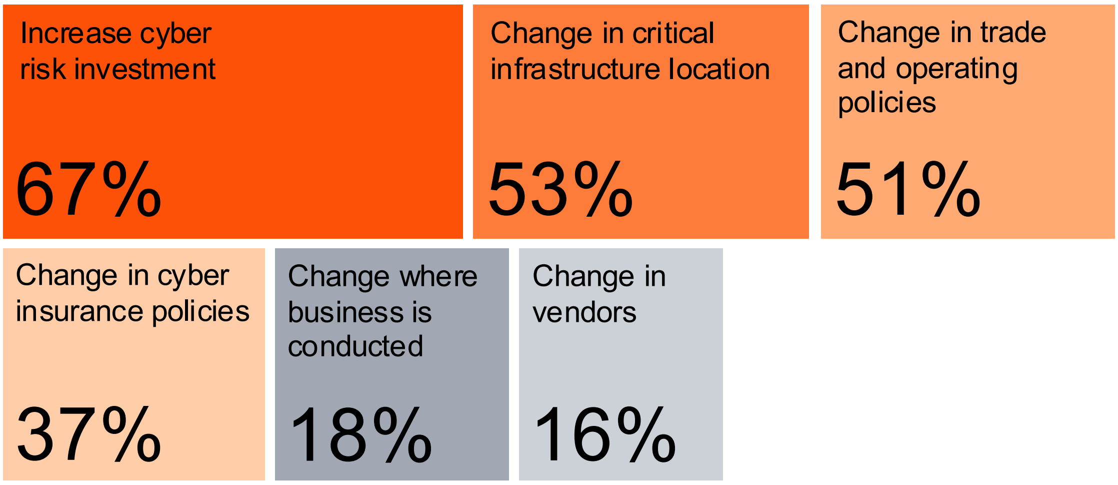
2026 Global Digital Trust Insights Survey

Malaysia highlights

Table of contents

01 Geopolitics are reshaping cyber vulnerabilities

Cyber strategy changes in response to current geopolitical landscape (% that ranked in their top 3 areas)



Q2: Over the next 12 months, which of the following areas of your organisation's cyber strategy is changing in response to the current geopolitical landscape? Base: All respondents in Malaysia=51

Today's cyber risks are shaped as much by geopolitics as by disruptive technologies. Upended alliances, trade disputes, weakened international institutions, and other destabilising trends are reshaping the threat environment, as well as traditional methods of doing business.

Responding to this geopolitical climate, 67% of business and tech leaders surveyed in Malaysia are making cyber risk investment their top three strategic priorities for the year ahead. They are also prioritising changes in critical infrastructure location (53%), trade and operating policies (51%), and to a slightly lesser degree, cyber insurance policies (37%).

These priorities broadly mirrors global findings, attesting to the borderless nature of cyber attacks.

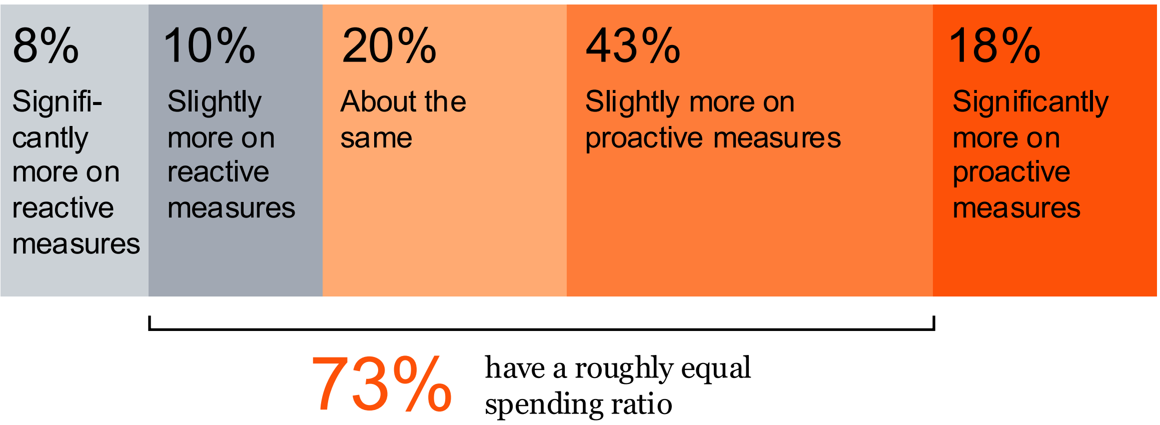
With disruption now the norm, cyber is a critical lever for resilience.

