Michael Page

Part of the ABC's of Technology series

HUMANS OF CYBERSECURITY:

Innovations and Hiring Trends in APAC

Insights from cybersecurity experts across Asia Pacific

March 2021

THE GLOBAL PANDEMIC'S IMPACT

Cybercrime
up 600%
as a result of COVID-19[1]

19 million
ransomware and phishing attacks were identified in Asia from Feb to May 2020, with many being coronavirus-themed[2]

74%
of organisations see cybersecurity enhancement as a top priority[3]

69%
of organisations changed their cybersecurity response plan due to COVID-19[3]

MARKET SIZE

Asia Pacific's cybersecurity market was valued at **US$30.45 billion** in 2019.

It is expected to register a **CAGR of 18.3%** for the period of 2020-2025.[2]

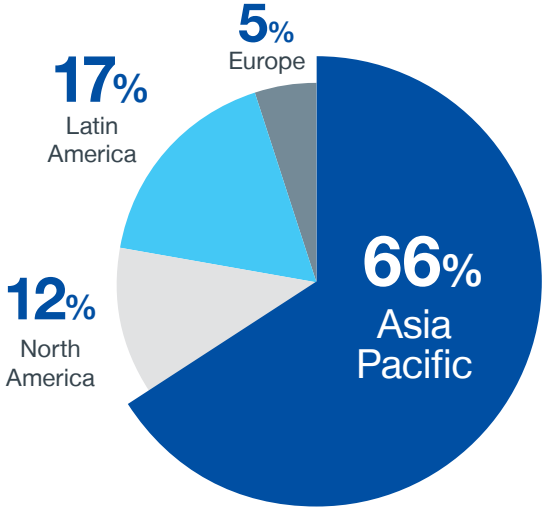
CAGR - Compound Annual Growth Rate

Sectors expected to be mostly impacted by cybersecurity breaches

- Financial Services & Banking
- E-commerce
- Healthcare & Life Science

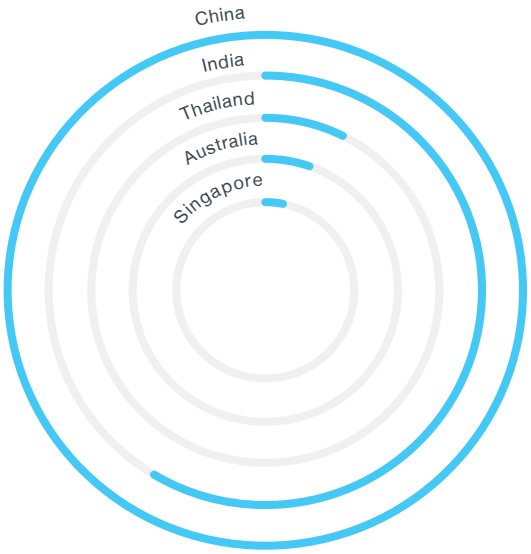
JOBS SNAPSHOT

3.1 million
unfilled cybersecurity jobs worldwide[4]



3-6 months
average time it takes to fill a cybersecurity position, according to ISACA[5]

CYBERSECURITY JOBS PREDICTION BY COUNTRY



New jobs by 2025[6]

China	2,686,020
India	1,508,536
Thailand	115,588
Australia	39,923
Singapore	8,769

TOP CYBERSECURITY RECRUITMENT CHALLENGES

43% Talent Shortage

25% Salary Budget

22% Underqualified Talent

IN-DEMAND SKILLS[7]

Access Management
Cloud Security
Compliance and Controls
Application Development Security
Data Privacy and Security Threat Intelligence
Security Strategy and Governance
Risk Management
Incident Response
Health Information Security

CYBERSECURITY TALENT WORLDWIDE

31% of new cybersecurity talent are consultants/contractors[4]

66% of cybersecurity professionals struggle to define their career paths[8]

60% of cybersecurity professionals aren't satisfied with their current job[8]

