2022 Global Digital Trust Insights (Malaysia report)

The C-suite guide to simplifying for cyber readiness, today and tomorrow

May 2022

pwc

The road to cyber readiness: Do Malaysian organisations have what it takes to be resilient?

Mounting cybersecurity threats and attacks by increasingly sophisticated perpetrators over the past two years are prompting organisations to take a hard look at the cyber readiness of their business.

While Malaysia is in transition to the endemic phase of COVID-19, what's clear is that attackers will continue to evolve in their tactics and strategies. The only defence businesses have is to step up their cyber readiness, being constantly vigilant to protect the organisation from cyber attacks.

The **2022 Global Digital Trust Insights (Malaysia report)** reveals some important learnings from a survey among 3,602 global business, technology and security executives including respondents from Malaysia and Asia Pacific. It presents insights into the level of cyber planning, adoption, and simplification required, as well as the current challenges and supply chain risks faced by Malaysian organisations.

Is your cybersecurity budget still relevant? Can the CEO make a difference to your organisation’s cybersecurity? Are you securing against the most important risks today and tomorrow? Or is your organisation too complex to secure? How well do you know the risks posed by your third parties and supply chain?

The report delves into some of these tough questions confronting Malaysian C-level executives. It is a call to action to close the gaps present in Malaysian organisations, through strategic efforts at the highest levels of the organisation as well as through organisation-wide collaboration and public-private collaboration.

Contents

Cybersecurity budgets are increasing but are these investments bearing sufficient fruit for companies?

If we looked back at the past few months, 2021 shaped up to be one of the most uncertain years for cybersecurity. The subdued sentiments of cybersecurity professionals is expected to continue. Ever more sophisticated attackers are exploiting our systems and networks, seeking - and finding - vulnerabilities.

Investments continue to pour into cybersecurity based on **PwC's 2022 Global Digital Trust Insights Survey**, a study of business, technology and security executives. 69% of organisations globally predict a rise in cyber spending in 2022 compared to 55% last year. More than a quarter (26%) predict cyber spending hikes of 10% or more; only 8% said that last year.

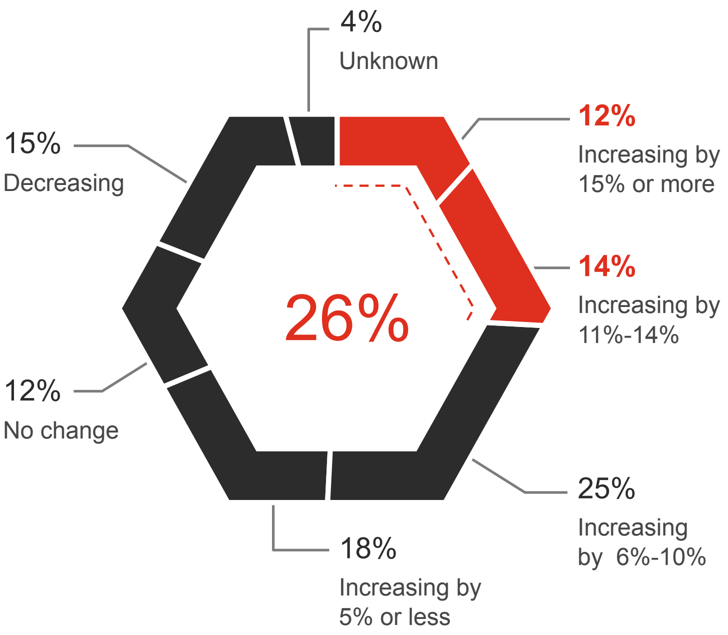
Organisations know that risks are increasing. More than 50% globally expect a surge in reportable incidents next year above 2021 levels.

Regionally, about one-fifth of respondents in the Asia Pacific (APAC) region, including Malaysian respondents expect a growth of more than 10% in their 2022 organisation cyber budgets. Similar to their global counterparts, more than 50% of Asia Pacific respondents expect an **increase or significant increase of reportable incidents** in their 2022 threat outlook, with ransomware and malware topping the list.

Vulnerabilities like an unprotected server containing 50 million records, for example, or a flaw in the code controlling access to crypto wallets — could be targeted by attackers.

