www.pwc.com/sg

The Global State of Information Security® Survey 2018

Singapore highlights

January 2018

pwc

Contents

Methodology

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 around the globe were invited via email to participate in the survey.

The results discussed in this report are based on the responses of more than 9,500 CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT as well as security practices from more than 122 countries.

38% of survey respondents are from North America, 29% from Europe, 18% from Asia Pacific, 14% from South America, and 1% from the Middle East and Africa.

This Singapore highlights report explores the responses of 83 respondents from the country across 15 industries including:

- Aerospace and defence
- Consumer products and retail
- Consulting/ Professional services
- Education/ Non-profit
- Energy/ Utilities/ Mining
- Entertainment and media
- Engineering/Construction
- Financial services
- Government services
- Health industries
- Hospitality/ Travel & leisure
- Industrial manufacturing
- Technology
- Telecommunications
- Transportation and logistics

Singapore key findings

Overview

The results from PwC's Global State of Information Security® Survey 2018 reveal 77% of respondents in Singapore detected one or more cyber incidents in the last twelve months. With the high frequency in which incidents occur, organisations must know what they need to protect and how to protect them.

While Singapore is ahead of the global and Asia Pacific average in a number of cybersecurity readiness measures, room for improvement remains.

This year's report observes "human error" or negligence as the weak link within organisations' cybersecurity framework. To mitigate rising risks, businesses are also turning to cyber insurance in addition to investing in security safeguards.

Cyber risks are no longer just a business issue but also concerns the security of the larger economy. Closer collaboration between government bodies, businesses and various institutions will be required to strengthen cyber defences at a national level.

With the proposed Cybersecurity Bill by the Ministry of Communications and Information (MCI) and Cyber Security Agency of Singapore (CSA), it is clear that the Singapore government is doing more to ensure that cyber incidents are mitigated and that potential damages are kept to a minimum.

59% of respondents

cited "compromise of sensitive data" as the biggest consequence of a cyberattack

Top three areas

where cyber incidents occurred:
1. Mobile device exploitation
2. Phishing
3. Employee exploitation

Only 25% of respondents

are very confident in their attribution capabilities

Current employees

emerged as organisations' top likely source of security incidents

56% of respondents

have taken steps to enhance their organisation's security posture to lower the insurance premium

61% of respondents

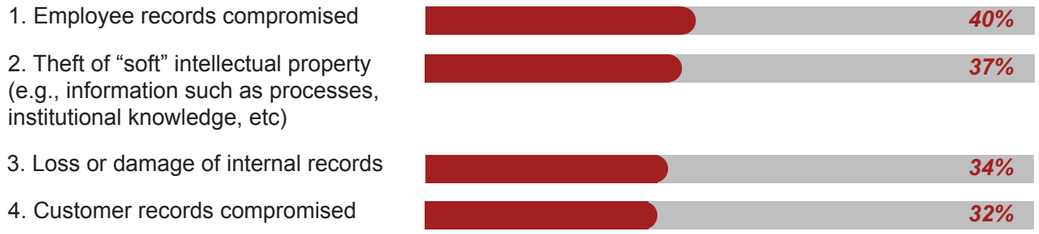
benefited from cybersecurity collaboration, seeing improved threat intelligence and awareness

Understanding the impact of cyberattacks

Based on the responses from business leaders surveyed in Singapore, whose organisation have experienced cyberattacks, the compromise of employee records emerged as the top impact as a result of security incidents (40%; Figure 1), followed by theft of "soft" intellectual property (37%) and loss or damage of internal records (34%).

