The state of SMB cybersecurity at a time of crisis

A report focused on SMB cybersecurity trends in APAC covering business readiness, vulnerabilities and priorities.

July 2020

pwc

Table of contents

Introduction 1

Key findings

A. SMBs and the cyber-readiness gap 3

B. Cybersecurity vulnerabilities among SMBs 7

C. SMB priorities 11

Conclusion 13

Survey respondent details 15

Introduction

PwC surveyed more than 1,000 small and medium-sized businesses (SMBs) across Asia Pacific during March 2020 – just as COVID-19 had reached pandemic status. The aim of the survey was to explore the current state of cybersecurity for SMBs in the region. Its results offer the first insights into how SMBs are responding to this unprecedented situation.

This report is based on responses from 1,133 IT decision-makers and business managers in SMBs in eleven Asia Pacific geographies – Hong Kong, Mainland China, Taiwan, Japan, Singapore, Malaysia, Thailand, Vietnam, Indonesia, Australia and New Zealand.

Our findings suggest that many SMBs are complacent about the levels of protection they have in place to defend themselves, however attacks are ever-increasing in sophistication and ingenuity. 57% of respondents had experienced an attack in the last 24 months, showing it's more important than ever for SMBs to heighten their defences, and employees' awareness of cyberattacks.

The timing of our study coincided with the COVID-19 pandemic, when vast numbers of employees found themselves having to work from home. This would have increased cybersecurity risks to organisations where the work culture and IT infrastructure are tailored toward work at the office.

PwC's Threat Intelligence Centre found that phishing email attacks targeting employees working from home (WFH) during this period increased as much as ten-fold[1]. For example, cybercriminals capitalising on fears of the coronavirus devised phishing emails convincing enough to trick victims into clicking on links to fraudulent websites. Employees who are abruptly required to work from home and IT systems that are unprepared for large-scale remote work may contribute to breaches of cybersecurity, helped by employees downloading company data to personal or third party storage facilities such as Dropbox, Microsoft OneDrive and Google Drive.

[1] According to cybersecurity incident response and investigation data from PwC's Threat Intelligence Centre.

Key takeaways

SMBs perceive themselves to be ready for cyberattacks, but may be overconfident

Key survey findings include that only 27% of SMBs have a dedicated cybersecurity team, while 20% say they have no in-house expertise at all. Many SMBs have not deployed basic cybersecurity tools – only 53% deploy antivirus solutions.

Despite this, SMBs expressed satisfaction with IT security teams – 84% gave scores of seven or more out of 10.

In addition, 90% of respondents are confident that their businesses would be able to detect an attack within one working day; 84% believe they could recover from a hit within 24 hours.

This high level of confidence is at odds with industry research showing an average 'dwell time' (the period between an attack and its detection) of 54[2] days among SMBs in Asia Pacific.

Our survey therefore reveals a misalignment between the confidence expressed by SMBs in their cybersecurity readiness and established industry research. This may explain why 57% of SMBs surveyed sustained cyberattacks over the last 24 months, with 76% of them suffering more than one hit. It may also explain the significant monetary damage suffered by SMBs. More than 30% suffered damage between US$50,000 and US$250,000, while 9% sustained damage of more than US$1 million.

SMBs are easy targets for cybercriminals

The finding that more than half of SMBs have reported attacks during the last two years suggests that they may be viewed as easy targets by cyberattackers, who understand that they do not have the security resources enjoyed by larger organisations. 70% of these attacks saw hackers, malware and other actors evade intrusion detection tools, while 65% bypassed antivirus solutions.

The top-three cyberattacks on SMBs were caused by viruses and malware, web-based attacks and phishing attacks, while the most vulnerable endpoints were desk/laptop computers and web servers.

Data breaches were mainly perpetrated by hackers, while others were identified as mistakes by third parties, malicious insiders and negligent employees or contractors. The relatively high incidence of data breaches caused by third-parties is a reminder to companies that when they outsource work they do not automatically outsource their data protection responsibilities and liabilities.

Employees are considered crucial by SMBs as a first line of defence against cyberattacks

This survey reveals that IT-security priorities are determined by SMBs' leadership, with many regarding cybersecurity awareness and education among staff as high priority. They also express a preference for simple detection and response mechanisms that allow employees to form part of their cyber defence, rather than implementing multiple layers of complex technologies that require maintenance and frequent upgrades.

The wish to involve staff is particularly relevant to fighting off phishing attacks, because it is invariably an employee who decides whether to click on a link in an email purporting to be from a legitimate entity.

*Recommendations on cybersecurity for SMBs can be found at the end of this report.

[2] According to research conducted by California-based cybersecurity expert FireEye.

Key findings

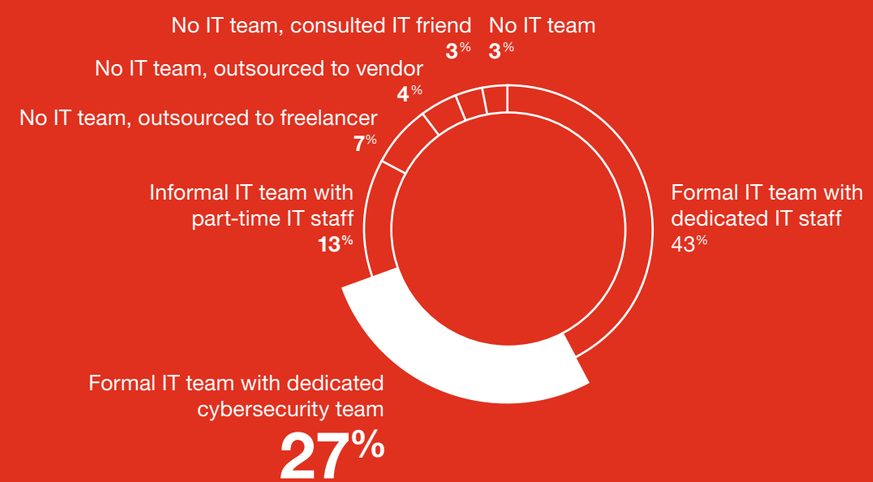
A. SMBs and the cyber-readiness gap

Most SMBs surveyed express confidence in their cybersecurity measures and say they are well prepared to defend themselves against attacks.

Some 70% reported they have a formal IT team in place, while only 27% said they have a dedicated cybersecurity team. Without dedicated cybersecurity team, SMBs are not able to constantly fine-tune their cyber defence strategy. This suggests a lack of capability.

Only 27% of SMBs have a dedicated cybersecurity team

How is your current IT department / cybersecurity team structured?



