Digital Trust Insights 2023: The Southeast Asia Perspective

Southeast Asia leaps forward to a cyber-ready future

Southeast Asia faces a challenging cybersecurity landscape

This decade of digital change has brought a new paradigm of productivity and innovation in Southeast Asia – digital tools and modern internet capabilities have become essential, helping to pave a pathway to long-term prosperity and growth. Post-Covid-19, businesses and institutions all over the world are embracing distributed and diverse information technology (IT) setups to ensure business resilience and explore new growth opportunities.

However, these businesses' needs have created an emerging set of risks for cybersecurity professionals, as the accelerating adoption of digital tools has expanded the range of available 'attack surfaces' for cybersecurity threats. Meanwhile, complex technology stacks pose challenges for legacy cybersecurity solutions.

An increasingly digitally connected Southeast Asia poses ripe opportunities for adversaries to exploit existing and emerging vulnerabilities and risks in a region already challenged by significant cybersecurity incidents and lagging regulatory actions. Research has shown that the Southeast Asia region remains a hotspot for cybersecurity threats[1].

Fortunately, cybersecurity professionals in the region are responding in kind.

PwC recently conducted a survey of C-suite executives on their cybersecurity progress since 2020 and found that spending on cybersecurity in Southeast Asia has surged over the years as leaders zero-in on their biggest risks[2]. Cybersecurity has also risen to the top of boards' priority lists as an increase in threats and large-scale data breaches has become more common, placing their customers at risk.

Based on the survey findings, this report explores what cybersecurity progress has been made in Southeast Asia since 2020, and what challenges leaders and decision makers expect to see grow in importance in future.

[1] Shannon Williams, "Cybersecurity loopholes prevalent in South East Asia," SecurityBrief, September 27, 2022, https://securitybrief.asia/story/cybersecurity-loopholes-prevalent-in-south-east-asia

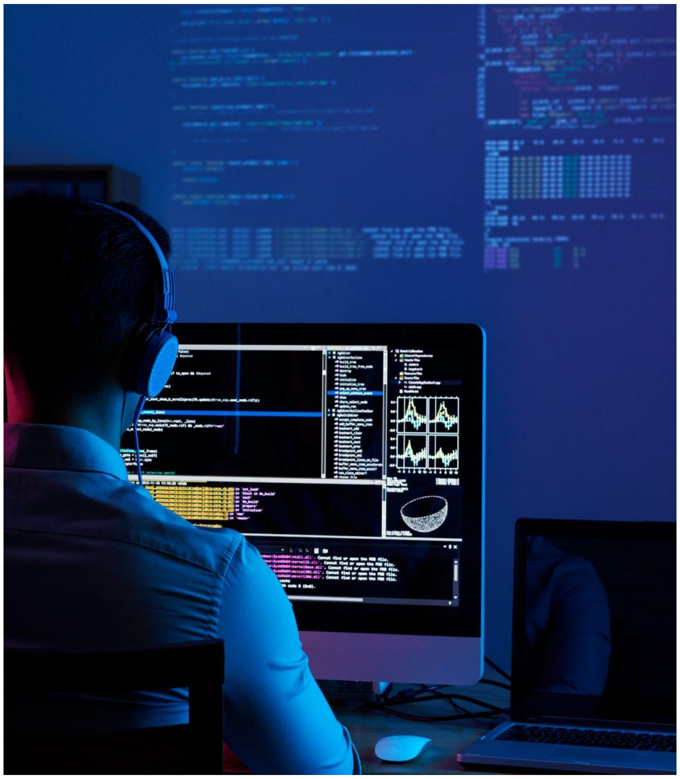
[2] This report on the state of Southeast Asian cybersecurity is derived from PwC's 2023 Global Digital Trust Insights report, which can be accessed at https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html

Cybersecurity progress in Southeast Asia

Companies are taking action to become cyber-ready amid a heightened threat landscape

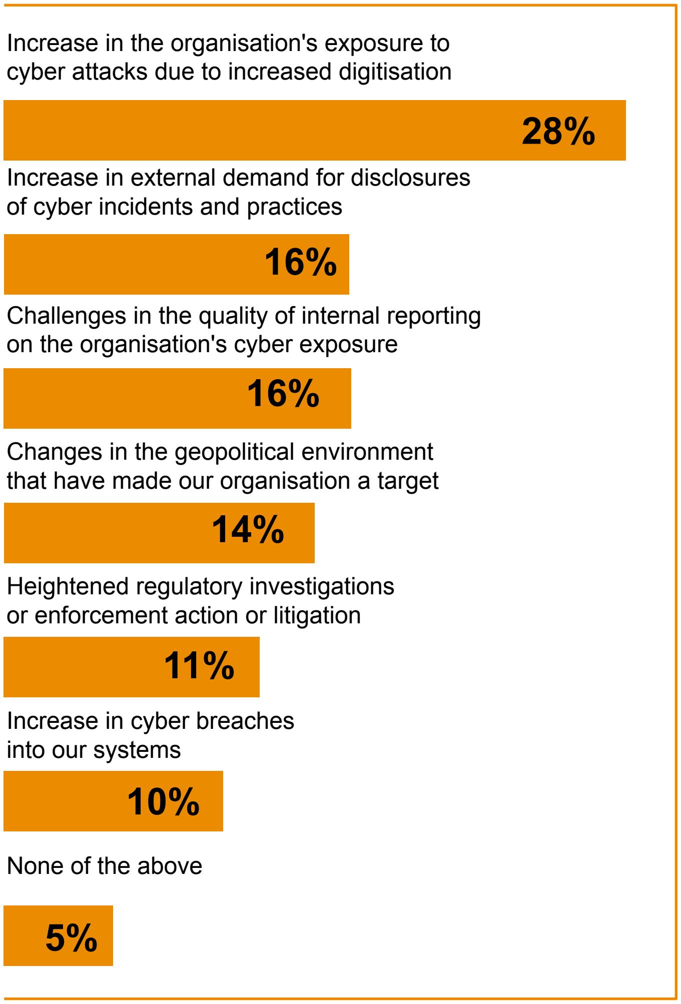
Amid Southeast Asia's immense diversity, there are distinct commonalities between countries as reflected in their shared histories and long-established connections. This is true even from a cyber perspective – as countries across the region rapidly digitalise, they are faced with similar opportunities and struggle to deal with the same risks posed by emerging technologies.

According to PwC's survey, since the start of the decade, Southeast Asian companies have seen the threat of cyber-attacks rise significantly in line with increased digitalisation of their operations (28%), mirroring a global trend.