Figure 1. Top 5 areas where businesses in Singapore have been compromised due to cybersecurity incidents

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

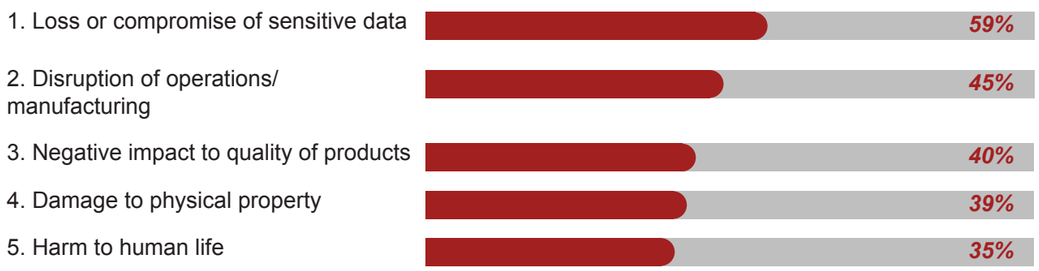


Base: Singapore - 63
Source: The Global State of Information Security® Survey 2018

When it comes to emerging technologies, businesses in Singapore are cautious of their associated risks. According to nearly six in 10 respondents in Singapore, a successful cyberattack on automated or robotic systems could have major consequences on their business, especially in the compromise of sensitive data (59%; Figure 2), followed by disruption to operations or manufacturing (45%).

Figure 2. Top 5 critical results of a successful cyberattack according to Singapore businesses surveyed

Q: If your organisation uses automation and/or robotics, what do you believe are the most critical results of a successful cyberattack against those systems?



Base: Singapore - 82
Source: The Global State of Information Security® Survey 2018

The high level of concern surrounding data security may be attributed to the recent public consultation on the proposed mandatory data breach notification regime under Singapore's Personal Data Protection Act (PDPA), which has brought data protection back to the forefront of the business leaders' agenda. After all, companies that fail to comply with the PDPA may face heavy penalties including fines of up to S$1 million and reputational damage.

Losses or damages incurred from disrupted operations caused by cyberattacks can be far reaching. Singapore recognises that not only does such disruption pose as a threat to businesses, but to the larger economy and nation as well. The undertaking of mitigating potential disruption to operations does not solely rest on businesses alone. The gravity of this matter is pronounced in Singapore's proposed Cybersecurity Bill put forward by the MCI and the CSA as the city state moves forward in strengthening its security governance and legislative framework. The Bill outlines the imperative of ensuring essential services and operations remain unaffected despite cyberattacks. It further identifies Critical Information Infrastructures (CIIs) which are necessary for the continuous delivery of essential services that are fundamental to the operations of national security, defence, public health, and public safety.

The Achilles' heel in cybersecurity systems: Human error

Responses from Singapore scored lower than the global and regional average when it came to questions around confidence in their attribution capabilities (Singapore: 25%, Asia Pacific: 47%, Global: 39%; Figure 3). This suggests that the majority of companies that could potentially fall victim to cyberattacks may not have the ability to identify the culprits responsible.

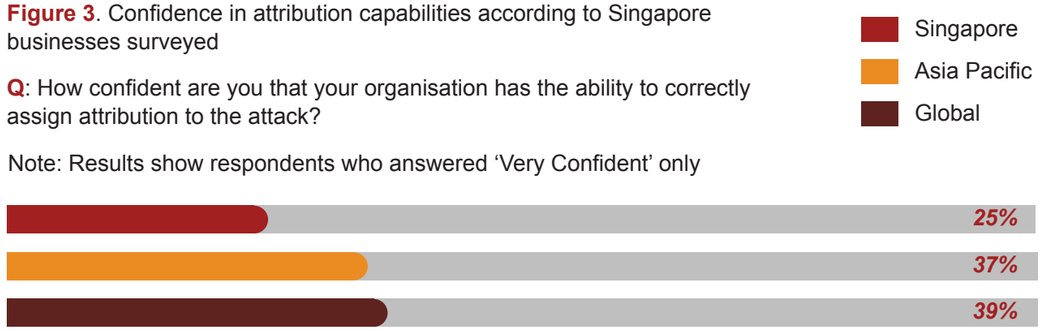
Despite the lack of confidence in their attribution capabilities, more than a third of Singapore respondents indicated current employees as their most likely source of incidents (38%) – up 13% from the year before (Figure 4).

