2025 Global Digital Trust Insights

Bridging the gap to cyber resilience: The C-suite playbook

Malaysia highlights | November 2024

Achieving cyber resilience at an enterprise level is critical in today's ever-evolving regulatory environment, made complicated by new avenues for potential attacks contributed by AI advancements, connected devices and cloud technologies.

Yet despite widespread awareness of the challenges, significant gaps persist. To safeguard their organisations, executives should treat cybersecurity as a standing item on the business agenda, embedding it into every strategic decision and demanding C-suite collaboration.

PwC's 2025 Global Digital Trust Insights survey of 4,042 business and tech executives from across 77 countries, including Malaysia (34 respondents), revealed significant gaps companies must bridge to achieve cyber resilience.

All of this points to the need for better C-suite collaboration and strategic investment to strengthen cyber resilience towards a more secure future.

About the global 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.

The Global Digital Trust Insights Survey was previously 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, beyond just security and technology executives.

Scan to download the global report or

click here

pwc

Threat outlook and emerging risks

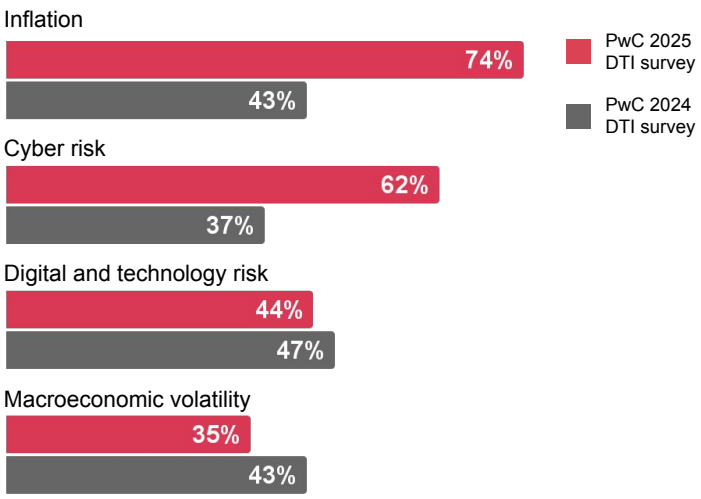
Navigating cyber threats: Establishing a shared vision for preparedness

Cyber risk now a top 3 risk priority

While the cybersecurity landscape continues to evolve, organisations are struggling with increasingly volatile and unpredictable threats. This year, like their global counterparts, Malaysian business and tech leaders have placed cyber risk among their top three concerns. In contrast, cyber risks only ranked fifth among Malaysian respondents in last year's survey.

Risk mitigation priorities for the next 12 months

(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)

Source: PwC 2025 Global Digital Trust insights, PwC 2024 Global Digital Trust Insights

Most concerning cyber threats over the next 12 months

44% Third-party breach

38% Hack-and-leak operations

38% Attacks on connected products

32% Cloud-related attacks

Executive call-to-actions: Creating a shared vision to combat cyber threats

Board: Understand the top cyber risks to the organisation and ask the tough questions of management. How are risks being mitigated? Do we have adequate plans and funding in place to proactively address risks and respond should an event occur?

CISOs: Highlight to the rest of the C-suite the threats that jeopardise your business most, especially if investment efforts need to be shifted.

CIOs and chief technology officers (CTOs): Based on conversations with the risk executives, gauge how certain threats can damage information and infrastructure security at large and which threats pose the biggest barriers to resilience.

CEOs: Meet regularly with the CRO and CISO to understand the threat vectors they're most concerned about. Make sure you're receiving regular reporting on current threat mitigation efforts.

CFOs: Gain deeper insight from the CISO and CRO on the most critical cyber management and investment priorities.