Digitalisation drives Southeast Asia's cybersecurity threat exposure

Which of the following has your organisation experienced since 2020? (Ranked top only)



Source: PwC 2023 Global Digital Trust Insights Survey

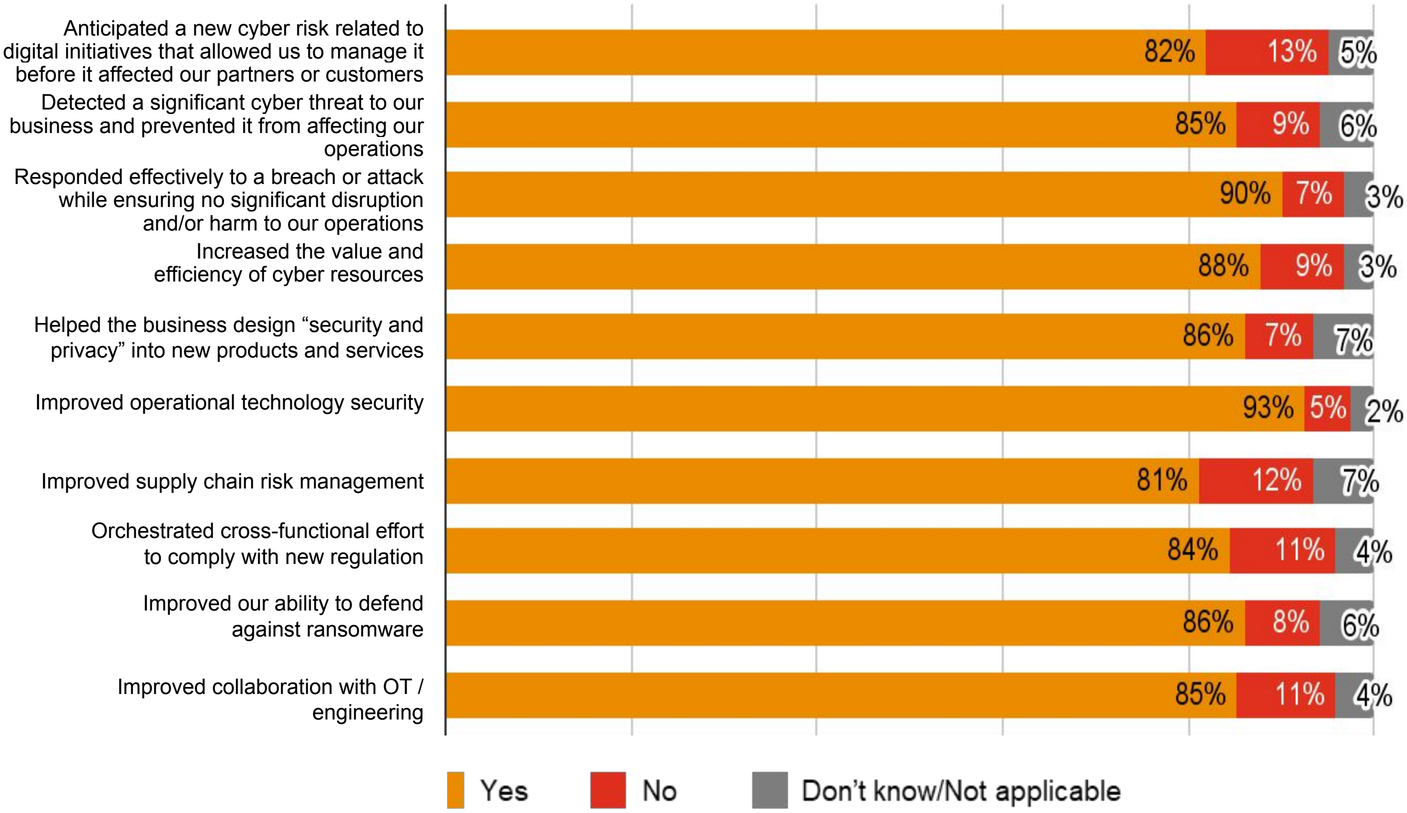
Southeast Asia's leaders are rising to the challenge by devoting more resources and attention to mitigate their cybersecurity risks. In 2021, cybersecurity spending in Southeast Asia topped US$3.2 billion, with expectations that this will increase 14% to reach US$6.1 billion by 2026[3]. The growing prevalence of data breaches and their impact on companies' reputations and investor value have pushed board members and the C-suite to exert more oversight and involvement on cybersecurity risks.

There is also a high degree of confidence among Southeast Asian companies that their cybersecurity teams have made improvements in mitigating their cyber risks over the last year, especially those associated with enabling remote and hybrid work (86%), accelerated cloud adoption (82%) and increased data volumes (82%).

Cybersecurity teams also score high marks when it comes to improving operational security (93%) and responding to cyber breaches or attacks (90%). Notably, Southeast Asian executives report more progress than their global counterparts, reflecting the region's strong efforts to close the gaps created by their relative nascency on the cybersecurity front.

Southeast Asia cybersecurity teams are ahead of their global counterparts

Has your organisation's cybersecurity team accomplished the following in the past 12 months? (Southeast Asia)



Source: PwC 2023 Global Digital Trust Insights Survey

Note: The percentages may not add up to exactly 100% as a result of their rounding to the nearest whole number.

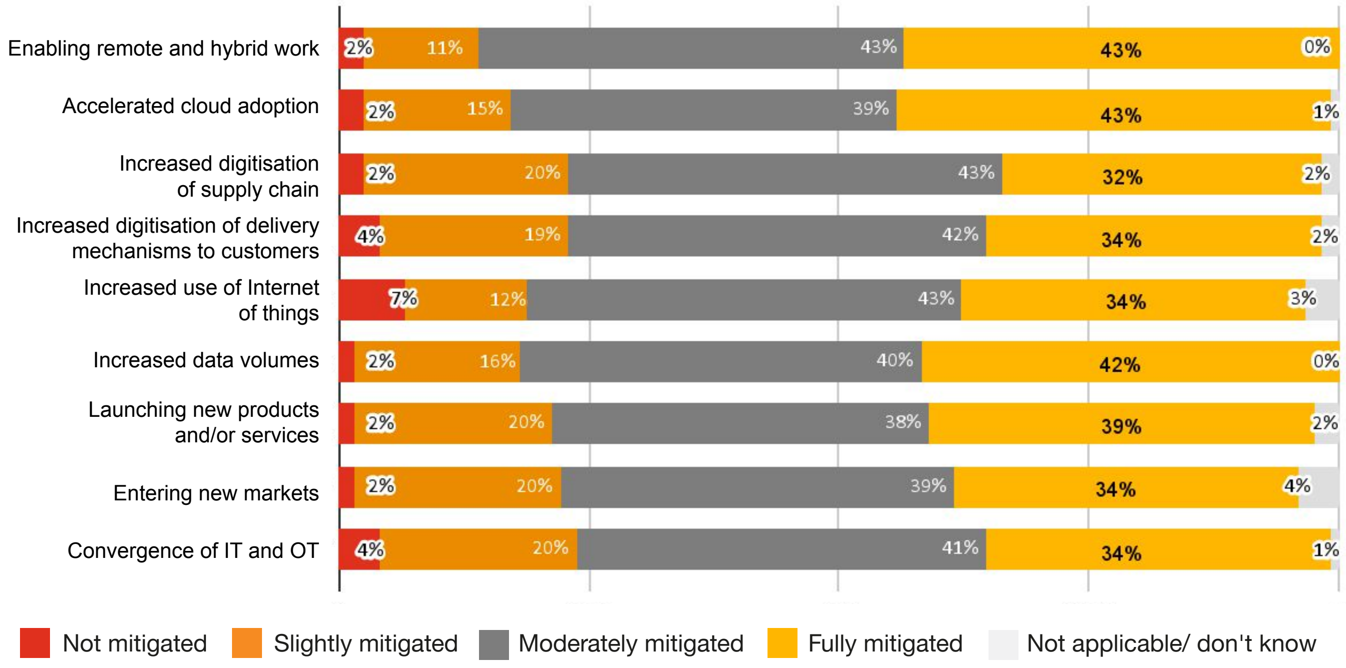
[3] "Cybersecurity Remains a High Priority in Southeast Asia as Organizations Embrace Digital-First Era and the Rise of Digital Sovereignty Concerns in the Region, Says IDC," IDC, October 26, 2022, https://www.idc.com/getdoc.jsp?containerId=prAP49798022

However, Southeast Asian companies still have a long way to go as rapid digitalisation across entire organisations poses an unending list of cybersecurity challenges. Compared to other parts of the world, Southeast Asia's cybersecurity regime is more nascent, and its cybersecurity workforce is smaller in relative terms. This has knock-on effects for their ability to ably respond to digitalisation risks – for example, though hybrid / remote work and data-based decision-making are the future, more than half of Southeast Asian firms have not fully mitigated their associated risks.