The consequences for an attack rise as our systems' interdependencies grow more and more complex. Critical infrastructures are especially vulnerable. And yet, many of the breaches we're seeing are still preventable with sound cyber practices and strong controls.

Figure 1: More than a quarter (26%) globally expect double-digit growth in cyber budgets in 2022



Question: How is your cyber budget changing in 2022?
Source: PwC, 2022 Global Digital Trust Insights

How should organisations respond?

A **three-step approach** to reduce an organisation's vulnerability to these attacks:

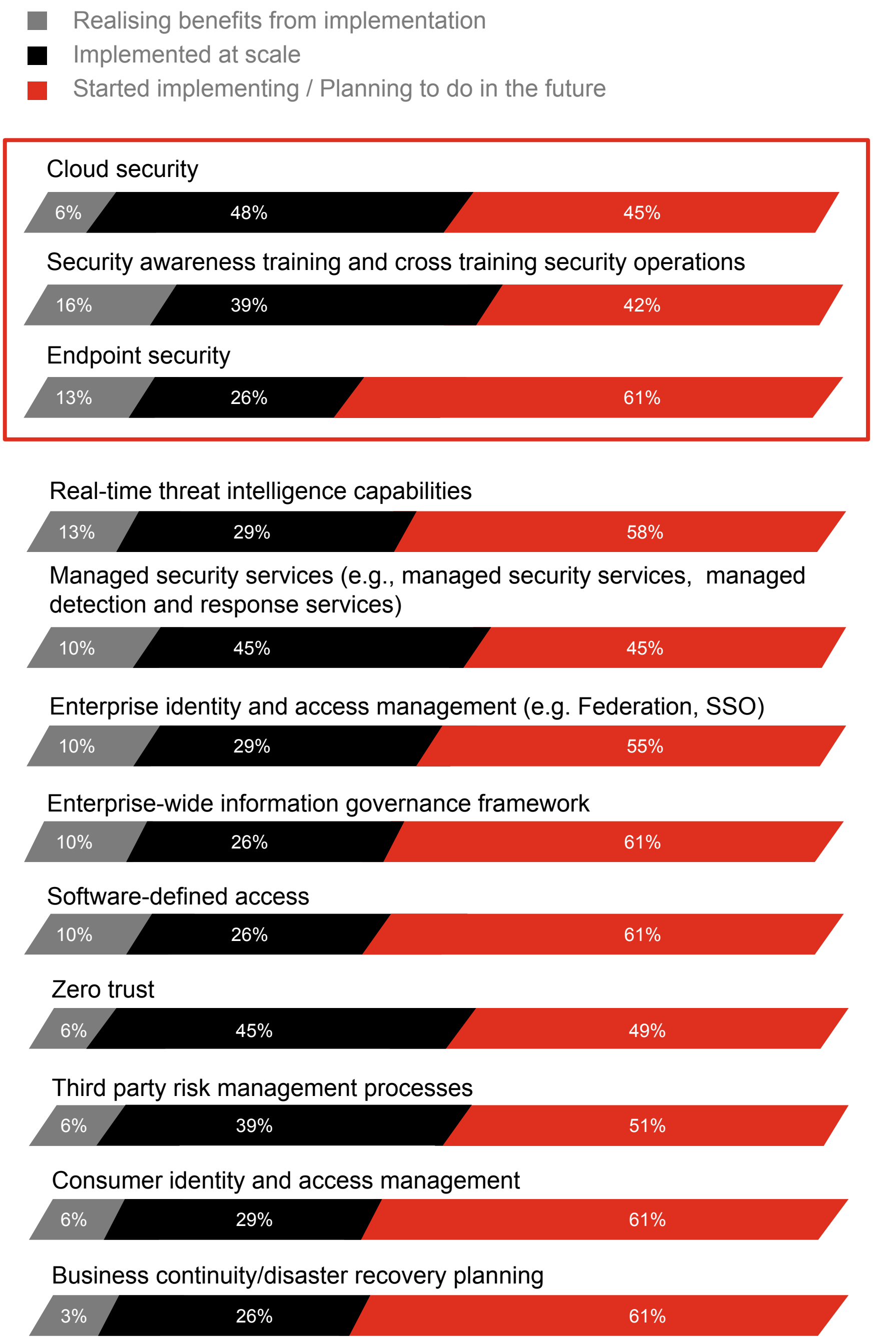
1 Understand and report your organisation's vulnerability to the threat

