pwc

Putting security at the epicentre of innovation

Digital Trust Insights 2024: Asia Pacific

Cyber investments continue upwards in Asia Pacific

Corporate focus on cybersecurity has deepened over the years in Asia Pacific. In most companies, cybersecurity budgets are set to expand further in 2024, reflecting its sustained place as an essential investment priority for organisations across the region.[1] Asia Pacific's security spending has steadily grown at a compound annual growth rate (CAGR) of 12.8% since 2022, and is expected to top out at US$52bn by 2027 as multiple cyber threats bear down on digitalising companies.[2]

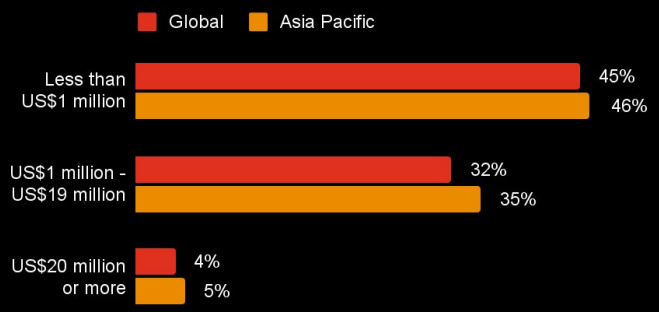
According to the 2024 edition of PwC's annual Digital Trust Insights (DTI) survey, 84% of Asia Pacific business and tech executives reported increases in their cyber budgets. These insights were gleaned from a survey of 683 business, technology and security executives in Asia Pacific conducted by PwC between May and June 2023. The survey comprised both technology- and business-side perspectives from a wide variety of industries and sectors.

What's driving increases in cyber investment?

- **Rising cost of breaches**. The number of mega breaches experienced by Asia Pacific organisations in the past three years has risen considerably; in 2023, 35% of organisations say they have experienced data breaches costing anywhere from US$1m to US$20m over the last three years.

Exhibit 1: Instances of high-dollar breaches are growing

Estimated costs to organisations most damaging data breach between 2020-2023



Q5. Thinking about the most damaging data breach you experienced in the past three years, please provide an estimate of the cost to your organisation.
Base: Security and information technology (IT) and chief financial officer (CFO) respondents in Asia Pacific (301)

Source: PwC, 2024 Global Digital Trust Insights

1. https://www.computerweekly.com/news/366571870/APAC-firms-bullish-on-IT-spending
2. https://www.idc.com/getdoc.jsp?containerId=prAP52008324

- **Awareness of the multi-faceted impacts of data breaches**. Organisations in Asia Pacific are also waking up to the reality of how cyber-attacks can damage reputations, customer confidence and operations, leading to losses of real and potential business opportunities. For more than half (54%) of organisations, the threat of losing customer, employee and transaction data is their top concern, while 46% and 41% respectively pick their impact on the company brand and revenues.

- **Tone from the top.** Though cybersecurity was considered solely a technology area in earlier years, mounting financial and non-financial costs are revealing its immense relevance to the business as a whole. As such, scrutiny on cybersecurity issues is intensifying, as evidenced by 95% of organisations saying they are bringing reporting on cyber risk exposure and mitigation measures to their boards.