As a result, only 17% of companies have fully mitigated their digitalisation-related cybersecurity risks. That being said, Southeast Asian firms appear to perform slightly ahead of global averages (15%), perhaps suggesting that the region is on a strong upward trajectory[4].

Remote work and cloud adoption lead to increased cybersecurity risks for Southeast Asia

On a scale of 1 to 10, to what extent has your organisation mitigated the cybersecurity risks associated with each of the following in the last 12 months?



Source: PwC 2023 Global Digital Trust Insights Survey

Note: The percentages may not add up to exactly 100% as a result of their rounding to the nearest whole number.

[4] This is in reference to digitalisation-related risks, such as enabling remote work; accelerated cloud adoption; increased digitalisation of supply chains; increased digitisation of delivery mechanisms to customers; increased use of Internet of Things; increased data volumes; and convergence of IT and OTT.

Facing a challenging landscape with better governance

Looking ahead, Southeast Asian companies will continue to face more cybersecurity risks as cloud and digital technology adoption grow in importance.

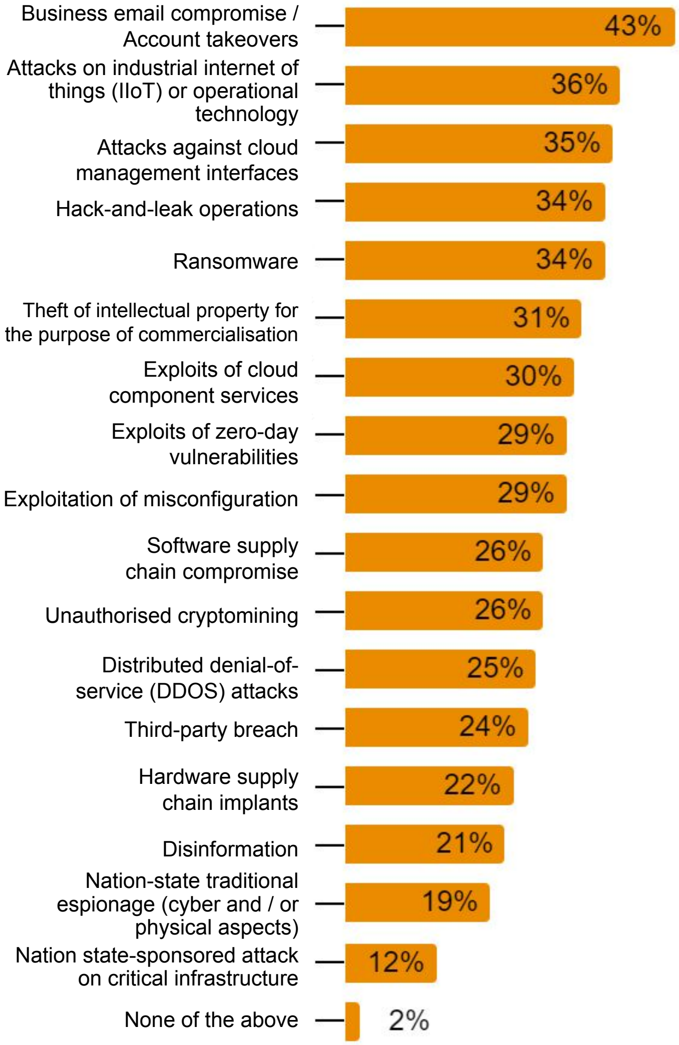
According to the survey, cloud-based pathways (47%) and web-based applications (46%) are expected to pose the biggest cybersecurity risks for Southeast Asian firms, although human / user errors (43%) will also play a considerable role. Executives are also wary of the risks posed by specific pathways into their companies' internal operations such as business emails and online accounts (43%), but also internet of things (IoT) devices and operational technologies (36%).

Many companies in Southeast Asia struggle with internally reporting on their cyber exposure, revealing that cyber risk mitigation remains fairly early-stage. This is underscored by the fact that companies in the region do not report significant increases in pressure to externally disclose their cyber incidents and practices, likely due to the under-development of regulatory frameworks.

However, some countries in the region reflect growing cyber legislation. Boards of companies in these countries are clearly focused on the impact of cyber risks on their business.

External adversaries are the chief source of cybersecurity risks in Southeast Asia

Which of the following attacks to your organisation do you expect to significantly increase in 2023 compared to 2022?



Source: PwC 2023 Global Digital Trust Insights Survey

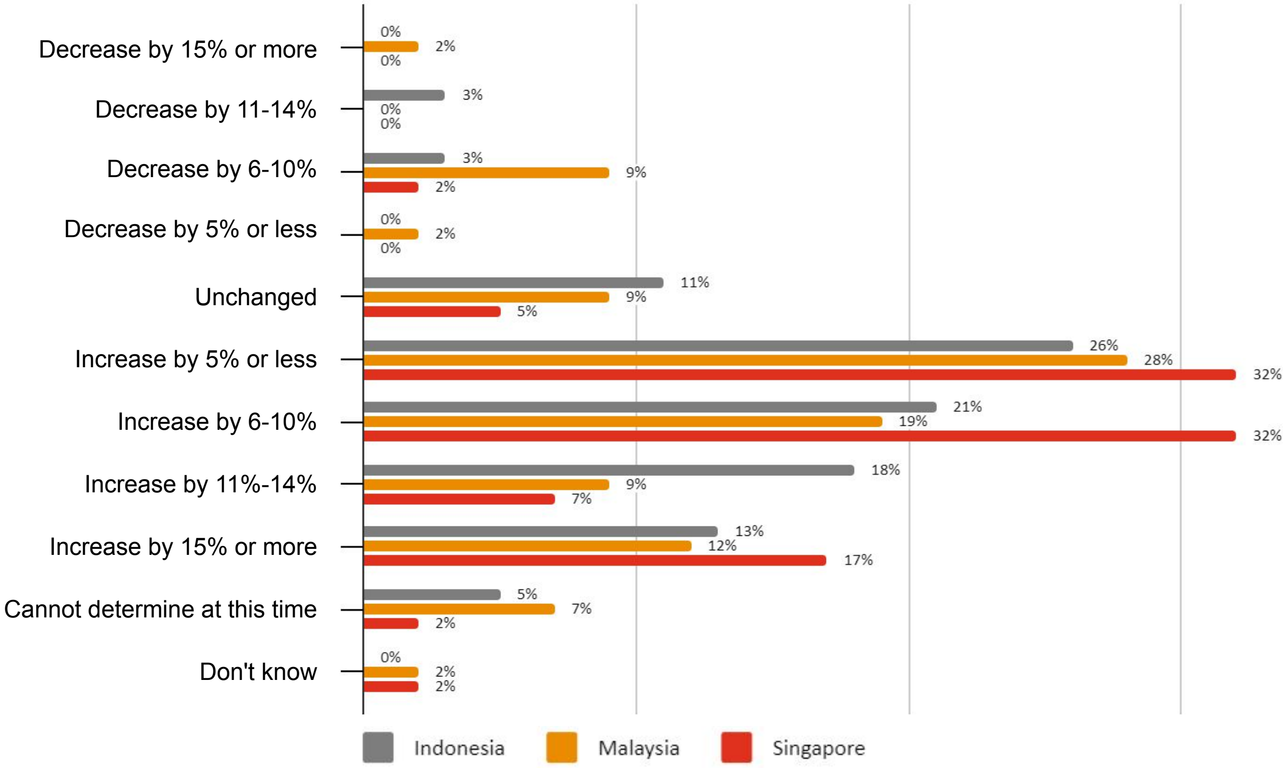
To meet these challenges, Southeast Asian firms are more likely to expand their cybersecurity teams' access to resources such as manpower and budgets at a higher rate than their global counterparts. In 2023, most Southeast Asian companies (78%) expect their cybersecurity budgets to increase, with especially strong optimism among Singapore (88%) firms. Comparatively, only 65% of firms globally say the same.