2 Deliver targeted improvements to immediately reduce risk, and validate your implementation

3 Build capabilities to deliver sustainable cyber risk reduction

Source: PwC, Responding to the growing threat of human-operated ransomware attacks, 2020

Figure 2: Few in Malaysia have realised benefits to-date, raising the question of what could be done better for future cyber investments



Question: To what extent is your organisation prioritising investments in the following?
Source: PwC, 2022 Global Digital Trust Insights

In general, we see a consistent trend globally ranging from 11% - 16% on **realising the benefits from implementing cyber investments**. A possible explanation as to why most organisations have yet to realise benefits from their implementation could be their late start in implementing cyber investments. Also, some leadership teams may struggle to clearly identify where to focus their efforts on in simplifying the areas that deliver the greatest benefits to the organisation.

We observed that nearly half of **Malaysian respondents** have started to plan and prioritise their cyber investments. In which, 6% of the organisations have invested and are realising benefits from **implementing cloud security**. Almost equal proportions of respondents also said they have realised benefits from **implementing security awareness training and cross training security operations (16% for both global and Malaysia), as well as endpoint security (13% for both global and Malaysia)**.

Very few Malaysian respondents (only 3%) are realising benefits from implementing business continuity planning (BCP), although 61% have started implementing or are planning to implement BCP in the future.

According to PwC's 2021 Global Crisis Survey, unexpected events like the pandemic reveal the importance of planning ahead and building resilience, with an effective response plan in place.

Simplifying cyber

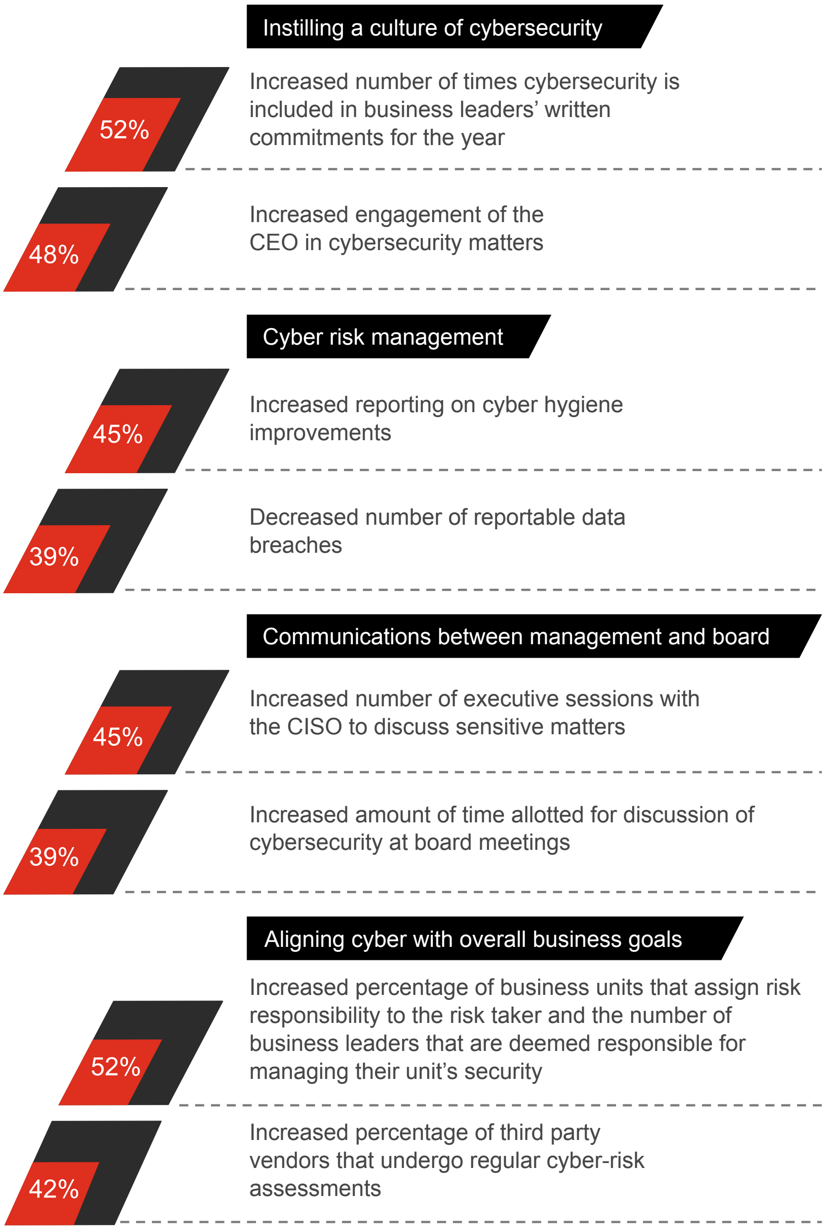
As digital connections multiply, they form increasingly complex webs that grow more intricate with each new technology. For instance, health trackers on phones have simplified our lives in different ways, together with other smartphone functions. The Internet of Things lets us perform myriad tasks by uttering a simple command. It also enables factories to run seamlessly, and lets our healthcare providers monitor our health from a distance.