Bottom line: People remain the critical aspect that can either make or break a cybersecurity framework regardless of the sophistication of an organisations' security technologies. Take for instance, the levels of access to systems and information which employees have. One careless, albeit unintentional, employee is all it takes to compromise an organisation's system and data security.

Figure 3. Confidence in attribution capabilities according to Singapore businesses surveyed

Q: How confident are you that your organisation has the ability to correctly assign attribution to the attack?

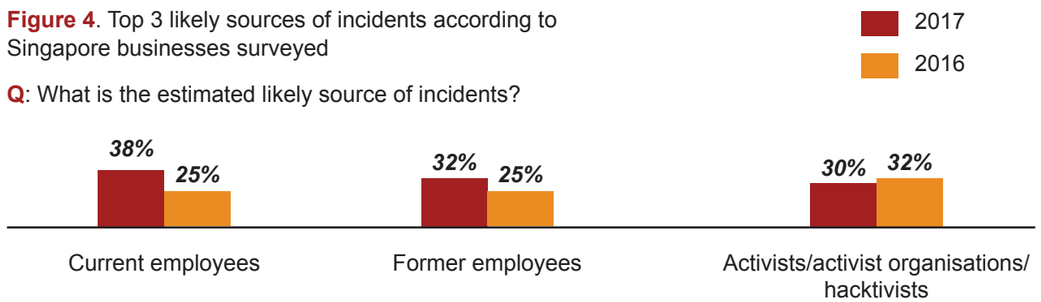
Note: Results show respondents who answered 'Very Confident' only



Base: Singapore - 63. Asia Pacific - 1392. Global -7768
Source: The Global State of Information Security® Survey 2018

Figure 4. Top 3 likely sources of incidents according to Singapore businesses surveyed

Q: What is the estimated likely source of incidents?



Base: Singapore 2017 - 63; 2016 - 63. Asia Pacific 2017 - 1388; 2016 - 1620
Source: The Global State of Information Security® Survey 2018

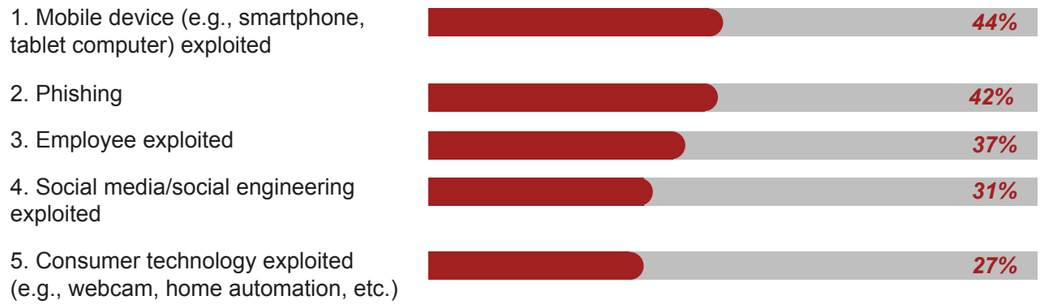
A strong cybersecurity culture where employees are trained to act as the first line of defence will be an organisation's greatest asset and cybersecurity safeguard. Businesses must ensure that they have a proper cybersecurity awareness programme in place to help employees identify common threats such as phishing, malware and ransomware. Furthermore, they must also educate their workforce on how staff can protect themselves against these risks followed by the timely reporting of potential threats.

Robust access control is also a necessity as it provides oraganisations with insight into their system users, and their levels of access, as well as the business reasons supporting the access by users. In addition, periodic access reviews must be conducted to ensure that only users with the necessary business reasons have access to relevant systems and data.

