www.pwc.com/sg

Global State of Information Security® Survey 2017

Singapore highlights

pwc

Phishing attack: Singapore's most prevalent cybersecurity and privacy threat

Overview of security incidents in Singapore

The threat of cyber attacks continues to grow. Executives are reporting that they detected more security incidents in the past 12 months, with the bulk of respondents (22%) detecting at least 3 incidents in the past year. More significantly, 13% reported that they identified 500 to 4,999 incidents, almost double the figure from the year before (Figure 1).

While certainly not new, the sophistication of phishing methods (eg. spear phishing) has evolved in recent years. In Singapore, around four in 10 executives 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 the Asia Pacific region and globally (Figure 2).

The upsurge of new phishing methods may potentially result in the widened dissemination of malware, which has also grown in complexity. Previously, in order to for a malware to invade a device, users would first need to download, run, and install a software. These days, new malware drive-by-download attacks are able to invade a computer through the click of a link.

Around a third of the executives surveyed cited activists, activist organisations and hacktivists as the most likely source of the security incidents that took place over the past 12 months (Figure 3).

Meanwhile, the compromise of employee records, followed by customer records, make up the top 2 issues organisations in Singapore experienced as a result of security incidents (Figure 4).

Figure 1 **Security incidents detected in the past 12 months**

Q: What is the number of security incidents detected in the past 12 months?

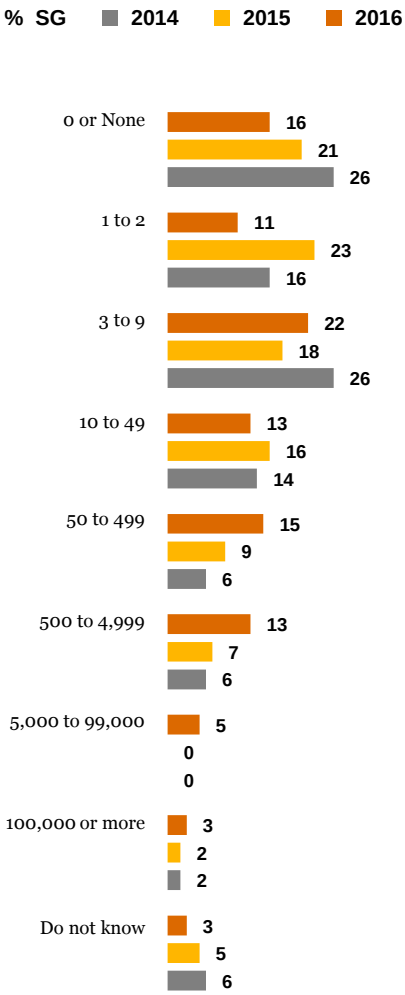


Figure 2 **Areas where security incidents occurred***

Q: How did the security incident(s) occur?