References

1 https://purplesec.us/resources/cyber-security-statistics/#:~:text=Cyber%20Security%20Risks,and%20health%20records%20left%20unprotected.
2 https://www.mordorintelligence.com/industry-reports/asia-pacific-cyber-security-market
3 https://www.crowdstrike.com.au/wp-content/uploads/2020/07/CrowdStrike-APJ-Survey-Summary.pdf
4 https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B
5 https://www.darkreading.com/cloud/it-takes-an-average-of-3-to-6-months-to-fill-a-cybersecurity-job/d/d-id/1334135
5 https://www.isaca.org/go/state-of-cybersecurity-2020
6 https://msit.powerbi.com/view?r=eyJrIjoiZWMyNjA0YzAtZGY4Zi00MTI1LTk4MjQtNWI1NTA5NDY1MzRjIiwidCI6IjcyZjk4OGJmLTg2ZjEtNDFhZi05MWFiLTJkN2NkMDExZGI0NyIsImMiOjV9
7 https://www.burning-glass.com/wp-content/uploads/2020/10/Fastest_Growing_Cybersecurity_Skills_Report.pdf
8 https://www.esg-global.com/hubfs/issa/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Nov-2017.pdf

On 15 July 2020, 45 high-profile Twitter users simultaneously posted a dubious tweet about a bitcoin scheme that was too good to be true. Users like Barack Obama, Bill Gates, Jeff Bezos, Elon Musk and Warren Buffett claimed that, for 30 minutes only, all bitcoin sent to a specific cryptocurrency wallet would be doubled as part of an elaborate charity drive. Within minutes, 320 bitcoin transactions were made, totalling up to more than US$110,000 in value.

The tweet turned out to be part of a bitcoin scam later described as "the worst hack of a social media platform yet". Three perpetrators were arrested soon after, with the mastermind being a 17-year-old teenager from Florida.

This was not the only major data breach in 2020. Marriott International lost the personal data of more than 5.2 million hotel guests in March; more than 500,000 Zoom passwords were put on sale for less than one US cent each in April; in January 2019, Singapore's Ministry of Health lost confidential information belonging to 14,200 people diagnosed with HIV — the second major health data breach in six months. While it is evident that cybersecurity is a growing challenge for businesses around the world, of greater concern is the fact that most businesses — about 95% — do not have adequate cybersecurity practices in place, making them especially vulnerable to attacks.

Investing in the right tools is definitely a start, but one of the best ways to plug these security gaps is to hire the right cybersecurity talent. But what are the most relevant skill sets out there? With cybersecurity trends and threats evolving constantly, what kind of talent should businesses hire?

To answer these pressing questions, Michael Page reached out to business leaders, academics and Page consultants from across the Asia-Pacific region — here are the insights.

Top cybersecurity innovations and trends

1 A MORE SOPHISTICATED CLASS OF THREATS

Cybersecurity threats have evolved drastically in the last 20 years. "Around the year 2000, the concern at that time was about viruses. It was about applications that would attack other computers," recalls Faisal Yahya, Country Manager at PT Vantage Point Security Indonesia. However, with the rise of malware, ransomware, phishing and SQL injections to name a few, cybersecurity attacks are becoming more sophisticated by the day.

"Businesses can try to defend every asset and spend a lot of money on cybersecurity, but it only takes one attack to compromise your cybersecurity management," says Surya Nepal, Principal Research Scientist at CSIRO's Data61 and Group Leader of D61 Distributed Systems Security Department. "[It] requires a multidisciplinary approach through computer science and behavioural changes." With that said, Nepal admits that there are no perfect solutions, and that cybersecurity threats will never go away, "unless we stop connecting to the internet."

2 THE DECENTRALISATION OF CYBERSECURITY

Cybersecurity used to be much simpler. You kept the things you wanted to protect on a computer or server; then you build a virtual wall — or a firewall — around it. As Yahya puts the idea, it was akin to a medieval castle with a rampart that protects the most important assets.

In the past decade, however, advancements in technologies, such as 5G, the Internet of Things and cloud computing, have rendered such concepts obsolete. That's because more devices connected to the same network meant more potential points of attack for attackers. The COVID-19 pandemic, which forced employees to bring their work devices home en masse, only served to hasten that decentralisation of cybersecurity. "Your home internet connection is now part of your corporate network," says Dhillon Andrew Kannabhiran, Founder and Chief Executive Officer of Hack In The Box (HITB), the organiser behind the annual HITB Security Conference. "You're now exposing your corporate network to a far wider [array of] devices, because my home network has a smart television and a smart fridge. Companies aren't thinking about these things properly. Nobody is, really."

Decentralisation goes beyond the pandemic, too. Digital transformation, without the right controls in place, exposes the company to attacks as well. "Companies have embraced the digital way of functioning, [but] the amount of risks and exposures increase also," says Viren Parekh, Associate Director at Cipla, who leads the enterprise risk management team at this India-based pharmaceutical company. "If you're not nimble enough, if you go around scaling up digitally without the right controls, you will have more cyber-related risks."