Meanwhile, improving overall governance of cybersecurity is top of mind for the leadership in Southeast Asia, compared to other regions, pushing leaders to seek ways to embed cybersecurity as part of the board-level discussion.

More work needs to be done in terms of how companies handle, protect and dispose of personal data. Less than half of firms say that their cybersecurity teams have exceptionally delivered actions that would bolster consumer trust in their data security and privacy practices, or protect them from regulatory actions. These issues will only grow in importance, especially as data privacy and cybersecurity laws accelerate across the region. Over the course of a single year, three countries in the region issued legislation to protect consumer information[5].

Cybersecurity budgets are growing in Southeast Asia

How is your organisation's cyber budget changing in 2023?



Source: PwC 2023 Global Digital Trust Insights Survey

Note: The percentages may not add up to exactly 100% as a result of their rounding to the nearest whole number.

[5] A C-suite united on cyber-ready futures (PwC, 2022), https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/assets/pwc-2023-global-digital-trust-insights-main-report.pdf

C-suite playbook on cybersecurity

Board governance of cyber risks essential in building cybersecurity culture

There has been a significant shift in terms of how companies think about cybersecurity – it is no longer an issue for just IT executives, but a matter of board governance.

Almost 80% of Southeast Asian board members say their companies' growing exposure to cyber risks due to increased digitalisation has been the chief influencing factor in their decision to become more personally involved in cyber matters – almost 10% more than in other regions, where an increase in cyber breaches was a bigger factor.

Southeast Asian board members are becoming more proactive in cyber affairs due to their firm's growing exposure to cyber threats.

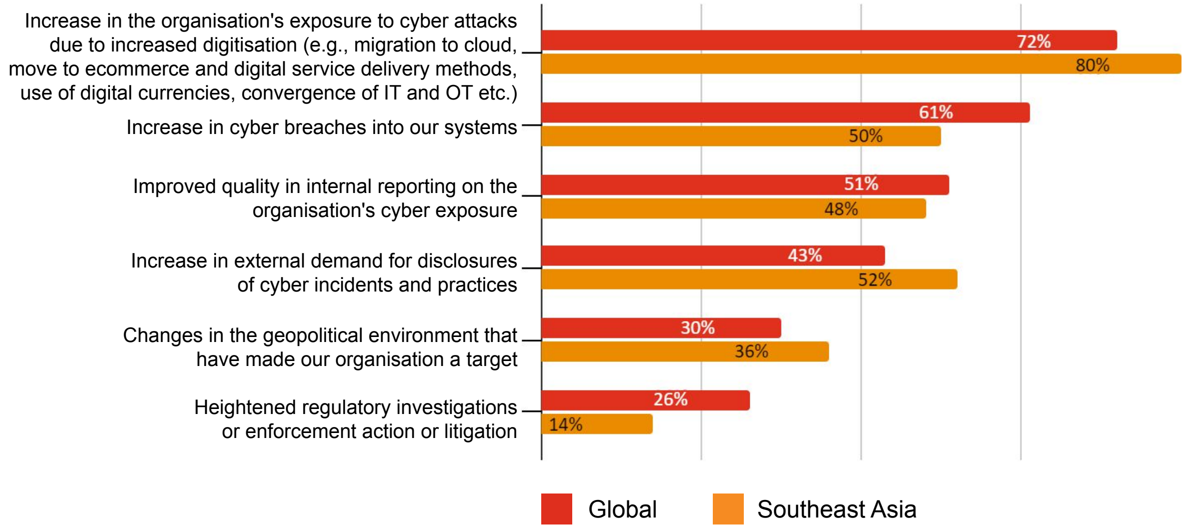
However, a secondary but increasingly critical driver of board involvement in the region is the heightened demand for external reporting for disclosures of cyber incidents and practices (52%). Though most board members are not cybersecurity domain experts, they are expected to understand, govern and mitigate these risks.

Some speculate that regulators in the region could soon require companies to disclose their cybersecurity governance capabilities.This includes the board's oversight of cyber risk, and how the management assesses and manages cyber risks. There is also the added expectation of more internal cybersecurity reporting (48%) as attacks can exert devastating effects on shareholder value and investor interest.

Board members in Southeast Asia do demonstrate some ability to govern cybersecurity risks in their companies. In particular, they are considered 'very effective' when it comes to aligning cyber investments and their most important risks (64%) and monitoring their firms' resilience to threats (60%), compared to their global counterparts.

As data breaches become more common, board members look to get involved

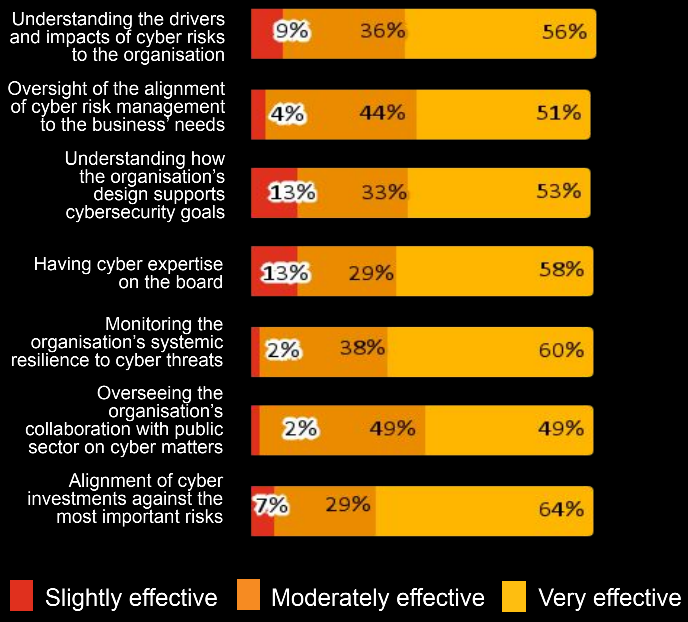
Of the following events which your organisation has experienced since 2020, which, if any, have influenced you / the board to become more personally involved in cyber matters in your organisation? (Ranked in top three)



Source: PwC 2023 Global Digital Trust Insights Survey

Board members in Southeast Asia outperform global peers

In your view, how well does your board exercise governance over the following areas of cybersecurity in your organisation today?