Intrusion-protection, detection systems (50%) and firewalls (48%) are the most common managed security tools. Only 53% of SMBs have antivirus solutions in place – indicating that many SMBs have not deployed the most basic cybersecurity tools.

The information-security tools deployed include web application firewalls (WAF), Cloud Access Security Broker (CASB) software and scanners for detecting vulnerabilities in applications.

Looking at the most commonly used tools in individual geographies, 53% of SMBs in Vietnam use application vulnerability scanners, while 46% use database-activity monitoring and runtime application self-protection tools.

In Japan, 38% of SMBs use static, dynamic or interactive application-security testing procedures, along with application delivery-controller tools, while 47% have deployed file-integrity and activity-monitoring tools. Turning to Hong Kong and Thailand, 44% of SMBs use security information and event management solutions.

On average, 55% of SMBs in Malaysia, Vietnam and Indonesia engage in managed vulnerability scanning of networks, servers, databases or apps – suggesting a healthy adoption of security hygiene practices.

In Mainland China, 62% of respondents use identity and access management tools. 50% of SMBs in Thailand use advance threat-defence technologies – the highest such score in Asia Pacific, followed by Indonesia at 46%. More than half of those surveyed in Malaysia and Indonesia have DDoS protection in place, probably as a result of the proliferation of such attacks on financial institutions there.

Which of the following applications or IT security technologies/software tools do you currently use? [Multiple selection]

What type of managed security tools is/are currently in place? [Multiple selection]

Some 20% report having no in-house expertise. Of the remaining, 84% are confident in the capability of the IT security teams, scoring them 7 or more out of 10 in terms of effectiveness.

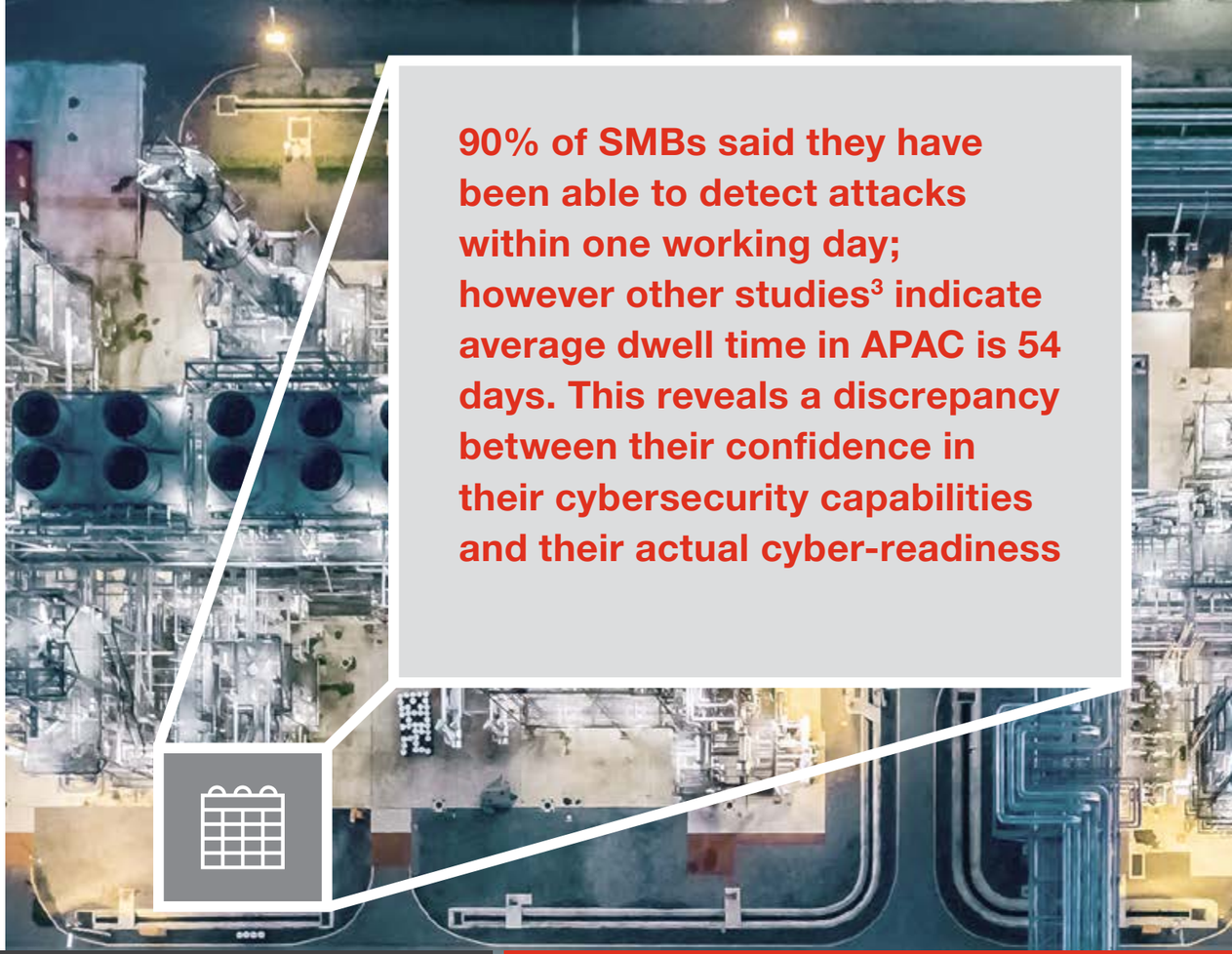
As many as 90% of SMBs say they have been able to detect attacks within one working day; those in Mainland China claim to have been able to do so in just minutes. Nearly half of Australian respondents say they have been able to respond within an hour.

In addition, 84% of respondents across the eleven markets say they have recovered from an attack within just 24 hours.

Other research, however, suggests the average 'dwell time' (the period between an attack penetrating an organisation and being detected) is 54[3] days and the dwell time of external attack is 131 days among SMBs in Asia Pacific.