02 Where investment meets impact

Spending on reactive vs proactive measures

Reactive:
Response, customer care, remediation, recovery, litigation, fines, etc.

Proactive:
Monitoring, assessments, testing, controls, training, governance, etc.



Q13: Is your organisation spending more resources on reactive or proactive cybersecurity measures? Base: All respondents in Malaysia=51

*Unsure (2%)

**Sums may not total 100 due to rounding.

In cybersecurity, relying primarily on reactive measures is more costly, risky, and unsustainable.

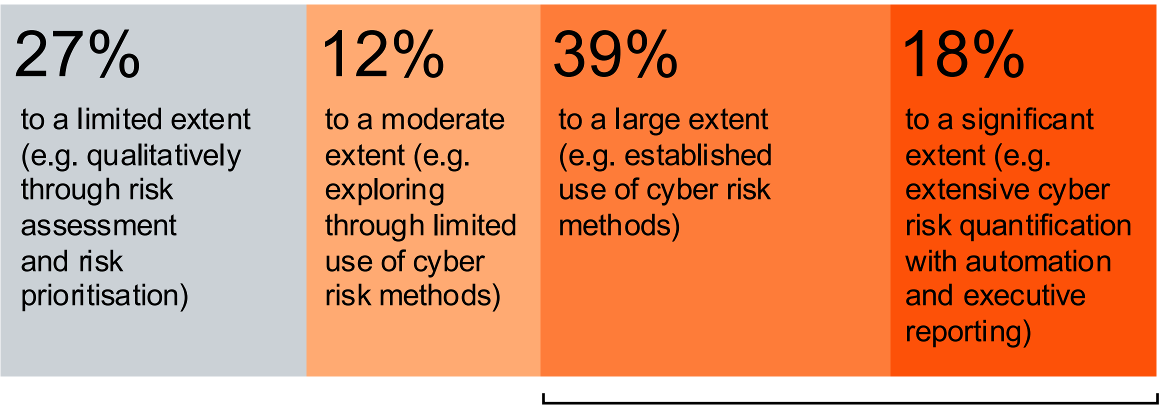
However, there is still a sizeable group still splitting attention, where 73% spend about the same on reactive and proactive measures or slightly more on either. Few (18%) are in the sweet spot of investing significantly more on proactive steps.

While proactive spending sits in the security leader's budget and is easy to track, reactive costs are dispersed across the business—legal, communications, operations, IT, product, marketing, government relations—and include harder-to-quantify costs such as lost opportunities and reputational damage. The true cost of reacting can easily be underestimated.

And cyber threats are not slowing down. The National Cyber Security Agency (NACSA) recorded 4,625 cybersecurity incidents in 2024—a 43% increase from the previous year. The stakes are too high to rely on reactive defences alone.

03 Putting a price on cyber risk

Measurement of financial impact of cyber risks



27% to a limited extent (e.g. qualitatively through risk assessment and risk prioritisation)

12% to a moderate extent (e.g. exploring through limited use of cyber risk methods)

39% to a large extent (e.g. established use of cyber risk methods)

18% to a significant extent (e.g. extensive cyber risk quantification with automation and executive reporting)

57% use cyber risk quantification to measure financial impact to a significant or large extent

Q12: To what extent is your organisation currently measuring the potential financial impact of cyber risks (i.e. risk quantification)? Base: Security leaders, CFOs, CEOs, CROs and the Board in Malaysia=33

*Unsure (3%)

**Sums may not total 100 due to rounding.

Encouragingly, most, if not all, leaders surveyed are already viewing cyber through a financial lens.

Malaysia is well ahead of the Asia Pacific average on cyber risk quantification. While only 49% of Asia Pacific organisations report using quantification to a significant or large extent, organisations in Malaysia are notably out in front (57%).