Source: PwC 2023 Global Digital Trust Insights Survey

Note: The percentages may not add up to exactly 100% as a result of their rounding to the nearest whole number.

To fill gaps in their subject knowledge, Southeast Asian leaders are focusing on improved reporting mechanisms (69%) and more internal and external training for board members (53%).

However, one hurdle to better cybersecurity governance may lie in the disparities between board and C-suite priorities. Board directors tend to focus on reputational and financial risks, while chief information security officers (CISOs) are concerned with service and operational disruptions.

The survey reflects this dissonance: a fifth (20%) of board members say improvements are needed in terms of how the organisation's cybersecurity and overall strategies align, while 42% have only somewhat effective cyber expertise on their board. Thus, slightly fewer Southeast Asian executives (54%) can describe their board's cyber expertise, compared to global averages (59%).

This misalignment between board and C-suite priorities can create significant impacts in terms of how cybersecurity risk is understood—and thus, governed—and how much focus is allocated.

As a result, 39% and 46% of Southeast Asian executives say that their cybersecurity budgets are not informed by or well-allocated against quantifications of cybersecurity risks. These numbers are slightly lower than the global averages (49% respectively) but they demonstrate the disjunction between priorities that can impede significant impact from board-level governance.

Call to action:

Boosting board expertise and bridging terminology gaps

The board should see its role as directly in conversation with the needs of CISOs and their teams. Business and IT imperatives are not at cross-purposes, but two sides of the same coin, which is why boards must gain the necessary expertise to provide governance and advice on this issue. On their part, boards may want to explore adding members with cybersecurity expertise. Organisations can also play a part by taking the initiative to provide more training for board members from both internal and external parties to equip them with the ability govern cybersecurity risks with confidence.

With good training and exercises, board members can better understand how poor cybersecurity can result in not just financial impacts due to fines or compensation but also immense reputational damage and lost business. In the long term, these issues can affect stock prices, thereby emphasising their relevance to the board's governance responsibilities.

Cybersecurity risks should be integrated into the company's overall risk map as key components of their operational and strategic decision-making processes. In doing so, boards can increase the amount of time allotted to cybersecurity matters by making it a routine part of regular C-suite updates, while also meeting stakeholder demand for more transparency and disclosure.

CISOs also have a part to play in bridging the language barrier with boards by simplifying or preparing intuitive presentations that help members understand how cybersecurity risks interact with business goals and objectives. These risks can be quantified with relevant metrics or familiar financial numbers, presented in a visual format such as a scorecard or dashboard.

Bolster cloud security to realise the promise of the remote-work revolution

The hybrid work revolution has been the defining work trend of the post-pandemic reality. The health crisis prompted a global work-from-home experiment, and its long-term impacts are already visible in the growing popularity of remote work and distributed workplaces.

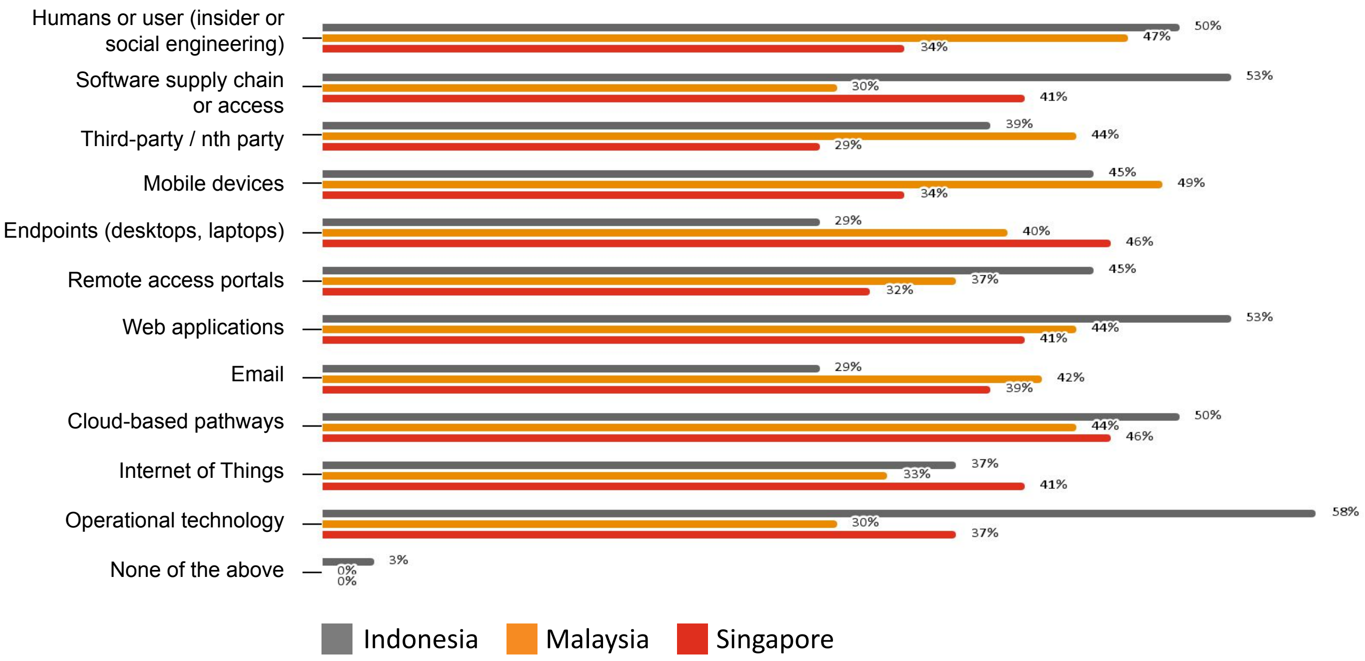
These changes have prompted an acceleration in the adoption of cloud-based solutions. Across Southeast Asia, companies are planning to increase their cloud spending[6]. A significant portion of this growth is taking place in public cloud environments, which companies are leveraging to deploy enterprise applications, or move wholesale into digital-first solutions.

However, by moving away from on-premise infrastructure, firms have expanded their attack surfaces, making them more vulnerable to adversaries. Cloud-based pathways (47%) and web-based applications (46%) are expected to pose the biggest cybersecurity risks for Southeast Asian firms.

Cloud-based pathways and web-based applications are anticipated to pose the biggest cybersecurity threats for Southeast Asian businesses.

Cloud and web pose biggest cyber threats, but human errors are still prevalent

For each of the pathways by which adversaries can gain access to your systems, please select those that you expect to significantly affect your organisation in 2023 compared to 2022.



Source: PwC 2023 Global Digital Trust Insights Survey

[6] Martin Dale Bolima, "IDC Finds Cloud Use in Southeast Asia Growing Exponentially," Data&StorageAsean, August 25, 2022, https://datastorageasean.com/daily-news/idc-finds-cloud-use-southeast-asia-growing-exponentially

Cloud security tends to be more fluid and dynamic than ‘typical’ on-premise cybersecurity, requiring a sense of ‘shared responsibility’ from both the client-firm and the service providers[7]. However, as cloud adoption is still maturing in Southeast Asia, there is still a lack of cybersecurity protocols from end-users, resulting in poor visibility and governance across their cloud-based systems.