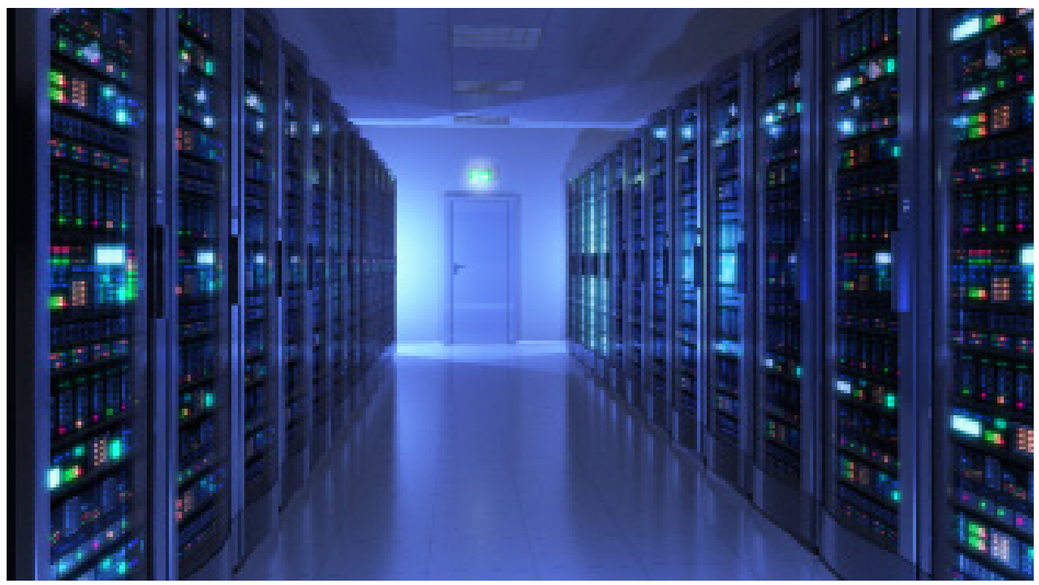
In Singapore, responses reflected that security incidents primarily occurred through the exploitation of mobile devices (44%; Figure 5), followed closely by phishing (42%) which further suggest susceptibility to threats due to human error or negligence. As new phishing methods put users at greater risk of being invaded by malware.

Figure 5. Areas where security incidents occurred

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



Base: Singapore - 62
Source: The Global State of Information Security® Survey 2018



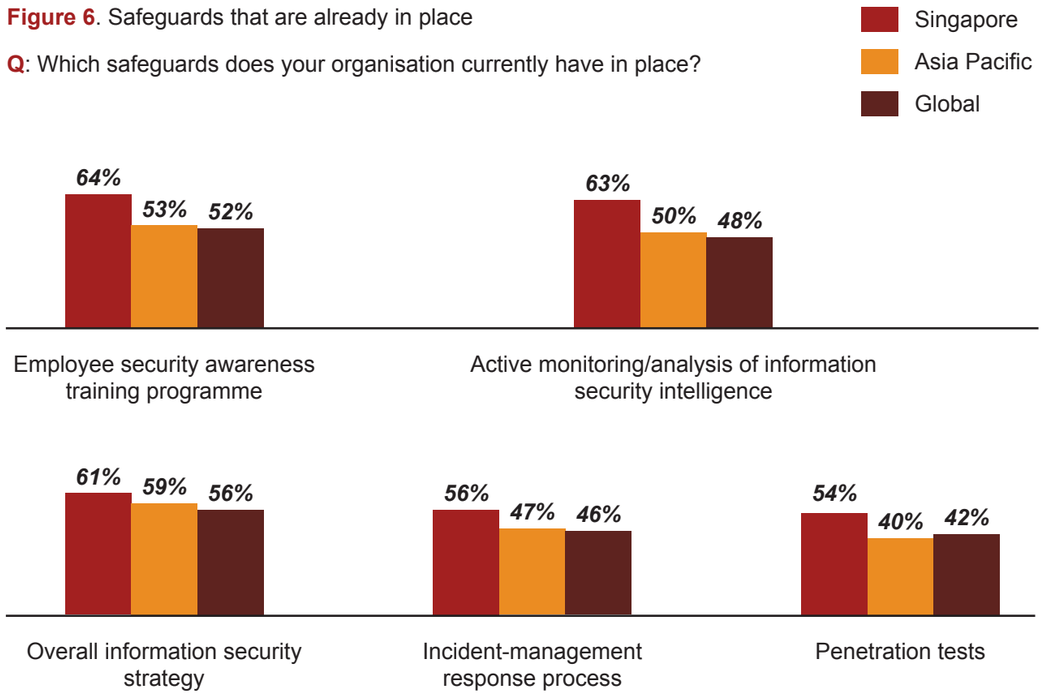
Protection is two-fold: Security safeguards and cyber insurance