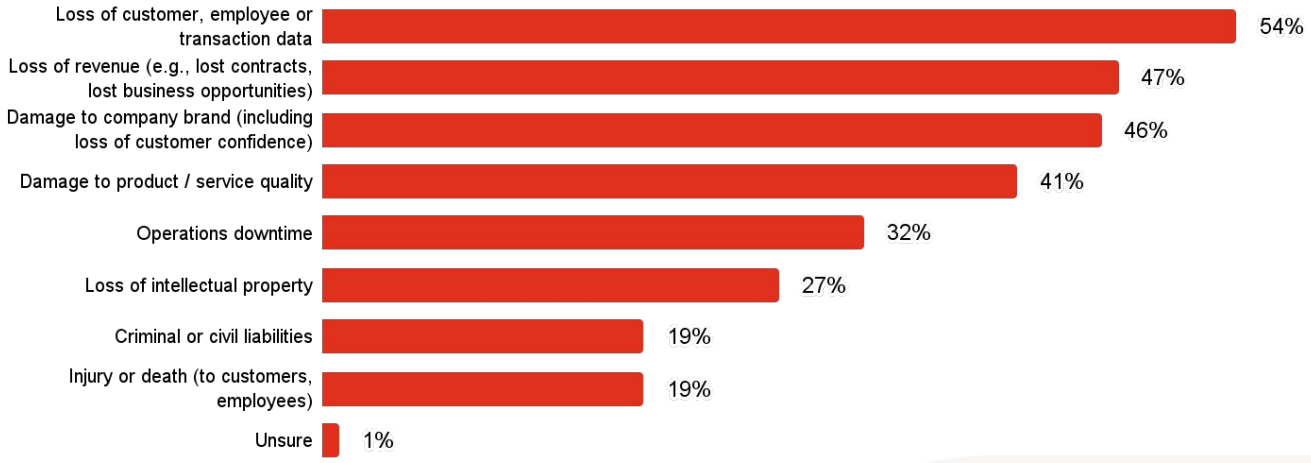
  That heightened scrutiny is translating into cybersecurity issues rising to the top of boardroom agendas. In **PwC's 2023 Annual Corporate Directors Survey,** 64% of organisations report that board meeting time devoted to cybersecurity risk has increased over the past year. Organisations are also emphasising the need for more cyber skills at the board level, with 46% pursuing additional skilling on the topic and 19% adding members with cybersecurity expertise within the last 12 months.[3]

  With these new skills and expertise, board members will be better equipped to request more reporting on cybersecurity issues from management. Greater scrutiny on management's progress on driving better cybersecurity performance will eventually trickle down to an organisation's rank-and-file, further embedding these principles at the heart of an organisation's risk management strategies and actual operations. This will help fuel investments to support post-breach recovery, while also enhancing prevention and resilience.

- **Regulation gains momentum.** Board-level scrutiny will likely only increase over time as momentum mounts for cybersecurity legislations and data protection laws in multiple jurisdictions across Asia Pacific. These are expected to inflate compliance costs – as noted by 42% of respondents – while also placing organisations at greater risk of incurring significant fines. In Singapore, for example, cyber incidents can now cost organisations up to SGD$1m or 10% of their annual turnover; Indonesia's regulators have set their rate at 2%.[4] A series of high-profile data breaches in Australia in 2022 led to amendments where non-compliant organisations may be liable for significant fines of at least AUD$50m or more.[5]

Exhibit 2: Data and revenue losses and reputational damage are top concerns for Asia Pacific organisations

Organisations' top concerns for the outcomes of potential cyber-attack in the next 12 months



Q4. Over the next 12 months, which of the following potential outcomes of cyber attacks is your organisation most concerned about?
Base: Asia Pacific respondents (683)

Source: PwC, 2024 Global Digital Trust Insights

3. https://www.pwc.com/us/en/services/governance-insights-center/library/assets/pwc-gic-acds-2023.pdf
4. https://www.lexology.com/library/detail.aspx?g=126a6e48-f0c4-4f90-9e2d-886844ee578b
5. Ibid.

Investments with impact

While many organisations are rightly concerned about obtaining sufficient investments to fuel their technology strategies, the true challenge will be figuring out how to prioritise spending for maximum impact. Today's technology teams and leaders are not just grappling with a more complex and expanding threat landscape, but with budgets also under pressure.

So, how do leaders make their dollars go further?

- Helping leadership understand their cyber risk exposure will be key to ensuring security teams have the financial support and organisation-wide buy-in they need to see their projects to completion.
- Conducting a proper assessment provides a solid foundation for leaders to establish a security strategy that accurately prioritises the biggest risks to ensure effective budget allocation and prevent overlapping security solutions.
- When it comes to prioritising investment, security leaders need to consider not only where investment will make the greatest business impacts but also stay alert to how these investments could create new risks to the business itself.

Those with data breaches costing US$1m or more in the past three years are more likely to acknowledge that they need to integrate their multiple cybersecurity solutions. This suggests opportunities for optimisation in cyber investment.

