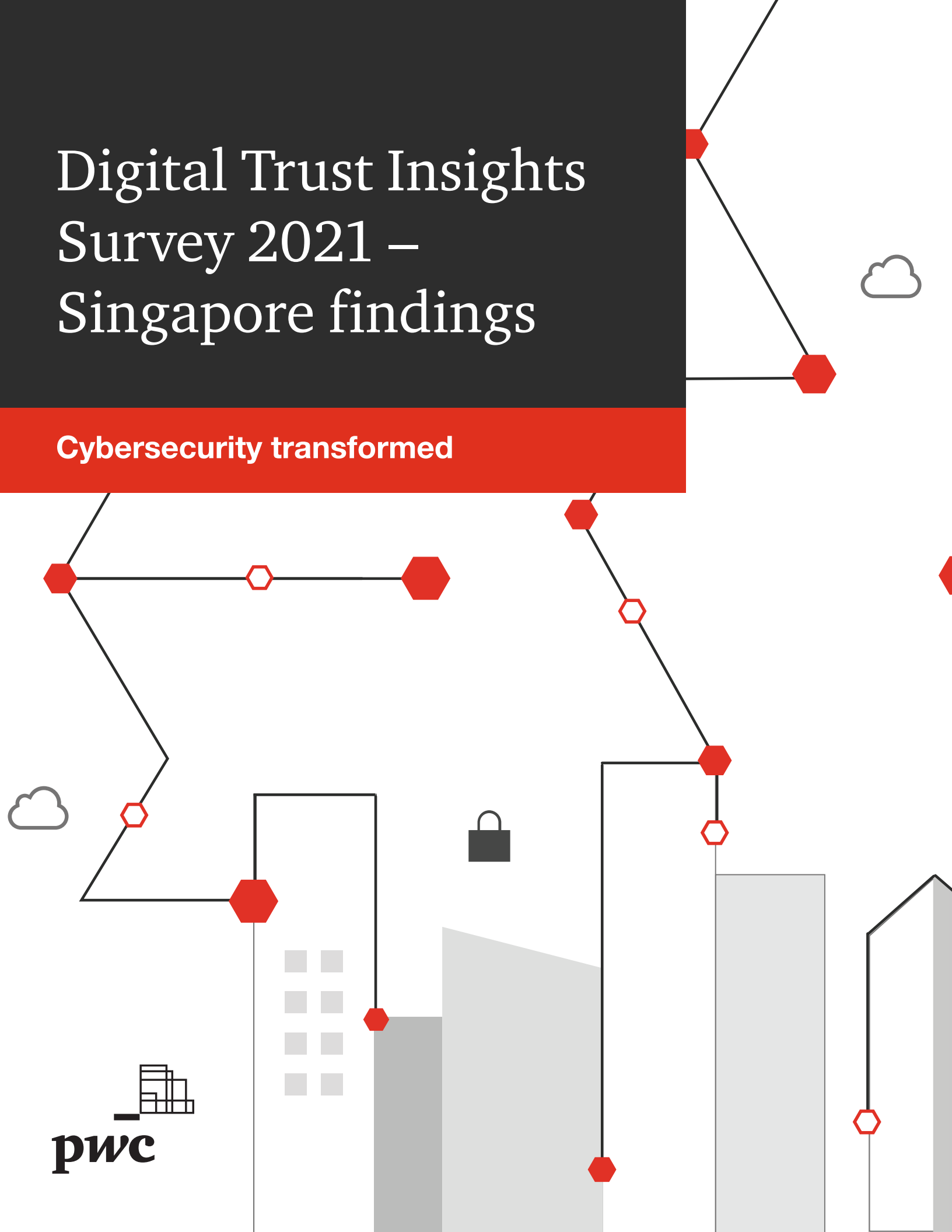
Digital Trust Insights Survey 2021 – Singapore findings

Cybersecurity transformed



pwc

Content

Introduction

Cybersecurity transformed

Decades after emerging from under the IT wings, the cybersecurity profession has matured. Armed with the insight and foresight that only experience and wisdom can provide, cyber stood at a critical, pivotal, and exciting time for the industry, and the organisations and people it served.

With COVID-19, enterprises accelerated their digitalisation programs, further boosting their cyber investments as part of their renewed business models. Security leaders worked closely with business teams, to strengthen the resilience of organisations as a whole. New digital solutions added layers of protection and automated continuously monitoring systems for a simpler, more integrated approach to security. As a result, cyber managed to level the playing field with attackers, pushing back and fending off like never before.

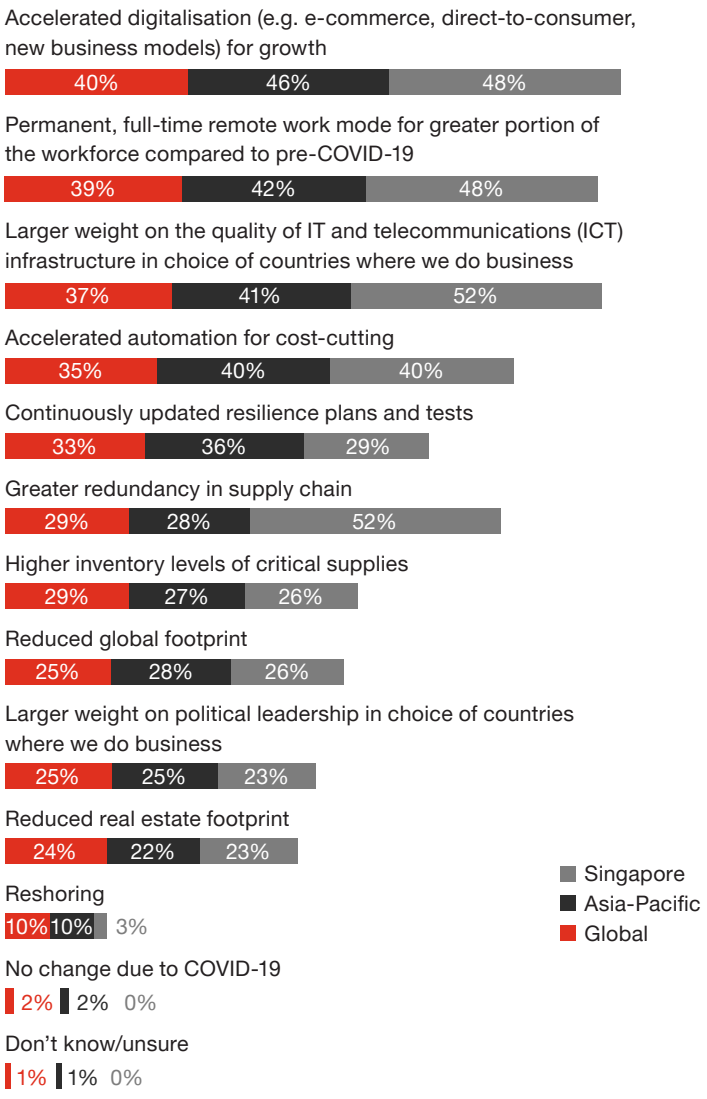
Today, a digital-first strategy is key to pivoting back to a steady growth path, and securing the future of businesses in the new world. Cyber is undoubtedly integral to the digital-first strategy. It's heartening to see Singapore CEOs and boards, much like in other parts of the world, teaming up with CISOs today like never before. Enterprises are integrating cyber with business as a whole amid increasing threat outlook. The idea simply is to increase business resilience and create greater business value - and this is what we found in our Global Digital Trust Insights 2021 survey of 3,249 business and technology executives around the world, aside from what's changing and what's next in cybersecurity.

In this report, we keep focus on the top Singapore findings of the survey. Nearly half the Singapore companies surveyed are prioritising accelerated digitalisation (e.g. e-commerce models, direct to consumer, new business models, virtual workforce) in the next year (Exhibit 1). The majority of them are placing a larger weight on IT and telecommunications infrastructure of countries where they do business. Despite the challenging economic environment, about 32% see their headcounts surging up to 5% and 16% see it surging even beyond 5%. (Exhibit 1A).