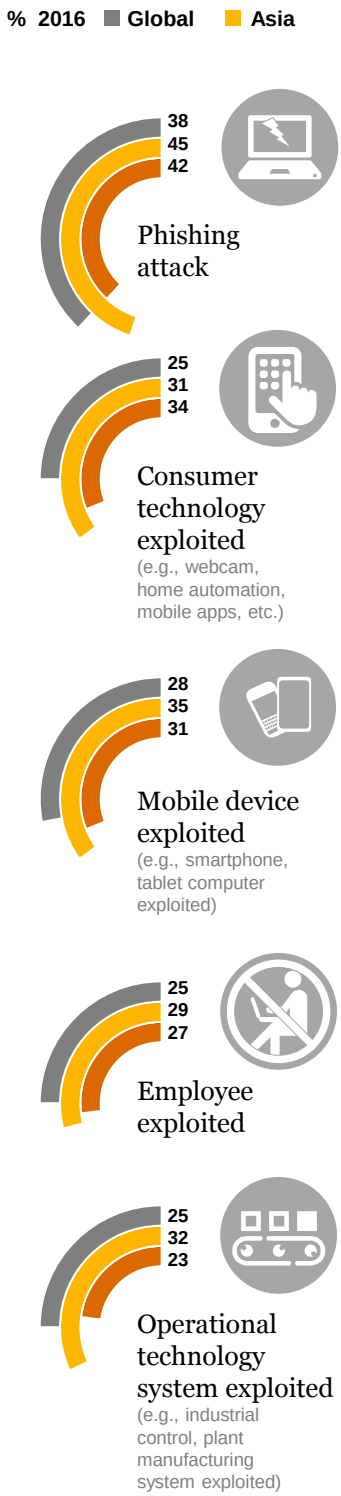
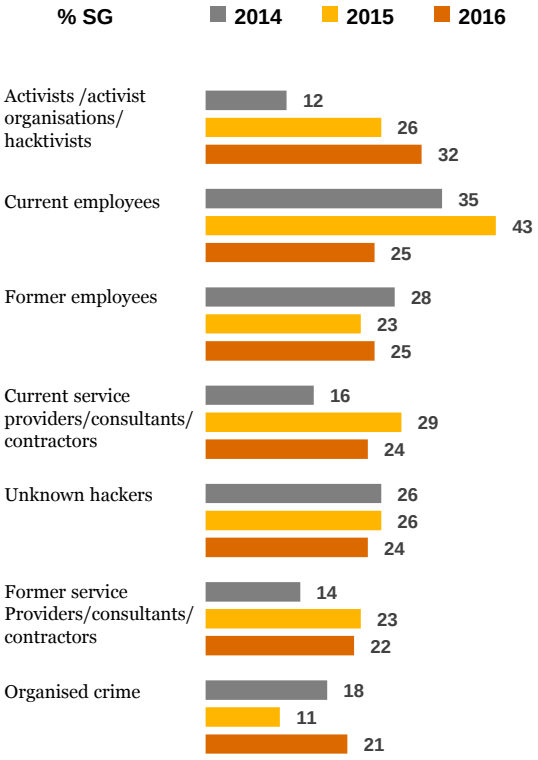


Figure 3 **Likely sources of security incidents***

Q: What is the estimated likely source of incidents?

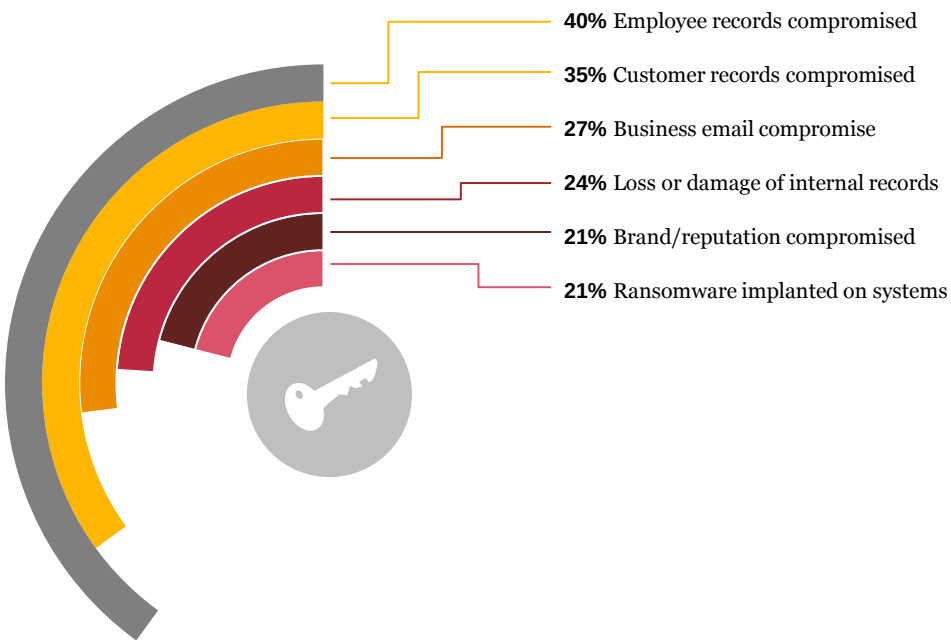


*Refers to the top 5 results from respondents from Singapore

Figure 4 **Areas where business have been compromised***

Q: How was your organisation impacted by the security incidents?

