Digital Trust Insights 2025: Singapore highlights

Singapore findings from the 2025 Global Digital Trust Insights

pwc

Overview of 5 gaps

As part of the Global Digital Trust Insights 2025, PwC surveyed 69 business and tech executives in Singapore and found significant gaps companies operating in Singapore must bridge before they can achieve cyber resilience:

1 Gaps in implementation of cyber resilience

2 Gaps in preparedness

3 Gaps in chief information security officer (CISO) involvement

4 Gaps in regulatory compliance confidence

5 Gaps in cyber risk measurement

To bridge these gaps, companies need to make strategic investments in key areas.

01

Gaps in implementation of cyber resilience

Despite heightened concerns about cyber risk, only **2%** of respondents globally say their company has implemented cyber resilience actions across their organisation in all areas surveyed.

Only 21% of global respondents said their cybersecurity teams usually (i.e. 81-100% of the time) allocate cyber budget to the organisation's top risks. This may be caused by a lack of strategic foresight, insufficient resources as well as a reactive – rather than proactive – approach to cybersecurity.

In Singapore, the proportion of respondents indicating that their cybersecurity teams usually allocate cyber budget to the organisation's top risks is slightly higher at 29%. Even so, it still points to significant weaknesses in cyber budget allocation.

Bridging the gap

To support the implementation of cyber resilience across the organisation, executives need to facilitate a more strategic approach to cyber budget allocation. This requires them to embrace a shift from reactive to proactive cybersecurity strategies, including better risk anticipation and a commitment to continuous improvement.

Wake-up call

- Have you implemented cyber resilience actions spanning across people, processes and technology within your organisation?
- Does your cybersecurity team allocate cyber budget to the most pressing cyber risks faced by your organisation?