Exhibit 1

COVID-19 has accelerated digitalisation and the adoption of new ways of working

Q: Which of the following changes are most likely to be impacts of the COVID-19 experience in your industry?



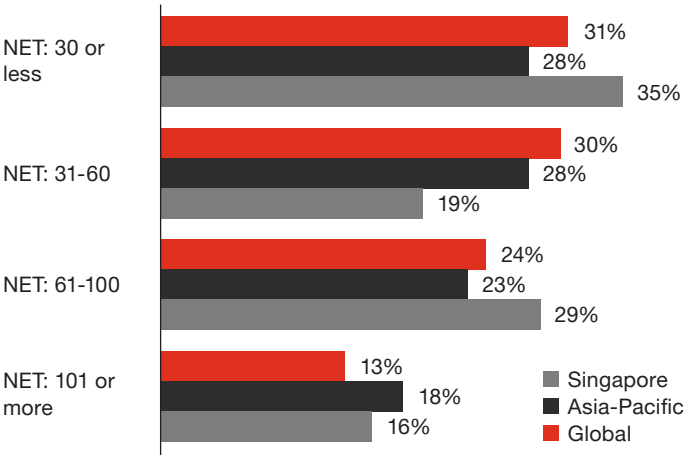
Base: All respondents (Global, 3249; Asia-Pacific, 595; Singapore, 31)

Exhibit 1A

Cybersecurity headcounts continue to surge despite the economic impact of COVID-19

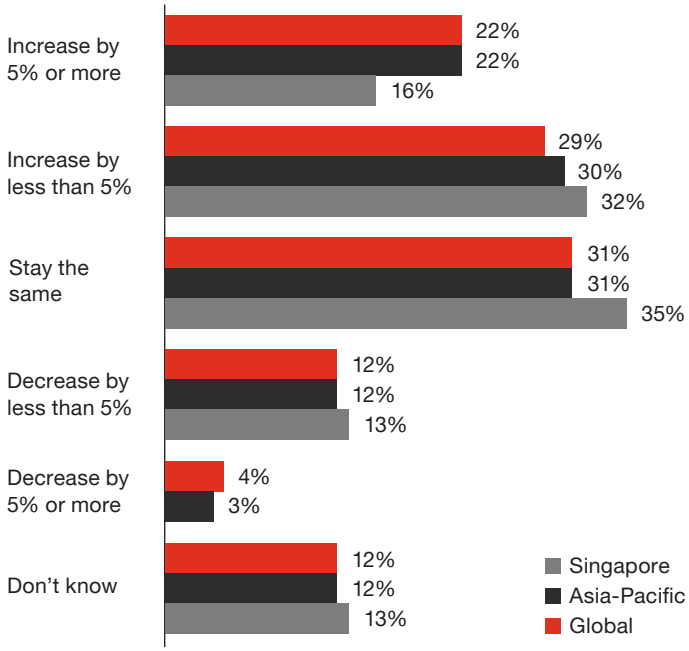
Q: (a) What is the current FTE in your cybersecurity team? (b) How is headcount for your cybersecurity team changing in the next 12 months?

Current FTE



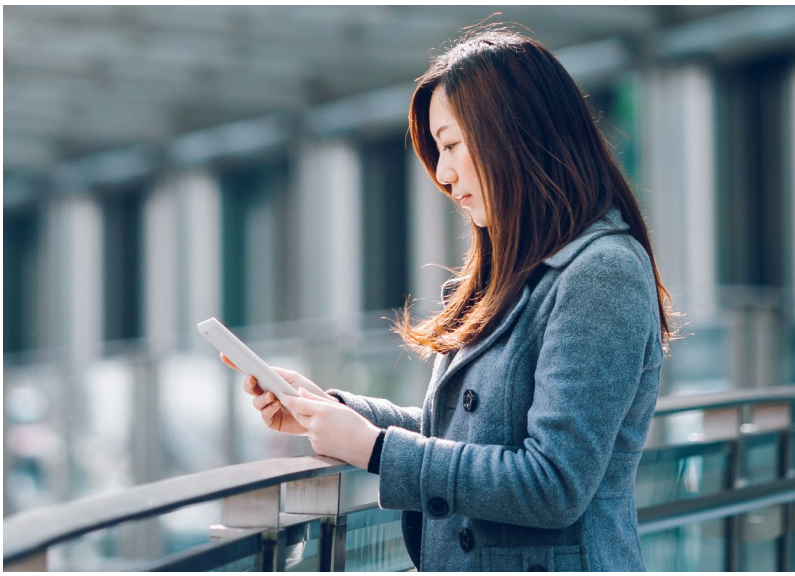
Base: All respondents (Global, 3249; Asia-Pacific, 595; Singapore, 31)

Change in headcount



This publication will cover the five key insights and priorities from the Singapore region:

1. Increasing threat outlook
2. Focusing on greater resilience testing, and embedding cybersecurity in the overall business strategy
3. Getting the most value for every cybersecurity dollar
4. Shifting toward new approaches and thinking around cybersecurity
5. Future-proofing the workforce



Key Singapore insights

1. Increasing threat outlook

For 84% of Singapore organisations, transitioning to remote work during the pandemic revealed urgency for the organisations to modernise capabilities such as identity and access management, endpoint protection and mobile device management (Exhibit 2A). One of the biggest impacts of such accelerated digitalisation is the potential surge in digital attacks and cyber threats. **Remote work set-ups**, accomplished hastily to enable business continuity, have brought increased exposure to threats.

The threats with the most potential impact, Singapore executives said, are attacks on Internet of Things (65% voted significantly negative impact' or 'negative impact'), social engineering (61%) and cloud service provider (55%) (Exhibit 2). Interestingly, the Singapore region's threat outlook in these areas are far higher than that of global executives. It does not come across as a surprise that Singapore has an increased threat outlook as compared to other territories, given it is ahead of its global peers in terms of accelerated digitalisation and rapid adoption of cloud and IoT - 77% of Singapore executives believe that moving more services and infrastructures to the cloud is foundational for the next generation of business solutions in our organisation.

Also, with the Singapore government defining the 11 critical infrastructures*, local executives are more aware and cognizant of what the critical business services are and how it would impact them.

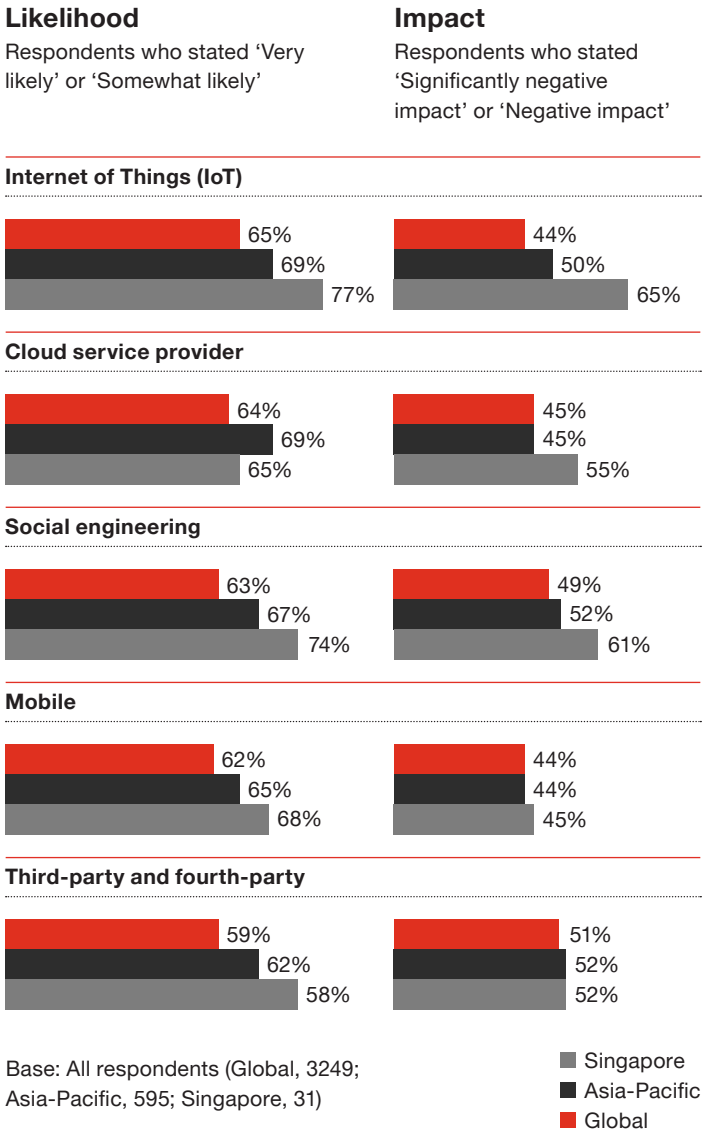
*Source: https://www.csa.gov.sg/legislation/cybersecurity-act