% SG 2016



*Refers to the top 5 results from respondents from Singapore

Moving forward with cybersecurity and privacy

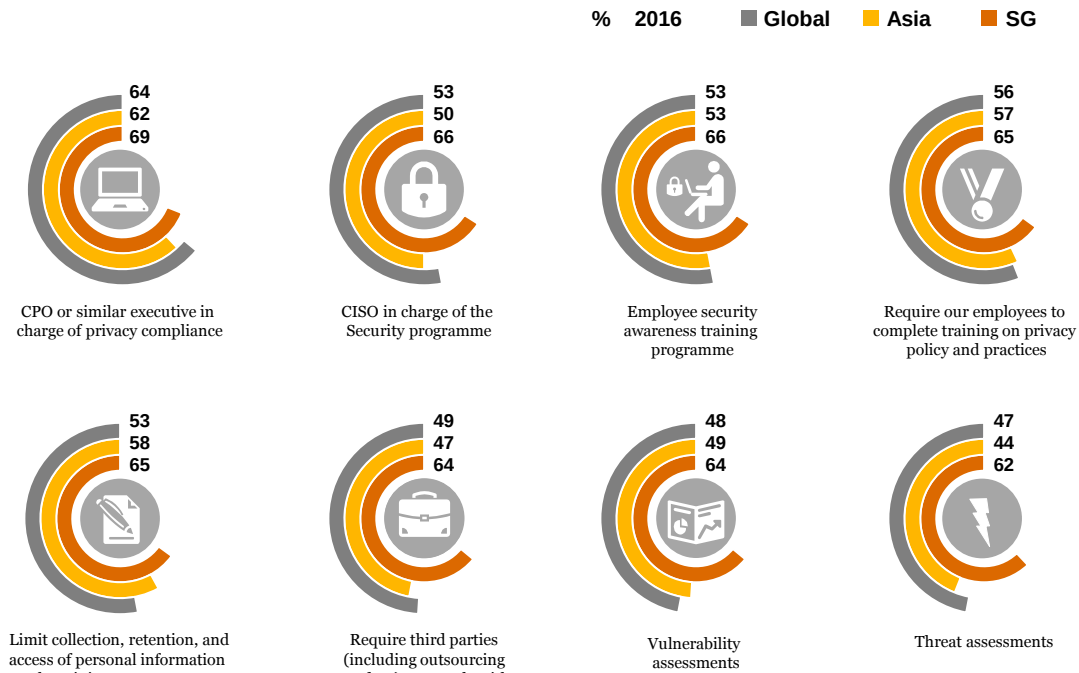
Honing the basics: Investing in talent

Organisations that hew to the basics of cybersecurity—fundamentals such as employee training, up-to-date policies and controls, and a commitment to readiness and resilience—will be better prepared to manage simple attacks and preserve resources for more complex incidents.

In Singapore, talent emerged as the main safeguard that majority of organisations invest in (Figure 5). This includes employing experts such as Chief Privacy Officers (CPO), as well Chief Information Security Officers (CISO), and ensuring employees receive and complete the required training. 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 (Figure 3).

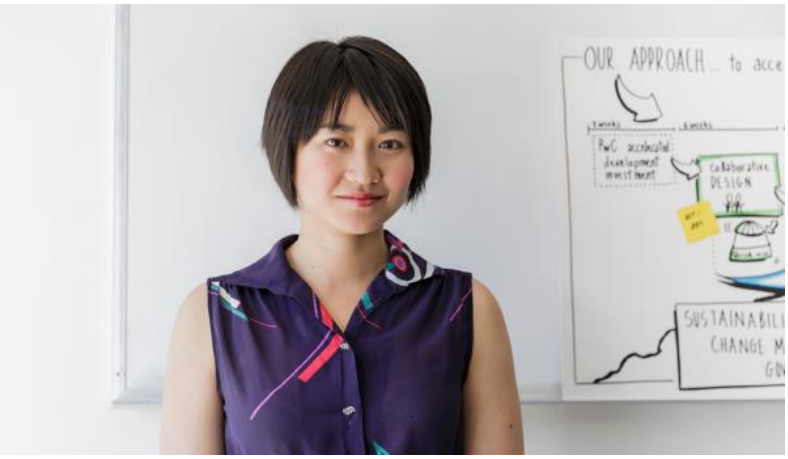
Figure 5 **The fundamental safeguards***

Q: Which safeguards do your organisation currently have in place?