Human error will also play a considerable role, as reflected in executives’ concern of the cybersecurity risks posed by business emails and online accounts (43% in Southeast Asia). This is a particularly problematic issue in countries where digital literacy remains fairly low[8] and phishing scams are prevalent[9].

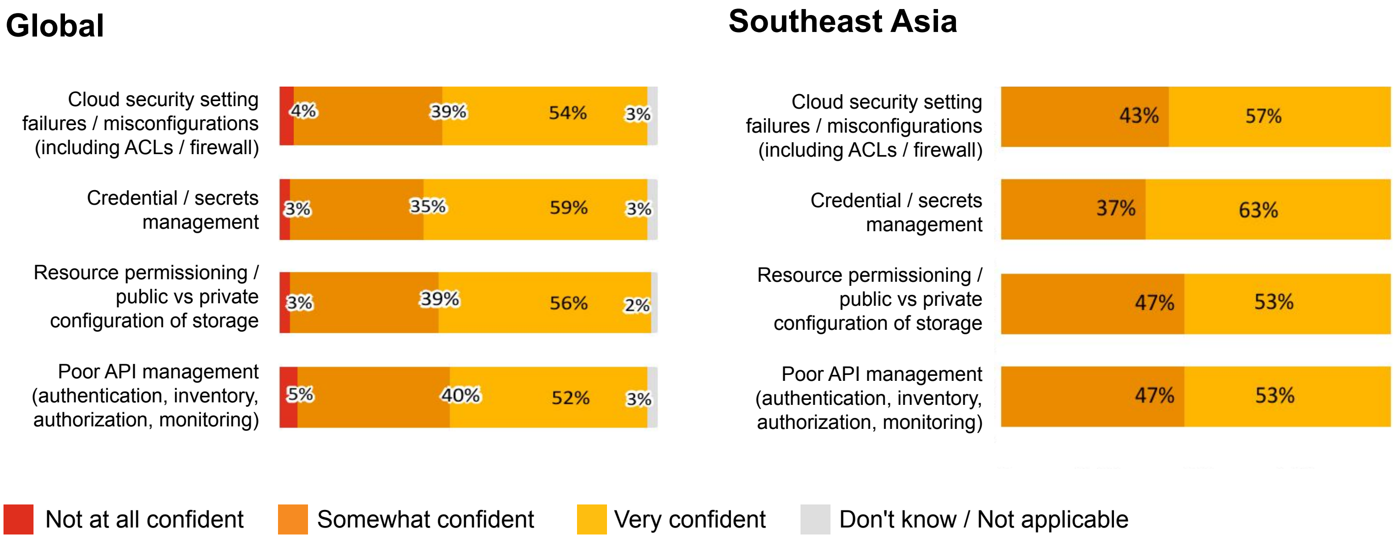
The combination of expansive cloud adoption, poor mitigation protocols and plain-old human error has resulted in most companies encountering cybersecurity incidents in their cloud environments, ranging from data breaches and intrusions to data leaks.

However, companies do not think the risks of cyberattacks outweigh the benefits of expanding their cloud service footprints, which include significant cost-savings, flexibility and mobility. The cloud has in many ways become integral, non-negotiable business components, with companies of all sizes adopting online platforms to run their businesses.

Compared to global averages, more respondents in Southeast Asia expect that attacks to their cloud management interfaces (35%) and cloud component services (30%) will increase in 2023. Rather than turning away from the cloud, Southeast Asian companies are more confident than global counterparts in their ability to bolster their systems against attack by issuing stronger credential/secrets management (63%) and minimising security failures or misconfigurations (57%).

Executives confident they’re shielding from cybersecurity attacks

With regard to your cloud environment, how confident are you that your organisation is secured appropriately against the following reasons for cloud security breaches?



Source: PwC 2023 Global Digital Trust Insights Survey

[7] Kathleen Casey, "Shared Responsibility Model," TechTarget, April 2022, https://www.techtarget.com/searchcloudcomputing/definition/shared-responsibility-model

[8] Stephanie Davis, “Media literacy training for Southeast Asian communities,” The Keyword, October 28, 2021, https://blog.google/around-the-globe/google-asia/media-literacy-southeast-asia/

[9] “Cyberthreats in South and Southeast Asia: Identifying phishing attacks and how to prevent them,” EngageMedia, August 24, 2022, https://engagemedia.org/2022/phishing-south-southeast-asia/

Call to action

To embed cloud security, collaborate across organisations

As companies look to modernise their systems, CISOs and their teams must work with their organisational counterparts to embed a culture of cybersecurity. CISOs should look to partner with their chief investment officers (CIOs) and chief technology officers (CTOs) to plan for cloud security controls before cloud adoption begins.

This strategy should encompass adopting frameworks that view cybersecurity as a foundational feature, such as zero-trust architecture where sensitive data is identified and validated at various interaction points, resulting in multiple, protective micro-perimeters[10]. Companies may also consider building infrastructure-as-code and DevSecOps tooling into their foundational systems to more effectively set the right cybersecurity checks on cloud platforms and solutions.

When working with a public cloud provider, organisations should aim to clearly define the shared responsibility they have over their cybersecurity priorities. From the beginning, CISOs and their teams must distinguish between security on the cloud and security in the cloud.

CISOs may also want to engage with other potential collaborators within the business to integrate cloud security in day-to-day business and technology processes. This could look like working with chief operations officers (COOs) or chief financial officers (CFOs) to ensure these systems are well-resourced for ensure long-term sustainability.

[10] "Zero Trust architecture: a paradigm shift in cybersecurity and privacy," PwC, October 22, 2021, https://www.pwc.com/sg/en/services/reimagine-digital/cybersecurity/zero-trust-architecture.html

Focus on data security and privacy to build trust in consumers

Data is the currency of the future, providing crucial insights that businesses of all sizes can leverage to improve customer experiences and make big strategic decisions.

The world is sitting on a mountain of data, with quintillions more generated everyday – however, customer trust in companies' ability to responsibly handle their data is at an all-time low as news of breaches fill media headlines. Across various industries, Southeast Asian business have been hit hard by data breaches and ransomware attacks[11].

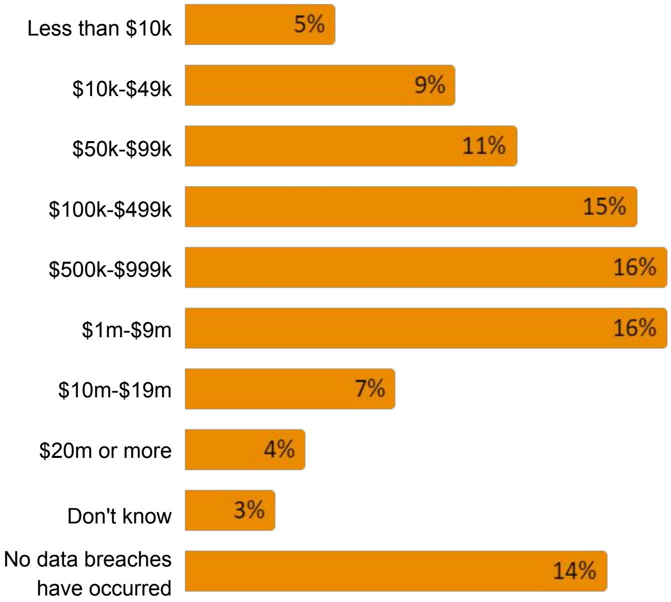
These breaches have taken a significant toll on consumers' trust in companies. A 2020 study by Okta revealed that firms' data ethics play a key role in how much customers trust in a brand – if firms fall prey to a data breach (18%) or intentionally misuse or sell users' personal data (34%), customers are unlikely to purchase from them again[12].