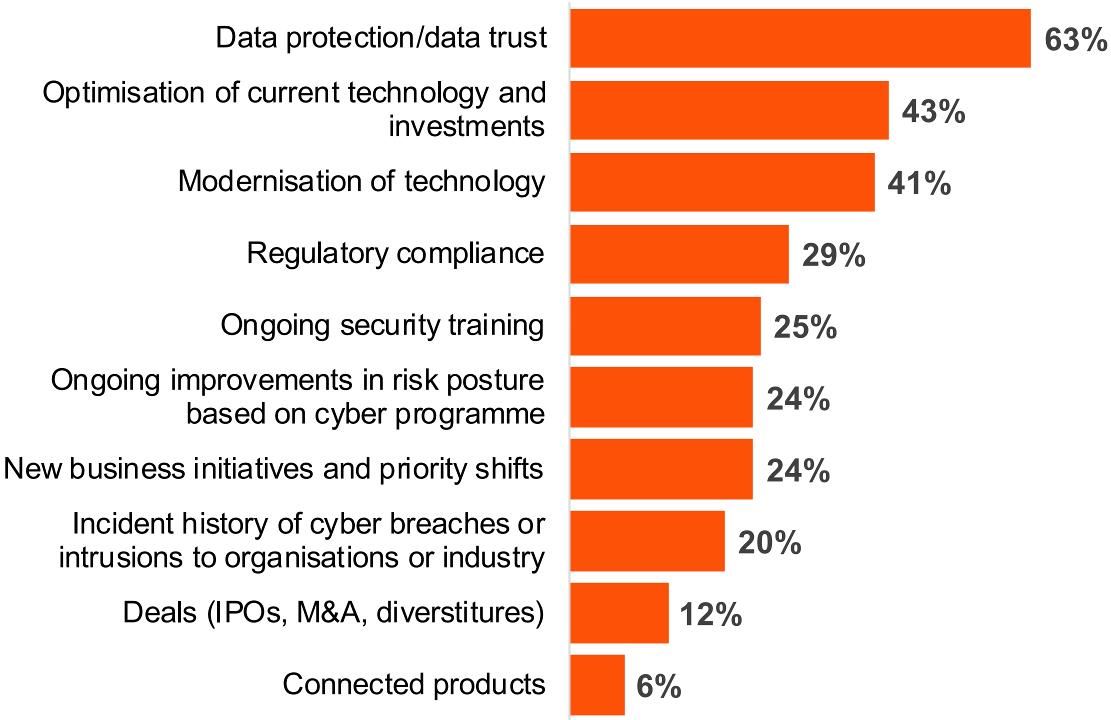
But dig deeper and only 18% are doing this to a significant extent, employing automation to quantify risks.

Business leaders need credible, actionable cyber risk reporting insights to assess the threats the organisation faces and judge how best to respond.

Bridging that gap starts with threat-led scenarios and disciplined control evaluation. Then, it should evolve into an AI- and intelligence-led predictive risk capability that continuously models emerging and third-party threats and reports probable business impact.

04 Data protection/data trust: A top priority for business and tech leaders

Factors influencing organisation's cyber spend priorities in Malaysia (% that ranked in their top 3 areas)



Q10: Which of the following factors are influencing your cyber spend priorities over the next 12 months? Base: All respondents in Malaysia=51