**Refers to the top 5 results from respondents from Singapore*

Integration of innovative safeguards with business strategies

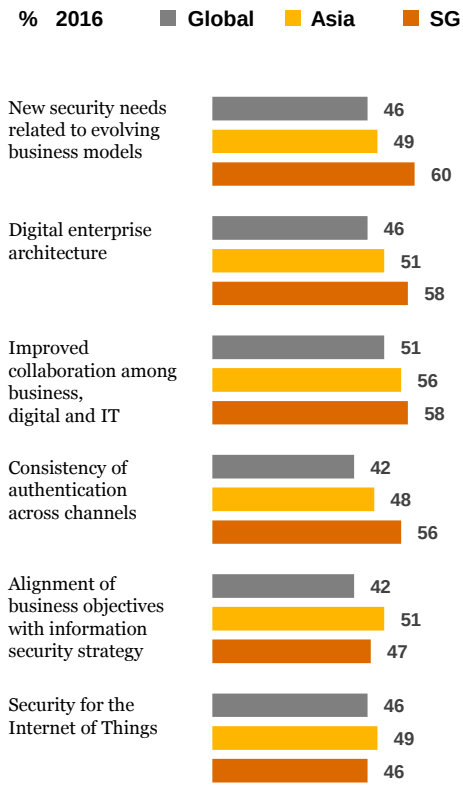


Increasingly, businesses are exploring new opportunities to create value and competitive advantages by integrating cybersecurity with digital business strategies. 74% of executives surveyed said their organisations have increased cybersecurity spending as a result of the digitisation of their business ecosystem.

Among the top three security safeguards organisations in Singapore plan to invest over the next 12 months are: new security needs related to evolving business models, digital enterprise architecture, and improved collaboration among business, digital and IT (Figure 6). The results signal organisations' commitment to improving their interoperability between functions and the integration of cybersecurity with the digitisation of their business framework.

Figure 6 **Cybersecurity spending priorities for the next 12 months***

Q: What types of security safeguards do your organisation plan to invest in over the next 12 months?



*Refers to the top 5 results from respondents from Singapore

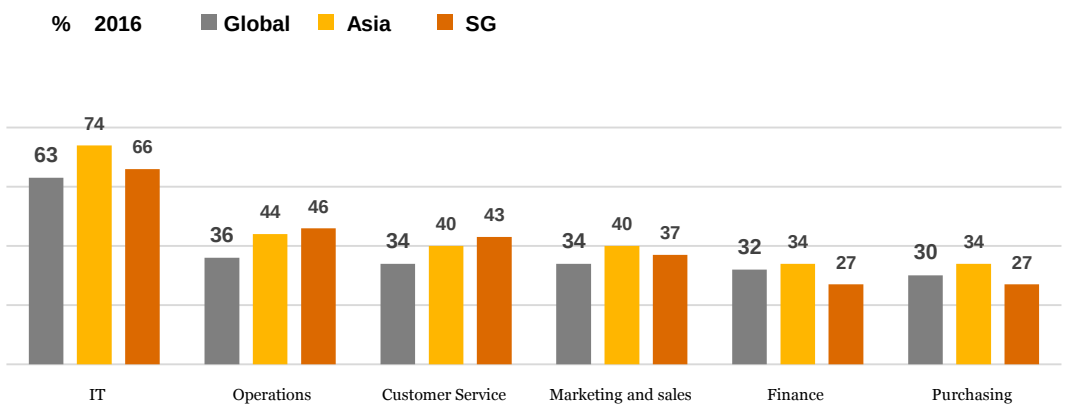
Greater trust in the cloud with stronger safeguards

As trust in cloud models deepens, organisations are running more sensitive business functions on the cloud. Today, the majority of organisations in Singapore (66%) run IT services in the cloud. Additionally, 46% were found to entrust their operations functions to cloud providers (Figure 7).

However, the synthesising of more business intelligence to the cloud presents wider risks and threats which businesses need to safeguard against. To do this, more companies are anticipating risks with analytics and threat intelligence. This year, 55% of surveyed executives said they use big data analytics to model for and identify information security incidents. Furthermore, among the respondents who use managed security services, 60% said they use service providers for real-time monitoring and analytics.

Figure 7 **Business functions that are run in the cloud***

Q: What business function areas do your organisation run in a cloud environment?



Refers to the top 5 results from respondents from Singapore

Moving beyond passwords to advanced authentication

‘123456’ remains the most commonly used password today. 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 the country reported that the employment of advanced authentication has made online transactions more secure for their organisations.