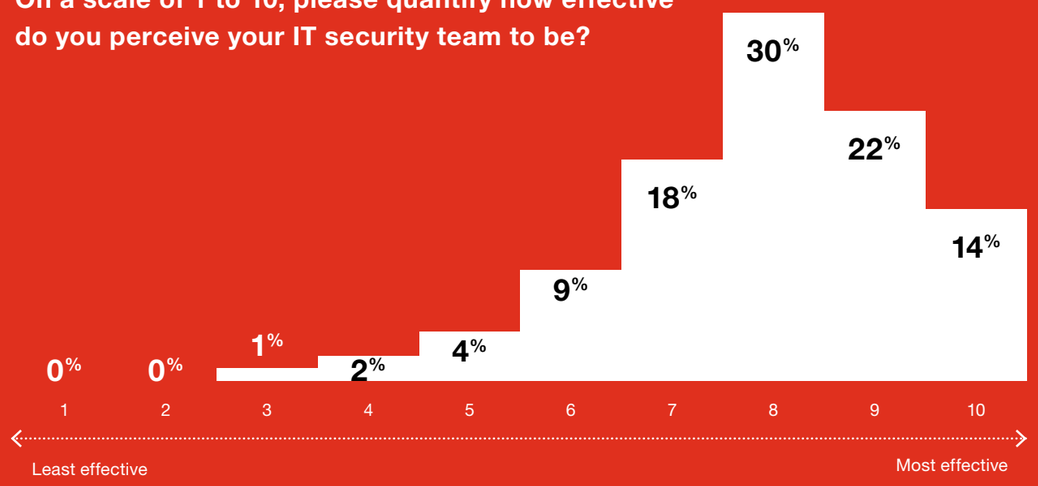
The disparity between these dwell time statistics and claims made by SMBs in this survey reveals a discrepancy between their confidence in their cybersecurity capabilities and their actual cyber-readiness. Another concern is that SMBs appear to underestimate the scale of everyday threats from cybercriminals.

The core finding that 57% of respondents have been attacked during the last two years suggests that SMBs are viewed as easy targets by attackers, as they do not have the substantial cybersecurity resources dedicated to protecting larger enterprises.

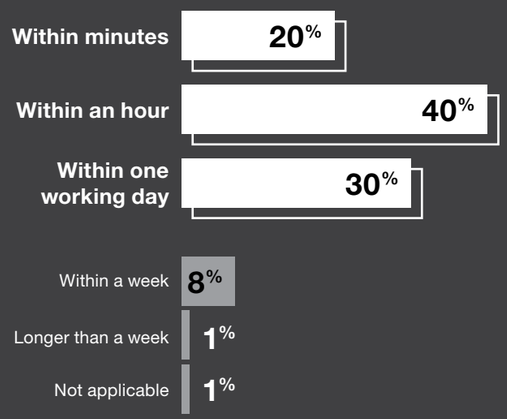


90% of SMBs said they have been able to detect attacks within one working day; however other studies[3] indicate average dwell time in APAC is 54 days. This reveals a discrepancy between their confidence in their cybersecurity capabilities and their actual cyber-readiness

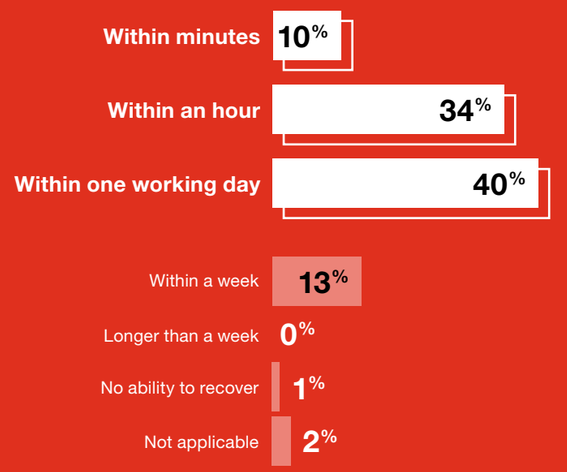
On a scale of 1 to 10, please quantify how effective do you perceive your IT security team to be?



How long after the most recent cyberattack did you realise the issue?



How long did it take your organisation to fix & recover from the most recent cyberattack?



[3] According to research conducted by California-based cybersecurity expert FireEye.

B. Cybersecurity vulnerabilities among SMBs

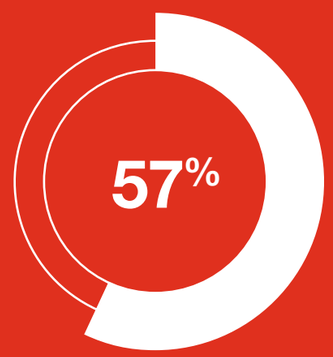
Evidence shows that cyberattacks are pervasive among Asia Pacific's SMBs. The fact that 57% have reported attacks during the last 24 months suggests a significant risk to SMBs. This is reinforced by the finding that 76% of those attacked sustained more than one hit during the two-year period.

70% of the attacks saw hackers, malware and other attackers evading intrusion-detection tools, while 65% bypassed antivirus defences.

57% of SMBs surveyed sustained cyberattacks over the last 24 months, with

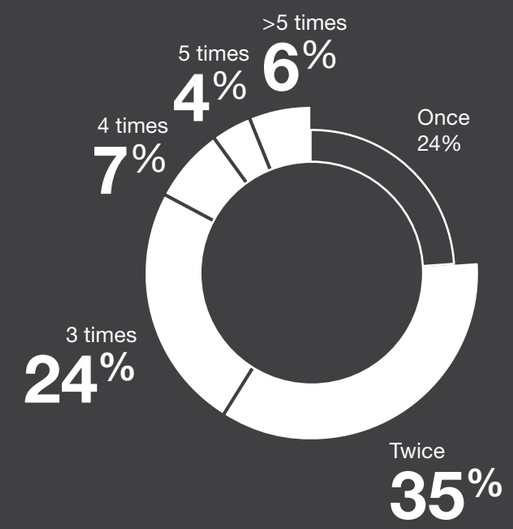
76% of them suffering more than one attack

Has your organisation experienced a cyberattack?



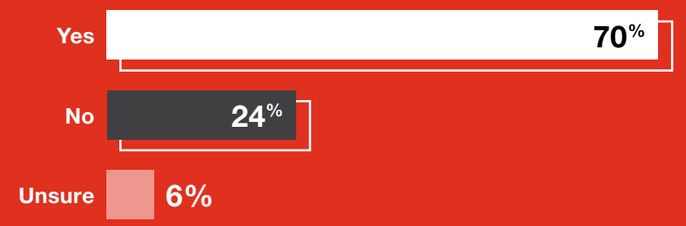
of the SMBs experienced a cyberattack in the last 24 months

How many times has your business experienced a cyberattack in the past 24 months?

