Oct 05, 2016 12:01 +08

Phishing emerges as top cyber threat to organisations in Singapore, finds new PwC report

Date	**5 October 2016**

Contact	**Natalie Choo** Tel: +65 6236 4309 Mobile: +65 9738 1415 E-mail:natalie.yl.choo@sg.pwc.com **Candy Li** Tel: +65 6236 7429 Mobile: +65 8613 8820 E-mail:candy.yt.li@sg.pwc.com

- **Phishing Becomes Top Threat:** Phishing is the most-cited vector of cybersecurity incidents this year, with 42% of businesses in Singapore reporting phishing incidents.
- **Employee Training Remains a Top Priority for Data Privacy:** 65% of respondents in Singapore currently require employees to complete privacy training.
- **Moving Beyond Passwords to Advanced Authentication:** Many businesses are turning to advanced authentication technologies to add an extra layer of security and improve trust among customers, with 70% in Singapore using hardware tokens for authentication.

Singapore, October 5, 2016– There is a distinct shift in how organisations are now viewing cybersecurity, with forward-thinking organisations understanding that an investment in cybersecurity and privacy solutions can facilitate business growth and foster innovation. The Global State of Information Security® Survey 2017, released today byPwC in conjunction withCIO andCSO, examines how executives are adopting technology and collaborative approaches to cybersecurity and privacy to manage threats and achieve competitive advantages.

Globally, many organisations no longer view cybersecurity as a barrier to change or as an IT cost. Singapore is not an exception. According to the survey, 74% of respondents in Singapore said they have increased IT security spending as a result of digitisation of their business ecosystem as organisations not only create products, but they also deliver complementary software-based services for products that extend opportunities for customer engagement and growth.

In Singapore, talent emerged as the main safeguard that organisations invest in. The top three safeguards organisations have implemented relate to talent employing experts such as Chief Privacy Officers (CPO), Chief Information Security Officers (CISO), and ensuring employees receive and complete the required training (refer to Figure 1). Correspondingly, the percentage of executives which cited current employees as their organisations' most likely source of security incidents dropped from 43% last year to 25% this year, suggesting that these efforts paid off.

Fig 1. Top 4 safeguards organisations in Singapore have in place	
CPO or similar executive in charge of privacy compliance	69%
CISO in charge of the security programme	66%
Employee security awareness training programme	66%
Require our employees to complete training on privacy policy and practices	65%

"There is a distinct transformation in how business leaders are viewing cybersecurity and technology – no longer seeing technology as a threat and understanding that cybersecurity is a vital component that must be adopted into the business framework," said Vincent Loy, Asia Pacific Cyber Leader, PwC Singapore. "It's no longer enough to identify the threats and risks as they are constantly evolving. As Singapore is a highly connected market, all the more organisations cannot rest on their laurels."

There should be continued effort in ensuring adequate cybersecurity measures are in place. With the advent of more sophisticated phishing methods, around four in 10 executives in Singapore (42%) reported their organisations fell victim to phishing attacks in the past 12 months, making it the most pervasive cybersecurity and privacy threat faced by organisations in the country, as well as in Asia Pacific (45%) and globally (38%).

"These new phishing methods put users at greater risk of being invaded by malware. For example, the drive-by-download attack allows malware to invade a computer through the mere click of a link," said Tan Shong Ye, IT Risk Assurance Leader, PwC Singapore. "Well-disguised phishing attacks do not necessarily bring users to a suspicious site, but may also direct users to legitimate sites that have been hacked. Organisations must continue to invest in employee training, and help them recognise phishing attacks to mitigate the risk of malware."

Users' disregard for strong password practices is one reason organisations in Singapore and worldwide are turning to advanced authentication technologies to add an extra layer of security as well as to improve trust among customers and business partners. 54% of executives surveyed in

Singapore reported that the employment of advanced authentication has made online transactions more secure for their organisations.

The top advanced authentications in Singapore currently have in place include: hardware (70%) and software (57%) tokens and multifactor authentication (55%). Hardware tokens appear to be preferred as they add a physical dimension to security. While software tokens are more convenient to implement and use, hardware tokens are more tamper-resistant compared to their software counterparts explaining the high adoption of hardware tokens.

"One notable use of multi-factor authentication in Singapore is the introduction of the two-step verification or 2FA for all government portals," added Jimmy Sng, Cybersecurity Leader, PwC South East Asian Consulting. "Multi-factor authentication often takes the form of a combination of hardware and software tokens. As we move toward more tamper-resistant methods of authentication, biometrics will rise with 40% of respondents in Singapore reflecting that it is a top priority in the next 12 months. Biometrics will not emerge as a standalone, but as a new safeguard to be assimilated into multi-factor authentication."

"Designing and implementing a cybersecurity and privacy program is challenging enough, but once a program is in place components must be thoroughly integrated, professionally managed and continuously improved. As this can be difficult for resource-constrained organizations, many are adopting managed security services and utilizing open-source software," said Bob Bragdon, VP/publisher of CSO.

ENDS

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

To explore the survey findings in Singapore, visit: www.pwc.com/sg/gsiss.

METHODOLOGY

The Global State of Information Security® Survey 2017 is a worldwide study by PwC, *CIO* and *CSO*. It was conducted online from April 4, 2016, to June 3, 2016. 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 133 countries. Thirty-four percent (34%) of respondents were from North America, 31% from Europe, 20% from Asia Pacific, 13% 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 atwww.idgenterprise.com.

About PwC

Contacts

Siew Ling Ong
Press Contact
Manager, Brand and Communications
siew.ling.ong@pwc.com

Candy Li
Press Contact
Team Lead - Brand & Communications
candy.yt.li@pwc.com

Verlynn Heng
Press Contact
Senior Associate
Brand & Communications
verlynn.wy.heng@pwc.com
81251483