Regulatory development

Cyber regulations: Guiding companies towards resilience

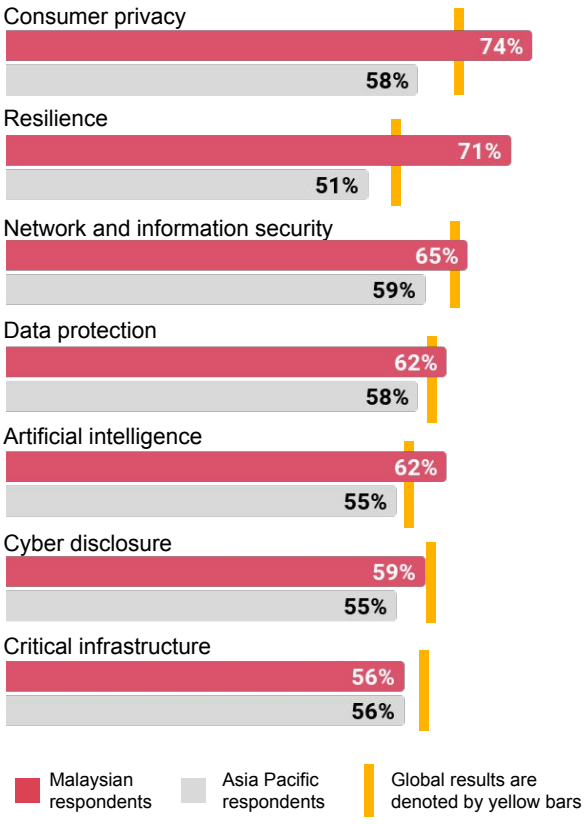
Cyber regulations drive positive change

Regulatory frameworks are prompting companies to swiftly comply with a growing array of requirements. A surge of new regulations — Personal Data Protection (Amendments) Bill 2024, Cyber Security Act 2024 — underscores the urgency for organisations to align their practices to these heightened expectations.

Malaysian respondents seem confident in their organisations' ability to achieve full compliance as 69% believe that regulations have helped their cybersecurity posture. This indicates that despite compliance challenges, regulations are enhancing cybersecurity capabilities and positively shifting mindsets about the value of greater integration in pursuing cyber resilience.

Confidence in organisation's regulation compliance

(showing % high confidence)



Q15. How confident are you in your organisation's ability to be in compliance with the following types of regulations that may apply to the geographic area(s) in which your organisation operates?

Source: PwC 2025 Global Digital Trust Insights

Cybersecurity regulations helped 69% of organisations

27% challenged our organisation to strengthen current cyber risk management programme, processes and governance approaches

21% helped our organisation become more resilient by mandating an industry-wide framework

12% helped our organisation establish guardrails for technology innovation and transformation efforts

9% led us to consider cyber managed services to address regulatory requirements

Q17. Which one statement, if any, best reflects the impact of new cybersecurity regulations on your organisation over the last 12 months?

Source: PwC 2025 Global Digital Trust Insights

Executive call-to-action to: Improving compliance posture collectively

Board: Stay abreast of emerging regulatory requirements and seek input from management on proactive measures being taken to prepare for new requirements. Understand management's approach to assessing and disclosing cyber incidents.

CISOs and CROs: Deliver frequent reporting to other executive leaders on the state of regulations that directly impact respective industry or territory needs, and work towards implementing technology and regulatory change management processes.

CEOs: Understand oversight responsibilities to guide compliance efforts, including any necessary coordination between different business units. Identify key questions to ask CISOs to close any knowledge gaps on compliance posture.

Chief Compliance Officers: Stay abreast of regulatory compliance requirements and collaborate with the CISO and CRO to incorporate proactive compliance measures and monitoring to periodically confirm compliance.

Chief Legal Officers (CLOs) and General Counsels (GCs): Determine the right amount of disclosure details needed to fulfil cyber programme reporting obligations, striking a balance between transparency and confidentiality.

CFOs: Verify the accuracy, completeness and defensibility of all regulatory disclosures of cyber risk management and programme posture. Develop a clear understanding of materiality and the specific impact of a cyber incident, incorporating cyber risk quantification to accurately assess and communicate potential risks.

Cyber investment and priorities

Investing in resilience, building trust

Cybersecurity and trust: The new competitive edge

Organisations increasingly view cybersecurity as a competitive advantage, with 62% of executives citing customer trust and 44% citing brand integrity and loyalty as areas of influence. As cyber threats escalate, a strong cybersecurity posture isn't just about protection — it's about building a reputation that customers and stakeholders can rely on. At a time when trust is paramount, companies that prioritise cybersecurity are better positioned to stand out as leaders in both safety and integrity.

