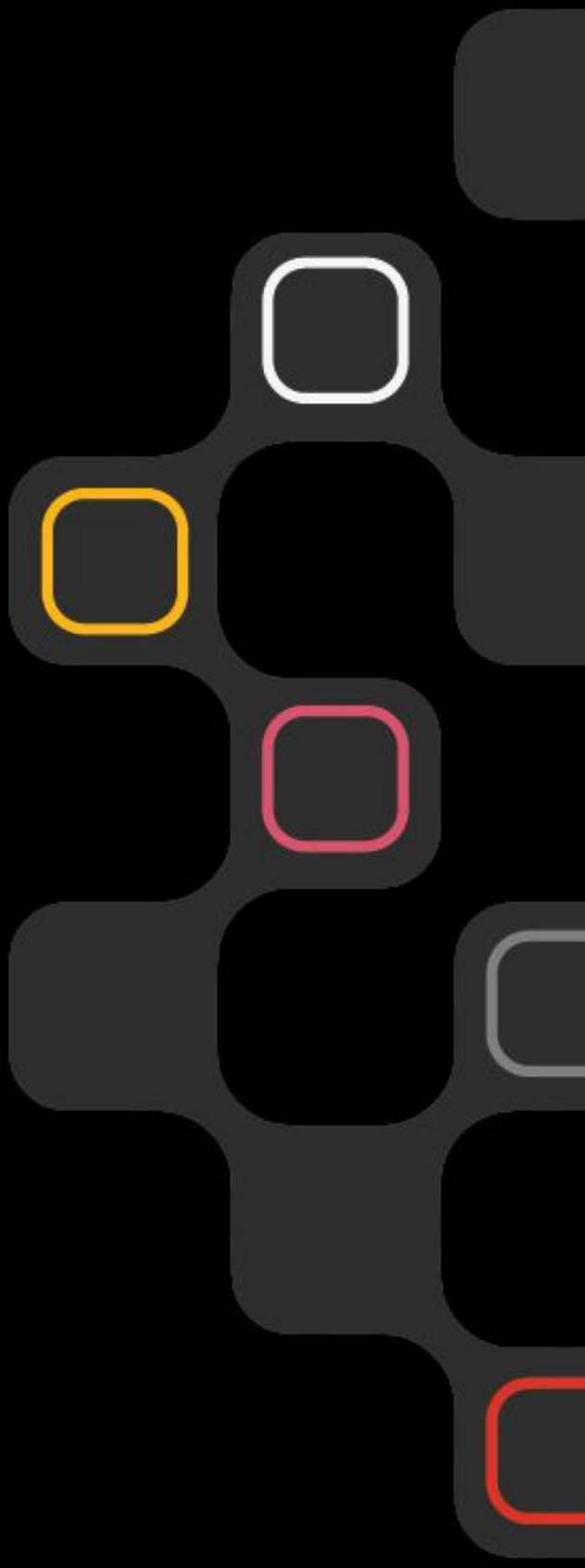
Malaysia report

Putting security at the epicentre of innovation

Findings from the 2024 Global Digital Trust Insights

Dec 2023



pwc

Content

Attention on cybersecurity has grown, but is it enough?

Although excitement and budgets for cutting-edge security programmes are increasing, the actual progress in improving security is slow, or in some cases stagnant.

PwC's 2024 Global Digital Trust Insights survey of 3,876 business and tech executives, including respondents from Malaysia, shows considerable room for improvement in cybersecurity.

Consider this: "Hack-and-leak" remains top concerns for Malaysian respondents, yet nearly a third still don't consistently incorporate data security and privacy features in their operations.

While it is encouraging to see cyber budgets in 2024 increasing at a higher rate compared to last year, further work is required to fully realise the benefits from cybersecurity initiatives. Currently, only half of Malaysian respondents are either fully or partially implementing cybersecurity but not yet realising its benefits.

With technology now at the heart of business, safeguarding it is core to protecting the enterprise. However, cybersecurity is facing four major shifts, each of which could be disruptive on its own:

- The need to modernise tech infrastructure amid cost-cutting and macroeconomic uncertainty
- Hybrid cyber threats blurring the lines between espionage and cybercrime, elevating cybersecurity to national security concerns
- The adoption of cloud and emergence of generative AI brings new threats and defence possibilities.
- Regulations requiring openness about cyber incidents could usher in a new era of transparency and collaboration

In today's innovative landscape, businesses are intertwining digital experiences with the latest technology tools. Cybersecurity must stand at the epicentre of this transformation.

Key highlights

69%

of business executives in Malaysia emphasise modernisation of technology with cyber investments