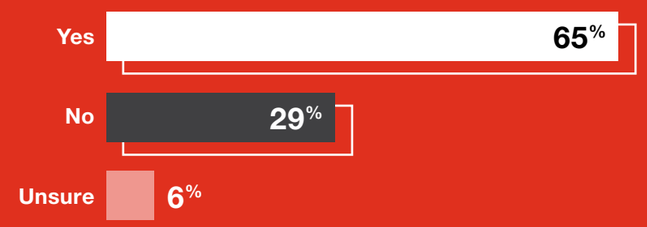


Has your organisation experienced situations when

a) exploits and malware have evaded your intrusion detection system?



b) exploits and malware have evaded your antivirus solutions?



The severity of these attacks is illustrated by significant monetary damage suffered by SMBs. More than 30% suffered damage between US$50,000 and US$250,000, while 9% sustained damage of more than US$1 million.

A breakdown shows that 50% of SMBs in Australia and Japan spent between US$50,000 and US$250,000. 10% in Singapore and New Zealand spent more than US$1 million, while respondents in Malaysia, Vietnam and Indonesia spent less than US$100,000. Moreover, ever-increasing levels of sophistication and ingenuity behind modern cybercrime suggest that many SMBs may have suffered attacks they don't even know about.

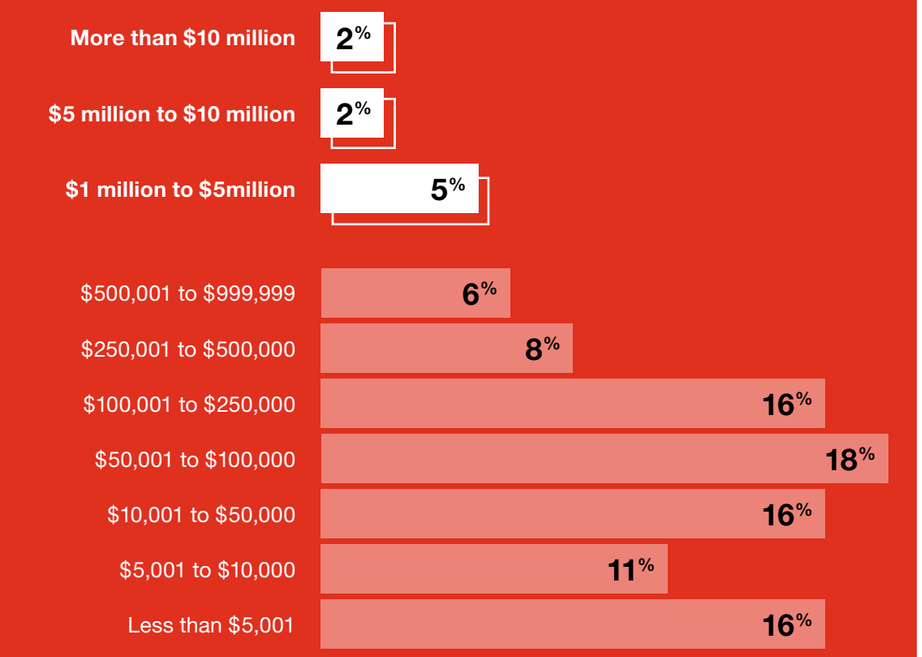
This survey was conducted as the COVID-19 pandemic took hold. At this time, defences may have been diminished by large numbers of employees with low levels of cybersecurity awareness working from home. Cybercriminals also seized the opportunity to make their phishing scams more convincing by linking them to the virus scare.

Findings identify phishing as one of the top-three attack types suffered – viruses and malware (51%), web-based attacks (38%) and phishing attacks (32%).

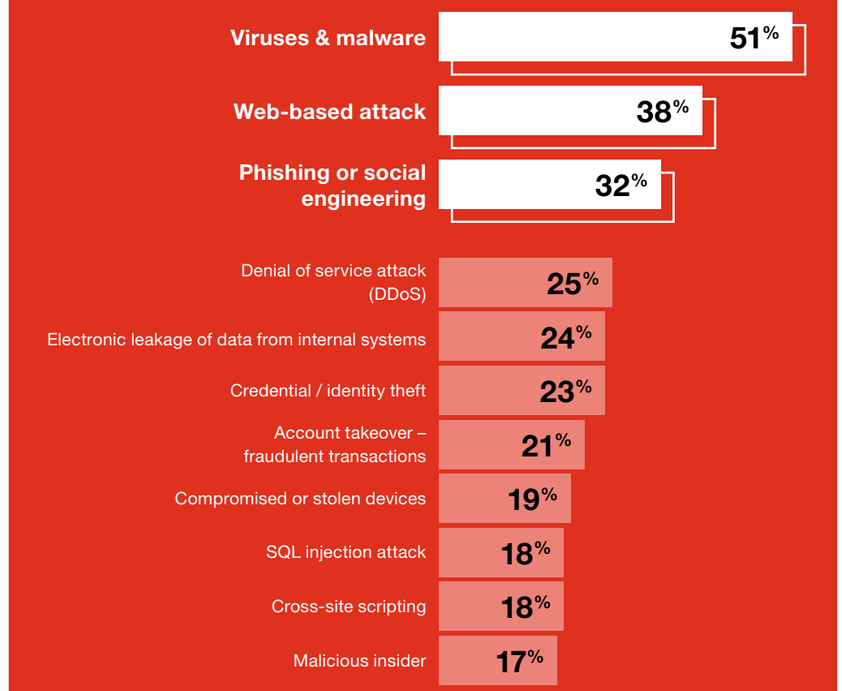
The high incidence of phishing attacks suggests that SMBs would benefit from employees being more aware of the need for cybersecurity and for keeping everyday threats at bay. This is particularly relevant, as it is invariably an employee who clicks on the link in an email purporting to be from a legitimate entity.

The most vulnerable endpoints were identified as desk/laptop computers (44%) and web servers (44%). While awareness of these vulnerabilities is encouraging, this is offset by the fact that only 53% of SMBs have antivirus solutions in place.