Companies understand that data privacy and security could be costly—more than a third of Southeast Asian firms (37%) estimate that data breaches could cost them more than US$1 million, at least, while the global share of such companies is 26%.

Despite this, most are not confident that they have put into place the necessary controls to mitigate risks of increased data volumes – only 42% of Southeast Asians say they have done so, compared to 34% globally.

Data breaches are extremely costly to organisations

Thinking about the most consequential data breach you experienced in the past three years, please provide an estimate of the cost to your organisation? (Global)



Source: PwC 2023 Global Digital Trust Insights Survey

[11] ASEAN Cyberthreat Assessment 2021 (INTERPOL, 2021), https://www.interpol.int/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf

[12] "The State of Digital Trust (Okta, 2021), https://www.okta.com/sites/default/files/2021-05/ASIA_DigitalTrustReport.pdf

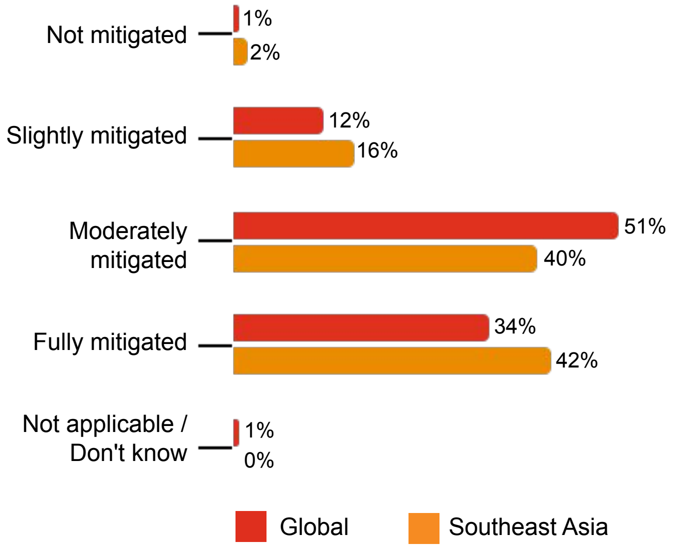
In fact, data security and privacy are the Achilles' heel of many organisations, with fewer than 5% of senior executives globally saying they always implement standard and leading practices to protect and govern customer data as listed in our survey. Southeast Asian firms perform marginally better than global averages when it comes to protecting customer data – for example, slightly more than half (52%) always ensure that the newest techniques are used to manage customer data, compared to the average 47%.

However, most data privacy efforts are only 'always implemented' in roughly half of all Southeast Asian organisations, leaving much room for improvement.

Companies that have strong data privacy practices tend to benefit from better customer trust. According to the global report, C-suite executives are 2.5 times more likely than not to agree that privacy programmes are valuable for their ability to enhance brand value and trust – but not all firms think this is enough. Around two in three of Southeast Asian respondents view cybersecurity and governance issues as hurdles that restrict or inhibit their ability to use data for decision-making (compared to 50% globally).

Although customer mistrust could potentially lead to reputational and financial damage, firms have done little to ensure data privacy

To what extent has your organisation mitigated the cybersecurity risks associated with increased data volumes in the last 12 months?

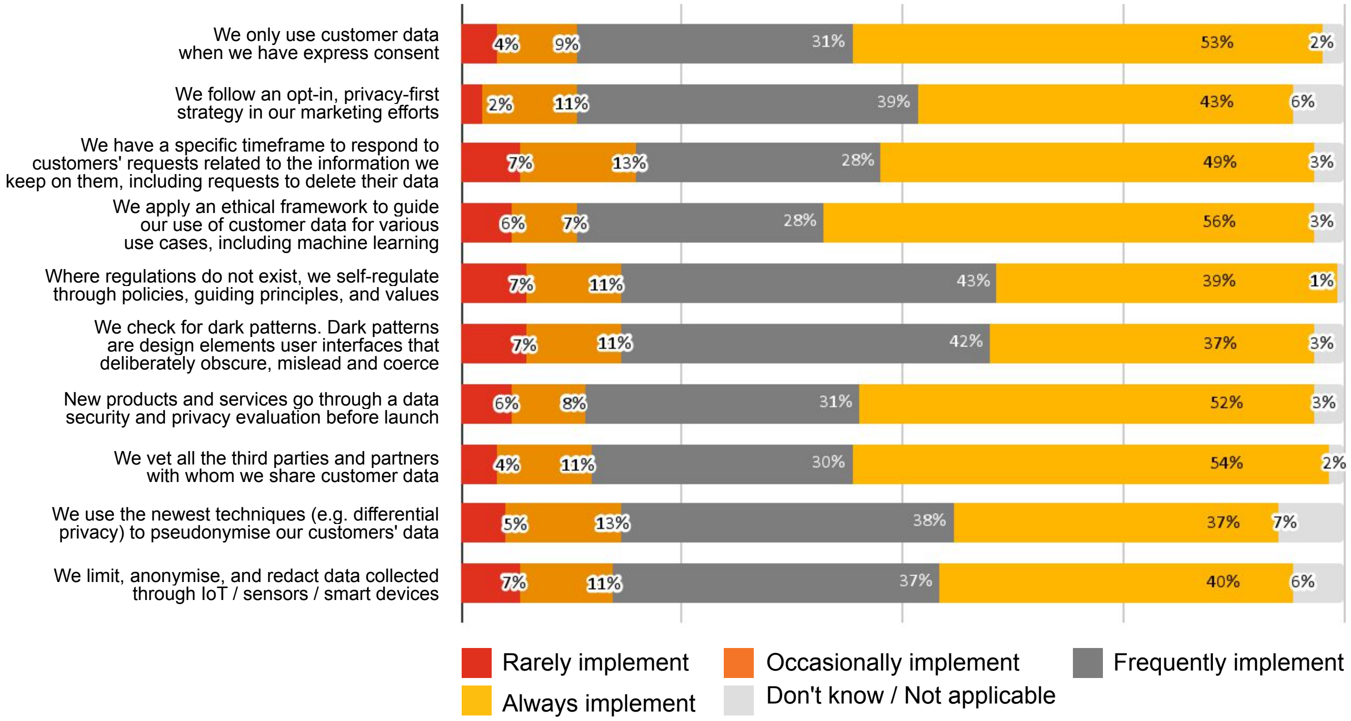


Source: PwC 2023 Global Digital Trust Insights Survey

Note: The percentages may not add up to exactly 100% as a result of their rounding to the nearest whole number.