"When we talk about the landscape of security, it is no longer being understood as a perimeter. Now we're talking about it as a mesh, like a spider's web," Yahya adds. This presents a major challenge for cybersecurity professionals because cybersecurity cannot just exist in one secure location — it now has to exist everywhere.

Ruan Youming, Chief Security Architect at Sangfor Technologies Inc, sees the same trends in Mainland China as well. "Boundary security has no advantage in the face of new security issues. Network boundaries are disappearing, and it is no longer useful to establish firewalls," he says. "Instead, the long-term defence system is the new trend, which emphasises defence linkage between multiple devices, which then reinforces the system as a whole."

> "Cybersecurity should be a gradual investment rather than a one-time hit. Start with: 'What assets are you protecting?' and 'What is important to you?' in order to develop a strategy around that.

Surya Nepal

Principal Research Scientist at CSIRO's Data61 and Group Leader of D61 Distributed Systems Security Department

3 SECURITY MIGRATES INTO THE CLOUD

Whereas cybersecurity analysis and detection used to be a manpower-intensive job, Ruan sees cybersecurity migrating increasingly into the cloud and becoming more automated.

In terms of automation, artificial intelligence is now able to detect abnormal traffic, terminal behaviours, as well as perform correlation analysis within specific systems. This also means that fewer people are required to protect and secure a larger network infrastructure, and the response to cyber attacks, too, can be performed faster and with higher accuracy.

Furthermore, security tools and services are moving into the cloud, which means that trust between enterprises and service providers will gain greater importance in the years ahead.

4 PROACTIVE VERSUS REACTIVE PROTECTION

As the cost and volume of cybersecurity attacks increase, enterprises can no longer take a reactive approach to cybersecurity. Instead, Yahya believes that the trend is moving towards a more predictive approach. “Companies can perform analyses of the current traffic data, and a cybersecurity professional can create a model [that] advises the company of future potential attacks and how to mitigate them,” Yahya elaborates.

Nepal, too, shares that sentiment. “A digital twin, or a virtual replica of a physical object or system, of a network or piece of infrastructure, enables the simulation of real-life operations and occurrences. This is a valuable tool in a cybersecurity team’s kit, as it allows them to see and think from the attacker’s point of view, and experiment with different attacks and approaches without compromising the

> The threat landscape is very adaptive and dynamic. Businesses need to reassess their plans all the time — and that requires leadership skills. That’s why governance, risk and compliance must be part of the daily tasks for every cybersecurity professional.

Faisal Yahya

Country Manager, PT Vantage Point Security Indonesia

DECODING COMMON CYBERSECURITY THREATS

MALWARE

A ‘malware’, or ‘malicious software’, breaches a network via a vulnerability, typically when a user clicks on a dubious link or email attachment. Once inside the system, the malware can block access to critical components of the network, install harmful software or obtain sensitive information.

PHISHING

When a fraudulent communication disguises itself as a reputable source to steal sensitive data, such as login information and credit card details.

DENIAL-OF-SERVICE ATTACK

This form of attack floods entire systems, services or networks with fake requests, which then prevents legitimate requests from going through. This eventually crashes an entire service and renders it unusable.

SQL INJECTION

A Structured Query Language (SQL) injection is when the attacker inserts a malicious code into the server, thus forcing it to reveal sensitive information.

MAN-IN-THE-MIDDLE ATTACK

This typically occurs on unsecured public WiFi, where attackers can insert themselves between your device and the network, then steal all your personal data in short order.

5 A PEOPLE-CENTRIC APPROACH TO SECURITY

original system."
"There are no 100% secure solutions. What we do every day can only take us to, at most, 99%," Yahya admits. That final 1% — the weakest link — is, unfortunately, us, the humans. "The vast majority of cybersecurity compromises arise from human behaviour, a domain in which technical solutions have limited efficacy," Nepal agrees. As such, a trend among cybersecurity practitioners is to focus more on humans within the cybersecurity ecosystem.

For example, Yahya explains that humans are still the first line of defence against such attacks as fallible as we are. "Educating them not only improves the security but at the same time it minimises the investment required for cybersecurity," he says. "We cannot focus only on the technical side only, but we need to have a holistic approach. It's a combination of the infrastructure and the employees."