67%

worry about hack-and-leak as top cyber risk

83%

will deploy GenAI for cyber defence in the next 12 months

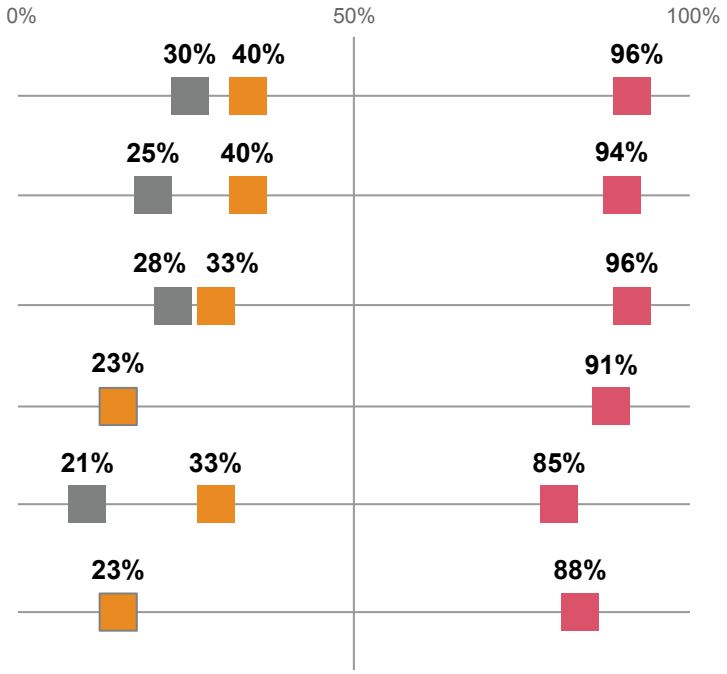
Source: PwC, 2024 Global Digital Trust Insights

Attention on cybersecurity has grown, but is it enough? (cont'd)

Malaysian businesses outpace the global average, but lag behind world's top performers*

Percentage who say that their cyber teams 'usually' (80% to 100% of the time) do this

Defence



Responds quickly to threats to emerge stronger from disruptions

Incorporates data security and privacy features into products, services, and third-party relationships

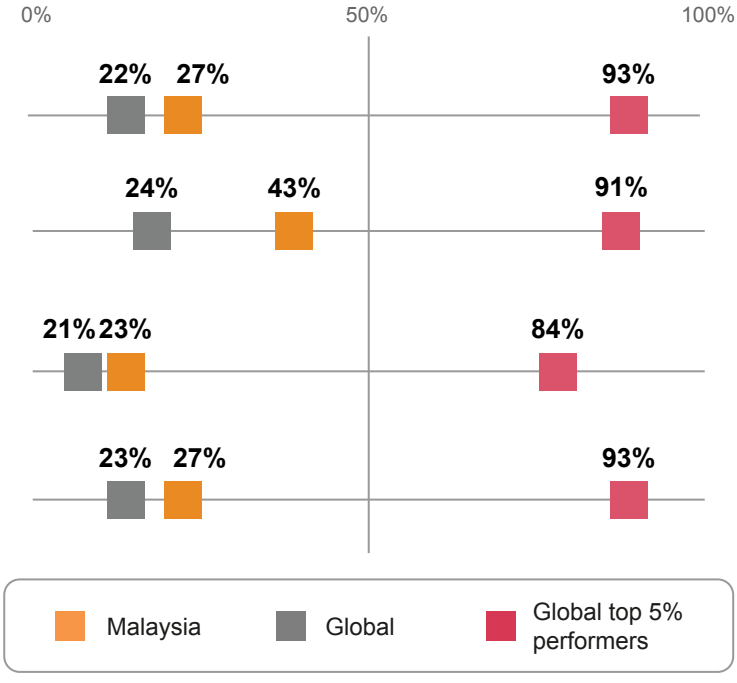
Puts controls in place throughout the organisation to prevent serious cyber disruptions

Allocates cyber budget to the top risks of the organisation

Maintains relationships with public sector to build resilience

Collaborates with other business units that affect the organisation's cybersecurity posture (e.g., software engineering, product management, procurement, etc.)

Growth disposition



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

Communicates cyber strategy and practices in a way that helps to build trust with customers and business partners

Expedites digital and other major organisational transformation initiatives (e.g., designing security and privacy into new products and services)

Brings insights on changing cyber risk exposure and mitigation measures to the CEO and board

Q26. Please indicate how consistently your organisation's cybersecurity team does the following.

*Note the sample size differences between Malaysia and the global dataset. Refer to page 15 for more information

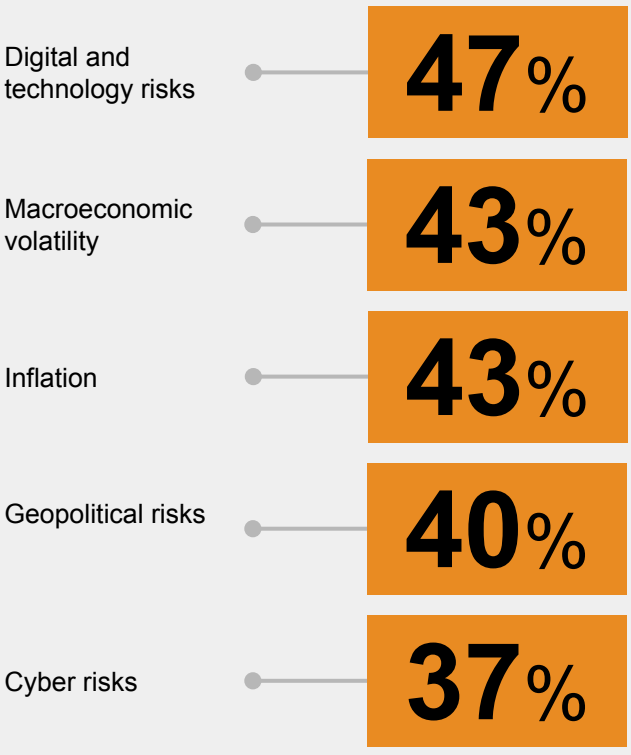
Source: PwC, 2024 Global Digital Trust Insights.