This year's findings reveal that Singapore companies emerged ahead of the global and regional average when it comes to having implemented key cybersecurity safeguards, suggesting more mature levels of cyber readiness (Figure 6). However, the results also suggest that a handful of companies remain unequipped to react to cyber incidents and manage cyber risks adequately.

More than four in 10 organisations surveyed in Singapore (44%) do not have an incident-response process, while a similar proportion say their companies have yet to conduct penetration tests (46%). At the same, more than a third of the respondents have yet to implement an employee security awareness training programme (36%) as well as an information security strategy (39%).

Figure 6. Safeguards that are already in place

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



Base: Singapore - 80. Asia Pacific - 1585. Global - 8531
Source: The Global State of Information Security® Survey 2018

The rise of organisations cyber security incidents has led to an increased demand for cyber insurance as companies rush to insure their business against data breaches and/or network disruptions. More than six in 10 organisations surveyed in Singapore have cyber insurance (61%; Figure 7), of which a below-average percentage of them have made (37%) and collected a claim (35%; Figure 8).

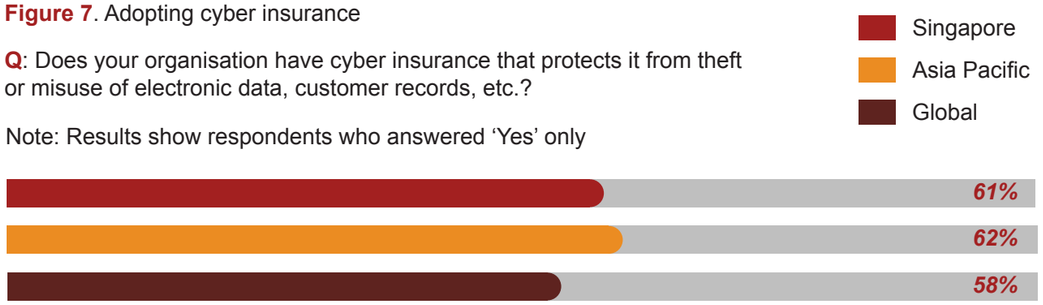
Simultaneously, a higher-than-average percentage of respondents from Singapore have taken steps to enhance their organisation's security posture in order to enjoy lower insurance premium (Singapore: 56%, Asia Pacific: 54%, Global: 47%).

In view of the Cyber Risk Management (CyRiM) programme in Singapore – a public-private partnership between the government, the insurance and the academic sectors aimed at developing the country's cyber insurance market – coupled with rising demand of cyber insurance, businesses can look forward to possible improvements in underwriting for cyber insurance and more sustainable premiums in the future.

Figure 7. Adopting cyber insurance

Q: Does your organisation have cyber insurance that protects it from theft or misuse of electronic data, customer records, etc.?

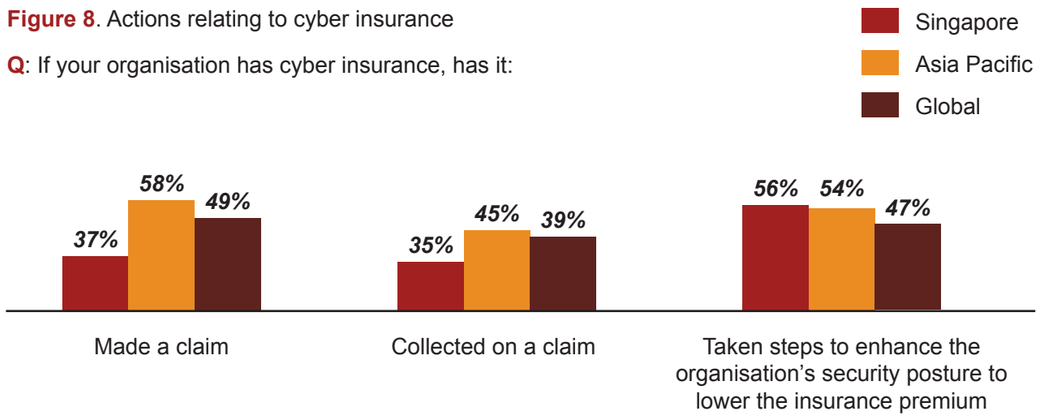
Note: Results show respondents who answered 'Yes' only