But the processes needed to manage and maintain all these connections — including cybersecurity — are getting more complicated, too.

Is the business world now too complex to secure? Leaders are sounding the alarm. Some 75% of global respondents to our 2022 Global Digital Trust Insights Survey say that too much avoidable, unnecessary organisational complexity poses “concerning” cyber and privacy risks.

But because some complexities are necessary, your enterprise should streamline and simplify its operations and processes consciously and deliberately.

Figure 3: Cybersecurity scorecard: 45% of Malaysian organisations report significant progress in the past two years on four fronts



Instilling a culture of cybersecurity

52%	Increased number of times cybersecurity is included in business leaders’ written commitments for the year
48%	Increased engagement of the CEO in cybersecurity matters

Cyber risk management

45%	Increased reporting on cyber hygiene improvements
39%	Decreased number of reportable data breaches

Communications between management and board

45%	Increased number of executive sessions with the CISO to discuss sensitive matters
39%	Increased amount of time allotted for discussion of cybersecurity at board meetings

Aligning cyber with overall business goals

52%	Increased percentage of business units that assign risk responsibility to the risk taker and the number of business leaders that are deemed responsible for managing their unit’s security
42%	Increased percentage of third party vendors that undergo regular cyber-risk assessments

Question: How much progress has your organisation made in the past two years?
Only the top two metrics are reported under each category.
Source: PwC, 2022 Global Digital Trust Insights

Are global concerns on organisational complexity shared by Malaysians?

Yes, nearly 80% of Malaysian respondents agreed that there is a high level of unnecessary complexity on data management and technology operations, although it can be avoided.

What's heartening is the proportion of Malaysian respondents (45%) who recognised a significant improvement in their organisation-wide cyber risk management practice in the past two years. Whereas, half of the local respondents reported seeing a significant progress in instilling a culture of cybersecurity within the organisation i.e. 52% see an increased number of times where cybersecurity is included in business leaders’ written commitments, while 48% see increased engagement of the CEO in cybersecurity matters.

Security-first leadership

Setting a security-first tone from the top

Globally, CEOs were more likely than non-CEOs to rate their level of support in six areas as “significant”.

The CEO role in cybersecurity: Closing the expectation gap between CEOs and other C-suite members

Global CEOs in our “most improved” group (those with the best cybersecurity outcomes over the past two years) are 14x more likely to provide significant support across all categories. Similarly, the non-CEOs in the most improved group are 12x more likely to say their CEOs provide that significant boost.

Things seem headed in the right direction in closing the expectation gap between global CEOs and others in the C-suite regarding the level of CEO involvement and support for cybersecurity. Interactions with the CEO on cyber matters have increased significantly in the past two years, according to 46% of our global survey respondents.