Exhibit 2

Singapore has a higher threat outlook than the rest of the world in the adoption of IoT, cloud and social engineering

Q: In your view, what is:

(a) the likelihood that these threat vectors are going to affect your industry in the next 12 months, and (b) the extent of impact, if it were to happen, on your organisation?



Base: All respondents (Global, 3249; Asia-Pacific, 595; Singapore, 31)

Key considerations for Singapore businesses

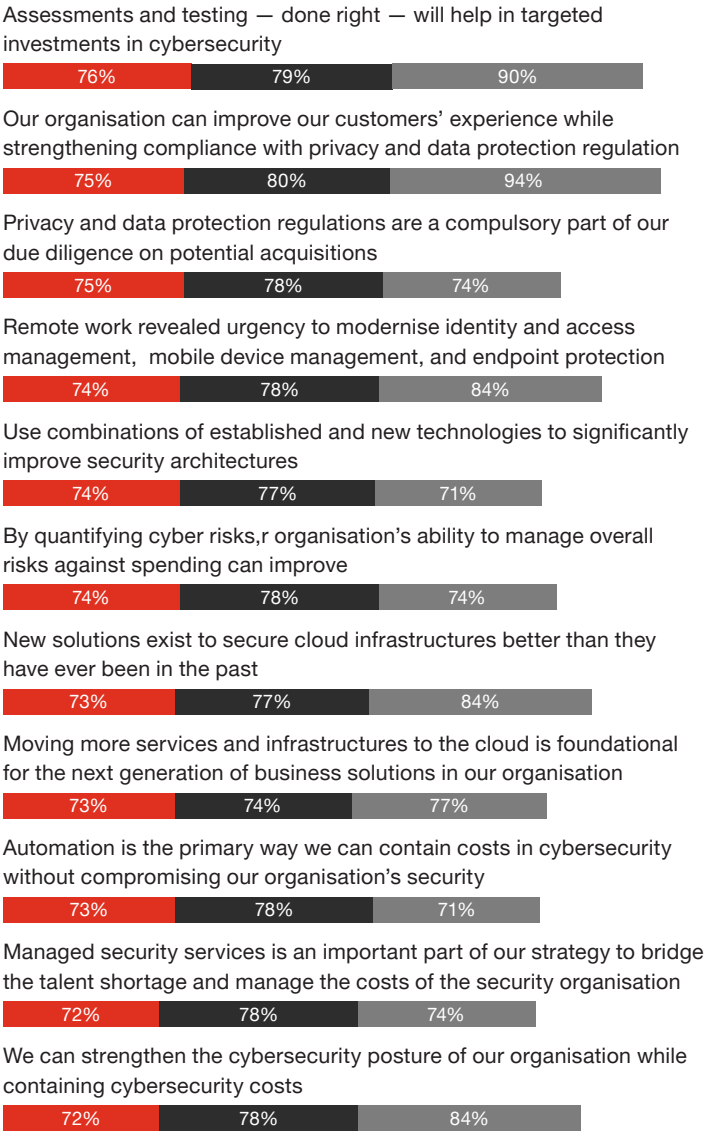
- **Identity management and data access:** For the scalability of cloud workloads and the flexibility of employees to work from anywhere, sensitive data is moving to the cloud and mobile devices, no longer in the corporate network and beyond the protection of the organisation's traditional perimeter controls. Instead of the network, the digital identity of the user becomes the new perimeter for security. Tight identity governance and privileged identity management is crucial. It is also important to ensure that protection of the data, travels with the data itself, regardless of its location and the devices that access it.
- **Understand the new world dynamics and anticipate potential threat situations:** Prepare comprehensive response strategies against each of these perceived threat situations. It's not just about prevention, it's also about reaction and response. Against the emergence of threats around 5G, IoT, cloud services, and social engineering among others, organisations need to actively craft comprehensive response strategies to manage potential digital risks.
- **Create a robust ongoing risk mitigation program:** The reality is, we can never fully prepare for a cyber attack. It is important to have a robust ongoing to risk mitigation program which is updated on a regular basis. Leverage threat intelligence to understand the risk landscape, identify emerging threats, undertake tabletop exercises to stay prepared with incident response planning, real-time monitoring system and a robust recovery strategy.

Exhibit 2A

Remote work during the pandemic revealed urgency for organisations to modernise capabilities.

Q: To what extent do you agree or disagree with the following statements about opportunities in cybersecurity in the next 12 months?

Respondents who stated 'Strongly agree' or 'Somewhat agree'



Base: All respondents (Global, 3249; Asia-Pacific, 595; Singapore, 31)

2. Focusing on greater resilience testing, and embedding cybersecurity in the overall business strategy

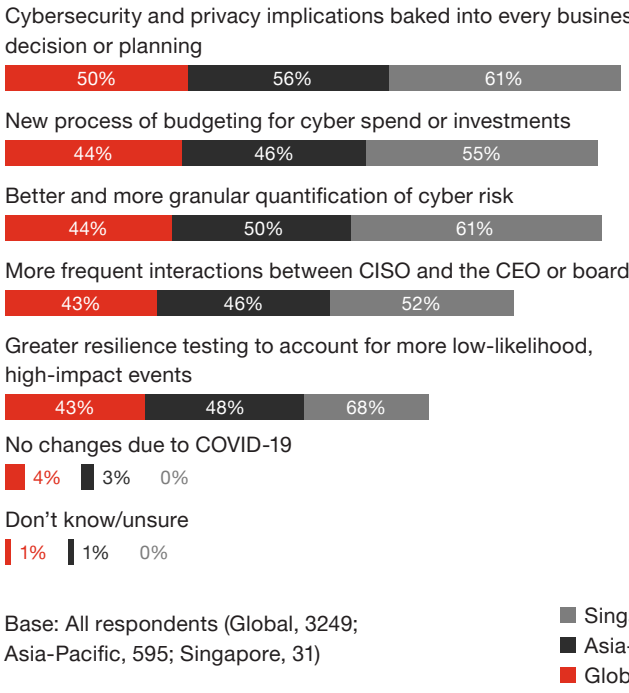
With an accelerated roadmap for a digital-first organisation and the consequent heightened risk of cyber attacks, the role of the CISO has changed forever. During COVID-19, it was found that CISOs were significantly involved in decision-making around pandemic responses that were both operational and transformational: whether it was enabling remote working, or setting up systems to remotely track productivity and employee safety.

The majority of Singapore businesses (68%) feel, COVID-19 has compelled businesses to place greater emphasis on resilience testing to account for more low-likelihood, high-impact events (Exhibit 3). Over three out of five (61%) Singapore organisations believed that digital business strategy and cybersecurity can no longer exist in silos, and that cybersecurity and privacy implications will be baked into every business decision in 2021. This highlights the organisations' focus on better planning and granular qualification of cyber risk. More than half (52%) have started bringing together their cybersecurity and business teams to collaborate for better outcomes. Businesses reported more frequent interactions between the CEOs and CISOs. Over two out of five (42%) local respondents noted that they will be investing on increased collaboration initiatives between the cyber and business side professionals in delivering business outcomes (Exhibit 4). Not a single organisation felt that COVID-19 would cause no change or impact at all.