Growing cloud and Generative AI (GenAI) adoption increases risks

While cyberattacks pose a serious threat to organisations, accelerating digital adoption is also creating a challenging cyber landscape for leaders to navigate.

Today, digital transformation is viewed as non-negotiable for organisations to remain competitive, resilient and relevant to customers who are demanding fast, high quality and seamless experiences. However, it is progressing at a pace and scale that are creating immense potential costs to organisations that go beyond cyber risks.

For organisations in Asia Pacific, digital adoption spans a wide range of technologies and solutions – where exactly are the majority of these risks arising from? Our report suggests that two segments in particular are focal points.

The cloud becomes critical

Cloud computing implementation is surging all across the region, with 95% of respondents reporting adoption in their organisation. By and large, given their relative age, most Asia Pacific organisations leapfrogged legacy, on-premise systems and went straight to more scalable, third-party cloud platforms which provided easier pathways to digital transformation.

Cloud computing enables organisations to collaborate more effectively, and also facilitates the rapid access to wider networks of information that is key to leveraging data analytics. By 2026, Asia Pacific's public cloud market could be worth US$153.6bn, with this value spread across businesses offering infrastructure, platform and software solutions.[6]

That said, even as organisations increasingly consider cloud adoption the key to competitive advantage and operational agility, the technology also makes it challenging for them to transform safely. Greater cloud adoption is not only exposing organisations to more cyber risk, but also introducing complexity into its operations and making them more reliant on third-party service providers.

6. https://www.idc.com/getdoc.jsp?containerId=prAP50555123

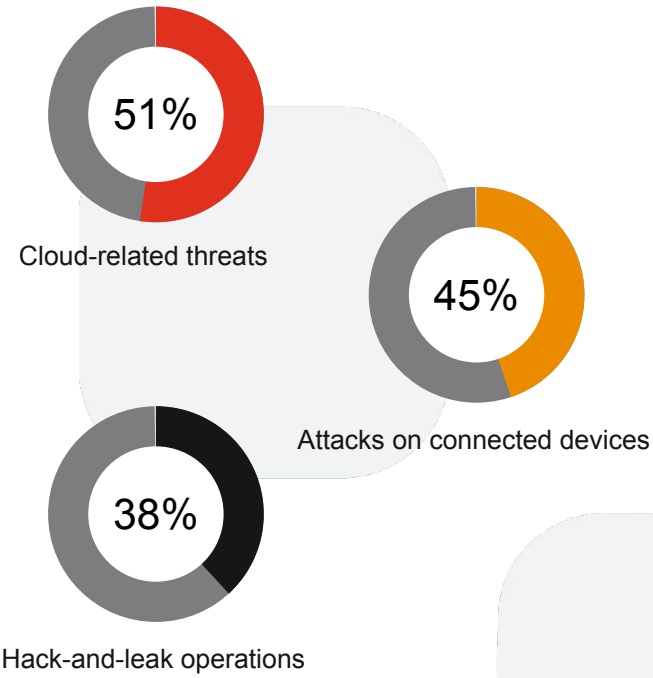
According to our survey, cloud-related threats are among the top three cyber concerns for 51% of Asia Pacific organisations over the next 12 months. That's followed closely by attacks on connected devices (45%), which also depend on cloud computing.

There are immense rewards to be gleaned from cloud adoption, as well as significant risks. Are organisations confident in their preparedness to withstand the threats posed by this key tool? Have leaders started implementing the strategies that are essential to embed resilience into their technology strategies? If not, what steps are needed to secure their organisations and transform safely?

These risks may also stem from organisations' relationship with their cloud service providers. Organisations must consider overall strategy to manage these external partners. What shared responsibilities will help navigate the risk landscape with their cloud service providers sustainably?

Exhibit 3: The cloud is both a source of value and risk for organisations

Top cyber threats to organisations over the next 12 months



Q3. Over the next 12 months, which of the following potential outcomes of cyber threats is your organisation most concerned about?
Base: Asia Pacific respondents (683)

Source: PwC, 2024 Global Digital Trust Insights

Risks and rewards in Generative AI

Similar dynamics are occurring with emergent technologies like Generative AI (GenAI). Since OpenAI's ChatGPT 3.0 burst onto the scene in late 2022, adoption of GenAI tools has grown considerably as businesses see its potential to improve process efficiency, automation and decision-making. Core to GenAI's appeal is its combination of ease of use and ability to generate high-quality, human-like content.