Base: Singapore - 79. Asia Pacific - 1685. Global - 9126
Source: The Global State of Information Security® Survey 2018

Figure 8. Actions relating to cyber insurance

Q: If your organisation has cyber insurance, has it:



Base: Singapore - 46. Asia Pacific - 1017. Global -5108
Source: The Global State of Information Security® Survey 2018

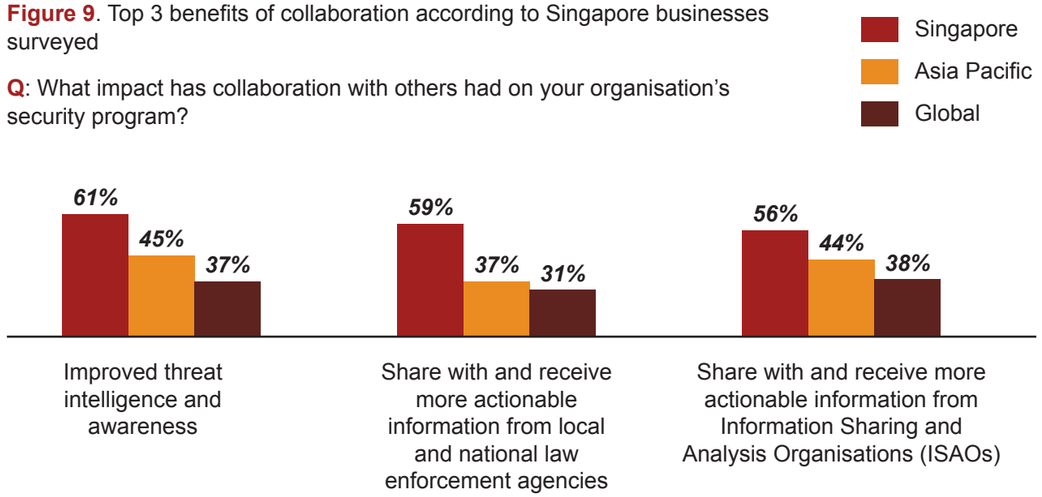
Stronger together through cyber collaboration

As mentioned in the earlier sections, the pervasive impact of cyberattacks extends beyond the business community. Industries and government leaders must work across organisational, sectorial and national borders to identify, map, and determine cyber-dependency and interconnectivity risks as well as surge resilience and risk-management.

Over the last few years, Singapore has continued to spur collaborations, insight and education in cybersecurity through the formation of the CSA, Singapore's Cybersecurity Strategy, the proposed Cybersecurity Bill, and various initiatives that encourage knowledge exchange across industries. The efforts seem to be paying off considering that results reveal businesses in Singapore are ahead of the global and regional curve in yielding results from cyber collaboration (Figure 9). More than half of its respondents attributed improved threat intelligence and awareness (Singapore: 61%, Asia Pacific: 45%, Global: 37%) as a result of collaborative efforts, followed by having received actionable information (Singapore: 59%, Asia Pacific: 37%, Global: 31%).

Figure 9. Top 3 benefits of collaboration according to Singapore businesses surveyed

Q: What impact has collaboration with others had on your organisation's security program?