While software token emerged as the more widely adopted advanced authentication safeguard at the global and regional levels, organisations in Singapore appear to have a stronger preference for hardware token partly due to its more tamper-resistant attribute (Figure 8). Taken in consideration that software token is a newer form of advanced authentication, businesses will need to take the necessary precaution to ensure that their base operating system and channels (e.g., mobile devices) are secured for the soft tokens to be delivered.

Singapore also leads by a close margin in the adoption of multi-factor authentication – comprised of a combination of authentication safeguards – which is extensively applied by its financial institutions on functions such as online banking, financial transactions, remote access and operations. The multi-factor authentication used for online banking, for example, often includes a combination of log-in passwords, hardware tokens, and one-time password (OTP) codes sent through mobile phones.

Cited by 40% of executives in Singapore as the priority safeguard that organisations will be looking into in the coming 12 months (Figure 9), biometrics deliver a unique set of convenience and efficiency whereby users are not required to remember passwords, and where the authentication payload does not expire. Additionally, biometrics may potentially be assimilated into multi-factor authentication systems as an additional layer of security in the future.

**Refers to the top 5 results from respondents from Singapore*

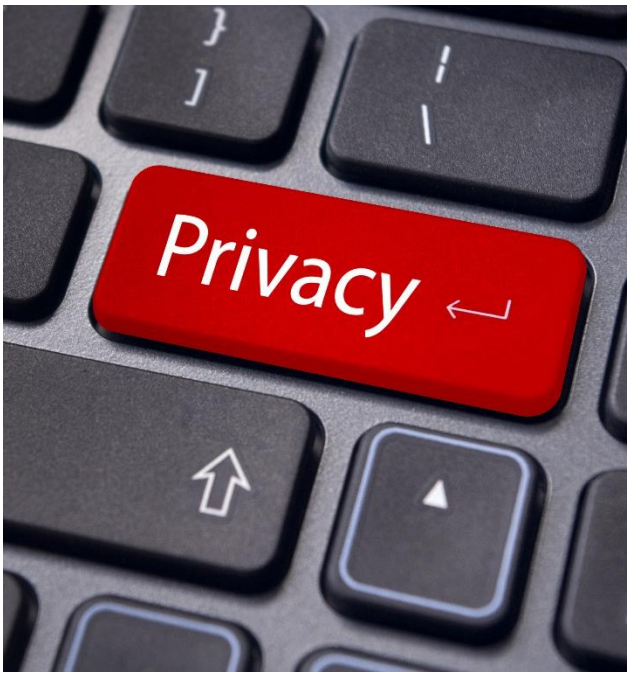
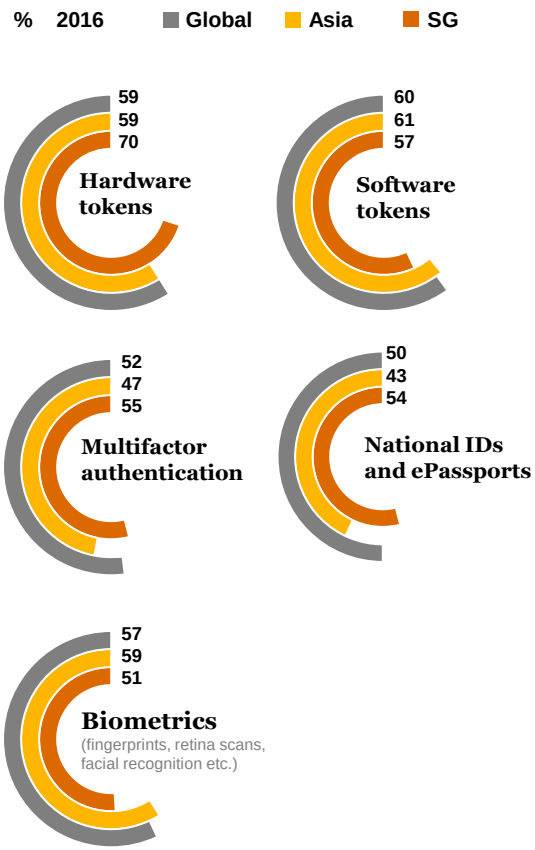