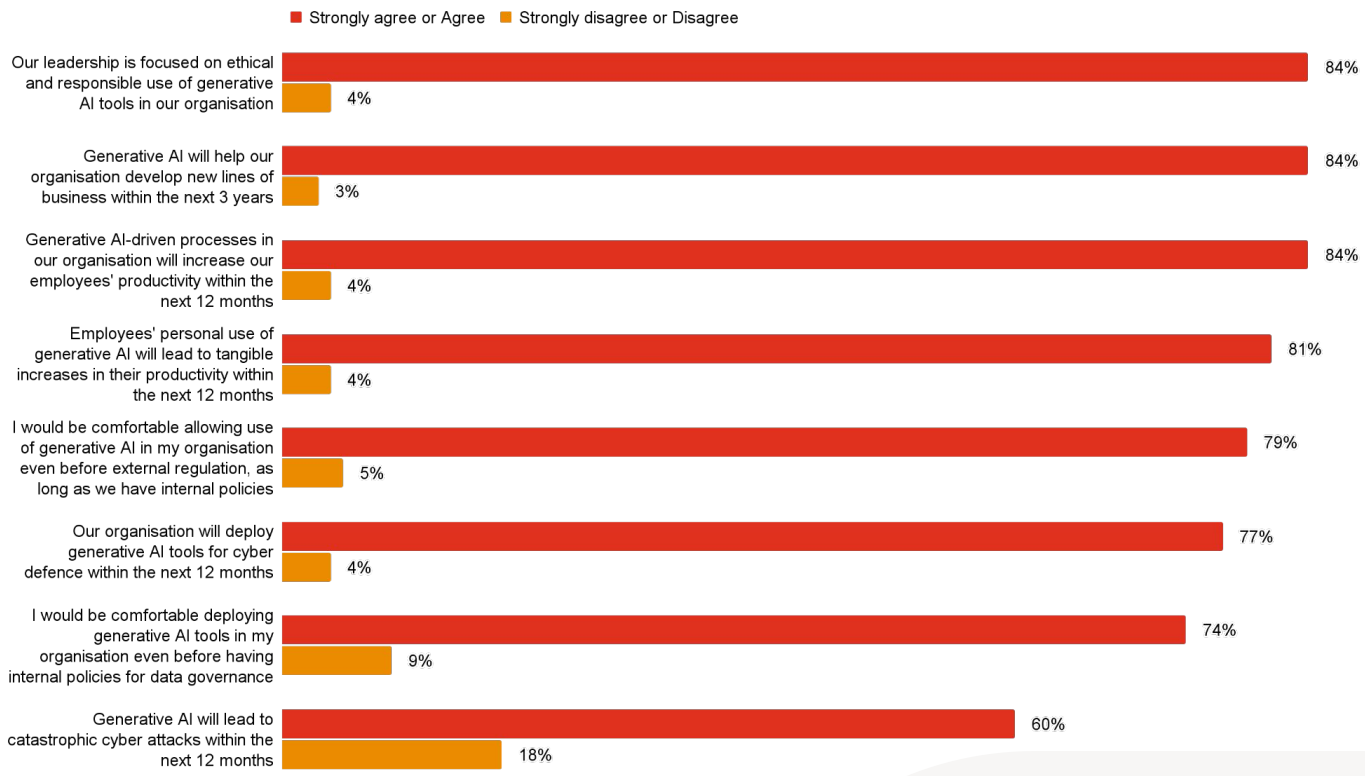
According to our survey, Asia Pacific organisations say that GenAI will help create new business within the next three years and increase employees' productivity levels. GenAI technology is likely to soon automate significant portions of employees' everyday tasks such as writing emails, ideation, and so on. GenAI tools are also being implemented by 77% of organisations to bolster cyber defence over the coming year.