Positioning cybersecurity as a competitive advantage

(showing % selected 'To a large extent')

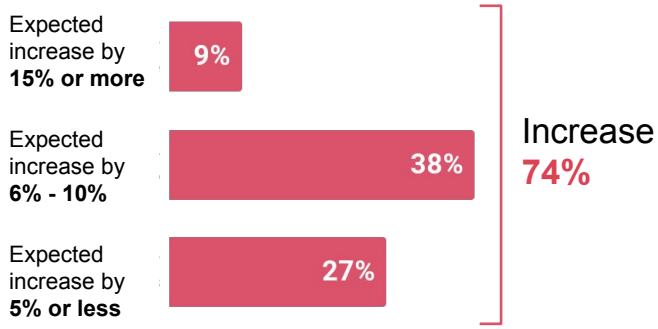
Q19. To what extent does your organisation position cybersecurity as a competitive advantage in these areas?

Source: PwC 2025 Global Digital Trust Insights

Cyber budgets are expected to continue growing in the next year

74% of organisations anticipate an increase in their cyber budget for the upcoming year, similar to the 76% last year. While the increases in cyber budget is a positive sign, they suggest organisations might still be playing catch-up in an evolving threat environment, raising the question of what more is needed for cyber resilience.

Cyber budget growth in 2025



Q7. How will your organisation's cyber budget change in 2025?

(The option 'Increase by 11% to 14% was excluded from the graph as it did not receive any responses)

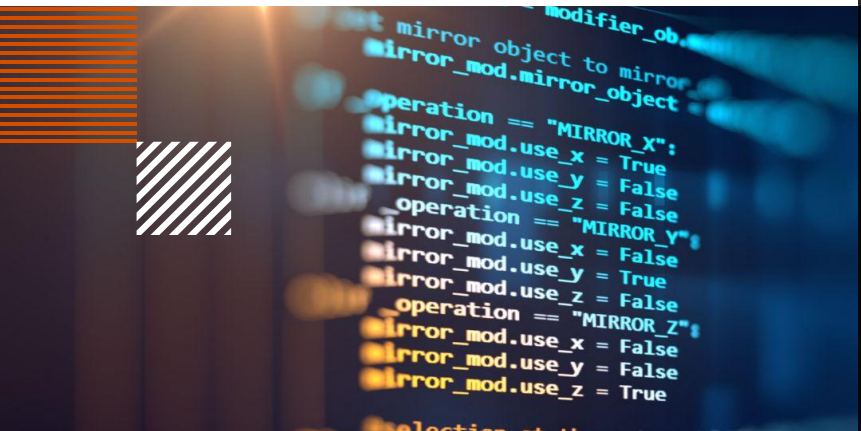
Source: PwC 2025 Global Digital Trust Insights

Executive call-to-action: Optimising cyber investments

CIOs, CTOs and CISOs: Translate the business case for data protection and cloud security investment priorities to CFOs based on the business value of key outcomes (e.g., reducing the time to recover mission-critical data or patching a system).

CDOs: Collaborate with tech, security and finance executives to pinpoint the most essential data security and integrity priorities to guide the information and cloud security investment strategy. Confirming data quality and readiness is necessary to increase security investments.

CFOs: Determine the business value of data protection and cloud security to gain stakeholder trust and make more informed cybersecurity investment decisions.



Cyber strategy and leadership

Is your cyber strategy and leadership driving real resilience?

Partial implementation isn't enough. Companies need to pick up the pace.

A review of 12 resilience actions* across people, processes and technology indicates that,

47% **or fewer executives believe their organisations have fully implemented any one of those actions**

6% **say all 12 resilience actions have been implemented across their organisation**

This leaves a glaring vulnerability — without enterprise-wide resilience, companies remain exposed to the increasing threats that could compromise operations.

Here are a few key areas that would benefit from cross-organisational attention.

- Establishing a resilience team (only **41%** of executives say this has been implemented across the organisation)
- Identifying critical business processes (only **41%** say this has been implemented across the organisation)
- Mapping technology dependencies (only **27%** say this has been implemented across the organisation)

Cyber resilience is a key priority. Why are so many companies lagging in critical areas?

Despite being a top priority among global and Asia Pacific respondents, only 15% of organisations in Malaysia usually** put controls in place and responds quickly to threats so their organisations can withstand serious cyber disruptions. In contrast, Malaysian cybersecurity teams tend to focus on delivering insights on cyber risks and regulatory changes to senior management. While raising cyber awareness at the top is important, they need to move beyond monitoring and start acting on these insights.