Cybersecurity at the heart of digital transformation

In line with global results, **digital and technology risks** stand out as significant concerns for Malaysian business leaders. However, it's worth noting that cyber risks rank fifth among Malaysian respondents, in contrast to their global counterparts who place it second, reflecting the perceived immediacy of other threats like macroeconomic volatility and inflation.

Digital and technology top the risk list

Risk mitigation priorities over the next 12 months (Ranked top five)



Q1. Which of the following risks is your organisation prioritising for mitigation over the next 12 months? (Ranked in top five).
Source: PwC, 2024 Global Digital Trust Insights.

However, given the increasing trend in digital transformation investments locally, it's virtually impossible to discuss digital transformation without addressing cybersecurity right away.

Hack-and-leak incidents, third-party breaches, and attacks on connected devices rank as the primary cyber threats that concern our Malaysian respondents. Evidently, data trust and cyber risk are central to today's business transformation.

This is unsurprising, considering the increased number of data breaches reported to the Personal Data Protection Department this year (the highest to date). 130 cases were reported up to June, marking a four-fold increase compared to the 30 cases recorded throughout 2022, as reported by New Straits Times.

Cybersecurity at the heart of digital transformation (cont'd)

These cyber threats are interlinked. Once malicious actors infiltrate systems and networks, they often cause extensive damage.

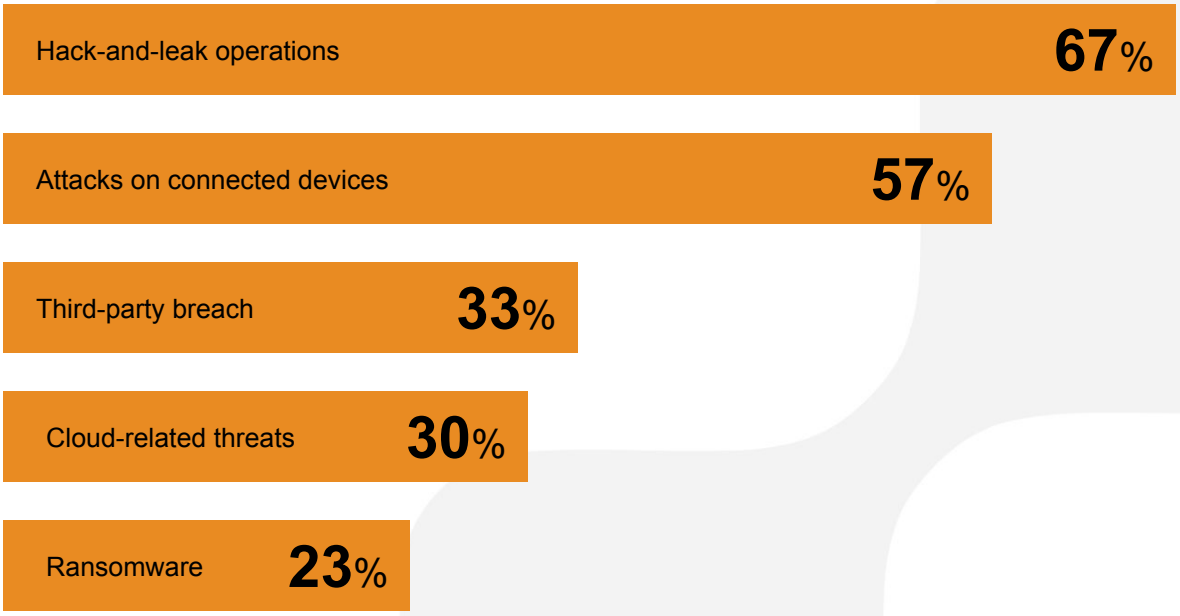
What starts as a hack can escalate into an advanced persistent threat as these bad actors remain within your system, gathering data and seeking new ways to cause harm. They might steal your data, initiate a ransomware attack, and even release the data despite paying the ransom.

Each of these incidents is problematic on its own, but when they occur together, they can severely disrupt your business operations and harm your reputation.