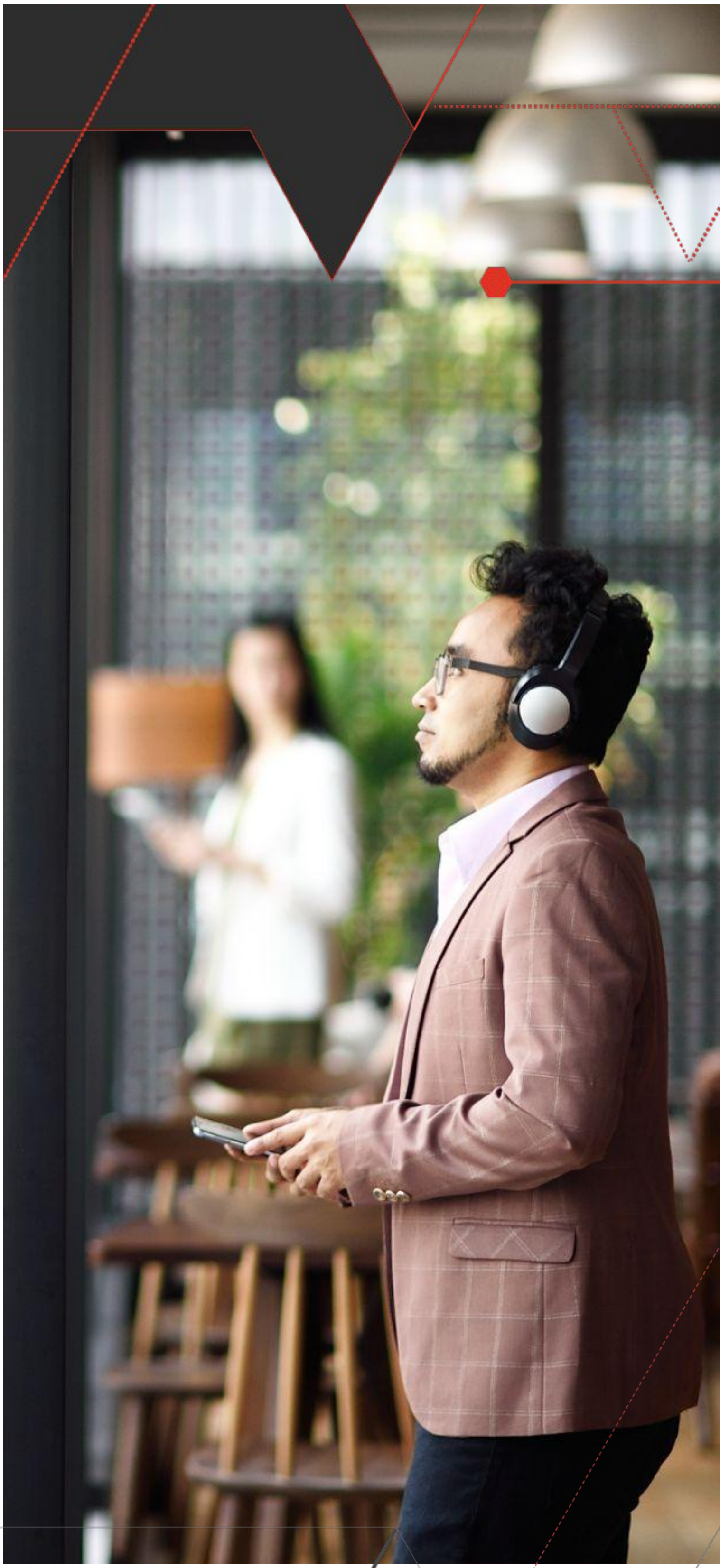
Figure 4: The top 3 views where global CEOs and non-CEOs are aligned

37%	CEOs say they provide significant support to their cyber leadership to ensure that they have adequate resources, funding and sufficient priority to carry out their responsibilities.
30%	Non-CEOs agree that their CEOs provide significant support in these areas.
34%	CEOs say they provide significant support to their cyber leadership on reducing investors’ uncertainty regarding organisational cyber risks.
29%	Non-CEOs agree that their CEOs provide significant support in reducing investors’ uncertainty.
36%	CEOs say they provide significant support to empower their cyber leadership to connect with confidence with their customers and business partners.
30%	Non-CEOs say that they receive significant support from their CEOs on connecting with confidence with customers and business partners.

Figure 5: Executives around the world put a lot of stock in cyber-savvy and engaged CEOs and boards — and tech breakthroughs that simplify cyber defense — for a more secure digital society by 2030

	Malaysia	Global
Develop a diverse workforce	1	7
Make signatory-nations accountable for responsible behaviors in cyberspace, according to norms in international agreements	2	6
Work with schools and universities to increase the cybersecurity awareness and knowledge in the general population	3	4

Question: In what ways does the cybersecurity field have to change so there is a more secure digital society by 2030?
Source: PwC, 2022 Global Digital Trust Insights



In Malaysia, organisations share the vision of building a digitally secured society within the next 10 years, however they are shifting their focus away from management and onto the workforce.