GenAI has the potential to be immensely impactful in the cybersecurity space by accelerating the pace at which security teams can identify risks and threats, thus levelling the playing field against intensifying attacks from bad actors.[7] Machine learning algorithms embedded in GenAI tools are capable of quickly analysing large amounts of data to detect unusual activity and even potentially pinpoint system vulnerabilities before an attack even occurs. For organisations, this poses an opportunity to take a more forward-looking attitude towards their cyber risks that prioritises resilience over reactivity.

That being said, there are causes for concern when it comes to GenAI.

In its current form, GenAI could become a source of disinformation as the technology does not always validate its sources, leading to biased or inaccurate content that have a misleading sheen of authenticity. 60% of Asia Pacific respondents think GenAI could pave the way for devastating cyber-attacks within the next year. GenAI could also fuel disinformation, which 17% of Asia Pacific respondents consider a top-three cyber threat.

Exhibit 4: Asia Pacific leaders see immense potential for value creation with GenAI



Q7. To what extent do you agree or disagree with the following statements about Generative AI?
Base: Asia Pacific respondents (683)

Source: PwC, 2024 Global Digital Trust Insights

7. https://www.techtarget.com/searchsecurity/tip/How-hackers-use-AI-and-machine-learning-to-target-enterprises

Given that the technology is still in its very early stages, organisations are undoubtedly still figuring out their first steps, but getting it right on AI from the beginning will be critical to long-term success and protecting their customers' trust. Establishing human oversight is key.

Are leaders thinking about what ethical and responsible use of GenAI in their organisation looks like? Have they started exploring initiatives to train employees on the right way to use these tools? Are they implementing the critical data security measures and compliance frameworks to safeguard their customers' data and maintain trust?

A battle on many fronts

While technology modernisation remains a major priority for organisations' business teams, they must remain mindful of the need to safely manage the risks arising from widespread and rapid digital adoption. These are not just cyber risks, but also include digital and technology risks such as greater operational complexity and disinformation that could disrupt organisations' ability to continuously deliver high-quality services without interruption.

This is emphasised by findings in our survey that in organisations across Asia Pacific, digital and technology risks and cyber risks are top priorities for mitigation.[8]

8. In the survey, digital and technology risks are defined as adverse consequences from new or frontier technologies, or an inability to execute digital transformation.

Addressing third-party risks

For many organisations, obtaining the resources and skills it needs to digitally transform and build up its technological capabilities often requires them to rely on third-party providers. These third parties can provide access to crucial, new skills, while also helping organisations balance costs, improve service speed and expand global reach.

- Among 29% of Asia Pacific organisations, managed services have been implemented in new areas of the business such as its security operations.
- Managed services are also a priority cyber investment area for 21% of organisations.

However, increasing dependence on a third-party ecosystem is itself a problem as this essentially creates points of vulnerability within the organisation that can be accessed by external actors.

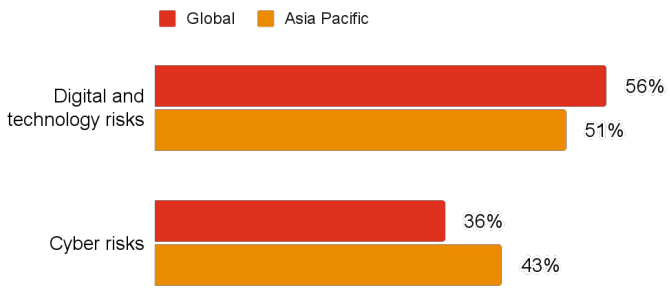
Consider how Asia Pacific organisations engage with cloud service providers, for example. Depending on the type of cloud (platform, software or infrastructure) or vendor (public or private), there could be varying levels of shared responsibilities between organisations and their third-parties. Aligning those responsibilities are key to an effective operational resilience strategy and risk mitigation.

The threat landscape is expanding in focus – it's not just about malicious actors and hackers who are creating problems, but also a wide network of potentially compromised providers sitting outside organisations' control with access to internal systems and data.

The survey reflects this: among the top cyber threats selected by Asia Pacific respondents, a majority are directly correlated with third-party ecosystems, including cloud platforms, connected devices and software supply chains. For 26% of Asia Pacific respondents, software supply chains are among the top third-party related cyber threats, followed by third-party breaches (25%) and exploits of zero-day vulnerabilities (14%).