Behaviours an organisation's cybersecurity team 'usually**' performs

(** 'usually' denotes 81% to 100% of the time)

Delivers insights on changing cyber risk exposure, regulatory developments and mitigation measures to the CEO and board

Collaborates with other parts of the business that affect the organisation's cybersecurity posture

Allocates cyber budget to top risk areas of the organisation

Anticipates future cyber risks given the macro environment, emerging technology and business strategy

Puts controls in place and responds quickly to threats so our organisation can withstand serious cyber disruptions

Q28. Finally, please indicate how consistently your organisation's cybersecurity team does the following.

Source: PwC 2025 Global Digital Trust Insights

Note:
*The 12 cyber resilience actions include: Reporting to external stakeholders (regulators, investors); Establishing a resilience team with members from functions like business continuity, cyber, crisis management; Establishing relationships with local law enforcement to help with analysis and responses; Identifying critical business processes; Developing cyber recovery playbook for IT-loss scenarios; Establishing protocols with major technology providers to coordinate incident responses; Running tabletop exercises and simulations; Sharing information with industry peers, through formal processes, to prevent systemic risks; Implementing cyber recovery technology solutions (including immutable backups); Mapping technology dependencies; Implementing tools for greater visibility of operational technology (OT) assets; Deploying quantum computing for cyber defence and resilience.

Cyber strategy and leadership

Is your cyber strategy and leadership driving real resilience?

Strategic priorities: Compliance, speed, and trust

Over the next 12 months, 41% of business and tech leaders plan to focus on improving regulatory compliance and reducing response times to incidents and disruptions. This suggests an increasing level of awareness of new regulatory requirements — such as the Cyber Security Act 2024 and the Personal Data Protection (Amendments) Bill 2024 — among Malaysian companies.

Improving customer and employee experience is also a top goal, reflecting cyber's strategic value as a trust builder and a key tool for safeguarding customers' and employees' interests.

Organisation's goals relating to cyber and privacy

(showing % ranked 1-3)

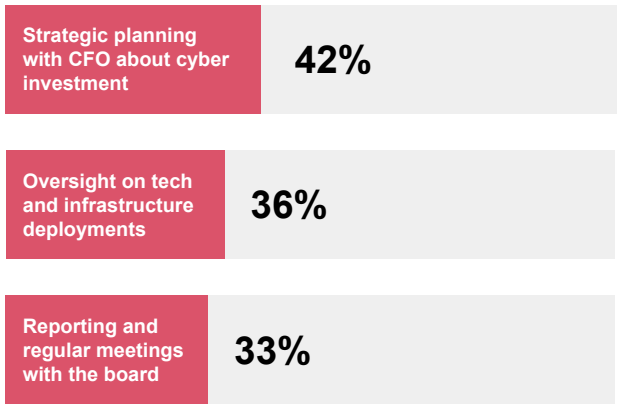
Q21. What, if any, are your organisation's strategy, people and investment goals relating to cyber and privacy over the next 12 months? (Ranked in top three)

Source: PwC 2025 Global Digital Trust Insights

Elevating the CISO: Aligning strategy with security

Many organisations miss critical opportunities by not fully involving their CISOs in key initiatives. This gap leaves organisations vulnerable to misaligned strategies and weaker security postures.

CISO involvement in business activities 'to a large extent'



Q21. How involved is your organisation's CISO in taking an active role in the following areas?

Source: PwC 2025 Global Digital Trust Insights

Executive call-to-action: Strategising for cyber resilience

Board: Stay informed about cyber risk programme developments, especially related to your organisation's cyber risk and threat exposure, to meet expanding oversight and governance responsibilities.

CISOs: Make the business case to the rest of the C-suite for why it's imperative that CISOs be involved in strategy, planning and oversight of the cyber risk mitigation and resilience strategy.

CEOs, CFOs and CIOs: Participate in cyber resilience assessments and exercises to better understand gaps and approaches CISOs might face for integrating leading practices, standards and controls.

“

The mandate has been given to businesses to build and defend digital trust. Organisations need to prioritise this, making cyber resilience everyone's responsibility - from the boardroom to the employee. While Generative AI brings new possibilities for cyber defense, it also introduces uncharted cyber risks.

Regulatory compliance needs to be viewed as an opportunity for stronger safeguards against cyber threats, beyond just a requirement. Every action and investment counts towards securing the future of your brand.

”

Clarence Chan
Digital Trust and Cybersecurity Leader, PwC Malaysia
+60 (12) 712 1285
clarence.ck.chan@pwc.com