Developing a diverse cyber workforce is the top priority for Malaysian organisations. While leadership drives the approach of an organisation toward cybersecurity, the capability of an organisation in efficiently managing cybersecurity stems from the ability of the workforce itself. Ensuring that the workforce is well equipped with not just the tools, but the skills to tackle cybersecurity is key in securing the digital posture of an organisation.

This is reinforced in PwC's 25th Annual Global CEO Survey where CEOs are recommended to recalibrate skills, by focusing on building capability and capacity locally, while also honing in on leadership skills including building empathy and a willingness to embrace debate. Having the fundamentals in place will be critical given the proportion of Malaysian CEOs polled in the Global CEO Survey (67%) having concerns about cyber risk as a threat to growth.

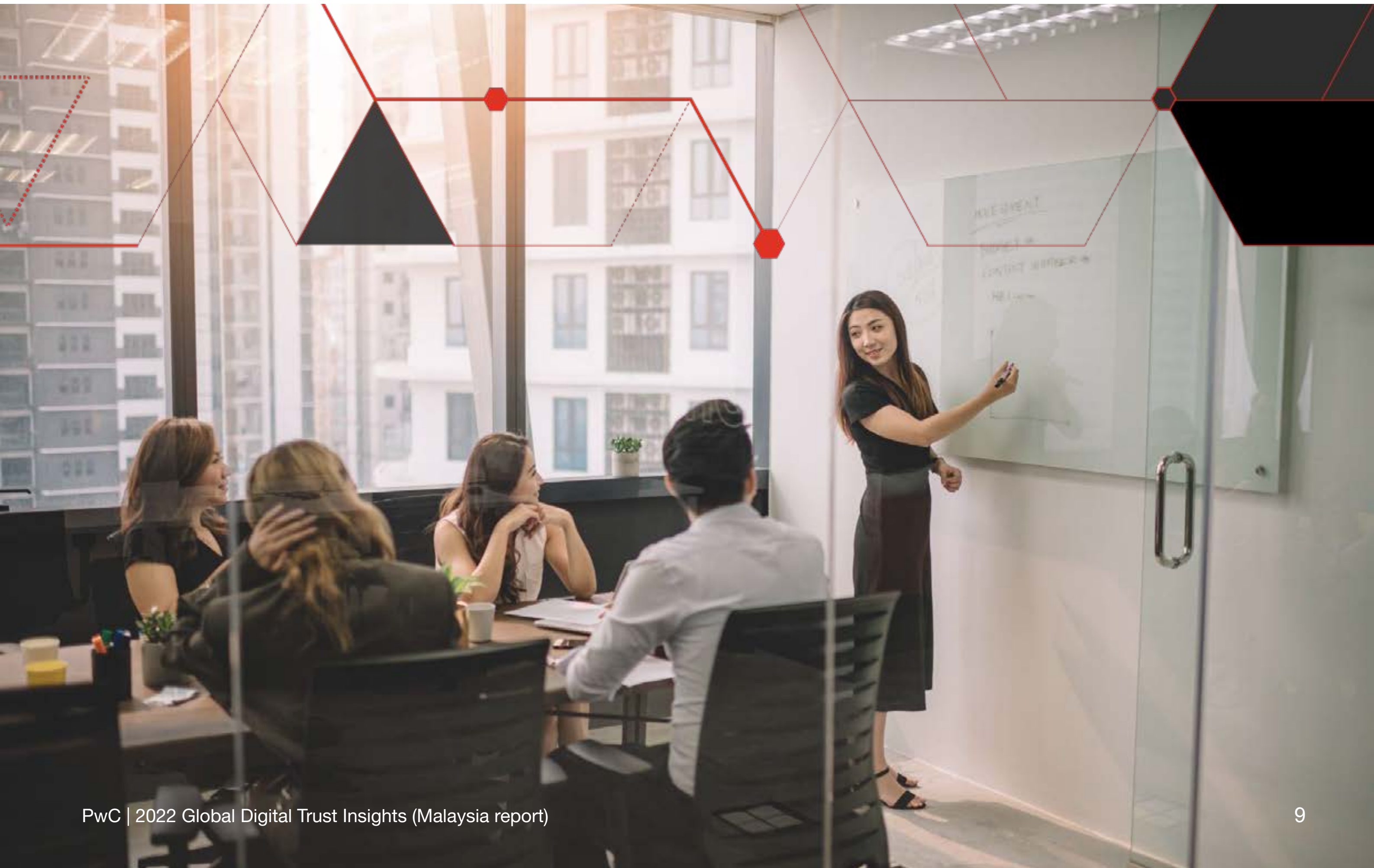
In contrast with global, organisations in Malaysia assign great importance to making signatory-nations accountable for responsible behaviors in cyberspace, according to norms in international agreements such as the Budapest Convention on Cybercrime (refer to chart on page 6). This would pave the way in creating a more secure digital society.