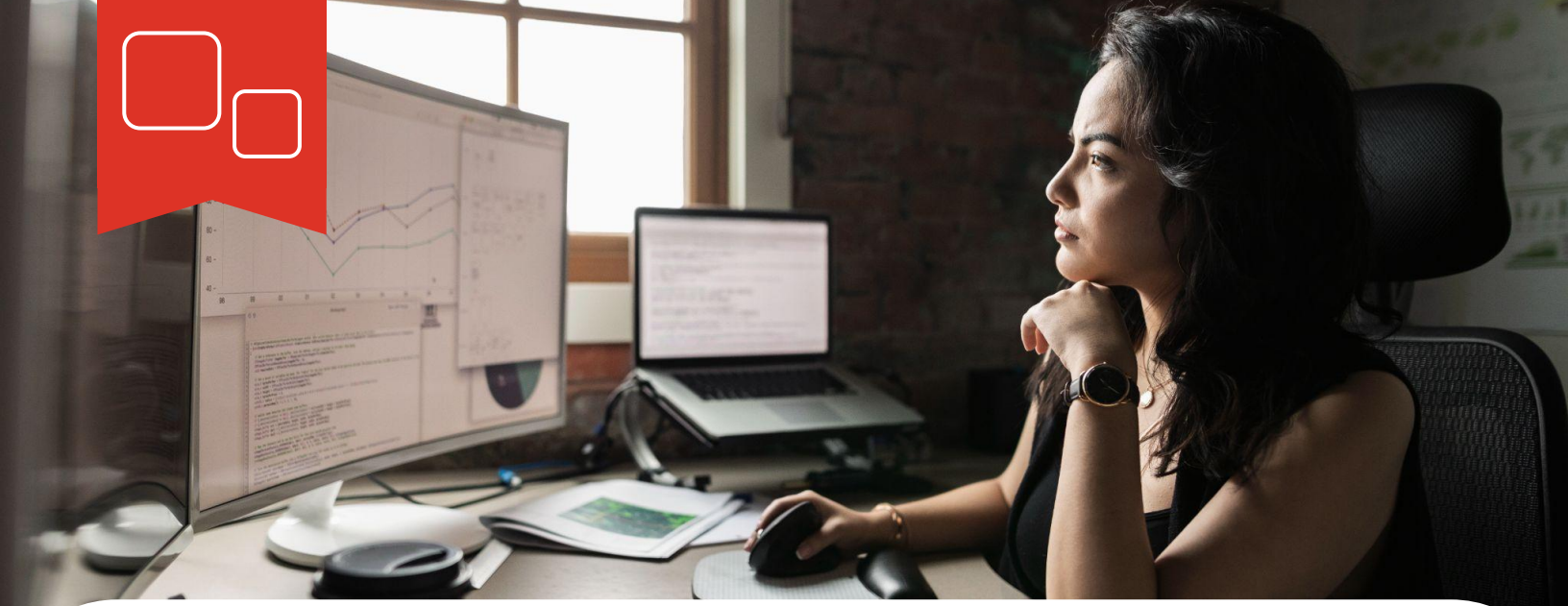
Mega breaches are on the rise in terms of frequency, scale, and cost. Globally, the percentage of those reporting incurred costs of $1 million or more for their worst breach in the past three years has increased from 27% to 36% over the last year.

Hack-and-leak incidents take the top spot

Top cyber threats over the next 12 months



Q3. Over the next 12 months, which of the following cyber threats is your organisation most concerned about? (Ranked in top three).
Source: PwC, 2024 Global Digital Trust Insights.



Cloud security: A growing challenge

Cloud use has invariably been synonymous with business innovation. It has enabled developers to seamlessly collaborate and adopt more flexible work arrangements without compromising on quality.

Cloud security ranked as the top cyber risk concern for nearly half of global (47%) respondents. In comparison, it only ranked fourth (at 30%) for Malaysian respondents. While this may allude that cloud technology is not the top priority for Malaysian organisations, it is picking up pace.

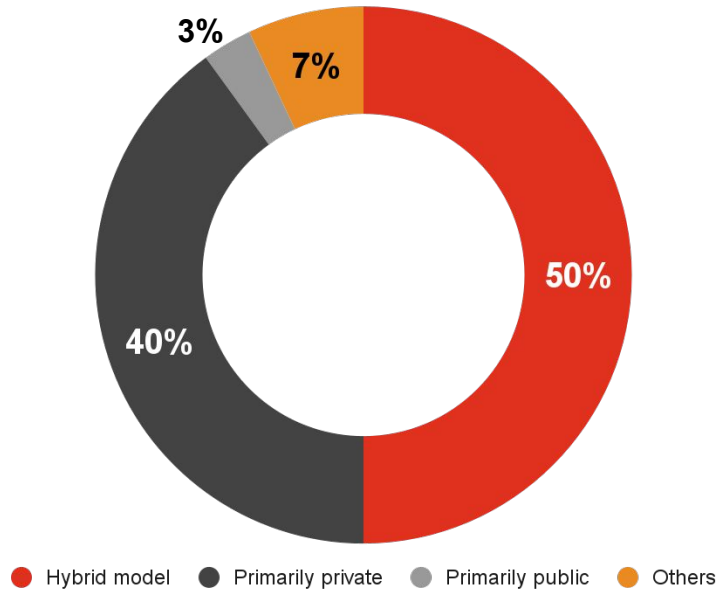
Demand for cloud services increased during the pandemic as organisations needed to ensure business continuity. In response, in February 2021, the Malaysian government approved the building of new data centres following its cloud-first strategy and the Malaysia Digital Economy Blueprint.

Besides public initiatives, Malaysian businesses also benefit from the lack of legacy infrastructure that has hindered some more mature economies from investing strategically in digital infrastructure.

Analysis shows that top performers in the survey tend to adopt a hybrid approach involving both public and private providers. They also implement agile, regularly updated plans to effectively address challenges associated with hyperscale cloud services.

Most Malaysian companies use a hybrid cloud model

Organisation's use of cloud service providers



Q16a. Which of the following best describes your organisation's use of cloud?
Source: PwC, 2024 Global Digital Trust Insights.

In a similar vein, Malaysian respondents are already taking steps in this direction, with 50% of them adopting a hybrid approach. This observation aligns with a Forrester report which highlights that 65% of Malaysian organisations deploy multiple cloud models (public, private and/or hosted private cloud).