Most Southeast Asia firms have room to improve data privacy practices

To what extent does your organisation implement the following? (Southeast Asia)

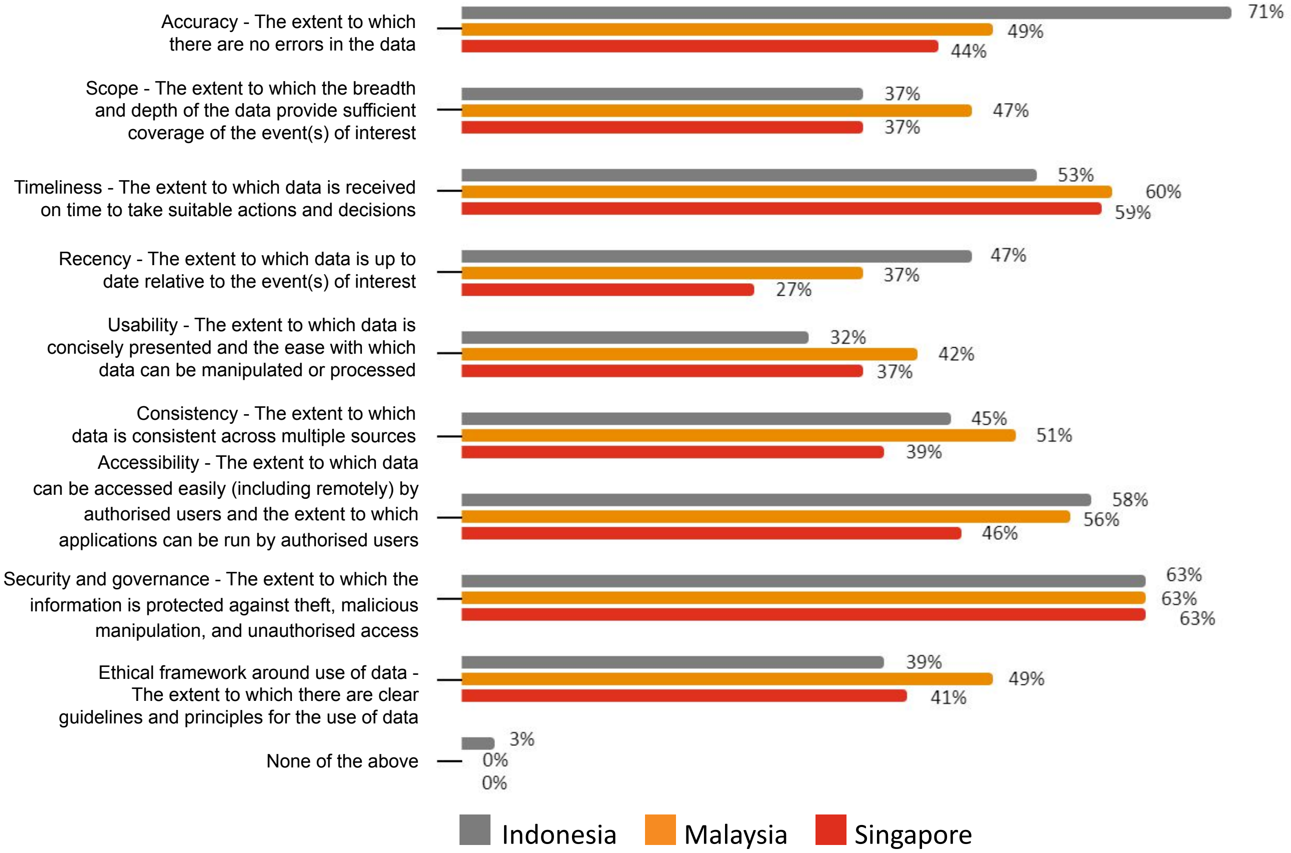


Source: PwC 2023 Global Digital Trust Insights Survey

Note: The percentages may not add up to exactly 100% as a result of their rounding to the nearest whole number.

Data security and privacy seen as inhibitors of Southeast Asian firms’ ability to make data-driven decisions

Which of the following areas most inhibit or restrict your ability to use data within your organisation for decision making?



Source: PwC 2023 Global Digital Trust Insights Survey

Call to action

Embed a security-focused mindset and leverage the right tools

First, firms must begin with a privacy-first attitude. By starting with an ethos of centering users’ data privacy, they ensure that privacy considerations are embedded in all businesses processes. Second, cybersecurity should be built in relation with privacy, with one aspect informing the other.

Companies need to think about how they can embed data ethics into their data management processes to efficiently address public concerns from the beginning. In doing so, they can also create the right kinds of reporting mechanisms to ensure the company remains in compliance with existing and emerging regulatory standards.

When CISOs centre privacy concerns in their work, they also better align cybersecurity issues with the organisation’s overall strategy while also creating a shared language that Board members can easily understand and pick up on.

To better serve customer demands for more privacy, companies can leverage privacy-enhancing technologies that align with data ethics. These tools can ensure firms are able to balance their need for data against their users’ privacy needs. This might include cryptographic encryption, differential privacy settings, machine-learning models, and AI-generated synthetic data, among others.

Concluding remarks: the need to keep adapting

As the cloud rapidly rewrites the rules of our digitalising present, it’s clear that cybersecurity teams have their work cut out for them. Cyber threats will only continue to grow in scale and speed, driving companies to invest more to ensure their users’ safety and their long-term sustainability.

Fortunately, the progress that has been made since 2020 has been significant. Now more than ever, companies are awake to the challenges and opportunities posed by a security-focused strategy. The wealth of resources and board-level attention being poured into ensuring cybersecurity is an embedded feature of all business processes is encouraging. Still more must be done – companies must focus those resources to address external threats and embed a sense of constant vigilance across every internal process.

As we look ahead to the next decade of digital growth, expertise, resources and adaptability will be foundational to firms’ cybersecurity capabilities, but the key differentiator will be companies’ willingness to evolve and collaborate across functions. In bringing these ingredients together, firms will be able to address new scenarios as and when they emerge and drive long-term resilience.

About the survey

PwC's Digital Trust Insights 2023: The Southeast Asia Perspective is a survey of 122 business, technology and cybersecurity executives across three countries in Southeast Asia (Indonesia, Malaysia and Singapore), conducted in July and August 2022.

A little more than half are executives in companies with global annual revenues of more than US$1 billion, and they are from a range of industries: Industrial manufacturing (25%), Financial services (24%), Tech, media, telecom (19%), Retail and consumer markets (19%), Energy, utilities, and resources (8%), Government and public services (3%) and Health (2%).

The Southeast Asia survey is a part of the 2023 Global Digital Trust Insights survey of 3,522 business, technology, and cybersecurity executives (CEOs, corporate directors, CFOs, CISOs, CIOs, and C-Suite officers).

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

Contact us to learn more

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

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

Alex Tan
Partner, Cyber & Forensics
and Crisis Leader,
PwC South East Asia
Consulting, PwC Malaysia
alex.tan@pwc.com

Vo Tan Long
Partner, PwC South East Asia
Consulting, PwC Vietnam
vo.tan.long@pwc.com

Vilaiporn Taweelappontong
Partner, PwC South East Asia
Consulting, PwC Thailand
vilaiporn.taweelappontong@pwc.com

Chairil Tarunajaya
Partner, PwC South East Asia
Consulting, PwC Indonesia
chairil.tarunajaya@pwc.com

Veronica Bartolome
Partner, PwC South East Asia
Consulting, PwC Philippines
veronica.r.bartolome@pwc.com

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

Tan Shong Ye
Partner, Digital Solutions,
PwC Singapore
shong.ye.tan@pwc.com