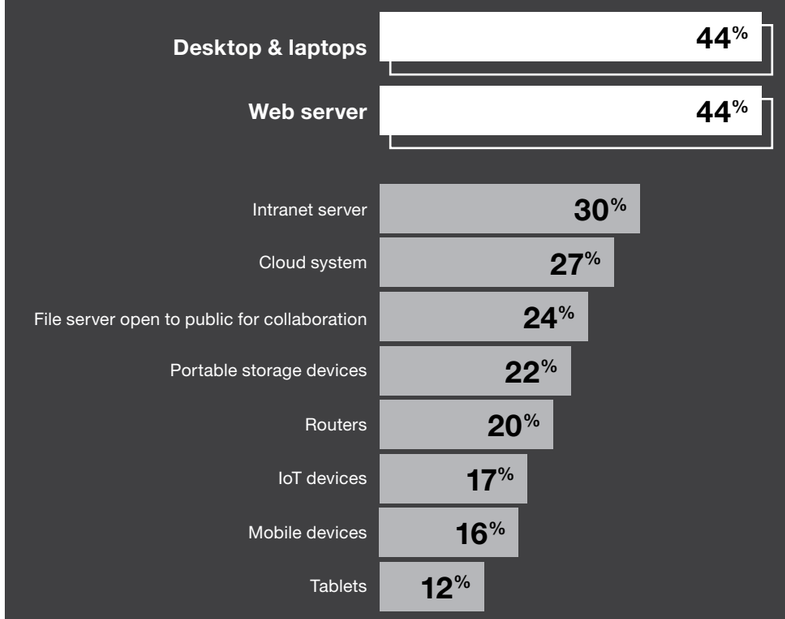
Approximately, how much did disruption to normal operations cost your organisation? (USD)



What type of cyberattacks did your business ever experience? [Multiple selection]



What were the entry points for the attack? [Multiple selection]



Data breaches were perpetrated mainly by hackers (48%), while others were identified as mistakes by third parties (40%), malicious insiders (37%) and negligent employees or contractors (36%).

On average, 44% of respondents across the eleven geographies surveyed reported having suffered a data breach in the last 24 months. That figure rises to 50% when we focus on Thailand, Vietnam, New Zealand and Malaysia.

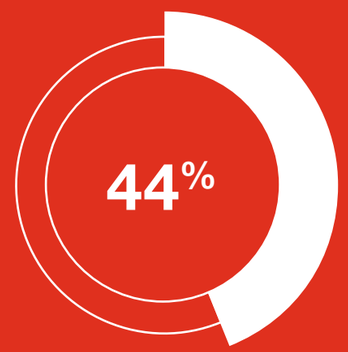
The fact that 57% have suffered attacks over the last 24 months, and 44% have sustained data breaches, suggests that cyber attackers enjoy a successful hit rate – even if the numbers are skewed by some SMBs taking multiple hits.

Some 60% of the data breaches reported by SMBs in the developed markets of Australia, New Zealand and Singapore were the result of mistakes by third parties.

The relatively high incidence of data breaches caused by third-party mistakes implies that companies need to understand that outsourcing work to third parties does not automatically mean their data protection responsibilities and liabilities are also outsourced. Any financial, regulatory or reputational fallout as a result of mistakes made by third-party organisations will impact the client rather than the vendor. This indicates that a key element of any vendor selection/contracting procedure is a robust due diligence process.

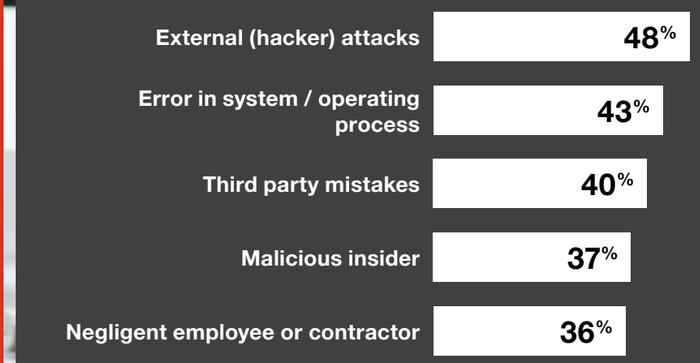
44% of respondents throughout the 11 geographies surveyed reported they had suffered a data breach in the last 24 months

Has your organisation experienced an incident involving the loss or theft of sensitive information about customers, target customers or employees (i.e. data breach)?



of the SMBs experienced an incident involving loss or theft of sensitive information in the past 24 months.

What were the root causes of the data breach? [Multiple selection]



C. SMB priorities

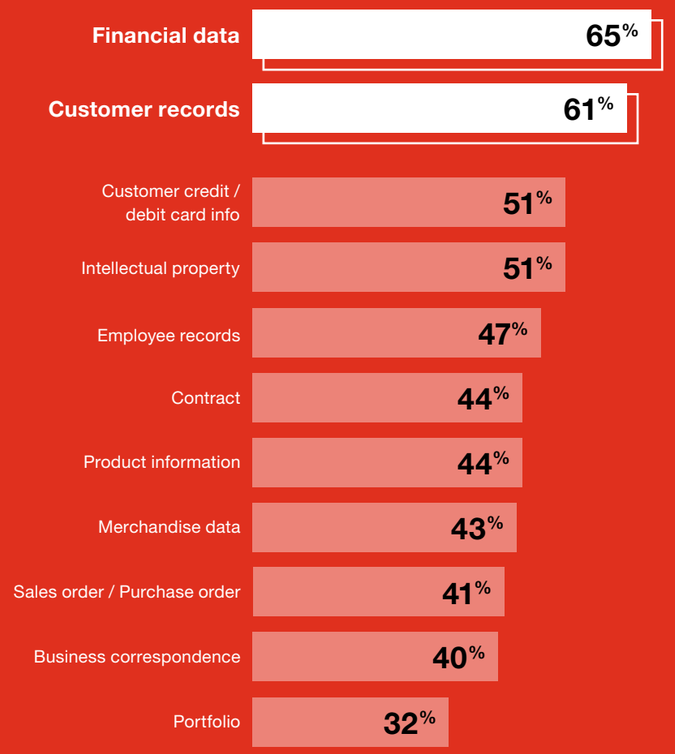
This survey reveals that IT security priorities are determined by leadership and 39% said they have allocated 11-20% of their IT budget to cybersecurity.

SMBs start to give growing importance in monitoring suspicious online activity and protecting data, especially on financial and customer data. Legal and regulatory compliance requirements are a significant influence on SMB attitudes toward data security issues.