Given the pace of technological adoption, today's threat landscape is also evolving quickly with increased uncertainty and exposure driving the need for a more robust resilience plan. These resilience strategies are not just about shoring up organisations' ability to quickly recover from a disruption, but also fortifying itself with the resources to prevent and withstand an attack or adverse event.[9]

Exhibit 5: Digital and tech risks rise to equal importance with cyber risks



Q1. Which of the following risks is your organisation prioritising for mitigation over the next 12 months?
Base: Asia Pacific respondents (683)
Source: PwC, 2024 Global Digital Trust Insights

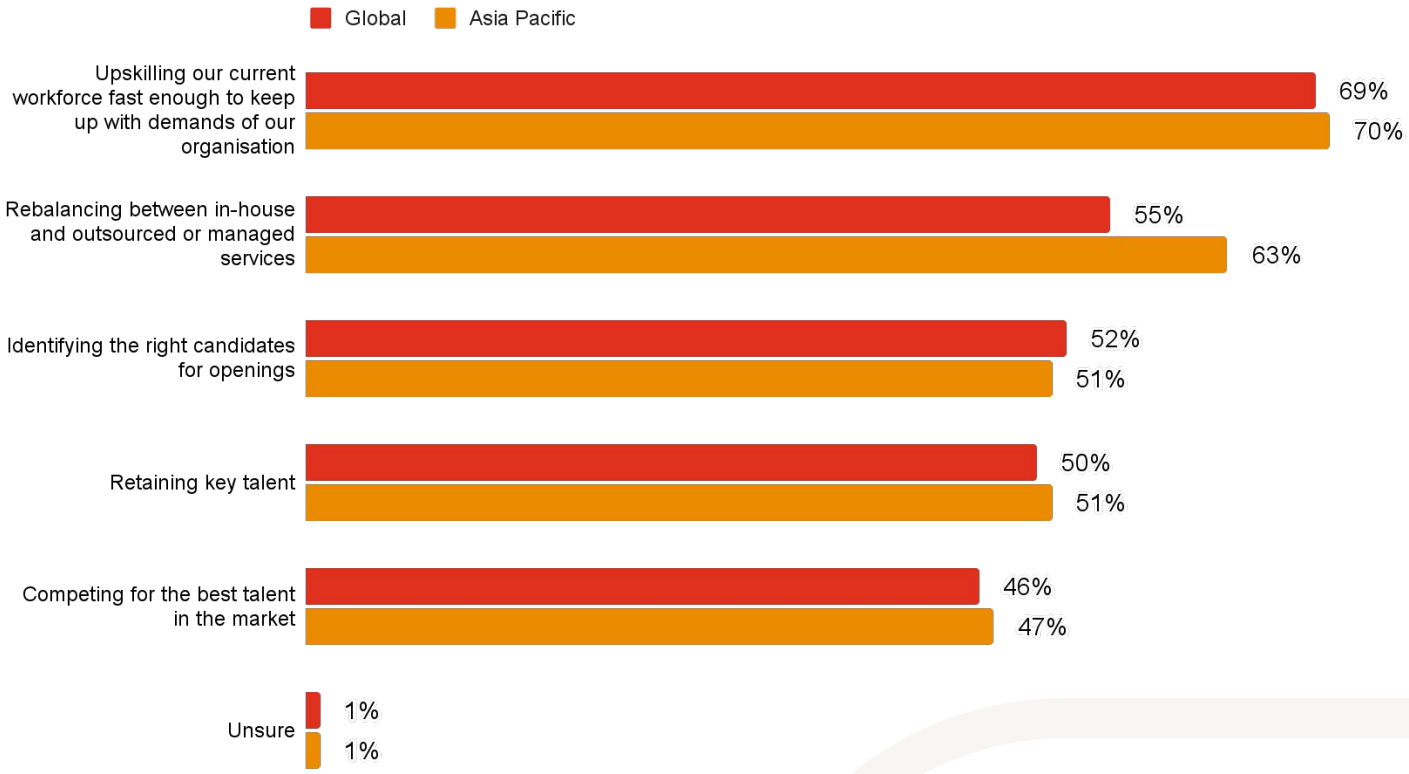
9. https://www.pwc.com/gx/en/asia-pacific/asia-pac-time/asia-pacific-time-report-2.0.pdf

Organisations are aware of the problems of over-relying on third-parties: 63% of organisations acknowledge the need to rebalance between in-house capabilities and outsourced or managed services.

