## Business Leaders Gaining on Cybersecurity Risks, according to the PwC CIO and CSO Global State of Information Security® Survey 2016

- *New tools are helping to transform cybersecurity frameworks, yielding holistic, integrated safeguards against cyberattacks*
- *Cloud computing has had a significant impact on technology innovation in the past decade, and it is increasingly central to secure interconnected digital ecosystems*
- *The Internet of Things are expected to increase the stakes for securing cloud-based networks as the number of internet connected devices continues to surge to greater than 30 billion by 2020*
- *There was a 38% increase in detected information security incidents, as well as a 24% boost in security budgets observed in 2015*

**NEW YORK, NY and FRAMINGHAM, MA October 7, 2015 –** Year after year, cyberattacks continue to escalate in frequency, severity and impact. However, prevention, detection methods and cybersecurity innovation are on the rise as forward-leaning business leaders focus on solutions that reduce cybersecurity risks and improve business performance. The Global State of Information Security® Survey 2016 released today by PwC US in conjunction with CIO and CSO examines how executives are looking towards new innovations and frameworks to improve security and mitigate enterprise risk.

As cyber-risks become increasingly prominent concerns in the C-suite and boardroom, business leaders are increasingly rethinking cybersecurity practices, focusing on a nexus of innovative technologies that can reduce enterprise risks and improve performance. The vast majority of organizations – 91% – have adopted a security framework, or more often, an amalgam of frameworks. These technologies are yielding considerable opportunities to improve cybersecurity and produce holistic, integrated safeguards against cyber-attacks.

"We are seeing more of what we once saw as a risk, being turned into possible solutions," said David Burg PwC's Global and US Advisory Cybersecurity Leader. "For example, many organizations are embracing advanced authentication as a cloud service in place of solely password based authentication."

The adapting of traditional cybersecurity measures to an increasingly cloud-based world is an example of this effort with considerable investments being made to develop new network infrastructure capabilities that enable improved intelligence gathering, threat modeling, defense against attacks and incident response. According to the report, 69% of respondents said they use cloud-based security services to help protect sensitive data and ensure privacy and the protection of consumer information.

Connected to the emergence of cloud-based systems, Big Data and the Internet of Things are each ascendant technologies that present a host of cyber challenges and opportunities. In the case of Big Data, often considered a cyber liability, 59% of respondents are leveraging data-powered analytics to enhance security by shifting security away from perimeter-based defenses and enable organizations to put real-time information to use in ways that create real value.

As the number of internet connected devices continues to surge, the Internet of Things will inevitably increase the stakes for securing cloud-based networks. Investment intended to address these issues doubled in 2015, but at this point only 36% of survey respondents have a strategy specifically addressing the Internet of Things.

"There is no one-size-fits-all model for effective cybersecurity. It's a journey toward a future state that starts with the right mix of technologies, processes, and people skills," added Burg. "With those components in place, cybersecurity potentially serve as an indispensable ongoing business enabler."

Over the past three years, the number of organizations that embrace external collaboration has steadily increased. Sixty-five percent of respondents report they are collaborating with others to improve security. As more businesses share more data with an expanding roster of partners and customers, it makes sense that they also would swap intelligence on cybersecurity threats and responses.

"An advanced and enhanced information security program will not only enable companies to better defend against cyberthreats, it will also help create competitive advantages and foster trust among customers and business partners," said Bob Bragdon, VP/publisher of CSO.

Additional notable findings this year include:

- **Information security spending increases:** Respondents boosted information security spending significantly, reversing last year's slight drop in security spending. This year respondents boosted their information security budgets by 24% in 2015.
- **Evolving Cybersecurity Roles:** 54% of respondents have a CISO in charge of the security program. The most frequently cited reporting structure is the CEO, CIO, Board and CTO, in that order.
- **Increasing Board Involvement**: 45% of boards participate in the overall security strategy. This deepening of Board involvement has helped improve security practices in numerous ways.
- **Mobile Payments Going Mainstream**: 57% of respondents have adopted mobile payments systems - but the ecosystem continues to rapidly evolve as new partnerships are formed among a constellation of technology, financial, retail and telecommunications firms.
- **Investing in Insurance**: Technically adept adversaries will always find new ways to circumvent security safeguards. That's why many businesses (59%) are purchasing cybersecurity insurance to help mitigate the financial impact of cybercrimes when they do occur.

- **Government Surveillance Impacting Buying Decisions**: Purchases in certain countries are either under review (34%) or happening less frequently (22%) as a result of hearing about reports that the government is conducting surveillance on hardware, software and/or services from certain countries.

To explore the survey findings by industry and region, visit: www.pwc.com/gsiss.

**NOTE TO EDITORS:** Please reference the study as "The Global State of Information Security® Survey 2016, a worldwide survey by *CIO, CSO* and PwC." Source line must include *CIO*, *CSO* and PwC. Survey results will be covered in depth on CIO.com and CSOonline.com in October.

**METHODOLOGY**
The Global State of Information Security® Survey 2016 is a worldwide study by PwC, *CIO* and *CSO*. It was conducted online from May 7, 2015, to June 12, 2015. Readers of *CIO* and *CSO* and clients of PwC from around the globe were invited via email to take the survey. The results discussed in this report are based on the responses of more than 10,000 executives including CEOs, CFOs, CISOs, CIOs, CSOs, vice presidents, and directors of IT and information security from more than 127 countries. Thirty-seven percent (37%) of respondents were from North America, 30% from Europe, 16% from Asia Pacific, 14% from South America, and 3% from the Middle East and Africa. The margin of error is less than 1%.

**About CIO**
CIO is the 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 strategic marketing services, CIO Forum on LinkedIn, CIO Executive Council 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 http://www.idgenterprise.com/.

**About CSO**
CSO is the 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, strategic 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.

**About PwC**
*At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.*

*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.*