percent, while those attributed to current and former service providers, consultants and contractors rose 15 percent and 17 percent, respectively. "Many organizations often handle the consequences of insider cybercrime internally instead of involving law enforcement or legal charges. In doing so, they may leave other organizations vulnerable if they hire these employees in the future," added Bragdon.

Meanwhile, high profile attacks by nation-states, organized crime and competitors are among the least frequent incidents, yet the fastest-growing cyber threats. This year, respondents who reported a cyber-attack by nation-states increased 86 percent – and those incidents are also most likely under-reported. The survey also found a striking 64 percent increase in security incidents attributed to competitors, some of whom may be backed by nation-states.

Effective security awareness requires top-down commitment and communication, a tactic that the survey finds is often lacking across organizations. Only 49 percent of respondents say their organization has a cross-organizational? team that regularly convenes to discuss, coordinate, and communicate information security issues.

PwC notes that it is critical for companies to focus on rapid detection of security intrusions and to have an effective, timely response. Given today's interconnected business ecosystem, it is just as important to establish policies and processes regarding third parties that interact with the business.

"Cyber risks will never be completely eliminated, and with the rising tide of cybercrime, organizations must remain vigilant and agile in the face of a constantly evolving landscape," said PwC's Burg. "Organizations must shift from security that focuses on prevention and controls, to a risk-based approach that prioritizes an organization's most valuable assets and its most relevant threats. Investing in robust internal security awareness policies and processes will be critical to the ongoing success of any organization."

To download a copy of the *2015 Global State of Information Security Survey* and learn more about PwC's capabilities, visit: http://pwc.to/GSISS15

NOTES TO EDITORS:
Proper citation of the study is "The Global State of Information Security® Survey 2015, a worldwide survey by *CIO, CSO* and PwC." Source must include *CIO*, *CSO* and PwC. Survey results will also be covered in depth on *CIO.com* and CSOonline.com in October.

Methodology
The Global State of Information Security® Survey 2015 is a worldwide study by PwC, *CIO* and *CSO*. It was conducted online from March 27, 2014 to May 25, 2014. Readers of *CIO* and *CSO* and clients of PwC from around the globe were invited via e-mail to take the survey. The results discussed in this report are based on responses of more than 9,700 CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security practices from more than 154 countries. Thirty-five percent of respondents are from North America, 34 percent from Europe, 14 percent from Asia Pacific, 13 percent from South America, and four percent from the Middle East and Africa. The margin of error is less than one percent.

About *CIO* and *CSO*

CIO is the premier content and community resource for information technology executives and leaders thriving and prospering in this fast-paced era of IT transformation in the enterprise. The award-winning *CIO* portfolio—CIO.com, *CIO* magazine (launched in 1987), CIO executive programs, CIO marketing services, CIO Forum on LinkedIn and CIO primary research—provides business technology leaders with analysis and insight on information technology trends and a keen understanding of IT's role in achieving business goals. Additionally, *CIO* provides opportunities for IT solution providers to reach this executive IT audience. *CIO* is published by IDG Enterprise, a subsidiary of International Data Group (IDG), the world's leading media, events, and research company. Company information is available at www.idgenterprise.com.

CSO is the premier content and community resource for security decision-makers leading "business risk management" efforts within their organization. For more than a decade, *CSO*'s award-winning Web site (CSOonline.com), executive conferences, marketing services and research have equipped security decision-makers to mitigate both IT and corporate/physical risk for their organizations and provided opportunities for security vendors looking to reach this audience. To assist CSOs in educating their organizations' employees on corporate and personal security practices, *CSO* also produces the quarterly newsletter *Security Smart*. *CSO* is published by IDG Enterprise, a subsidiary of International Data Group (IDG), the world's leading media, events and research company. Company information is available at www.idgenterprise.com.

The Global State of Information Security® is a registered trademark of International Data Group, Inc.

About PwC

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 157 countries with more than 195,000 people who are committed to delivering quality in assurance, tax and advisory services. Find out more and tell us what matters to you by visiting us at www.pwc.com/sk.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.