02

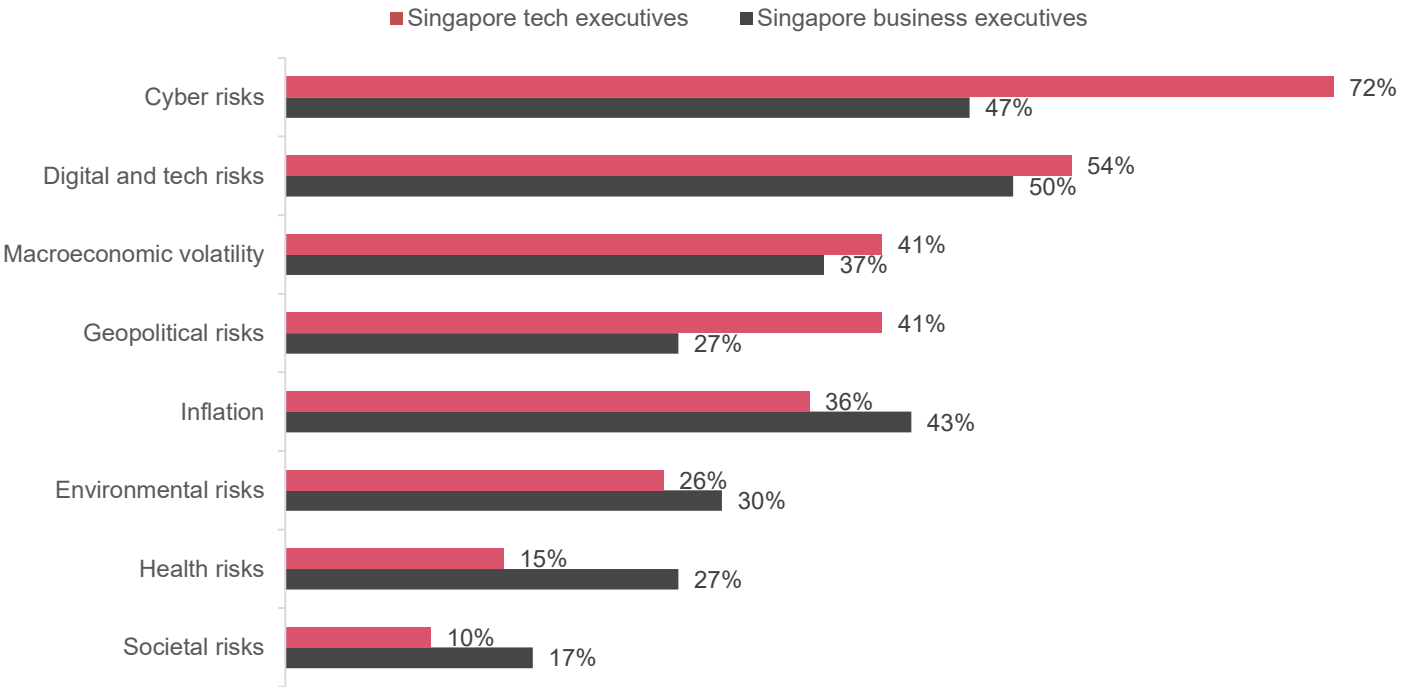
Gaps in preparedness

There is a strategic divide between business and technology executives when it comes to key risks for mitigation. Furthermore, organisations feel they are the least prepared to address the cyber threats they deem most concerning.

Similar to global data, Singapore data reveals that there is a strategic divide between the risks that are being prioritised for mitigation by business and technology executives. 72% of tech executives in Singapore rank cyber as the highest risk for mitigation, compared to 47% of business executives, who rank digital and technology risks as the highest risk for mitigation. The divide between business and technology executives is also echoed in the investment areas that they believe should be prioritised in the coming year. Technology executives prioritise cloud security (41%) as the top cyber investment over the next year, while business executives prioritise technology and cyber infrastructure modernisation as well as the optimisation of existing technology and investments (43%).

Risk mitigation priorities for business vs tech leaders

(showing % ranked 1-3)



Q1. Which of the following risks is your organisation prioritising for mitigation over the next 12 months? (Ranked in top three)
Base: All Singapore respondents = 69
Source: PwC 2025 Global Digital Trust Insights

02

Gaps in preparedness

There is a strategic divide between business and technology executives when it comes to key risks for mitigation. Furthermore, organisations feel they are the least prepared to address the cyber threats they deem most concerning.

Both business (60%) and technology (62%) executives in Singapore find common ground when it comes to cloud-related threats, deeming them the most concerning cyber threat over the next 12 months. Yet, cloud-related threats are also ranked by 42% of Singapore respondents as the threat their organisations are least prepared to address. Similar sentiments among Singapore respondents can be seen in relation to attacks on connected products, which came in as the second most concerning cyber threat (45%) and the fourth threat organisations are least prepared to address (24%).

Finally, Singapore respondents indicate that emerging technologies, like cloud (87%) and generative artificial intelligence (GenAI) (77%), have increased the attack surface for their organisations. In response to an enlarged attack surface, 94% of Singapore respondents have increased their risk management investment in AI governance.

Bridging the gap

- To safeguard critical assets and maintain trust, align business and cybersecurity priorities by balancing the prioritisation of cyber risks with economic pressures. Regular cross-functional assessments will keep strategy and priorities in sync.
- To ensure organisations are prepared to address the most concerning cyber threats, they should adopt a threat-informed cyber investment. This involves prioritising investments in the most pressing cyber risks and examining more closely where resources are being used across people, process and defence capabilities.
- With the continuous adoption of new technologies, stay one step ahead of evolving threats through continuous assessment of new vulnerabilities and investments in advanced security measures. This calls for close collaboration between technology, security, risk and legal teams.

