Oct 27, 2017 00:01 +08

Organisations are failing to prepare effectively for cyberattacks, says PwC

Date	27 October 2017
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
Follow/ retweet	@PwC_Singapore

- Fifty-nine percent of survey respondents in Singapore cite compromise of sensitive data as the biggest consequence of a cyberattack, followed by the disruption of operations (45%) and harm to product quality (40%).
- Forty-four percent of the 9,500 executives in 122 countries surveyed say they do not have an overall information security strategy (39% in Singapore, 41% in Asia).
- Forty-eight percent do not have an employee security awareness training programme (36% in Singapore, 47% in Asia), and 54% don't have an incident-response process (44% in Singapore, 53% in Asia).
- When cyberattacks occur, most victimised companies say they cannot clearly identify the culprits. Only 39% of survey respondents say they are very confident in their attribution capabilities. In Singapore, this is even lower with only 25% of respondents indicating they are very confident in their attribution capabilities.

Singapore, 27 October 2017 – Massive cybersecurity breaches have become almost commonplace, regularly grabbing headlines that alarm consumers and leaders. But for all of the attention such incidents have attracted in recent years, many organisations worldwide still struggle to comprehend and manage emerging cyber risks in an increasingly complex digital society.

Executives worldwide acknowledge the increasingly high stakes of cyber insecurity. In PwC's newly launched Singapore cut of its 2018 Global State of Information Security® Survey (GSISS), fifty-nine percent of survey respondents in Singapore cite compromise of sensitive data as the biggest consequence of a cyberattack, 45% cite the disruption of operations and 40% cite harm to product quality.

Yet despite this awareness, many companies at risk of cyberattacks remain unprepared to deal with them. Thirty-nine percent in Singapore say they do not have an overall information security strategy. Thirty-six percent in Singapore say they do not have an employee security awareness training programme, and 44% say they do not have an incident-response process.

Tan Shong Ye, Digital Trust Leader, PwC Singapore said: "Companies need to be able to identify their critical information infrastructure and know how to protect it. When cyberattacks happen, the focus will be to get systems and operations back to business-as-usual as quickly as possible. Knowing what needs to be protected and then assessing the risk will enable organisations to be better prepared for when an incident occurs"

How cyber interdependence drives global risk

Case studies of non-cyber disasters have shown that cascading events often begin with the loss of power—and many systems are impacted instantaneously or within one day, meaning there is generally precious little time to address the initial problem before it cascades. Interdependencies between critical and non-critical networks often go unnoticed until trouble strikes. Many people worldwide—particularly in Japan, the United States, Germany, the United Kingdom and South Korea—are concerned about cyberattacks from other countries. Tools for conducting cyberattacks are proliferating worldwide. Smaller nations are aiming to develop capabilities like those used by larger countries. And the leaking of US National Security Agency (NSA) hacking tools has made highly sophisticated capabilities available to malicious hackers.

When cyberattacks occur, most victimized companies say they cannot clearly identify the culprits. Only 25% of survey respondents say they are very confident in their attribution capabilities.

The soaring production of insecure internet-of-things (IoT) devices is creating widespread cybersecurity vulnerabilities. Rising threats to data integrity could undermine trusted systems and cause physical harm by damaging critical infrastructure.

Meanwhile, there is a wide disparity in cybersecurity preparedness among countries around the world. In our 2018 GSISS, the frequency of organisations possessing an overall cybersecurity strategy is particularly high in Japan (72%), where cyberattacks are seen as the leading national security threat, and Malaysia (74%). Organisations in Singapore are behind these leading economies with only 61% possessing an overall cybersecurity strategy, slightly ahead of the Asia average of 59%.

Pierre Legrand, Asia Pacific Technology Consulting Leader, PwC said: "Few business issues permeate almost every aspect of business like cybersecurity does today. Having a clear cybersecurity strategy brings companies one step closer to being prepared for cyber incidents, but it doesn't stop there. Once that strategy is in place, organisations must have the right expertise to effectively put that strategy into action."