Figure 8 **Advanced authentication technologies currently in place***

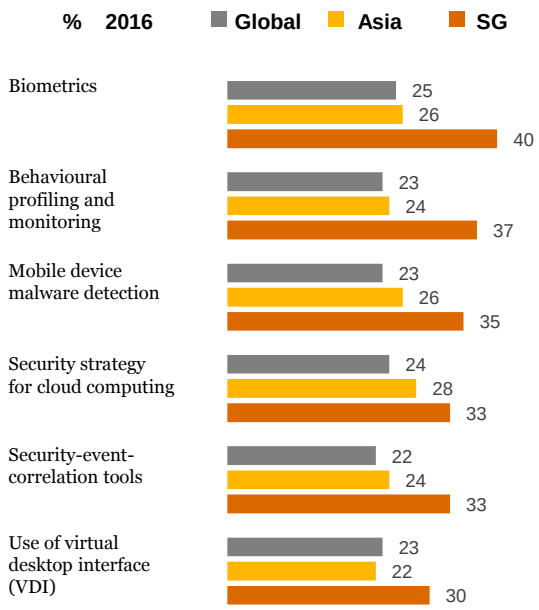
Q: Which of the following advanced authentication technologies does your organisation currently have in place?



**Refers to the top 5 results from respondents from Singapore*

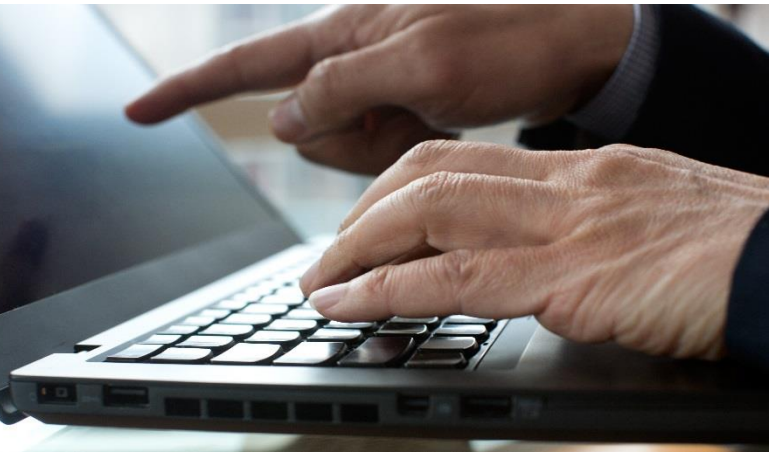
Figure 9 **New safeguards priority for the next 12 months***

Q: Which safeguards do your organisation not have in place, but is a top priority over the next 12 months?



*Refers to the top 5 results from respondents from Singapore

Leveraging open-source software for competitive advantage

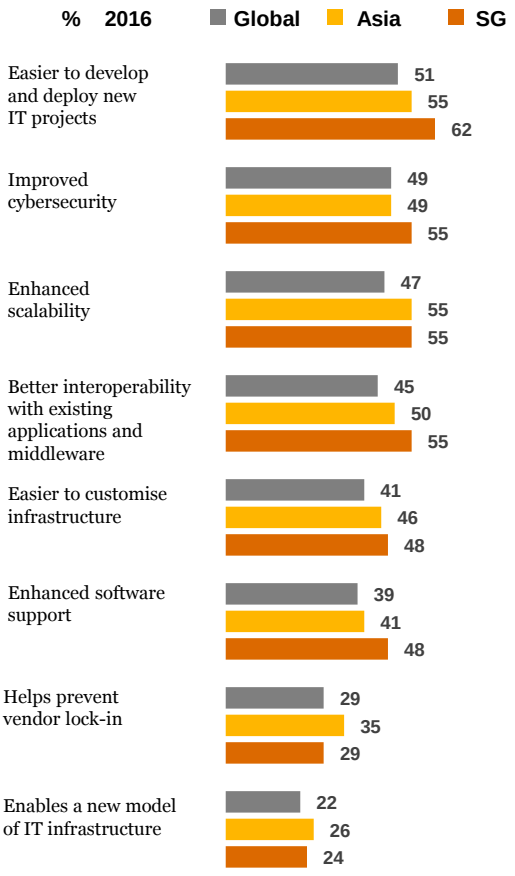


The adoption of open-source software represents a major shift in how organisations develop and run on-premises solutions as well as deliver IT services. More than half of the executives surveyed in Singapore (55%), in the Asia Pacific region (64%) and globally (53%) reported their organisations are already using some form of open-source software.