Wake-up call

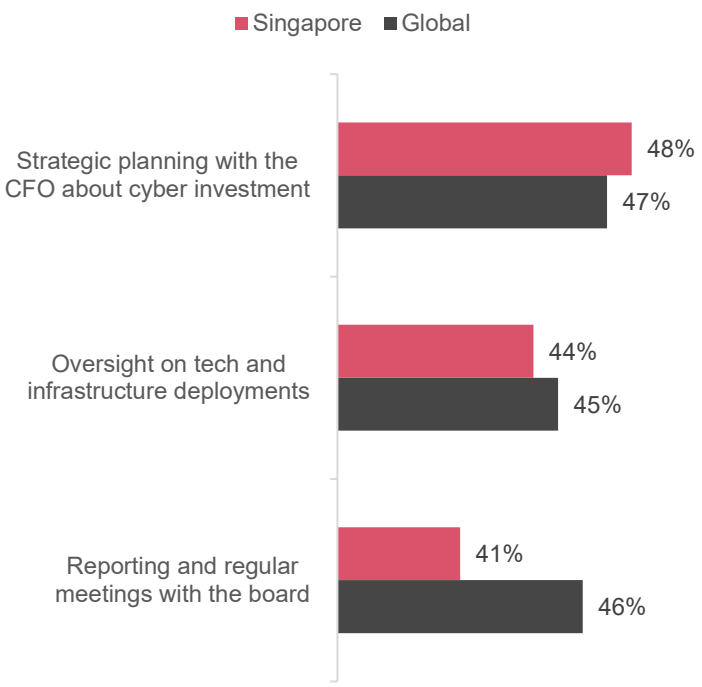
- Have you ensured alignment between business and technology executives in your organisation?
- How prepared is your organisation to address the most concerning cyber threats?
- What is your organisation doing to secure the adoption of new technologies?

03

Gaps in CISO involvement

Fewer than half of executives say their CISOs are involved to a large extent in strategic planning, board reporting and overseeing tech deployments.

Globally and in Singapore, the value that CISOs deliver is limited by the lack of their involvement in key areas. Fewer than half of CISOs are involved to a large extent in activities, such as:



By excluding the CISO from these key business activities, organisations are wasting their critical insights, which would otherwise enable the proactive navigation of cybersecurity as a core enterprise risk.

Bridging the gap

Give your CISO a seat at the table. Involving them at the highest levels of strategic decision-making allows your organisation to align its approach to safeguarding critical assets and driving resilience.

Wake-up call

Have you involved your CISO in key strategic areas to ensure cybersecurity is treated as a top business priority?

04

Gaps in regulatory compliance confidence

CEOs and CISOs/CSOs have different levels of confidence in their company's ability to comply with regulations, especially regarding AI, resilience and critical infrastructure.

Globally, there is a 13% point gap in confidence between CISO/CSOs and chief executive officers (CEOs) regarding compliance with AI, resilience and critical infrastructure regulations. This may be because the CISO's day-to-day role exposes them more to the operational difficulties, resource constraints and potential vulnerabilities that may hinder cyber compliance.

Despite differing confidence levels, 96% of global respondents report that cybersecurity regulations have propelled the growth in their organisations' cyber investment in the last 12 months. All (100%) Singapore respondents concur with the catalytic role that regulations play in increasing enterprise cyber investment. Looking forward to the next 12 months, 77% of global and 81% of Singapore respondents expect their cyber budget to increase. This growth in spending needs to be aligned to current and future risks to maximise the returns on every dollar spent.

Furthermore, more than three-quarters (78%) of global respondents believe regulations have been beneficial in challenging, improving or increasing their cybersecurity posture. More than four in five (81%) of Singapore respondents are on the same page.

Bridging the gap

To bridge the gap in confidence levels between CISOs/CSOs and CEOs, there needs to be better communication and alignment. CISOs need to step up and more effectively communicate the business implications of cyber risks to the leadership team with data-backed insights. This relates to the third gap we had previously identified in CISO involvement, meaning that the leadership team also needs to provide the CISO not only with the airtime to communicate cyber risks, but also the resources and support required to meet regulatory demands.