However, they cannot address these third-party risks without considering that these issues also emerge out of other organisational challenges such as skills shortages and rapid technology adoption. Leaders are aware of this, as reflected by an emphasis in Asia Pacific on upskilling (70%) and retaining or identifying key talent (51%) as pathways to bringing their tech needs under their control and purview, which could reduce their overall need to hire external vendors. There may also be a need for reskilling as organisations prepare the workforces to manage the new roles and responsibilities emerging from greater digitalisation.

Exhibit 6: Company leaders are aware of the need to rethink how they rely on third parties

Priorities in organisation's cyber talent strategy over the next 12 months



Q15. Which of the following is your organisation prioritising in its cyber talent strategy over the next 12 months?
Base: Asia Pacific respondents (683)

Source: PwC, 2024 Global Digital Trust Insights

Centering risk in the transformation journey for long-term resilience and success

In an increasingly complex business environment, organisations are constantly juggling between competing—and complementary—priorities, but as trends and contexts collide, this old approach is no longer sufficient.

To address today's complex and interconnected risks, modern business must expand its vision and break the barriers between functions, strategies and goals. True resilience is not just about their ability to recover from an incident, but to pre-empt possible danger and put in place the resources to withstand any adverse event.

How can organisations build resilience through integrated risk management?

Organisations need to start considering how they can establish an integrated risk management framework that brings together a multifaceted and nuanced picture of the company's risks as they relate to technology and digital adoption, third-party engagement and operational structures.

We are already seeing how some enterprises are actively moving towards an integrated approach to not just resilience building, but also risk management. Most Asia Pacific respondents (97%) have either already integrated or are planning to in the process of integrating cyber initiatives into their resilience strategies and initiatives.

As they start to build the resources to take an integrated risk management approach, leaders can begin by focusing on several key strategies:

- Establish shared strategy and objectives throughout the organisation, ensuring these goals cut across subject matter, function and level.
- Align related risk subjects across different functions to embed synergy and power better cross-organisation decision-making for better accountability and awareness at all levels.
- Establish more board oversight and accountability for cyber risks. This could include recruiting more directors with cyber experience, providing more education to current directors on cybersecurity principles, and enhancing communications with technology leaders.
- Integrate cyber risks into the organisation's overall risk framework, with the help and support of security leaders on-the-ground.
- Identify and emphasise investment in tech assets that have the most business and security impact in the long term.
- Develop a comprehensive workforce strategy that prioritises organisation-wide digital upskilling initiatives and talent development, balanced with the use of third-party subject matter experts. Underlying this framework should be robust risk management practices to enhance overall resilience and adaptability in the face of evolving cyber threats.

Contact us to learn more

Raymond Teo
Partner and Cyber Leader,
PwC South East Asia Consulting,
PwC SIngapore
raymond.pj.teo@pwc.com

Jimmy Sng
Partner,
Technology Risk Services Leader,
PwC Singapore
jimmy.sng@pwc.com

Kyra Mattar
Partner,
Digital Solutions,
PwC Singapore
kyra.mattar@pwc.com

Richie Tan
Partner,
PwC South East Asia Consulting,
PwC Singapore
richie.tan@pwc.com

Jayme Metcalfe
Partner,
Digital Solutions,
PwC Singapore
jayme.ph.metcalfe@pwc.com

Mark Jansen
Partner,
Data Trust Services Leader,
PwC Singapore
mark.jansen@pwc.com

Rishi Anand
Partner,
PwC South East Asia Consulting,
PwC Thailand
rishi.a.anand@pwc.com

Winston Nesfield
Partner,
AI Advisory Leader, PwC South East Asia Consulting,
PwC Singapore
winston.nesfield@pwc.com