Cloud security: A growing challenge (cont'd)

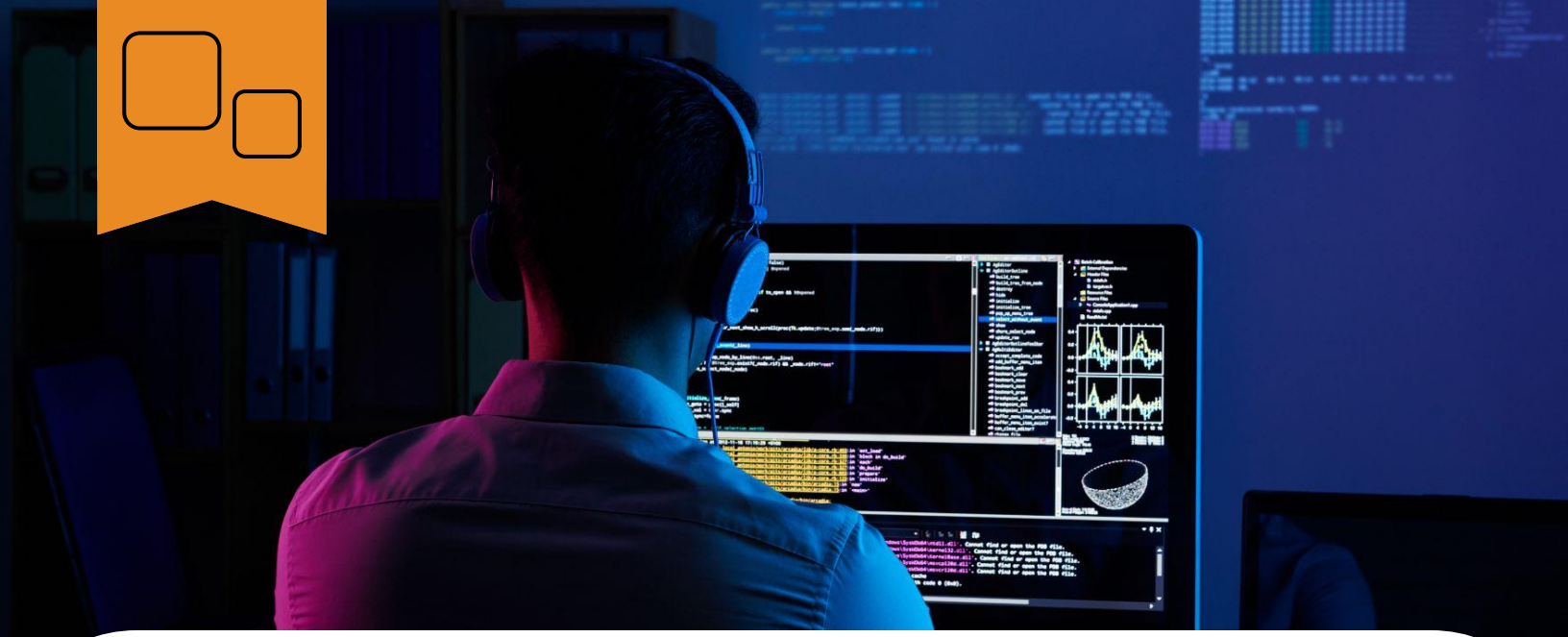
However, the growing utilisation of cloud services brings along its distinct challenges. In our 2023 Global Digital Trust Insights survey, 40% of Malaysian respondents anticipate a surge in significant cyber attacks targeting cloud management interfaces and cloud component services. This underscores the urgency for Malaysian businesses to initiate and consistently enhance their cloud risk mitigation strategy.

The C-suite challenge is this:
How do you work together and with your cloud security providers to make headway in defending the most important entry points to your systems and assets via the cloud?

So many cloud risks, so few plans to manage them

Organisation's position on cloud service provider challenges

Q19. To what extent has your organisation addressed the following challenges with your cloud service provider(s)?
Source: PwC, 2024 Global Digital Trust Insights.



Generative AI usage for cyber defence on the rise

According to a report by MyDIGITAL, Generative AI (GenAI) holds the key to unlocking an estimated USD$113.4 billion in productive capacity for Malaysia—equivalent to 28% of GDP in 2022. Workforce sentiments generally support this as 50% of Malaysian respondents in PwC's Asia Pacific Workforce Hopes and Fears 2023 survey say GenAI will help them increase productivity at work.

This trend extends to using GenAI for cyber defence in instances where cyber teams are overwhelmed by the sheer number and complexity of human-led cyber attacks, both of which continually increase.

GenAI for cyber defence

83%

Malaysian respondents say they'll use GenAI for cyber defence in the next 12 months

50%

are already using it for cyber risk detection and mitigation

37%

are already seeing benefits to their cyber programmes because of GenAI - mere months after its public debut

Q7. To what extent do you agree or disagree with the following statements about Generative AI?
Q10. To what extent is your organisation implementing or planning to implement the following cybersecurity initiatives?
Source: PwC, 2024 Global Digital Trust Insights.

Generative AI usage for cyber defence on the rise (cont'd)

Vendors are pushing the envelope on what GenAI can achieve. Some of which have started to bundle their large language models together with their cyber tech solutions. Microsoft Security Copilot intends to provide GenAI features for security posture management, incident response and security reporting. Google announced Security AI Workbench for similar use cases.

The three most promising areas for GenAI use in cyber defence are:

Threat detection and analysis

Cyber risk and incident reporting

Adaptive controls

But for businesses to fully unleash GenAI's capabilities in cyber defence, they will need a ready workforce. It is inevitable that upskilling is required, and Malaysian employees are aware of this.