While threat actors can be state sponsored, individuals leveraging on automation or threat services offered by third parties pose an increasing risk to the general cyberspace. The continual growth in threat actors due to empowerment of technologies to the individual, further emphasises the need for collaboration between nations to jointly deter cyber threats and collectively lay the foundation for a secure digital society.

Policy developments in Malaysia

Aligned with the vision of a secure digital society, respondents from Malaysia concur that cybersecurity awareness and knowledge should be embedded within the education of an individual. Survey results suggest that Malaysians value the importance of tackling cyber risks from a national policy perspective. In the Malaysia Digital Economy Blueprint, incorporating digital skills into education is under the thrust factor “build agile and competent digital tallent”. Initiatives such as cybersecurity and data science upskilling programmes are to be championed in driving digital acumen in the general population.

Malaysian organisations indicate the importance of support in tackling cyber risks from a national policy perspective, rather than solely depending on the organisation and the industry. Collaborating with other nations to jointly deter cyber threats can collectively lay the foundation for a secure digital society.



Being cyber-ready: Improvements in incident response times and confidence of leaders key to Malaysian respondents

When it comes to near term goals in the next three years, Malaysian respondents (in contrast with global respondents) indicated their main focus on **improving response times to incidents and disruptions**, while respondents globally prioritised increasing prevention of successful attacks. This can be indicative of the reactive approach by Malaysian organisations in responding to incidents.

Coming in as a number two priority for Malaysian respondents within the next three years is improving the confidence of leaders in the ability of the organisation to manage present and future threats. This includes the ability to continuously demonstrate to management the pay-off in cybersecurity risk management investments. Comparatively, in the global scene, it is observed that organisations are now reaping the benefits of cybersecurity investments in the past year. This enhances leadership confidence in driving investments to manage present and future threats.

Figure 6: Cyber ready for today and tomorrow: goals for the next three years

	Malaysia	Global
Faster response times to incidents and disruptions	1	2
Improved confidence of leaders in our ability to manage present and future threats	2	3
Lower costs of managing risks	3	8

Question: In the next three years, what goals will you be focused on, in relation to the changes you will be making in cyber strategy, people and investments?
Source: PwC, 2022 Global Digital Trust Insights

Considering the rise in high profile human-operated ransomware attacks over the past year, organisations will be better prepared in mobilising an effective response if they are proactive in implementing **threat prevention and detection methods**. Encouraged practices include regularly conducting vulnerability scanning and monitoring to ensure vulnerabilities are rapidly remediated, disabling or restricting access to internet-facing services, and enforcing multi-factor authentication to reduce the impact of compromised credentials.

Is your organisation too complex to secure?

Be deliberate about simplicity and simplification

In an overly complex organisation, it’s easy for the left hand not to know what the right hand is doing — and the consequences for cybersecurity and privacy can be dire. Aligned with the global trend, 75% of Malaysian respondents say their companies are too complex, avoidably and unnecessarily so, and nearly as many say such complexities pose “concerning” cyber and privacy risks to their organisations.