Parekh sees user awareness as key to cybersecurity. "Hackers now try to mimic the IDs of people they know you're interacting with to get a better click rate out of you. So we train our employees to recognise these trends and identify whether something is out of the ordinary," he explains. "I am happiest when I get an email from our colleagues, asking 'Can you check out this email for me?' It means that people are paranoid, which is a good thing sometimes."

Nepal agrees. "Implementing a cyber hygiene programme from a human-centric point of view is central. When new staff join a business, they go through an induction programme. What's missing is cybersecurity. Staff need to be much more cyber aware and understand how to practise good cyber hygiene within the organisation so that all their people are educated. The solutions have to be invisible and non-intrusive."

ADVICE
FOR TRENDS IN CYBERSECURITY

CELEST WEN

Manager,
Technology
Michael Page Shenzhen

"The trend now is that many senior researchers are moving to the business world and building their cybersecurity teams. Overseas talent with relevant cybersecurity skill sets are also returning home to work."

HOUDA EL FATNI

Managing Consultant,
Technology (Commerce)
Michael Page Japan

"Cybersecurity candidates are in high demand, which is why clients must emphasise their employee value proposition. Explain your benefits and career progression opportunities to attract and retain the best high potential candidates out there."

"Cybersecurity is insurance. Why do you buy insurance? Because, in case something happens to you, you want to have that safety blanket — it's the same thing. You implement security not because you want a security incident, but when it does happen, you want these processes in place. It's not after the fact. You cannot afford it.

Dhillon Andrew Kannabhiran

Founder and Chief Executive Officer of Hack In The Box

6 SECURITY CHALLENGES ABOUND — BUT SUPPORT IS ON THE WAY

According to studies, cybersecurity breaches have increased by 67% since 2014, and each violation carries an average cost of US$3.92 million — a worrying trend. With that said, cybersecurity-related opportunities are on the rise as well. In Australia, where Nepal is based, the cybersecurity landscape has significantly improved in the last five years alone.

For example, governments are dedicating more resources to reinforce the cybersecurity ecosystem, which comprises research, innovation, defences and academia. The Australian government, for one, launched its Cyber Security Strategy 2020 last August, which will invest AU$1.67 billion to build new security and law enforcement capabilities, assist industries to protect businesses and raise the community's understanding of how to be secure online.

Other Asia-Pacific nations are ramping up their efforts as well. According to the Deloitte Cyber Smart Index 2020, Singapore, South Korea, Australia and New Zealand all rank highly in cyber preparedness, featuring 'strong digital legislation and high rates of research and development that signals a matured grasp of cybersecurity affairs. Singapore, which ranks at the top, even announced in 2018 a US$30 million grant to incentivise local enterprises to prioritise security countermeasures upgrades. In terms of spending on cybersecurity, however, the Chinese government outstrips other countries in the Asia Pacific, with US$7.9 billion spent on cybersecurity in 2019 — the second highest in the world after the US. Globally, the International Data Corporation estimates that worldwide cybersecurity spending will top US$174.7 billion by 2024.

ADVICE

FOR TRENDS IN CYBERSECURITY

KYLE BURNETT

Manager, Technology
Michael Page Australia

"Cybersecurity has consistently been a top five growth job in Australia according to both SEEK and LinkedIn data. As an emerging field, talent demand is high. However, we are now starting to see a significant graduate pool, as well as people looking to transition who have built a career in another field. Businesses that we work with for hiring cybersecurity talent are looking for points of difference on CVs. Certifications from the likes of ISACA or completing an internship with companies such as Cyber CX are strong examples, as well as those who have designed their own security project at home."

RYAN FAULDS

Senior Consultant,
Cyber and
Information Security
Michael Page Australia

"The increased demand for cybersecurity specialists goes hand-in-hand with the increase in malicious activity across the Australian economy. According to our meetings with tech leaders, there is a shortage of cybersecurity talent across all areas. For companies in need of cybersecurity skills, consider what's driving candidates in the market. We've seen a trend in the best talent joining organisations that are aligned closely to ongoing learning and development opportunities, as well as a positive and flexible team cultures. Keep in mind the emerging nature of the cybersecurity market, as well as the importance of transferable skills when recruiting."

Top hiring trends in cybersecurity

1 HIGHER-END SKILLS ARE IN DEMAND

"There are skill gaps across all cybersecurity industries [and] at every level. On the research side, the market is struggling to fill positions, as there are still not enough cybersecurity researchers in Australia," Nepal says. "There are more gaps in the public sector side, and government agencies are trying to hire at the top end of the market."