42% think that AI will create opportunities for them to learn valuable new skills

28% believe AI will require them to learn new skills that they are not confident they have the capacity to learn

68% think that digital skills are important to their career

Source: PwC, Asia Pacific Workforce Hopes and Fears 2023 survey

The C-suite challenge is this: How do you wield the new tools without inviting **new risks** to flare up in the organisation and in society? What should you do to **upskill your workforce**?

Regulations: Providing a safe place to play and grow

According to our recent 26th Annual Global CEO Survey, 63% of Malaysian CEOs see regulatory change as the primary source of potential industry disruption. While conventional wisdom suggests that new regulations can hamper revenues, a substantial number of respondents believe that regulations can boost confidence to explore, experiment, innovate and compete.

Malaysians are particularly concerned about three types of regulations for ensuring their organisation's future growth: privacy rights harmonisation (47%), mandatory reporting of cyber risk management (43%) and operational resilience requirements (43%).

Malaysians can expect changes to these areas as several regulations are being updated to enhance the country's resilience against cyber threats. For example, a new Cybersecurity Bill is set to be tabled in 2024 and efforts are underway to update the Personal Data Protection Act (PDPA), incorporating provisions such as mandatory breach notification, data protection officer requirements and a revamp of cross-border data transfer policies.

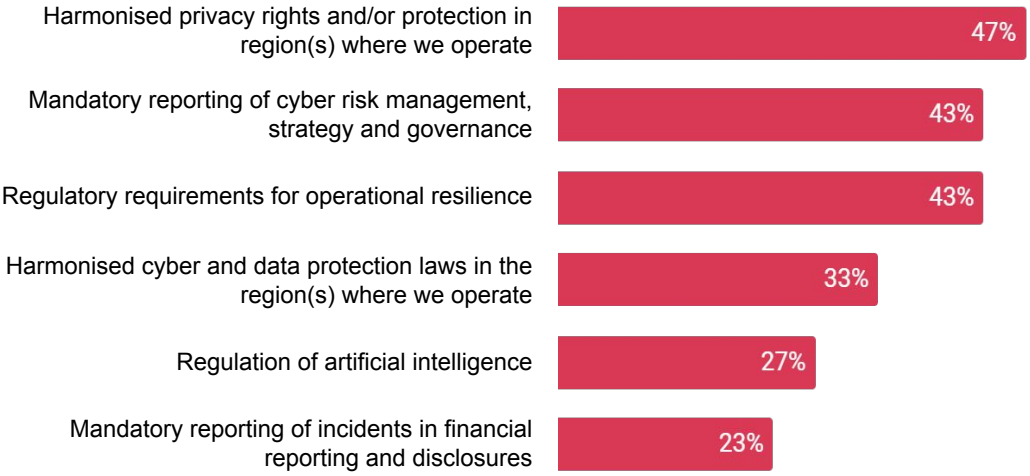
As 5G and AI take centre stage, efforts are underway to align regulations with the challenges and opportunities these technologies bring. RM60 million has been allocated in Budget 2024 to CyberSecurity Malaysia for developing a 5G Cyber Security Testing Framework and promoting local 5G expertise to manage cyber vulnerabilities during the transformation.

While Malaysian respondents currently prioritise AI regulation (27%) less than their global counterparts, the impending impact of AI technology has prompted the government to consider creating a legal framework through a proposed AI Act. The proposed Act will provide a legal dimension to the National Artificial Intelligence Roadmap 2021-2025, which currently serves as a guideline for responsible AI development.

Regulations: Providing a safe place to play and grow (cont'd)

Regulations that could change cybersecurity

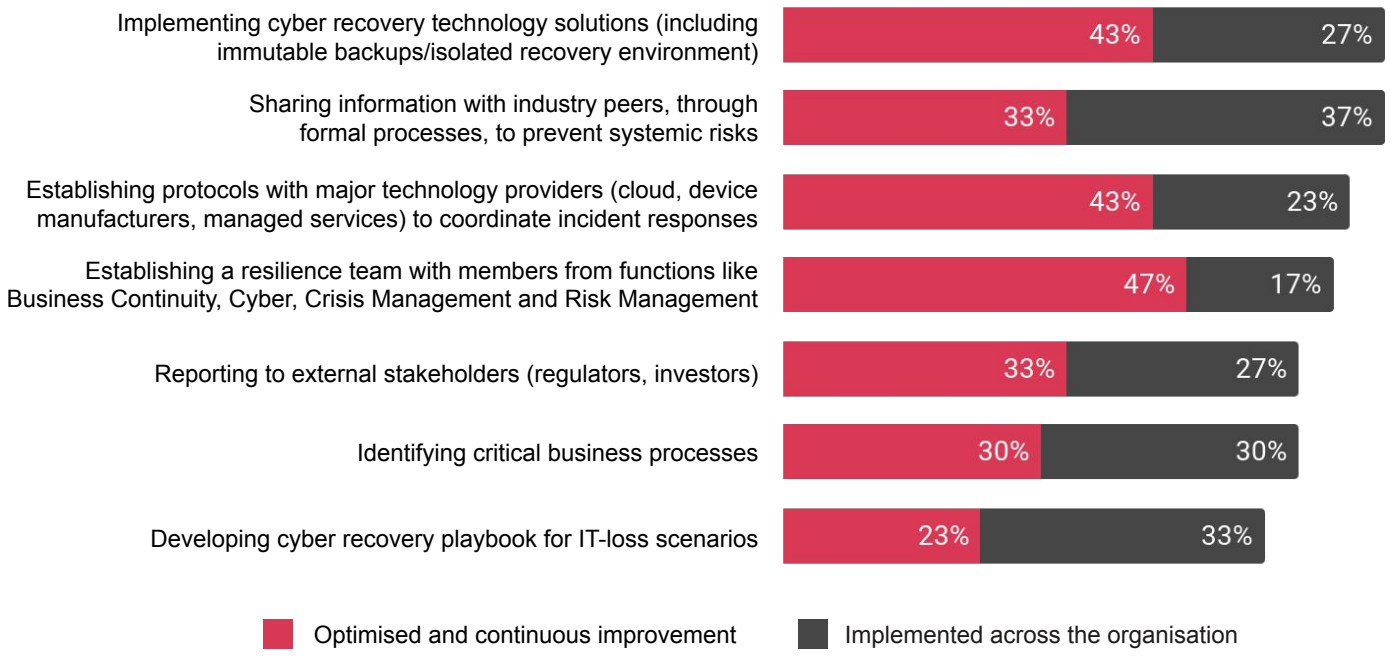
Regulatory goals and principles with the greatest impact to organisation's future revenue growth (Ranked top three)



