Press Release

Date	October 2, 2014
Contact	**Marina Mello**, PwC Bermuda Tel: 1-441-299-7184/1-441-505-3127 e-mail: marina.mello@bm.pwc.com
Pages	3

A severe and present danger: Cybersecurity incidents more frequent and costly, but budgets decline, says PwC

Employees are most-cited culprits of incidents, Global State of Information Security® Survey 2015 finds

October 2, 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 today by PwC.

The survey was discussed at the ISACA Bermuda chapter's annual cybersecurity conference today at the Royal Hamilton Amateur Dinghy Club, featuring guest speaker **Kristen Hayduk, Advisory Security Manager for PwC US.** Ms Hayduk discussed several steps companies can take toward a strategic security programme, including identifying your most valuable information assets.

Detected security incidents have increased 66 percent year over year since 2009, the survey data indicates. And employees 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.

"Strategic security spending demands that businesses identify and invest in cybersecurity practices that are most relevant to today's advanced attacks," explained **Garth Calow, PwC Bermuda Advisory leader**. "It's critical to fund processes that fully integrate predictive, preventive, detective and incident-response capabilities to minimise the impact of these incidents."

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.

Matt Britten, PwC Bermuda managing director, Risk & Controls, said: "Cyber risks will never be completely eliminated, and with the rising tide of cybercrime, organisations must remain vigilant and agile in the face of a constantly evolving landscape.

"Organisations must shift from security that focuses on prevention and controls, to a risk-based approach that prioritises an organisation'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 organisation."

Assaults on big retailers
Over the past 12 months virtually every industry sector across the globe has been hit by some type of cyber threat. As the survey notes, assaults on major retailers reached epic levels in the past year, resulting in the theft of hundreds of millions of customer payment card records, a rash of litigation, and a rush to adopt a new payment card standard in the US. In the UK, payroll information and bank account numbers of 100,000 employees of a supermarket chain were stolen by a company insider and published online.

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 rose nearly doubled.

Organisations 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 organisations – with revenues of $100 million to $1 billion – witnessed a 64 percent increase in the number of incidents detected.

“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.”

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 organisations often handle the consequences of insider cybercrime internally instead of involving law enforcement or legal charges. In doing so, they may leave other organisations vulnerable if they hire these employees in the future, added Bragdon.

Meanwhile, high profile attacks by nation-states, organised 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 organisations. Only 49 percent of respondents say their organization has a cross-organization 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 having 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.

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 *CSO*online.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 helps 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. Tell us what matters to you and find out more by visiting us at www.pwc.com/bm.