In May 2017, G-7 leaders pledged to work together and with other partners to tackle cyberattacks and mitigate their impact on critical infrastructure and society. Two months later, G-20 leaders reiterated the need for cybersecurity and trust in digital technologies. The task ahead is huge.

Next steps for business leaders

So what can business leaders do to prepare effectively for cyberattacks? PwC recommends three key areas of focus:

C-suites must lead the charge and boards must be engaged: Senior leaders driving the business must take ownership of building cyber resilience. Setting a top-down strategy to manage cyber and privacy risks across the enterprise is essential.

Pursue resilience as a path to rewards—not merely to avoid risk: Achieving greater risk resilience is a pathway to stronger, long-term economic performance.

Purposefully collaborate and leverage lessons learned: Industry and government leaders must work across organisational, sectoral and national borders to identify, map, and test cyber-dependency and interconnectivity risks as well as surge resilience and risk-management.

Over the last few years, Singapore has continued to spur collaboration, insight and education in cybersecurity through the formation of the Cyber Security Agency of Singapore, Singapore's cybersecurity strategy, the proposed Cybersecurity bill, and many events that encourage cross-industry sharing of expertise. Although there is a push toward greater collaboration in the cybersecurity sector, 36% of respondents in Singapore indicated that they still do not formally collaborate with others in the industry to improve security.

Jimmy Sng, Digital Trust Partner, PwC Singapore said, "The benefits of collaboration are clear – more than half of respondents in Singapore indicated that they have had improved threat intelligence and awareness, and have received actionable information from such collaborations. As technology increases interconnectivity, public-private coordination is critical to effectively addressing cybersecurity."

Notes to editors:

1. The *Global State of Information Security® Survey 2018* is a worldwide study by PwC, *CIO* and *CSO*. It was conducted online from April 24, 2017, to May 26, 2017. Readers of *CIO* and *CSO* and clients of PwC from 122 countries were invited via email to take the survey.
2. The results discussed in this report are based on the responses of more than 9,500 business and IT executives including CEOs, CFOs, CISOs, CIOs, CSOs, vice presidents, and directors of IT and information security from 122 countries. 38% of respondents were from North America, 29% from Europe, 18% from Asia Pacific, 14% from South America, and 1% from the Middle East and Africa.
3. A range of public and private organisations were surveyed: 28%

of respondents were from small businesses with under $100m annual revenue, 46% of respondents were from organisations with revenue of $500 million+ and 4% were non-profit, government or education bodies.

4. In Singapore, there were 83 respondents across 15 industries including Aerospace & Defense; Consumer Products & Retail; Consulting / Professional Services; Education / Non-profit; Energy / Utilities / Mining; Entertainment & Media; Engineering / Construction; Financial Services, Government Services; Health Industries, Hospitality / Travel & Leisure; Industrial Manufacturing; Technology; Telecommunications; and Transportation & Logistics
5. A copy of the global report can be downloaded at: http://www.pwc.com/us/en/cybersecurity/information-security-survey.html

About CIO

CIO focuses on attracting the highest concentration of enterprise CIOs and business technology executives with unparalleled peer insight and expertise on business strategy, innovation, and leadership. As organizations grow with digital transformation, CIO provides its readers with key insights on career development, including certifications, hiring practices and skills development. The award-winning CIO portfolio—CIO.com, 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. The CIO Executive Council is a professional organization of CIOs created to serve as an unbiased and trusted peer advisory group. CIO is published by IDG Communications, Inc. Company information is available at www.idg.com.

About CSO

CSO is the premier content and community resource for security decision-makers leading "business risk management" efforts within their organization.

For more than 15 years, CSO's award-winning website (CSOonline.com), executive conferences, strategic marketing 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. Based on editorial coverage and design, the Folio Eddie awards named CSOonline.com as the best BtoB Technology Website in 2015 and 2016. 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 Communications, Inc. Company information is available at www.idg.com.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 236,000 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.

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