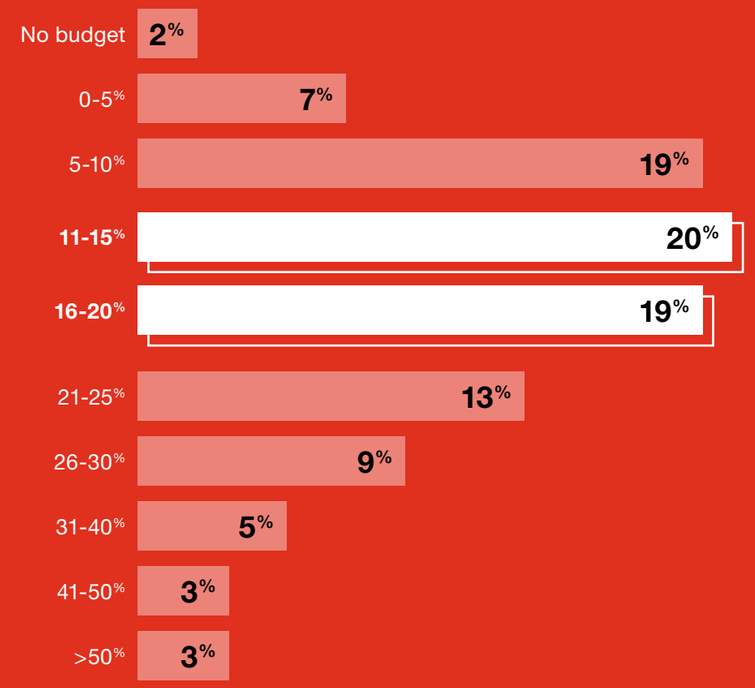
SMBs in Hong Kong, Australia and New Zealand emphasise protecting employee records, while Mainland China and Taiwan tend to prioritise merchandise data.

Respondents in Mainland China, Thailand and Vietnam tend to prioritise intellectual property, while 58% of SMBs in Mainland China and Vietnam want to keep contracts and other sensitive company data secure.

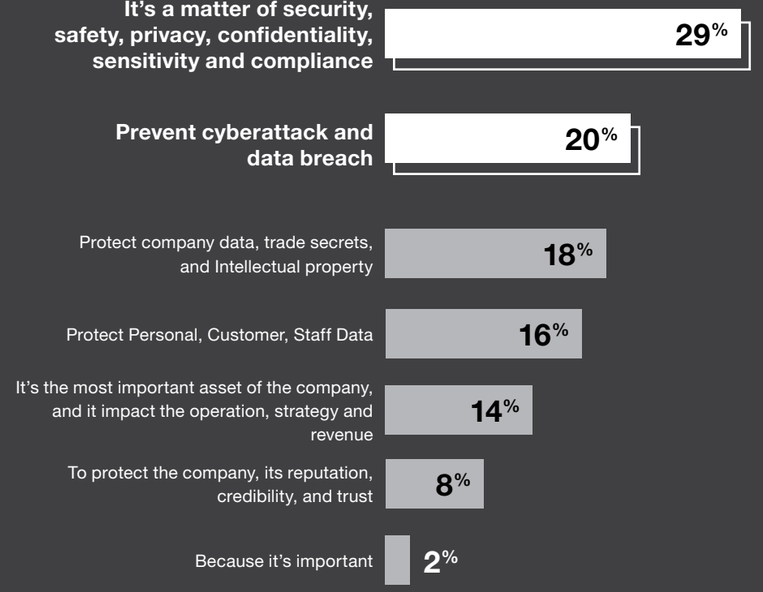
What types of information are you most concerned about protecting from cyberattackers? [Multiple selection]



What percentage of your organisation's IT budget is dedicated to cybersecurity?



Why is it so important to protect data for your organisation?

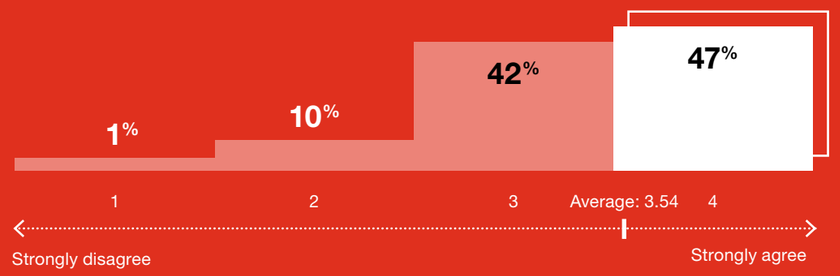


SMBs regard cybersecurity awareness and education among their staff as a high priority, and express a preference for tools that involve their employees in detecting threats and fending off attacks.

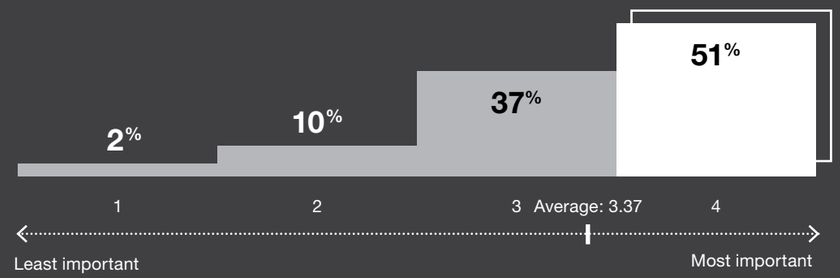
89% of SMBs agree to have staffs involved immediately in order to raise alerts of suspicious online activity and help prevent further damage. SMBs in Thailand and Indonesia are interested in robust cybersecurity tools that employees will find easy to use. Respondents in Singapore, Thailand, Indonesia, Vietnam and Mainland China are interested in tools that are compatible on multiple platforms. Respondents in Thailand, Australia, Japan, Mainland China and Malaysia prefer tools developed in partnership with a reputable brand.

89% of SMBs agree to have staffs involved immediately in order to raise alerts of suspicious online activity and help prevent further damage

How much do you agree or disagree – When there is a suspicious activity, company staff and other employees involved should be notified immediately and help to prevent further damage.



How important is it to you and your organisation for your staff to be aware of cybersecurity measures? [Scale: 1=least important, 4=most important]



Conclusion

High incidence of cyberattacks and data breaches amongst SMBs, and the impact is severe

Our survey shows that SMBs are easy targets for cyber attackers and may have too much faith in current protection that may be inadequate in the case of increasingly sophisticated attacks.

The cost associated with remediating cyberattacks is unsustainably high, as the SMBs we have surveyed report collectively spending many millions of dollars to recover from cyberattacks over the last two years alone.

Discrepancy between SMB's confidence in their cyber-readiness and actual reality

A discrepancy exists between the confidence SMBs have in their readiness to fight off cyberattacks and the reality illustrated by our survey results. For example, 57% of SMBs have suffered attacks over the last 24 months and 44% have sustained data breaches. This suggests cyber attackers enjoy a successful hit rate, even if the numbers are skewed by some SMBs taking multiple hits.

Respondents identified their most vulnerable endpoints as desk/laptop computers (44%) and web servers (44%), yet only 53% of SMBs had antivirus solutions in place to defend themselves.

Phishing emerged as one of the top-three attack types plaguing SMBs – viruses and malware (51%), web-based attacks (38%) and phishing attacks (32%). This is significant, as it is employees who face the dilemma of whether or not to click on a link in an email purporting to be from a legitimate entity.