Exhibit 3

Post COVID-19, organisations are factoring in cybersecurity implications into their decision making

Q: What are the top impacts of the COVID-19 experience for organisations on cybersecurity and the business?



Base: All respondents (Global, 3249; Asia-Pacific, 595; Singapore, 31)

Key considerations for Singapore businesses

- **Keep cyber regulations in mind for all business decisions:** For organisations to holistically and meaningfully embed cybersecurity into every major business decision, government regulations are key. The Singapore Personal Data Protection Commission (PDPC) is updating the Personal Data Protection Act to increase the responsibility of organisations in the event of data loss - via mandatory reporting and increased penalty. This brings cyber regulations to the forefront, with an increased need to invest in capabilities, processes and technologies to prioritise these considerations in all business decisions.
- **From day one:** As we can see from the survey, the majority of the organisations plan to bring together cybersecurity and business strategy - but this must be done from day one. Include cybersecurity and privacy personnel in digital transformation projects from the get-go—and evaluate whether they have the right skills aligned to design, build, and sustain digital transformation initiatives, or if external resources are needed. CISOs should also be involved in non-cyber projects, collaborating with risk, business, legal and tech leaders to protect and defend the organisation from new risks.
- **All leaders have a role to play:** While the role of the CISO has become more pivotal than ever before, it's also the collective responsibility of the Boards, COO, CEO and CTO to ensure cybersecurity and digital safety is baked into digital business strategy.

3. Getting the most value for every cybersecurity dollar

As entities digitise, every new digital process and asset becomes a new vulnerability for cyber attacks. Against the backdrop of cash flow challenges as well, getting the most value for every cybersecurity dollar spent is critical. To focus their cybersecurity spend over the next 12 months, the majority (55%) of Singapore businesses are investing in unifying cyber risk reporting across the organisation (Exhibit 4). Nearly half of them (48%) are looking to strengthen their security function's skill sets while 45% will be investing in advanced technologies to improve the effectiveness of their cyber defence capabilities. Cyber managers can do more with less, but to do so they need to quantify cyber risk and use the information to make smart choices that protect the business's security, privacy, and cash flow.

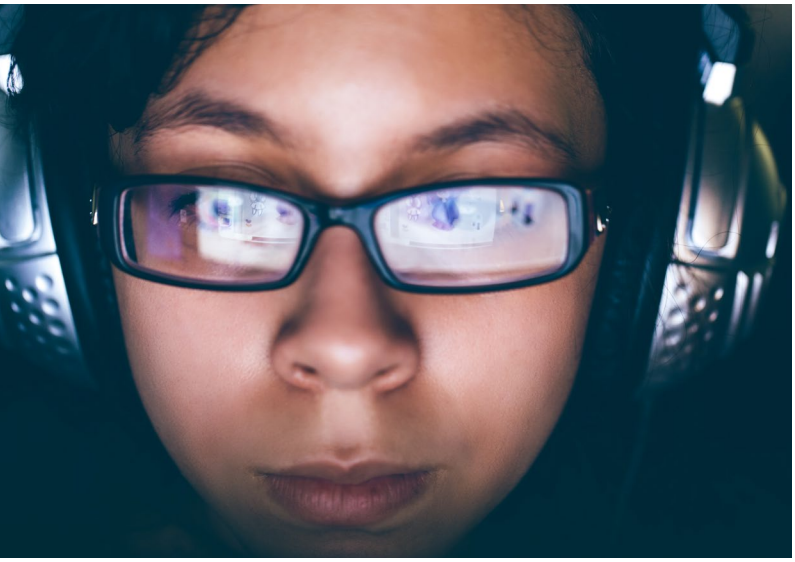


Exhibit 4

Singapore is prioritising the strengthening of security skill sets more than global organisations

Q: What are organisations investing in to manage cybersecurity in the next 2 years?

Base: All respondents (Global, 3249; Asia-Pacific, 595; Singapore, 31)

Key considerations for Singapore businesses

- **Quantify cyber risk and craft an investment strategy:** Often, when investing in cybersecurity, organisations do not have their pulse on the most pressing risks that should be prioritised for their organisation, and consequently find themselves with an unclear cybersecurity investment strategy. To ensure there is alignment between what you are investing in and the reduction of risk in your organisation, have a clear-cut strategy including (i) quantify your organisation's risks to guide the immediate investments, (ii) articulation of assets and systems that need protection, and (iii) considerations around the impact on data and supply chain.
- **Have a forward-thinking cyber strategy:** An effective cybersecurity investment strategy is always forward thinking. Ensure that it is aligned with securing the business of the future and your digitalisation objectives, rather than focusing spending on enhancing areas or infrastructure that might potentially become outdated, or even automated in the future.
- **Invest in innovation:** An important anchor to forward-thinking cyber strategy is innovation. With a clear understanding of your threats, explore and outsource new cyber technologies and tools which will save time and efforts, to architect your cyber defense and future-proof your organisation in a cost-effective manner.

4. Shifting toward new approaches and thinking around cybersecurity

Innovation is changing the cybersecurity game, giving new advantages to defenders and leveling the playing field with attackers. Moving toward in terms of new approaches and strategies, it is apparent that cloud security is the next big transformation. Majority of the organisations believe that moving more services and infrastructures to the cloud is fundamental to the next generation of business solutions. More than a third of the organisations in Singapore are accelerating cloud adoption while more than half of them (55%) are already implementing an integrated cloud and network strategy approach (Exhibit 5). This increases the need to manage the risks of cloud environments. More than four out of five (84%) are confident that new solutions exist to secure the cloud more than ever before (Exhibit 2A).

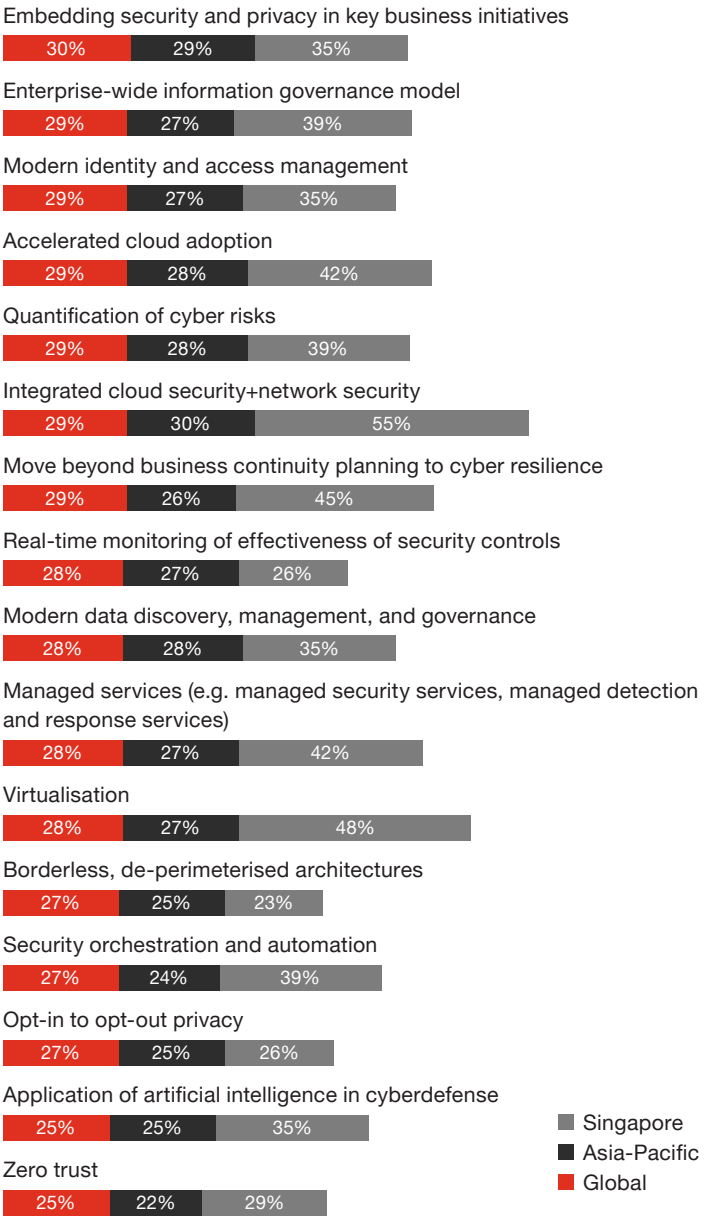
42% are implementing managed services (e.g. managed security services, managed detection and response services) - significantly higher than the global average of 28%, and are also planning to implement application of AI in cyberdefense, higher than the global average of 28%.

