News Release

Contacts:

For PwC:
Suzanne Dawson
LAK Public Relations, Inc.
sdawson@lakpr.com
212-329-1420

Kathryn Oliver
PwC US
kathryn.oliver@us.pwc.com
860-345-3550

For CSO:
Heather Davis
hdavis@idgenterprise.com
508-766-5375

For the FBI:
Jenny Shearer
jenny.shearer@ic.fbi.gov
202-324-3691

For the U.S. Secret Service:
Max Milien
max.milien@usss.dhs.com
202-406-5708

For CERT:
Richard Lynch
rlynch@sei.cmu.edu
412-268-4087

As Cybercrime Threats Continue to Escalate, 2013 State of Cybercrime Survey from PwC and *CSO* Finds Companies Aren't Doing Enough to Defend Themselves

Stark reality: respondents still do not understand the extent of threats and how to combat them; survey results point to serious implication to U.S. and global business if senior executives do not take action now

NEW YORK, June 20, 2013 – PwC US and *CSO* magazine today released the 2013 State of Cybercrime Survey, which reveals that while cybercrime threats are on the rise, current attempts to counter them remain largely unsuccessful. According to the report, organizations have made little progress in developing ways to defend themselves against both internal and external cyber opponents. Over 500 U.S. executives, security experts, and others from the private and public sectors were surveyed on their views on the state of cybercrime. The survey is a collaborative effort with PwC, *CSO* magazine, the U.S. Secret Service, the Software Engineering Institute CERT® Program at Carnegie Mellon University, and the FBI.

"The facts are clear: today's organizations are not taking the necessary steps to mitigate the risk of cybercrime, even in the face of increasingly serious and frequent threats," said David Burg, PwC principal in the firm's U.S. Advisory practice focused on cybersecurity. "PwC believes the time is *now* for organizations to take action. The threat to U.S. business and our nation's infrastructure is very real. Cybersecurity is a business imperative, and senior executives and Boards need to understand the challenges, educate their employees to raise awareness and increase vigilance, and apply cyber threat intelligence to help abate risks from sophisticated threat actors."

"Possibly the most alarming theme that came out of this year's survey results was that U.S. organizations are misjudging the severity of risks they face from cyber attacks from a financial, reputational, and regulatory perspective," said Bob Bragdon, vp and publisher, *CSO*. "Organizations have increased their

attack surface as a result of doing business in an increasingly interconnected and interdependent business landscape. Cyber threats can come from outside and inside the organization. Public awareness has been largely focused on the more sensational successful cyber espionage attacks from nation-states, but the fact is insiders with malicious intent also pose a great security risk."

Although the survey did confirm that attacks continue to range from targeted and sophisticated to fairly simple exploits of vulnerabilities created by years of underinvestment in security programs, technologies, and processes, PwC believes the cybersecurity challenge can – and must -- be met. In many cases companies can be successful in mitigating these attacks with a thorough cybersecurity strategy that is aligned to the business strategy and includes vigilant and proactive awareness of the threat environment, a strong asset identification and protection program and is supported by proactive monitoring and enhanced incident response processes. Attacks that are most severe, often from nation-states, should be faced in conjunction with government agencies.

"Insiders continue to be a threat that must be recognized as part of an organization's enterprise-wide risk assessment. Whether an incident is perpetrated by an employee, contractor, or trusted business partner with malicious intent or without, organizations should implement controls to prevent and detect suspicious activity and take action to consistently respond to the activity," said Randy Trzeciak, technical manager of the Insider Threat Center at CERT.

For the second year in a row, respondents identified insider crimes (33.73 percent) as likely to cause more damage to an organization than external attacks (31.34 percent). The study found that:

- Seventeen percent of respondents who had suffered an insider attack did not know what the consequences entailed;
- Thirty-three percent of respondents had no formalized insider threat response plan;
- Twice as many respondents indicated "non-malicious insiders" cause more sensitive data loss than malicious inside actors; and
- Of those who did know what the insider threat handling procedures were, the majority reported that the cases were handled in-house, without legal action or law enforcement involvement

"One of the key elements in defending against insider attacks is employee training and awareness," added Burg. "Insider threat actors often show early warning signs of malicious intent that IT security tools cannot detect, but which employees and managers will notice – and can respond accordingly."