Employee awareness for better security

SMBs place an emphasis on the importance of cybersecurity awareness and education among staff, and say they want tools that involve their employees in preventing cyberattacks. Respondents want staff to be able to respond immediately in order to raise alerts of suspicious online activity and mitigate further damage. This requires ongoing training to keep staff up to speed with the latest threats and defence mechanisms.

Our survey was conducted as the COVID-19 pandemic started to take hold, when huge numbers of employees were working from home. This may have eroded cybersecurity in terms of company data being downloaded into domestic environments and cybercriminals using the fear of contagion as a power source for their phishing scams.

How can SMBs improve their cybersecurity?

Here are recommendations from PwC

1

Remote access with scalability
Meet the WFH challenge with technologies that can be scaled up or down, according to need.

2

Strong security and privacy principles
Integrate a strong security and privacy foundation, so businesses can maintain critical business operations without giving rise to compliance issues.

3

Prioritise access for critical applications
Determine and prioritise applications critical to business operations run by employees.

4

Real-time, data-driven decisions
Deploy health survey and check-in apps that allow you to track staff working locations for better resources planning and decisions.

5

Governance and controls
Confirm your solutions are governed by controls that ensure availability and security of remote private access.

6

Employee awareness and guidance
Make sure your employees know what's expected of them and are aware of the resources available. Raise awareness among staff of financial scams and form an understanding of the action required in order to minimise financial loss.

7

Technology options
Be aware of your technology options in order to maintain a secure business environment and maintain cyber defences.

8

Incidence response and management
Be prepared to provide the incident response and crisis management support required to address critical security issues. And make sure an incident response team is always in a state of readiness to help minimise the negative impact of unplanned events.

9

Returning to workplace
Be particularly vigilant of phishing and other fraudulent emails during and after the COVID-19 crisis, when employees return to the workplace.

10

Practical guidance from Governments
Access information from Governments on practical cybersecurity awareness and technology steps to take to minimise the risk of a cyberattack.

Survey respondent details

We surveyed 1,133 IT decision makers and business managers in SMBs across eleven territories in Asia Pacific. They were Hong Kong, Mainland China, Taiwan, Japan, Singapore, Malaysia, Thailand, Vietnam, Indonesia, Australia and New Zealand, each of which produced up to 100 respondents.

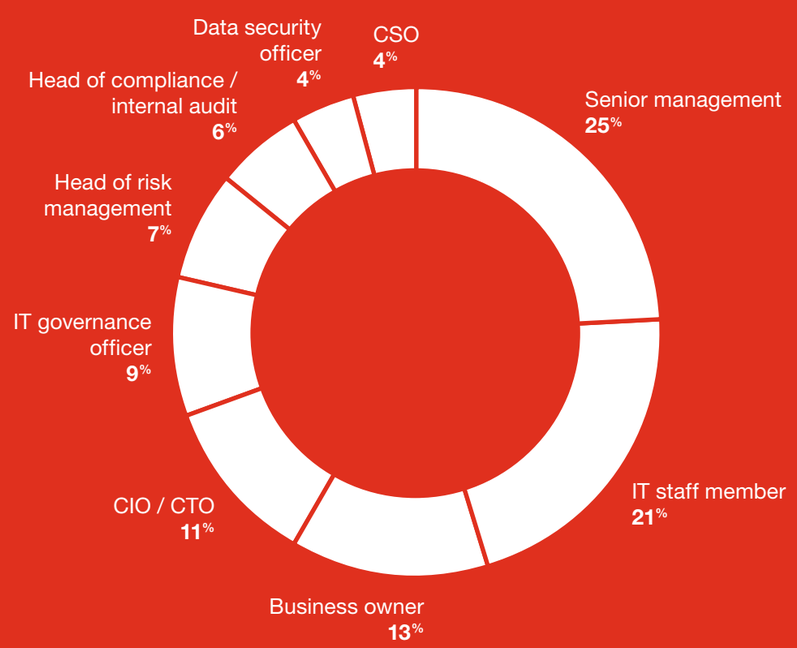
The SMBs involved have staff numbers ranging from 50 to 500 – 51% have between 50 and 300 workers, while 49% have between 301 and 500.

Of the respondents, 13% are business owners, 11% CIO/CTOs, 9% IT governance officers, 7% risk management heads, 6% compliance/internal audit heads, 4% data security officers, 4% chief security officers, 25% senior executives and 21% IT professionals.

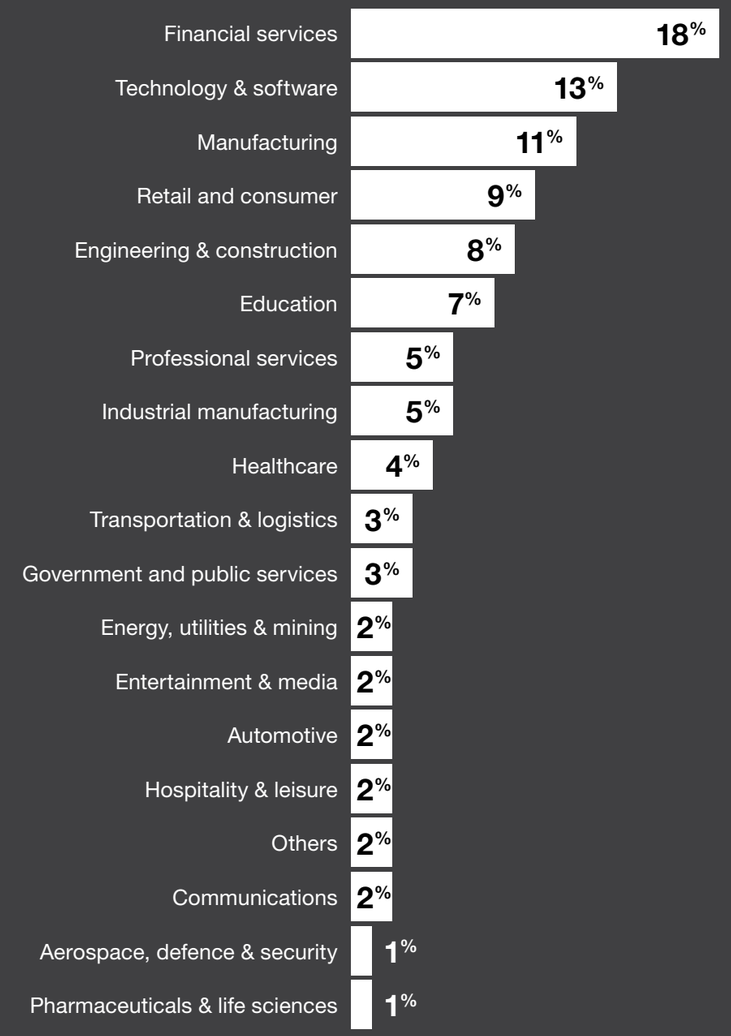
SMBs surveyed fall into the following industry categories: Financial services (18%), Technology & software (13%), Manufacturing (11%), Retail & consumer (9%), Engineering & construction (8%), Education (7%), Professional services (5%), Industrial manufacturing (5%), Health care (4%), Transportation & logistics (3%), Government & public services (3%), Energy, utilities & mining (2%), Entertainment & media (2%), Automotive (2%), Hospitality & leisure (2%), Communications (2%), Aerospace, defence & security (1%), Pharmaceutical & life science (1%) and others (2%).