Exhibit 5

More and more Singapore organisations are open to exploring new approaches of thinking toward cybersecurity

Q: To what extent is your organisation moving to the following new cybersecurity approaches or thinking?

Respondents who stated 'Implemented at scale'



Base: All respondents (Global, 3249; Asia-Pacific, 595; Singapore, 31)

Key considerations for Singapore businesses

- **Pre-empt new trends:** The data tells us that Singapore has always been an early adopter of cyber innovations, and with an increase in remote working, supply chain interconnectivity and data exchanges, organisations should also look to actively preempt the new trends and looming threats of IT.
- **Quantify cyber risk and invest in real-time monitoring:** Only 26% of organisations surveyed are quantifying their cyber risks and investing in real-time monitoring of effectiveness of security controls, which is a cause for concern. Without real-time monitoring, the return on investment in innovation in cybersecurity strategy will always be low.
- **Understand your risks:** Organisations risk defending and investing on certain threats that are less important versus threats that could be potentially devastating with their impact. More than ever, it is imperative to have an in-depth understanding of your organisation's primary cyber risks to guide your investment and innovation decisions.

5. Future-proofing the workforce

More than half the global respondents surveyed said they plan to add full-time cybersecurity personnel over the next year. More than one-fifth (22%) will increase their staffing by 5% or more.

There are no two ways about it, businesses need to upskill their workforce keeping in mind the cybersecurity landscape today, and ways in which it may change in the future. Skills that were earlier 'good-to-have' are now a must-have. Singapore businesses are now investing in the skills and knowhow of cloud solutions (48%), security intelligence (45%), and specific technologies like IoT and Blockchain (35%), as well as business enablers like project management (35%) and digital design (45%) (Exhibit 6).

These in-demand qualities correspond with the expanded role of the CISO as not merely a tech leader, but one who works with colleagues in the C-Suite and the business side to add value overall.

Social skills like 'critical thinking', 'adaptability' and 'creativity' are also in high demand - CISOs used to look for the person who knew the most about how to configure a firewall or identity and access management, for example. Not anymore. Good communications, good analytical thinking, and the ability to step outside the process and imagine new and better ways to do it — those soft skills are harder to teach.

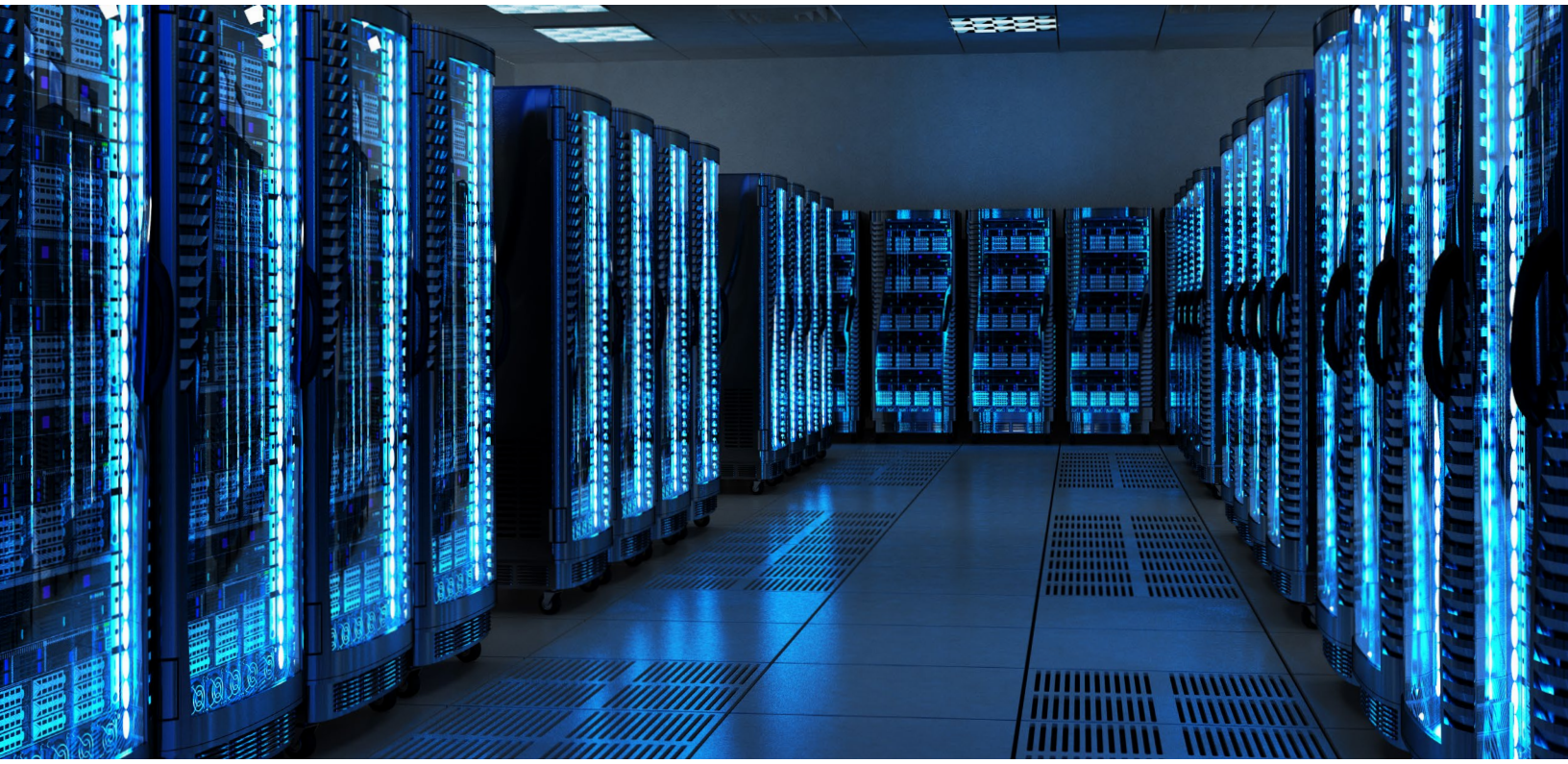
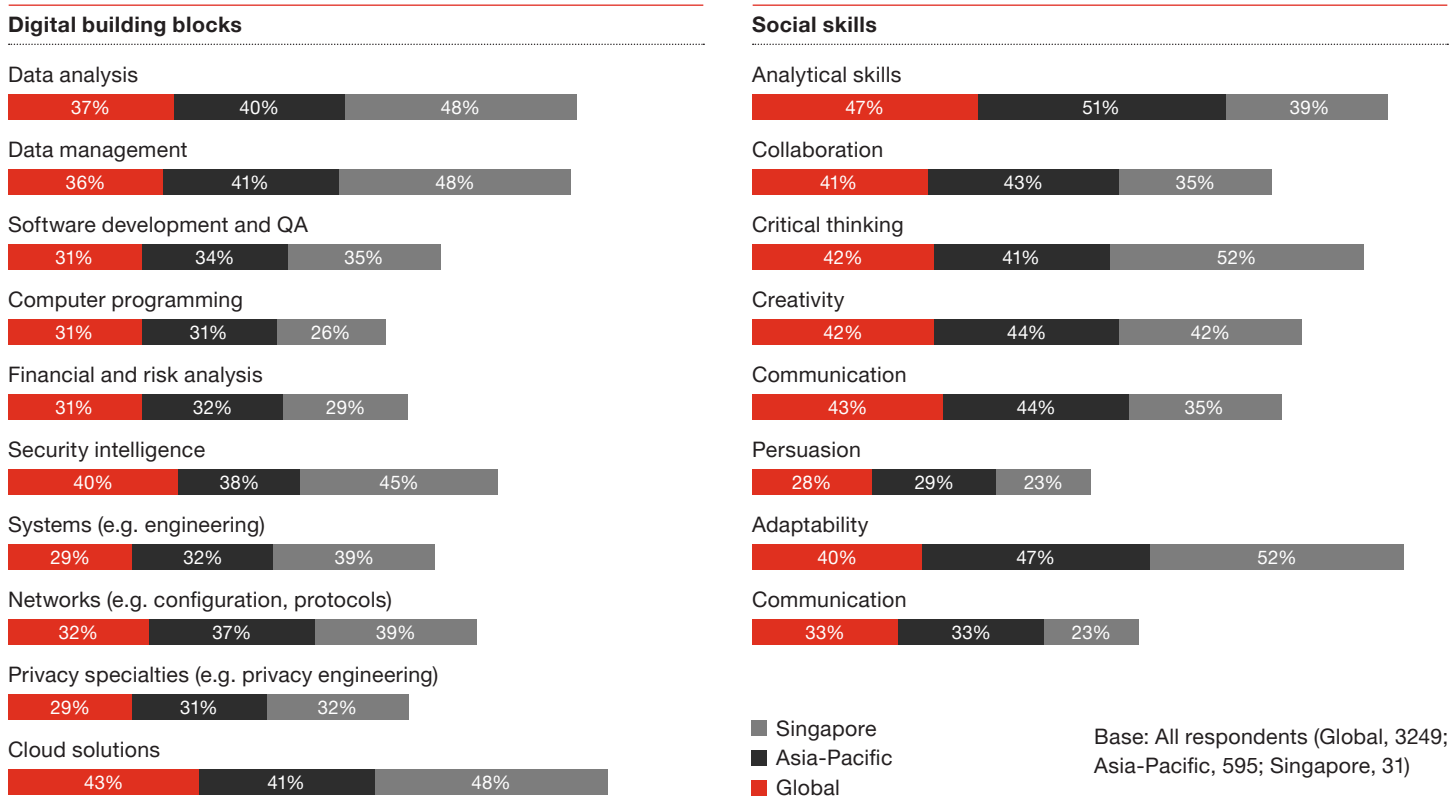