"The potential threat from insiders cannot be underestimated or dismissed as inconsequential," said Ed Lowry, Special Agent in Charge, Criminal Investigative Division, U.S. Secret Service. "In the current environment, any business model must include a comprehensive cyber security plan that addresses both physical and IT systems security threats. This plan should include education, training, and awareness of all employees and redundant auditing procedures that will help mitigate a single point of failure vulnerability."

"We must consistently get past the privacy and liability issues that arise in the private sector reporting cyber intrusions to the government," said FBI Executive Assistant Director Richard McFeely. "When that happens, we have seen recent notable examples of the power of private sector and government coming together to counter our cyber adversaries."

"Cybercrime is an equal opportunity event and an active cyber defense program is imperative for all organizations," continued Burg. "Today's business leaders need to step up and take a proactive stand to protect their business ecosystem."

For the full survey report, please visit: www.pwc.com/cybersecurity.

PwC's cybersecurity consulting professionals help organizations understand the complex cyber challenges they face today. PwC provides strategies for clients to adapt and respond to risks, and prioritize and

protect the most crucial assets to their business strategy and goals. For more information on PwC's cybersecurity point of view, visit: www.pwc.com/cybersecurity.

Methodology
The 2013 State of Cybercrime Survey was conducted by *CSO* magazine in collaboration with PwC, the U.S. Secret Service and the Software Engineering Institute CERT Program at Carnegie Mellon University. The survey was conducted between March 20 and April 25, 2013. Over 500 US executives, security experts, and others from the private and public sectors responded to the survey questions.

Note to Editors: References to the 2013 State of Cybercrime Survey must reference PwC, *CSO* magazine, the U.S. Secret Service and the Software Engineering Institute CERT Program at Carnegie Mellon University.

About *CSO* Magazine
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), publication, executive conferences, custom solutions 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.

About the United States Secret Service
The U.S. Secret Service has taken a lead role in mitigating the threat of financial crimes since the agency's inception in 1865. As technology has evolved, the scope of the U.S. Secret Service's mission has expanded from its original counterfeit currency investigations to also include emerging financial and cybercrimes. As a component agency within the U.S. Department of Homeland Security, the U.S. Secret Service, through their Electronic Crimes Task Forces, has established successful partnerships in law enforcement business and academic communities – across the country and around the world – in order to effectively combat financial and cybercrimes. More information can be found at: www.secretservice.gov.

About the Software Engineering Institute and the CERT Program
The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University. The SEI helps organizations make measurable improvements in their software engineering capabilities by providing technical leadership to advance the practice of software engineering. The CERT Program serves as a center of enterprise and network security research, analysis, and training within the SEI. For more information, visit the CERT website at http://www.cert.org and the SEI website at http://www.sei.cmu.edu.

About the FBI
As an intelligence-driven and a threat-focused national security organization with both intelligence and law enforcement responsibilities, the mission of the FBI is to protect and defend the United States against terrorist and foreign intelligence threats, including cyber-based attacks and high-technology crimes; to uphold and enforce the criminal laws of the United States; and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

About PwC's Advisory Practice
PwC's Advisory professionals help organizations improve business performance, respond quickly and effectively to crisis, and extract value from transactions. We understand our clients' industries and unique business challenges, and look across the entire organization — focusing on strategy, structure, people, process and technology — to help clients build their next competitive advantage. See www.pwc.com/us/consulting for more information or follow us @PwCAdvisory.

About PwC US
PwC US helps organizations and individuals create the value they're looking for. We're a member of the PwC network of firms in 158 countries with more than 180,000 people. We're committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com/US.

Learn more about PwC by following us online: @PwC_LLP, YouTube, LinkedIn, Facebook and Google +.

© 2013 PricewaterhouseCoopers LLP, a Delaware limited liability partnership. All rights reserved. PwC refers to the US member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

# # #