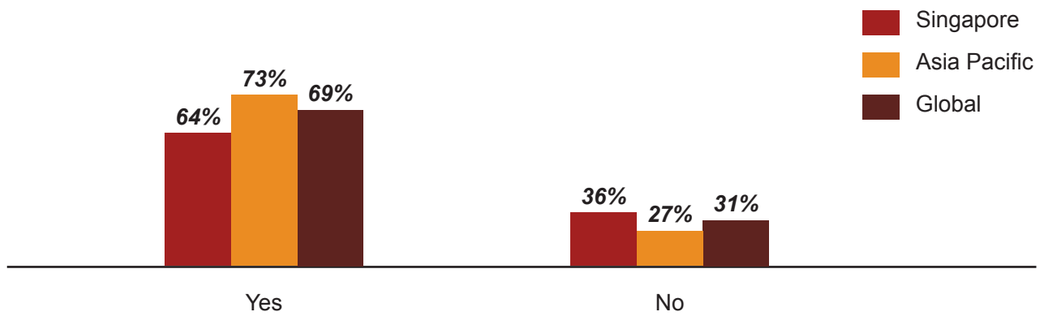


Base: Singapore - 46. Asia Pacific - 1097. Global -5345
Source: The Global State of Information Security® Survey 2018

It is interesting to note that despite having benefited from cyber collaborations, responses from Singapore fall behind both global and regional averages when it comes to collaborating with industry peers (Singapore: 64%, Asia Pacific: 74%, Global 69%; Figure 10).

Figure 10. Collaborating with industry peers on cybersecurity

Q: Does your organisation formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?



Base: Singapore - 81. Asia Pacific - 1697. Global -9235
Source: The Global State of Information Security® Survey 2018

In the meantime, Singapore businesses can look forward to the proposed Cybersecurity Bill, which aims to facilitate the sharing of cybersecurity information between the CSA, CII owners and victims of cyberattacks, as well as empower regulators to work closely with affected parties to resolve cyber incidents. This can provide the CSA with a better understanding on the key issues facing businesses, enabling the government body to share and equip organisations with relevant information that is constructive to fortifying their cyber defences. Ultimately, this will lead to strengthening Singapore's cybersecurity ecosystem.

Looking ahead

Taking lessons from the major cyber incidents that occurred in the past year (e.g. WannaCry and Petya), as cyberattacks become more sophisticated, institutions at all levels (business, government, academia and more) will need to work together and harder than ever to combat cybercrimes.

In anticipation of the proposed Cybersecurity Bill – expected to be rolled out in 2018 – identified CII owners will need to level up their game. They will need to ensure that they have the proper strategies and processes in place to implement effective CII protection plans and meet compliance requirements. As for companies that are unlikely to be CII owners, the Cybersecurity Bill should not be ignored as its proposed measures can serve as a guiding framework to enhance cyber readiness.

Among the fundamental building blocks to strengthening cyber defences businesses can consider are:

Performing data explorations to gain a better understanding of what information an organisation possesses, why they are valuable, where they are stored, and how the data flows through the organisation.

Conduct impact and risk assessments to understand and identify potential risks, assess the impact of these risks and how to manage them.

Businesses must be mindful that cybersecurity is not a one-time effort. For example, cyber risk assessment exercises need to be conducted on regular basis in order to identify and address new threats in a timely manner. Just as crucial, organisations must to shift their approach from being reactive to cyber threats and risks, to proactively taking measures to strengthen their security framework and safeguards.

The days of relying solely on the implementation of new security technologies as a cyber defence measure have passed. For any cyber strategy to be effective, it needs to be aligned with its organisation's business objectives, and must be sustained and enhanced by having the right talent, leadership, culture, processes and technology. Without the right training, governance, and tone from the top, even the most cutting edge security technology can be rendered ineffective.

Connect with our experts

Tan Shong Ye
Digital Trust Leader
Email: shong.ye.tan@sg.pwc.com

Jimmy Sng
Digital Trust Partner
Email: jimmy.sng@sg.pwc.com

Pierre LeGrand
Asia Pacific Technology Consulting Leader
Email: pierre.a.legrand@sg.pwc.com

pwc