The situation is similar in Mainland China as well. Ruan shares that cybersecurity is in a relatively nascent stage at the moment and, up until a few years ago, was not even a course in most Chinese universities. This has resulted in a huge demand for high potential cybersecurity talent, especially those who can build a cybersecurity infrastructure from the ground up. "As demonstrated in several leading market reports, the lack of talent is one of the dominant factors that hinders the development at home and abroad," explains Celest Wen, a manager of the technology sector at Michael Page Shenzhen.

The talent issue is not limited to Australia and Mainland China, either. Kannabhiran, whose company works with governments from all over the world, believes that the issue of talent crunch is universal. "The education systems are broken. Around the world, [companies want] to find the elites in cybersecurity, but they can't because universities are churning out less-than-qualified candidates," he explains. "Companies have to retrain them, send them for skill redevelopment, spend extra money and even develop their own internal testing and methodology."

The solution? Ruan's answer, at least in the short term, is to look abroad. "My suggestion is to bring in senior, high-end talent from overseas," he says. "Develop mid-level talent from within the company." Nepal also predicts that the demand for talent with higher-end skills is only going to grow stronger. That's because lower-end skill sets, given enough time, will eventually be replaced by artificial intelligence, which means that whatever you learn in a short course will not be sustainable in the long run.

2 SOFT SKILLS ARE IN HOT DEMAND

Cybersecurity is a highly collaborative role, so Yahya sees communication and writing capabilities as top soft skills among eligible candidates. Not only do cybersecurity professionals need to learn from each other, but they also have to 'sell' the importance of cybersecurity to various stakeholders. These are highly important soft skills that, to Yahya, are lacking at the moment.

Another emerging soft skill that is in demand is a growth mindset. The skills required of cybersecurity professionals change based on the most prevalent cybersecurity threats. In fact, according to Yahya, it often requires three to five years just for a cybersecurity professional to become proficient in one area of expertise, which is more than enough time for the threat landscape to evolve once again. As such, embracing change and having an adaptive mindset is key. "It's not about personal growth, but how you open yourself up to feedback, how you accept the feedback and create the right architecture for the company," he underscores.

3 CYBERSECURITY LEADERS AS STRATEGIC PARTNERS

"As a cybersecurity leader, you need to understand that security and business must complement each other and drive each other. You must not stand on the opposite side of the business, but think about everything from a business perspective," Ruan says. "That way, you will know when the best time is to lay out cybersecurity [plans and strategies], and what kind of security is needed."

Yahya takes it a step further. "In Indonesia, it is not about the numbers for cybersecurity professionals when it comes to a job. It is about how well the organisation as a whole can accept, say, a CISO role. In fact, the salary is the least important thing. They want to know if the business can cooperate

> Cybersecurity is different from AI or blockchain. It is not about empowering the business. It is about protecting the integrity of the business and solving internal security issues.
>
> **Ruan Youming**
>
> *Chief Security Architect at Sangfor Technologies Inc*

with him or her. One way to attract and retain top cybersecurity talent is to position them as strategic partners. They need to be part of the decision-making process. If they do not have cooperation from other functional departments, the turnover will be massively high."

Kedar Upadhye, Global Chief Finance Officer at Cipla, believes that autonomy is key to retention. "It's about the freedom to think and operate. We should give [qualified cybersecurity leaders] the autonomy to set the agenda, to shape the roadmap and appropriate budgets. We need to respect the individual's profession and expertise."

4 INCREASED FOCUS ON EMPLOYER BRANDING

Qualified cybersecurity professionals are hard enough to source as it is. When it comes to attracting — and retaining — the best of the best, Ruan has a few ideas. "You start by building a strong employer branding and a positive team culture," he shares. And by 'positive team culture', he means that employers must provide a strong platform for talent to try different verticals within cybersecurity. "As a leader, give talent development space and help them realise their value," he explains. "Short-term attraction of talent may depend on money, but in the long run, it still depends on the style of leadership."

Our deepest thanks to the insights from Surya Nepal, Principal Research Scientist at Commonwealth Scientific and Industrial Research Organisation (CSIRO) Data61 and Group Leader of D61 Distributed Systems Security Department; Faisal Yahya, Country Manager at PT Vantage Point Security Indonesia; Ruan Youming, Chief Security Architect at Sangfor Technologies Inc, and Dhillon Andrew Kannabhiran, Founder and Chief Executive Officer of Hack In The Box; Viren Parekh, Associate Director at Cipla; Kedar Upadhye, Global Chief Finance Officer at Cipla.