* Small and medium-sized business (SMB) refers to a business with 50 to 500 employees.

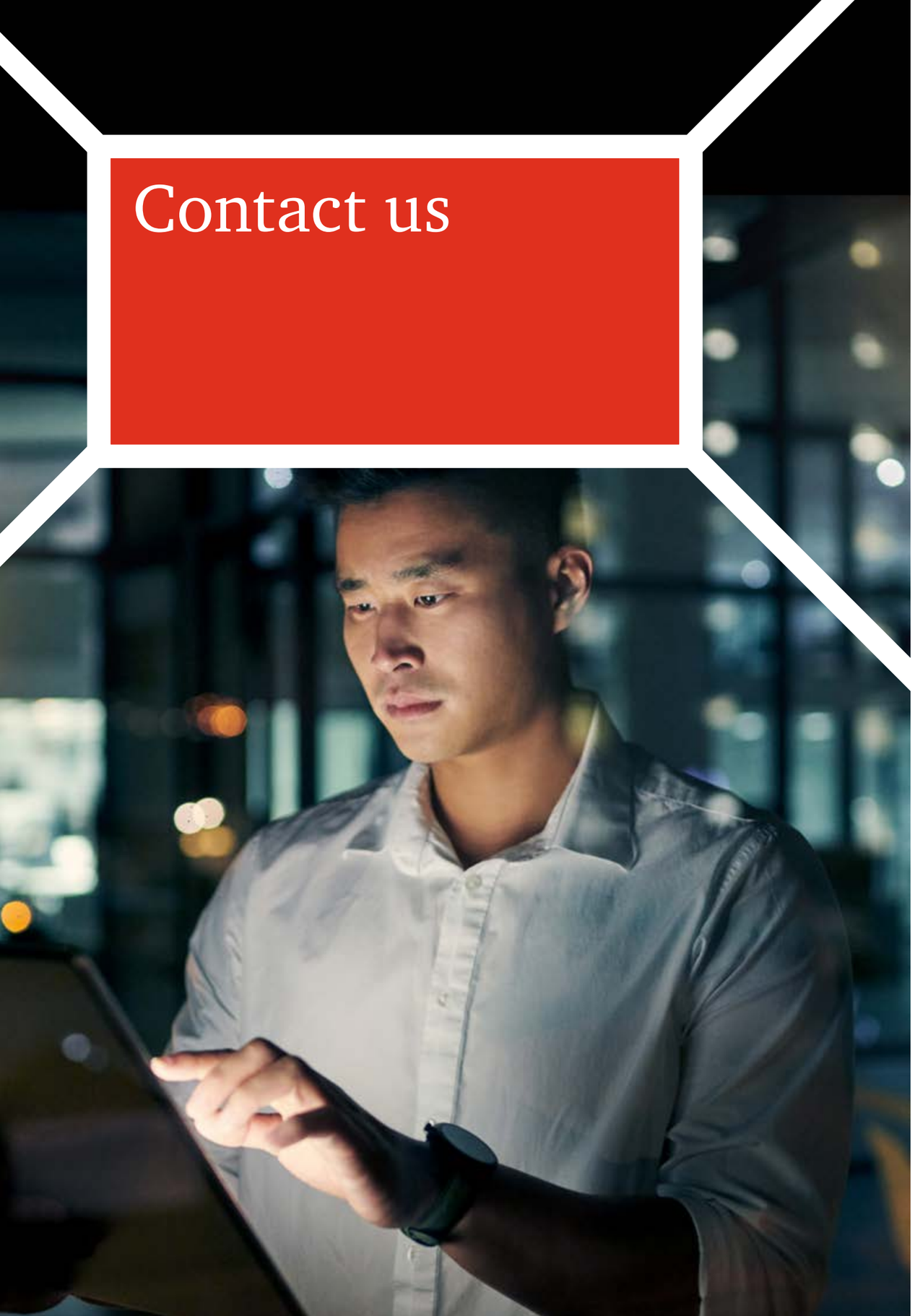
Positions of respondents



Industries of respondents' businesses



Contact us



Mainland China & Hong Kong	**Kenneth Wong** Risk Assurance Cybersecurity & Privacy Asia Pacific and Mainland China/Hong Kong Leader kenneth.ks.wong@hk.pwc.com	**Dennis Li** Partner dennis.y.li@cn.pwc.com
	Lisa Li Partner lisa.ra.li@cn.pwc.com	**Felix Kan** Partner felix.py.kan@hk.pwc.com
Australia	**Michael Cerny** Partner michael.cerny@pwc.com	**Peter Malan** Partner peter.malan@pwc.com
Indonesia	**Subianto** Partner subianto.subianto@pwc.com	
Japan	**Kazuhiro Hayashi** Partner kazuhiro.hayashi@pwc.com	**Kei Tonomura** Partner kei.tonomura@pwc.com
	Sean King Partner sean.c.king@pwc.com	**Takashi Ameniya** Partner takashi.amemiya@pwc.com
Malaysia	**Clarence Chan** Executive Director clarence.ck.chan@pwc.com	
New Zealand	**Adrian van Hest** Partner adrian.p.van.hest@pwc.com	**Anthony Steele** Partner anthony.j.steele@pwc.com
Singapore	**Freddy Wee** Partner freddy.wee@pwc.com	**Jimmy Sng** Partner jimmy.sng@pwc.com
	Shong Ye Tan Partner shong.ye.tan@pwc.com	
Taiwan	**Chin-Jui Chang** Partner chin-jui.chang@pwc.com	
Thailand	**Chat Thongsong** Director chat.thongsong@pwc.com	
Vietnam	**Pho Duc Giang** Director pho.duc.giang@pwc.com	