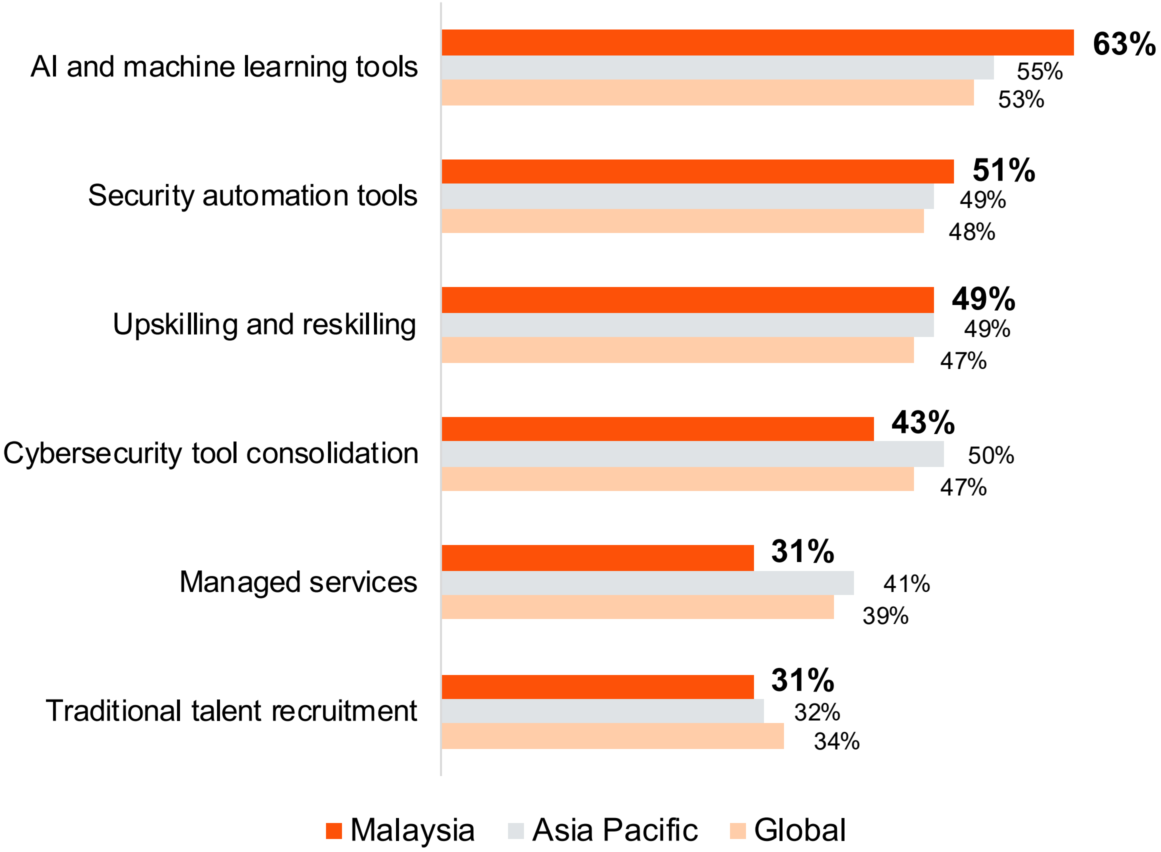
Top budget drivers vary across regions, but the common thread is clear: data protection and data trust ranks highest—at 63% in Malaysia versus 46% in Asia Pacific and 44% globally.

Strengthened privacy requirements are translating directly into investment. The recent gazetting of the Personal Data Protection (Amendments) Bill 2024 raises expectations on how personal data should be handled.

But it's more than just a matter of ticking the box. With 29% selected regulatory compliance as a top driver, organisations in Malaysia seem to be proactively investing to earn and keep customer trust, not only to meet the letter of the new law.

05 Automation and upskilling as twin engines of growth

Areas organisations are prioritising to address cyber talent gaps (% that ranked in their top 3 areas)



Q14. Which of the following is your organisation prioritising to address cyber talent gaps over the next 12 months? Base: All respondents in Malaysia=51

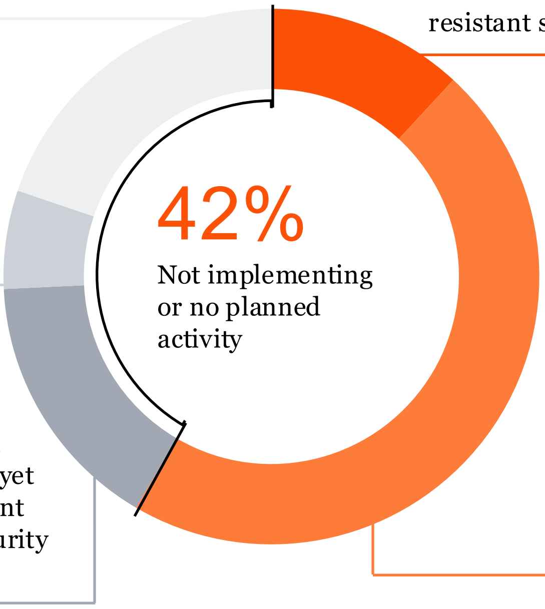
Cybersecurity workforce shortages continue to impede progress, especially as organisations push to operationalise AI, secure complex environments, and prepare for next-generation threats—prompting organisations to rethink how they scale capabilities.

Mirroring global trends, the focus of talent strategy in Malaysia is shifting away from traditional recruitment. Instead, Malaysian business and tech leaders are heavily investing in AI, automation tools, and continuous skill development.