Q24. Which of the following proposed regulatory goals and principles will have the greatest impact on your organisation's ability to secure future revenue growth? (Ranked in top three).
Source: PwC, 2024 Global Digital Trust Insights.

The slow progress on cyber resilience

Extent of implementation for key cybersecurity resilience actions



Q8. To what extent is your organisation implementing or planning to implement the following cyber resilience actions?
Source: PwC, 2024 Global Digital Trust Insights.

Regulations: Providing a safe place to play and grow (cont'd)

Malaysian organisations are taking charge of the situation through cyber resilience initiatives, such as implementing cyber recovery technology solutions (70%) and sharing information with industry peers to prevent systemic risks (70%).

However, more needs to be done to shield businesses from cyber threats. Based on a report by Cisco, organisations in Malaysia exhibited the lowest average security resilience score in the Asia Pacific region, with 80% having experienced a security incident in the last few years.

Global top performers in cybersecurity show us that prioritising investment in cyber capabilities is effective in defending businesses against cyber threats. 85% of them will be increasing their cyber budget in 2024, with 19% planning an increase of 15% or more. In Malaysia, only 10% plan to match this allocation in their budgets.

The best in class are more likely to have effective systems to protect them against serious cyber breaches (damages worth more than US$1 million). These companies are also likely to be more mature in terms of optimising cyber resilience actions and implementing cybersecurity initiatives.

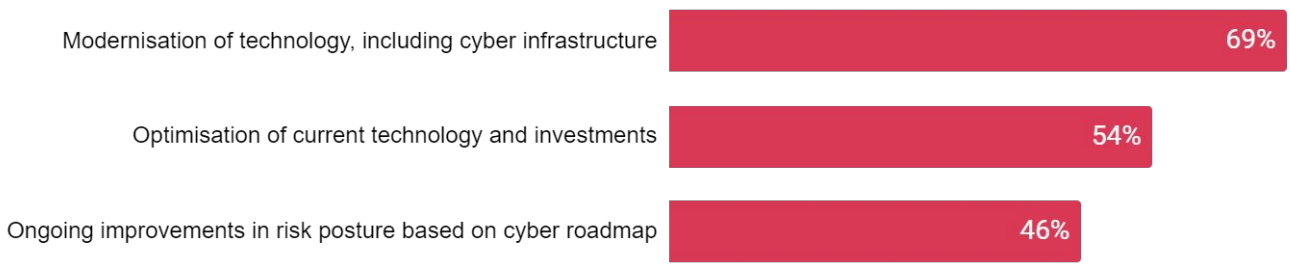
It is encouraging to see that simplifying cybersecurity tools remains a priority, with modernisation and optimisation being the key investment focus for 2024. Over two-thirds of Malaysian business leaders prioritise technology modernisation, while around half aim to optimise existing technologies and investments.

As new regulations surface, Malaysian organisations can glean insights from global peers and identify challenges in their cybersecurity plans early to sidestep regulatory compliance hurdles. Getting involved at the outset, such as by engaging in dialogue with ecosystem players and actively collaborating with regulators, is a vital step in building the path toward enhanced resilience.

The C-suite challenge is this: Amid regulatory uncertainty, can you give your organisation the room to innovate while keeping security and privacy by design? How do you turn this new regulatory environment into a source of competitive advantage?

2024 cyber budgets aim to modernise and make the most of existing tools

Malaysia business leaders - Cybersecurity investment priorities over the next 12 months (Ranked top three)



Q14b. Which of the following investments are you prioritising when allocating your organisation's cyber budget in the next 12 months? (Ranked in top three).
Source: PwC, 2024 Global Digital Trust Insights.

Dare to break cyber-as-usual

In 2024, do you dare to break out of the stasis and make the one or two bold moves in cybersecurity that will shield your organisation from threats? Some companies are already making strategic choices. The possibilities are diverse, so what's the best path for your organisation?