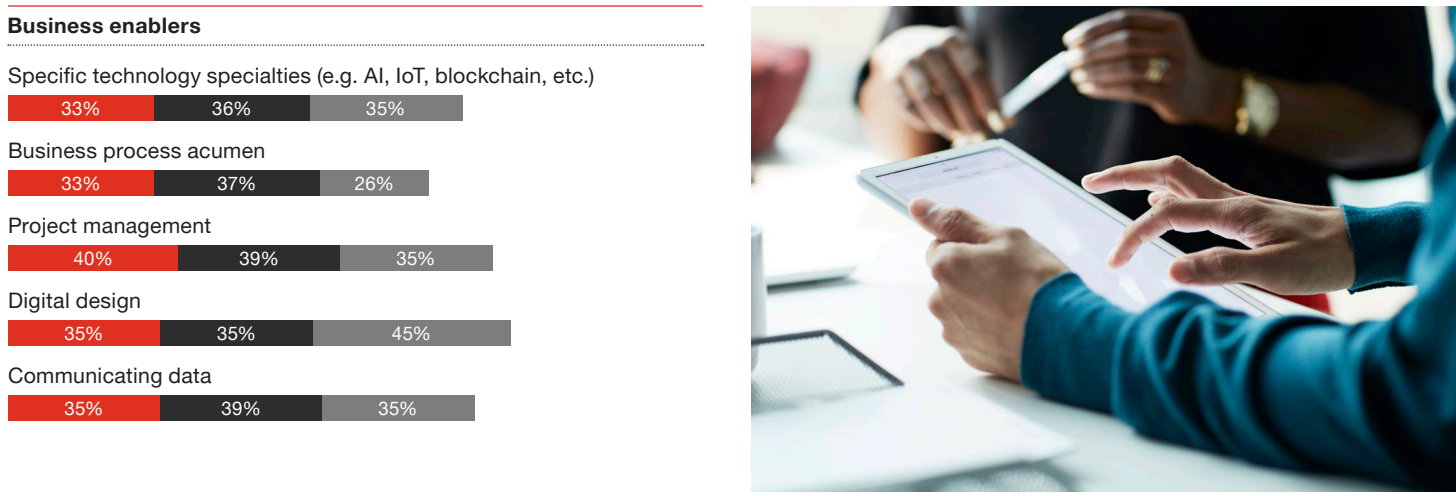
Exhibit 6

Along with technical skills, business and social skills are also the ask of the hour for new hires in the cybersecurity space

Q: Which of the following skills are you looking for in your new hires in the next 12 months?



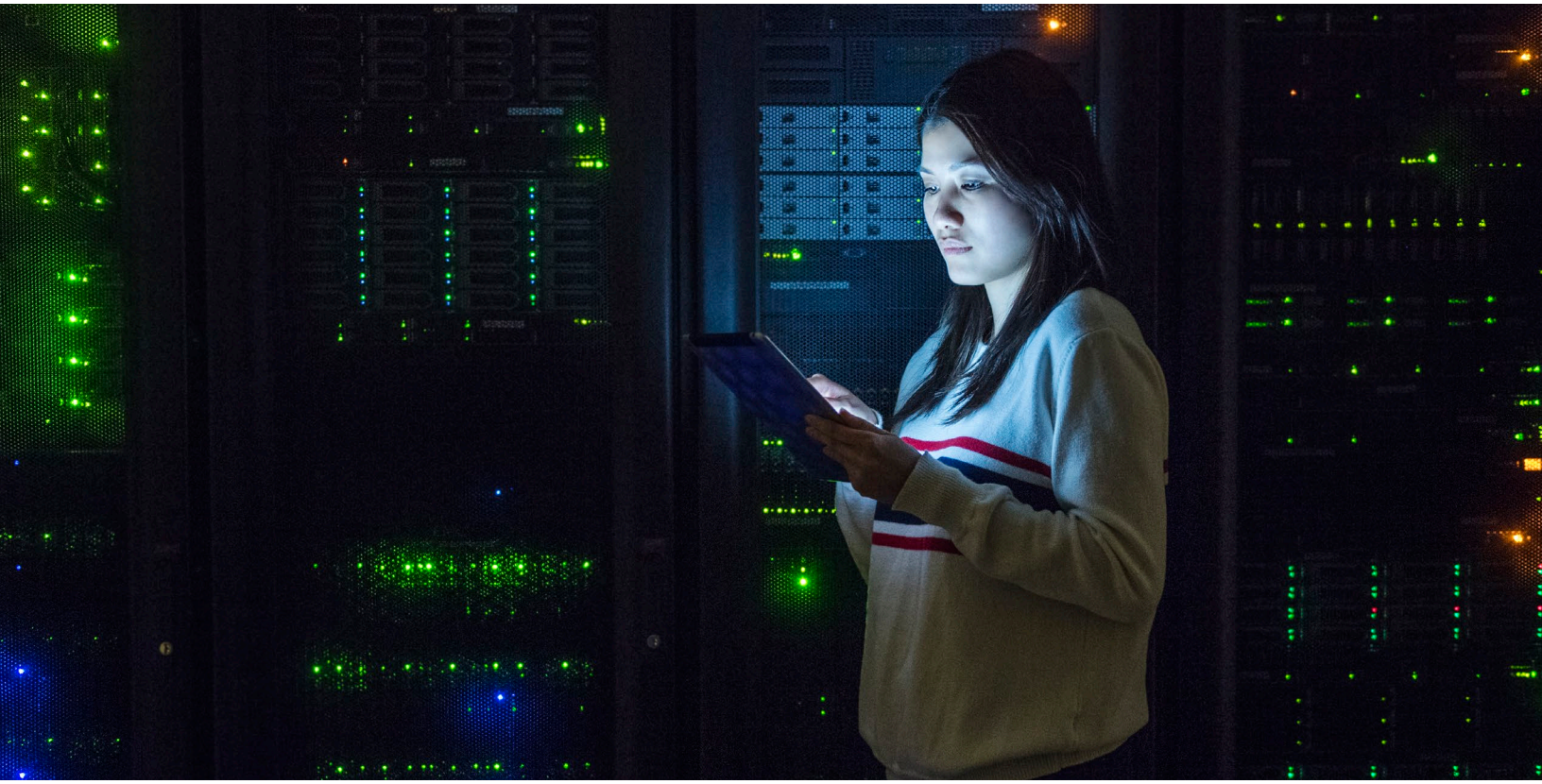
Base: All respondents (Global, 3249; Asia-Pacific, 595; Singapore, 31)