PAGE'S ADVICE

FOR HIRING IN CYBERSECURITY

MIKE SIERRA

Senior Consultant, Technology
Michael Page Philippines

"Companies need to think outside of the box when hiring security talent. Excellent candidate experience plays a vital role. Telling the story and the purpose of your company at the outset sets you apart from other companies that are in pursuit of the same talent."

DANNY GOH

Manager, Technology
Michael Page Malaysia

"Hiring managers need to understand the cybersecurity gaps within the company to know what talent to hire for. In fact, they must prepare to step in to provide relevant training. Most importantly, find someone willing to grow within the cybersecurity space."

SHINJIKA SHUKLA

Associate Director, Technology
Michael Page Singapore

"Talent shortage is a well-known fact for digital transformation-led jobs. Hence, it is important for employers to switch their mindset from hiring 'plug-and-play' profiles to profiles with the right aptitude, attitude and technology foundation."

About Michael Page Technology APAC

Michael Page understands the complexity and sophistication of hiring technology professionals. Our service combines the expertise of a specialist technology recruitment firm with the resources, reliability and professionalism of a global recruitment firm.

12
markets

46%
of roles placed are contract/temporary roles

172
consultants specialising in Technology-related roles

1,700+
Technology roles placed in 2020

318,000
Applications received from Technology professionals

More than
370,000
qualified Technology professionals in our APAC database

We recruit for all areas of Technology

- Leadership
- Data, Analytics, BI
- Emerging Technologies
- Software Development
- Delivery & Transformation
- Sales
- Product Development
- Infrastructure & Operations

About PageGroup

PageGroup is a leading international specialist recruitment group with a market capitalisation in excess of GBP 1 billion. We are listed on the London Stock Exchange as a FTSE 250 company and currently employ over 6,500 staff with 140 office locations in 37 countries. We are organically grown, and each PageGroup office has been established by our employees and conforms to the best practices and values common to our existing business.

We have the most extensive and accurate candidate database in Asia Pacific and an unparalleled global search capability. Our consultants are discipline specialists who possess true subject matter expertise. We promote a team-based environment and encourage consultants to focus on long term business relationships rather than one-off commissions.

Australia
Sydney, Chatswood, Parramatta, Canberra, Melbourne, Glen Waverley, Brisbane and Perth

enquiries@michaelpage.com.au
www.michaelpage.com.au

Hong Kong
Hong Kong

enquiries@michaelpage.com.hk
www.michaelpage.com.hk

Indonesia
Jakarta

enquiries@michaelpage.co.id
www.michaelpage.co.id

India
Mumbai, Delhi and Bengaluru

enquiries@michaelpage.co.in
www.michaelpage.co.in

Japan
Tokyo

enquiries@michaelpage.co.jp
www.michaelpage.co.jp

Mainland China
Beijing, Shanghai, Guangzhou, Shenzhen, Suzhou and Chengdu

enquiries@michaelpage.com.cn
www.michaelpage.com.cn

Malaysia
Kuala Lumpur

enquiries@michaelpage.com.my
www.michaelpage.com.my

Philippines
Manila

phenquiries@michaelpage.com.ph
www.michaelpage.com.ph

Singapore
enquiries@michaelpage.com.sg
www.michaelpage.com.sg

Taiwan
Taipei

enquiries@michaelpage.com.tw
www.michaelpage.com.tw

Thailand
Bangkok

enquiries@michaelpage.co.th
www.michaelpage.co.th

Vietnam
Ho Chi Minh City

vnenquiries@michaelpage.com.vn
www.michaelpage.com.vn

Rest of Asia
Serving the ASEAN region including Myanmar

enquiries@michaelpage.com.my
www.michaelpage.com.my

Get Connected. Stay Ahead.

PageExecutive

MichaelPage

PagePersonnel

PageOutsourcing

Part of
PageGroup

The **ABC's of Technology** is an exclusive technology-centric content series that explores the latest innovations and hiring trends in four high-growth areas: artificial intelligence, blockchain, cybersecurity and big data. Each report comes with insights and recommendations from technology experts, business leaders and Page's very-own consultants across the Asia Pacific. For more on where the technology sector is headed and the key skills you should hire for, begin your journey right here or check out our respective country website(s).