While reliance on managed services is lower in Malaysia than Asia Pacific (41%) and global (39%), they are strategic accelerators—stepping in to compensate for lack of skills as well as deliver speed, scale, and specialised knowledge.

In a threat environment that's growing more complex by the day, managed services offer a way to modernise defences without diverting focus from innovation and growth.

06 Quantum concerns grow, but readiness lags



20%
Unable to confirm at this time.

6%
Not started to consider and no plans to do so: Our organisation has not started to consider quantum-resistant security measures and has no plans to do so.

16%
Exploring: Our organisation has begun exploring but have not yet taken steps to implement quantum-resistant security measures.

42%
Not implementing or no planned activity

12%
Implementing: We are implementing quantum-resistant security measures.

47%
Piloting and testing: We have begun implementation and are at piloting and testing stage.

Q21. How far along is your organisation when it comes to quantum-resistant security measures? Base: All respondents in Malaysia=51

*Sums may not total 100 due to rounding.

Cybersecurity is a cat-and-mouse game. With quantum technology moving beyond the labs, what's clear is resilience and technological readiness must be prioritised to handle cyberattacks in a quantum-enabled world.

Some organisations are making progress, but almost half (42%) haven't considered or started implementing any quantum-resistant security measures—what's holding them back?

The top internal barriers are consistent worldwide and in Asia Pacific: talent gaps and rigid legacy systems.

37%	Gaps in technical expertise to adopt industry standards (e.g. NIST encryption standards)
36%	Gaps in dedicated quantum computing knowledge and resources
34%	Gaps in existing systems and/or data integration challenges

Q23. What are your organisation's biggest internal challenges to achieving post-quantum cryptography over the next 12 months? Base: Security leaders globally=1740

Cyber leadership

What leaders can do now

The Chief Information Security Officer (CISO) is tightly coupled to the engine room of the business—working collaboratively across different C-suite functions.

30%
weekly

47%
monthly

17%
quarterly

3%
only as needed

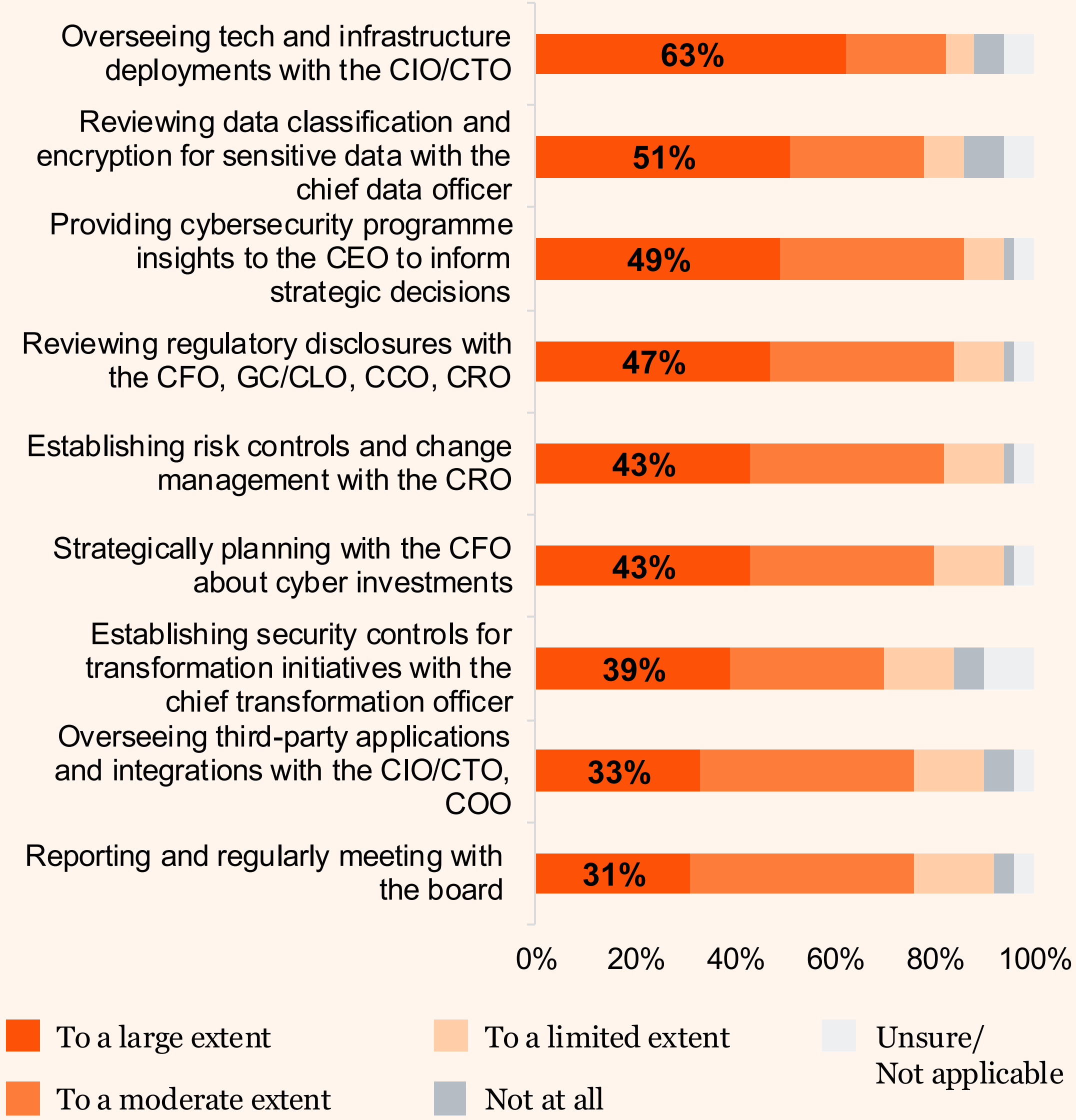
Q26: How frequently do you engage with your CISO on cybersecurity strategy and programmes?
Base: C-Suite in Malaysia excluding CISO=30
*Annual (0%); Not at all (0%); Unsure (3%)