Key considerations for Singapore businesses

Shaping the future of cybersecurity — one that is in step with the business — means hiring the people who are ready to work collaboratively with others to tackle new, as-yet-undiscovered problems and analyse information.

- **Identify skill gaps:** Conduct an organisational risk assessment to identify and address talent and skill gaps.
- **Define responsibilities:** Commit to putting the right roles and talent in place, with clearly defined responsibilities, to comprehensively address cybersecurity, privacy and data ethics challenges.
- **Upskill workforce:** Upskill your existing people based on the evolving needs of the market - today's digital trust workforce are well-rounded, aware individuals who holistically bring together people skills, business strategy, technology acumen and an awareness of risk implications.

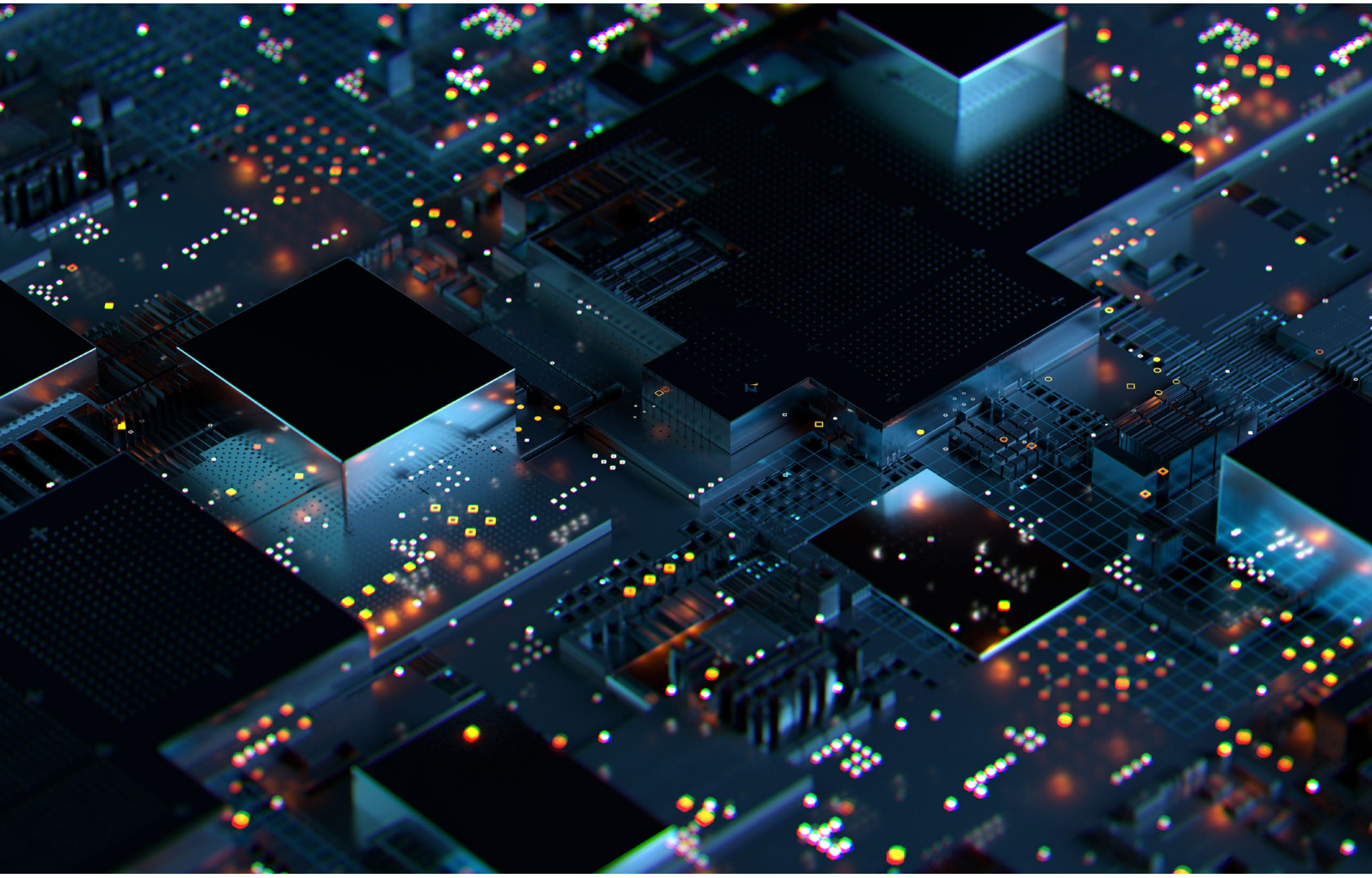


About the survey

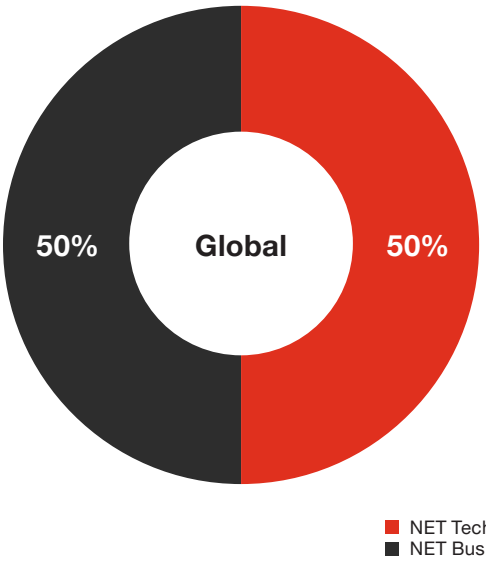
About the survey

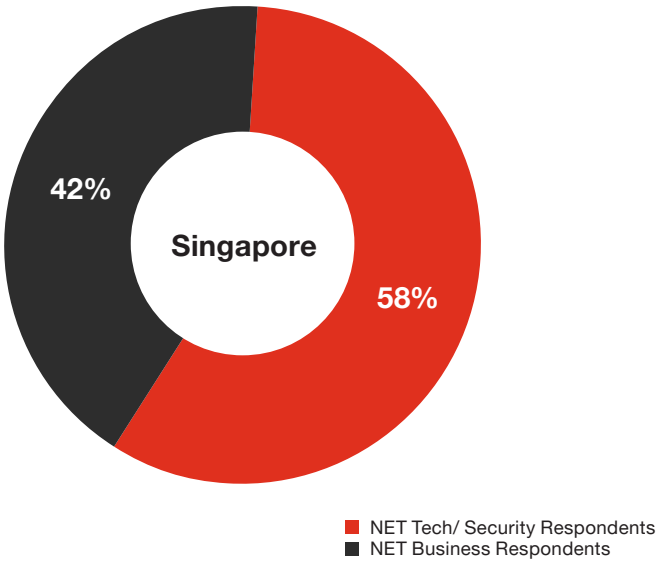
The 2021 Global Digital Trust Insights is a survey conducted in July and August 2020 of 3,249 global business, technology, and security executives (CEOs, corporate directors, CFOs, CISOs, CIOs, and C-Suite officers), 595 in Asia Pacific and 31 in Singapore.