Here are some points to consider:

Welcome cyber into the boardroom

Cybersecurity is a key concern for most companies, but is it a regular focus in your boardroom? Are you receiving valuable insights not only on cyber risks but also on how strategic initiatives impact business growth? Security is the foundation for various aspects of your business, and addressing your cybersecurity program head-on is crucial for the success of these initiatives

Position cybersecurity as as a driver for innovation

Business transformation and cyber transformation go hand in hand. The business and cybersecurity executives should treat cybersecurity as a competitive advantage to protect valuable assets, safeguard the brand and drive innovation for cost savings and growth.

Try new ways of managing cyber risks

Use more sophisticated approaches to cyber-risk modelling, such as scanning for threats using formulas specific to your company's sector, vision and strategy. Consider creating a risk-linked performance incentive for employees, or introducing a bug bounty programme that rewards independent security research. Adopt a cloud-first, centrally managed identity solution to secure your business expansion goals.

Use GenAI and automation to afford your team more time for creative thinking

Automation, GenAI and managed services offer continuous monitoring, while also handling routine tasks. This frees your teams from repetitive work, allowing them to focus on addressing new cyber threats and developing innovative ways to counter evolving threats.

Speak the language of trust, beyond regulatory compliance

Engage early to shape new rules in a way that promotes business success. Your expertise and experience in AI, the metaverse, cryptocurrency and privacy can offer valuable insights on these critical regulatory issues. Keep in mind that regulators may also grapple with the intricacies of cyber and tech.

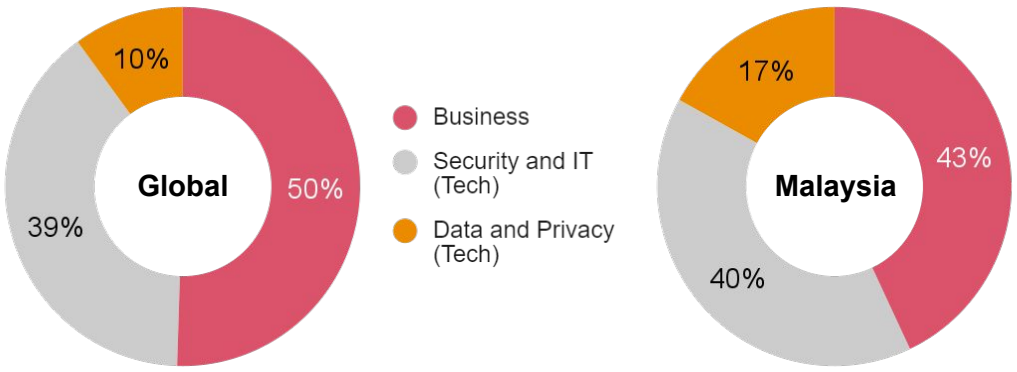
About the survey

The 2024 Global Digital Trust Insights is a survey of 3,876 business, technology and security executives (CEOs, corporate directors, CFOs, CISOs, CIOs and C-Suite officers) conducted in the May through July 2023 period. 683 were Asia Pacific respondents and 30 were from Malaysia.

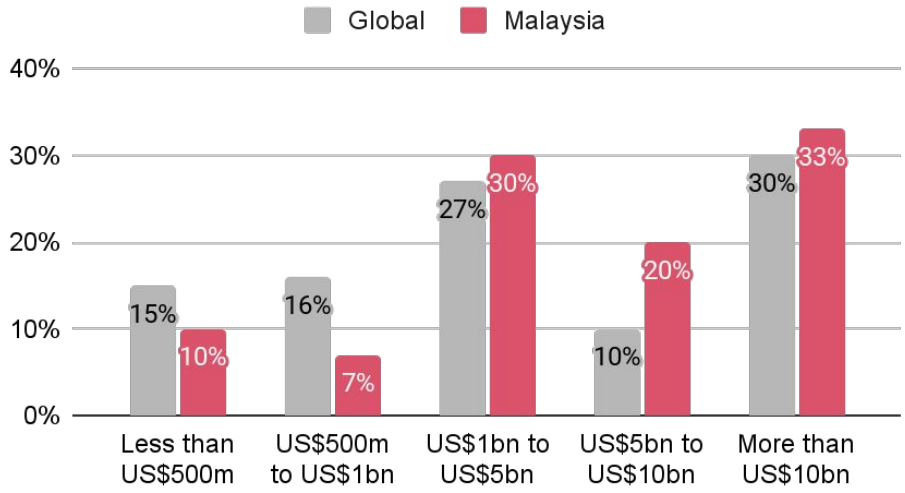
The Global Digital Trust Insights Survey had been known as the Global State of Information Security Survey (GSISS). In its 26th year, it's the longest-running annual survey on cybersecurity trends. It's also the largest survey in the cybersecurity industry and the only one that draws participation from senior business executives, not just security and technology executives.

Demographics

Job title



Company revenue



Contact us

Elaine Ng
Partner, Financial Services and
Risk Services Leader
PwC Malaysia

yee.ling.ng@pwc.com

Clarence Chan
Partner, Digital Trust & Cybersecurity Leader
PwC Malaysia

clarence.ck.chan@pwc.com

Alex Cheng
Director, Cyber Threat Operations
PwC Malaysia

alex.ct.cheng@pwc.com

Tanvinder Singh
Director, Cyber and Forensics,
PwC Malaysia

tan.singh@pwc.com