But cybersecurity, as it is a risk management issue, requires an organisation-wide approach—and that includes board engagement.

However, only about one-third say they regularly meet and report to the board to a large extent. That's strikingly lower than collaboration levels with executive peers.

Without frequent, decision-led board engagement, cybersecurity becomes an IT initiative rather than an enterprise risk-and-value decision.

Areas where the CISO works with the C-suite



Q24. To what extent does your CISO work with the C-suite in the following areas?
Base: All respondents in Malaysia except CISO=51

> “Perimeter thinking is yesterday’s answer to tomorrow’s risks. In a world riddled with geopolitical flux and unprecedented technology advances, executives are forced to reassess capabilities, talent, and technology.
>
> The firms that pull ahead will be those that make cybersecurity a board-led capital decision, weaving trust through data and AI so that cybersecurity becomes a source of resilience.
>
> **Clarence Chan**
>
> Partner, Digital Trust and Cybersecurity Leader, PwC Malaysia

PwC's 2026 Global Digital Trust Insights survey was conducted between May and July 2025 and captured the views of 3,887 business and technology executives across 72 territories, including 699 from Asia Pacific and 51 from Malaysia.

The survey reflects the views of business and tech leaders around the world on the challenges and opportunities to improve and transform cybersecurity in their organisation in the next 12 months—covering topics including risk and threat landscape, cyber strategy, artificial intelligence, quantum computing, and cyber leadership.

Contact us

Clarence Chan
Partner, Digital Trust and Cybersecurity Leader,
PwC Malaysia
clarence.ck.chan@pwc.com

Strategy, Governance, Risk and Compliance

Michael Sprake
Partner, Risk Consulting,
PwC Malaysia
michael.sprake1@pwc.com

Cathryne Teh
Director, Technology and Cyber Governance, Risk and Compliance,
PwC Malaysia
pei.gee.teh@pwc.com

Cyber Threat Intelligence and Security Operations

Alex Cheng
Director, Cyber Threat Operations,
PwC Malaysia
alex.ct.cheng@pwc.com

Technology and Architecture

Tanvinder Singh
Director, Cybersecurity and Privacy,
PwC Malaysia
tan.singh@pwc.com

Digital Forensic

Alex Tan
Deals Partner, Forensic Leader,
PwC Malaysia
alex.tan@pwc.com

Chuen Shiong Tee
Deals Partner, Forensic Services,
PwC Malaysia
chuen.shiong.tee@pwc.com

Alliances and Strategic Partnerships

Jason Low
Strategic Alliances Lead, Asia Pacific (Cybersecurity), PwC Malaysia
chee.hong.low@pwc.com