The Global Digital Trust Insights Survey is formally known as Global State of Information Security Survey (GSISS). PwC Research, PwC's global Centre of Excellence for market research and insight, conducted this survey.



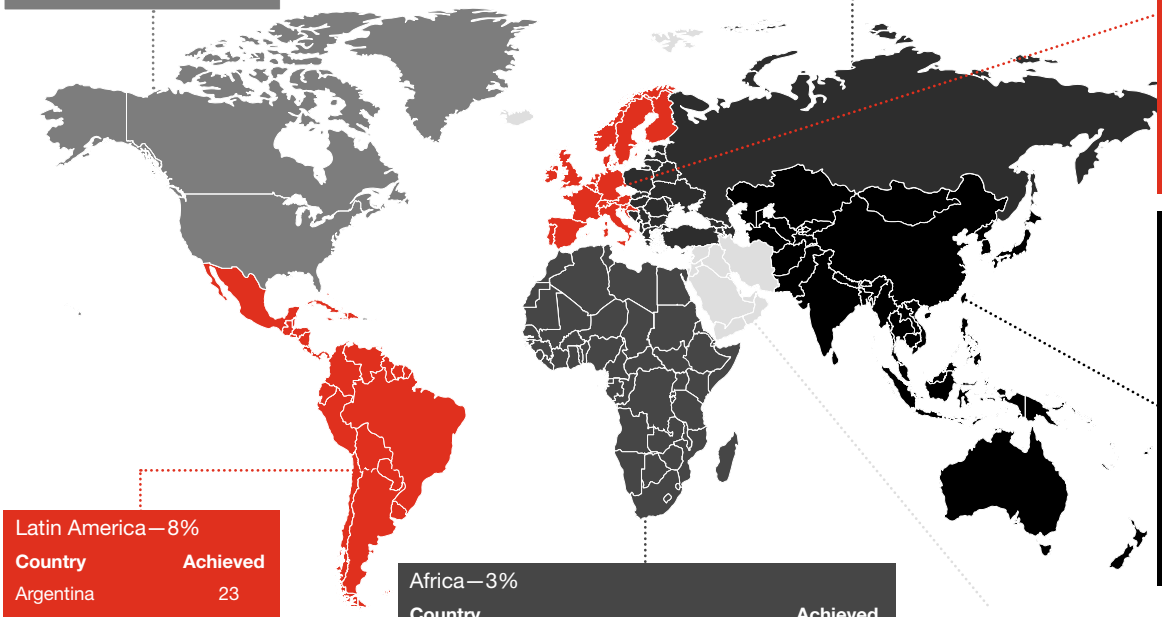
Job title





*Source: PwC, Global Digital Trust Insights Survey 2021, October 2020
Q: Choose the title that best describes your role. Base: All respondents (Global, 3249; Singapore, 31*)

Region



North America—29%

Country	Achieved
Canada	100
United States	843

Eastern Europe—4%

Country	Achieved
Romania	5
Russia	125
Ukraine	7

Western Europe—34%

Country	Achieved
France	188
Germany	263
Ireland	30
Italy	100
Netherlands	54
Spain	100
Sweden	40
Switzerland	56
United Kingdom	265

Asia Pacific—18%

Country	Achieved
Australia	100
China & Hong Kong	133
India	110
Indonesia	31
Japan	100
Korea	30
Malaysia	30
New Zealand	30
Singapore	31

Latin America—8%

Country	Achieved
Argentina	23
Brazil	109
Colombia	20
Mexico	120

Africa—3%

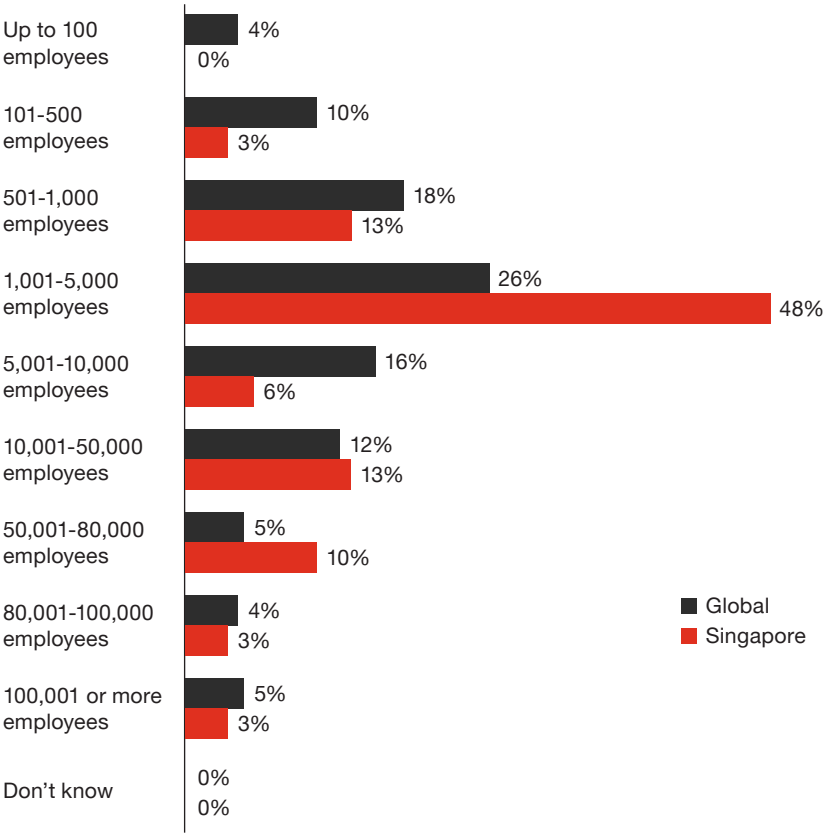
Country	Achieved
East Africa (Kenya, Uganda, Tanzania)	18
South Africa	51
Southern Africa (Botswana, Malawi, Namibia, Zimbabwe)	5
West Africa (Nigeria, Ghana)	31

Middle East—3%

Country	Achieved
Bahrain	10
Kuwait	10
Oman	10
Qatar	10
Saudi Arabia	30
UAE	31

Source: PwC, Global Digital Trust Insights Survey 2021, October 2020: base 3,249
Q: In which country do you primarily work?

Employee size and gender



NET: Less than 1,000

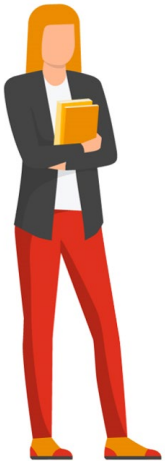
Global: 32%
Singapore: **16%**

NET: 1,000 - less than 50,000

Global: 54%
Singapore: **68%**

NET: 50,000 - less than 100,000

Global: 9%
Singapore: **13%**



Female

Global: 28%
Singapore: **19%**

Male

Global: 71%
Singapore: **81%**

Q5 How many employees does your organisation have globally? Base: All respondents (Global, 3249; Singapore, 31*)
Q6 What is your gender? Base: All respondents (Global, 3249; Singapore, 31*)

Reimagine digital for your cybersecurity function:

https://www.pwc.com/sg/en/services/reimagine-digital/cybersecurity

Contacts

Shong Ye Tan
Digital Trust Leader
PwC Singapore
+65 9820 3623
shong.ye.tan@pwc.com

Freddy Wee
Cybersecurity and Privacy Partner
PwC South East Asia Consulting
+65 8511 6817
freddy.wee@pwc.com