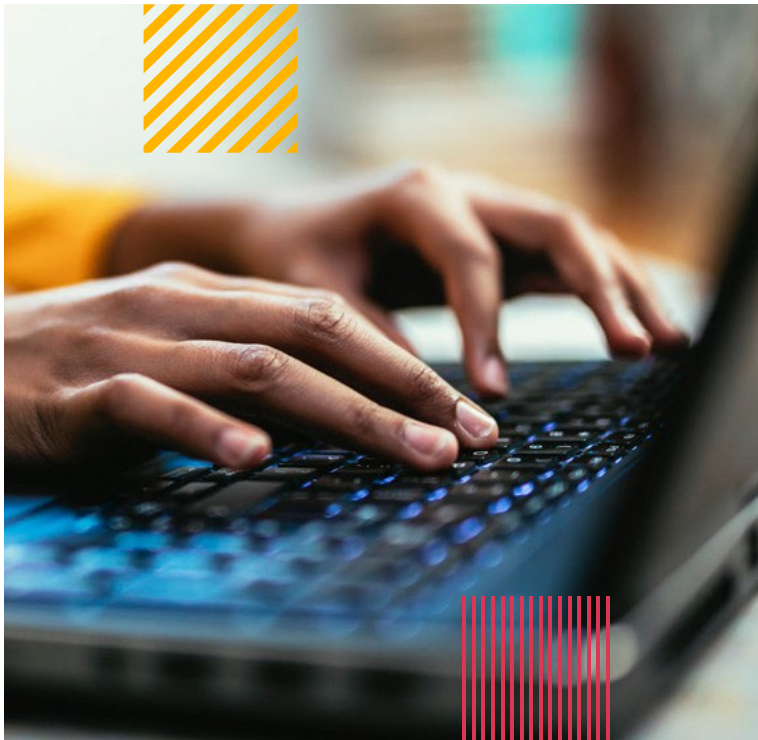
Wake-up call

For CISOs/CSOs

Have you crafted a compelling business case for cyber investments, supported with data and insights?

For CEOs

Have you enabled your CISO in facilitating compliance with cyber regulations with ample airtime, resources and support?



05

Gaps in cyber risk measurement

Although executives acknowledge the importance of measuring cyber risk, fewer than half do so effectively, with only 15% globally measuring the financial impact of cyber risks to a significant extent.

As cyber threats rapidly evolve in scope and sophistication, quantifying cyber risk has become an essential practice. Yet, challenges – like data quality issues and output reliability – have stymied broader adoption. Globally, only 15% of respondents say their organisations measure the financial impact of cyber risks to a significant extent, even though 88% and 87% believe measuring cyber risk is important for prioritising cyber investments and allocating resources to areas of highest risk, respectively.

Singapore organisations appear to outperform their global peers, with 37% of respondents indicating that their organisations measures the financial impact of cyber risks to a significant extent, perhaps due to more stringent regulations and/or a more mature cybersecurity landscape. Yet, this means that more than three in five (63%) – a majority – of organisations do not do so.

Data issues have been identified by 44% of global and 55% of Singapore respondents as a considerable challenge to quantifying the financial impact of cyber risk. However, the top challenge for global and Singapore respondents differs, with 45% of global respondents citing uncertainty around the intended scope of risk quantification outputs and 64% of Singapore respondents citing legal / regulatory concerns (e.g., risk quantification outputs that create potential legal exposure).

Bridging the gap

To bridge the gap in cyber risk measurement, organisations need to address the obstacles that hinder organisations from quantifying the financial impact of cyber risks. By tackling the challenges and fully integrating cyber risk quantification into the organisation's strategic process, leaders can build trust into the outputs for them to inform decision-making related to cyber investments.

Wake-up call

- Have you routinely quantified the financial impact of cyber risks in your organisation?
- If not, what obstacles are preventing you from doing so?

About this report

The 2025 Global Digital Trust Insights is a survey of 4,042 business and technology executives conducted in the May through July 2024 period.

A quarter of the executives are from large companies with $5 billion or more in revenues. Respondents operate in a range of industries, including industrials and services (21%); tech, media, telecom (20%); financial services (19%); retail and consumer markets (17%); energy, utilities and resources (11%); health (7%) and government and public services (4%).

Respondents are based in 77 countries. The regional breakdown is Western Europe (30%), North America (25%), Asia Pacific (18%), Latin America (12%), Central and Eastern Europe (6%), Africa (5%) and the Middle East (3%).

In Singapore, there were 69 respondents: 44% are business leaders, 56% are technology leaders. Nearly one-third (29%) of the executives are from large companies with $5 billion or more in revenues.

The Global Digital Trust Insights Survey had been known as the Global State of Information Security Survey (GSISS). Now in its 27th year, it's the longest-running annual survey on cybersecurity trends. It's also the largest survey in the cybersecurity industry and the only one that draws participation from senior business executives, not just security and technology executives.

PwC Research, PwC's global Centre of Excellence for market research and insight, conducted this survey.

Contact us

Greg Unsworth
Digital Business and Risk Services Leader
PwC Singapore
greg.unsworth@pwc.com | LinkedIn