Businesses are adopting open-source software for several reasons. The applications can be scaled quickly and effectively. In many cases, open-source applications have been collaboratively developed and tested by security talent across industries. The software is also typically available at little or no cost, providing an inexpensive method to create new solutions. For organisations in Singapore, open-source technology is most appreciated for its ease in developing and deploying new IT projects, ability to improve cyber security posture, and enhanced scalability (Figure 10).

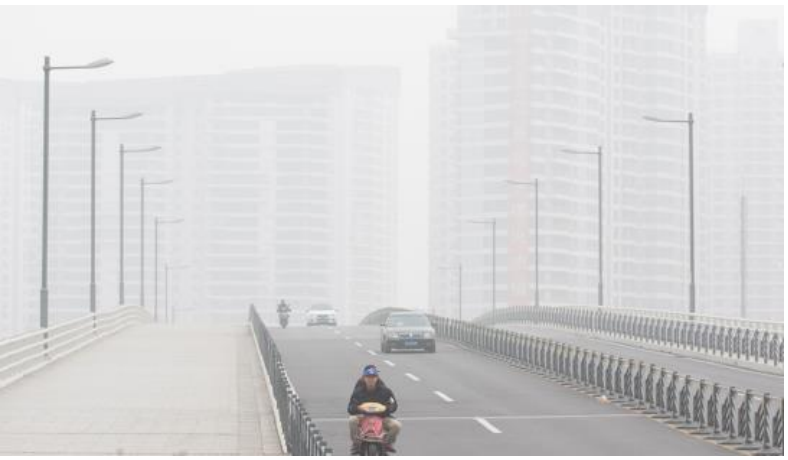
Figure 10 **Benefits of open-source software***

Q: What impact has the use of open-source software had on your organisation?



*Refers to the top 5 results from respondents from Singapore

Then, now and opportunities for the future



Technology and cybersecurity progress over the past decade has been astonishingly swift and sweeping.

The digital business model was an enigma to many companies a decade ago. In 2007, most organisations simply did not understand the advantages of a digital business model, much less how to implement one.

Fast forward 10 years, there is a distinct shift in how organisations are now viewing cybersecurity today. Businesses no longer view technology as a threat, barrier to change, or an IT cost. Furthermore, considering that 74% of executives surveyed in Singapore said they are boosting spending on security as a result of digitisation, organisations have come to understand that combining digital business models with cybersecurity can enable them to confidently create entirely new digital platforms, products and services.

Many are already implementing foundational elements—cloud computing, sophisticated data monitoring and analytics, and open source technologies, to name a few—and integrating digitalisation with cybersecurity and privacy.

The future is ultimately unknowable. But we believe we'll see advances in technologies such as artificial intelligence, machine learning, sophisticated advanced authentication technologies and adaptive controls. When combined on the cloud, they will deliver new architectural models and powerful cybersecurity and privacy capabilities that will help organisations get ahead of both sophisticated and mundane threats.

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 participate in the survey.

The results discussed in this report are based on responses of more than 10,000 CEOs, CFOs, CIOs, CISOs, CSOs, VPs and directors of IT and security practices from more than 133 countries.

Thirty-four percent (34%) of survey respondents are from North America, 31% from Europe, 20% from Asia Pacific, 13% from South America and 3% from the Middle East and Africa.

All Singapore focused figures and graphics in this report were sourced from the survey results of 79 executives surveyed in the country.

The margin of error is less than 1%; numbers may not add to 100% due to rounding.

Get in touch with our team

Visit www.pwc.com/gsiss to access the full Global State of Information Security® Survey 2017.

Meanwhile, feel free to get in touch with our local experts:

Vincent Loy
Cyber, Data & Analytics, and Financial Crime Leader
Email: vincent.j.loy@sg.pwc.com

Tan Shong Ye
IT Risk Assurance Leader
Email: shong.ye.tan@sg.pwc.com

Jimmy Sng
Cybersecurity Leader, South East Asian Consulting
Email: jimmy.sng@sg.pwc.com