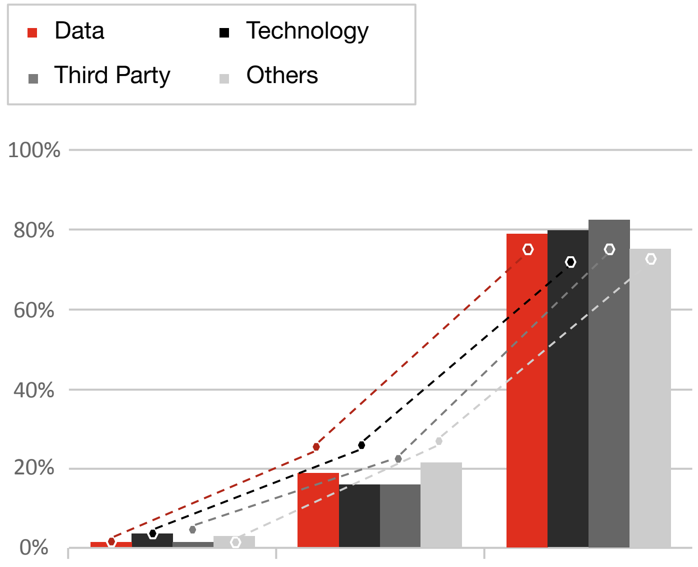
Data, technology and third party governance - areas of concern for Malaysian respondents

Technology infrastructure (87%), multi-vendor environments (84%) and data infrastructure (77%) were ranked highest among areas of “unnecessary and avoidable” complexity.

Increasingly, executives have indicated that the growing complexity of organisations have caused difficulty in understanding the operational processes of an organisation. Not surprisingly, a majority of Malaysian respondents have indicated growing concerns over risks in the area of data infrastructure (81%) and technology infrastructure (77%).

Organisations tend to be more concerned about cyber and privacy risks arising from complexities in data and technology infrastructure, closely followed by adaptation of multi-vendor environments (i.e. cloud environments).

Figure 7: Malaysian executives report high levels of complexity in their organisations, leading to "concerning" cyber and privacy risks



	1	2-5	6-10
■ Level of complexity	Not complex at all	Reasonable or necessary levels of complexity	Avoidable, unnecessary levels of complexity
- -●- - Level of risk	No risk at all	Manageable levels of risk	Concerning levels of risk

Questions: In your view, how complex are the following operations in your organisation, on a scale of 1 to 10? How significant are the cyber and privacy risks posed by complexity in these areas in your organisation?

Source: PwC, 2022 Global Digital Trust Insights

The costs of complexity

Complexity isn’t bad in and of itself. Often, it’s a by-product of business growth. The larger an organisation, the more complex it will naturally be, needing more people and technologies to serve a growing customer base.

The costs of creating unnecessary complexity are not obvious, and it’s hard to create urgency around combatting complexity — that is, until an attack occurs.

In our article 'Simplifying cybersecurity', we illustrated how simplification can improve security. At a global retail organisation, six vendors managed customer contacts. Two of those vendors’ systems had been breached in the past. After consulting with the CEO and board, the new operations director reduced the vendor list to two vendors. This simplification improved security: Monitoring two vendors is easier than keeping tabs on six, making information access easier to control, and the retailer could more readily back up the smaller cache of customer data.

What are the top consequences of complexity among Malaysian respondents?

Malaysian and global respondents are aligned in their views on **financial losses** as the most significant implication of successful data breaches or cyber attacks.

A key difference is, “inability to sustain growth for the long term”, in which most of the larger Malaysian organisations often have a dilemma over keeping up with the newest cyber trends and reducing operational complexity.

System changes for newer technologies are harder to implement as it involves more complex processes and resources. As a result, most business leaders might be questioning the returns as compared to the costs invested on these changes.

Figure 8: In all industries, Malaysian and global respondents are aligned in three out of four areas of top consequences of complexity

	Malaysia	Global
Financial losses due to successful data breaches or cyber attacks	1	1
Inability to sustain growth for the long term	2	5
Inability to innovate as quickly as the market opportunities offer	3	2
Lack of operational resilience or inability to recover from a cyber attack or technology failure	4	3

Question: In your view, What are the most important consequences of complexity on your business?
Source: PwC, 2022 Global Digital Trust Insights

The move to simplification

We find that businesses know the risks of complexity, yet only 32% of our Malaysian respondents have performed any streamlining of their operations and nearly one-third say they've done nothing at all or are just getting started. But a shift appears to be underway.

Simplifying an organisation takes time, requiring changes in viewpoints and company culture. That's not easy to achieve, but the payoffs are worth it. Globally, we observed that the companies that had the best cybersecurity outcomes over the past two years (most improved) are 5x more likely to have streamlined operations enterprise-wide.

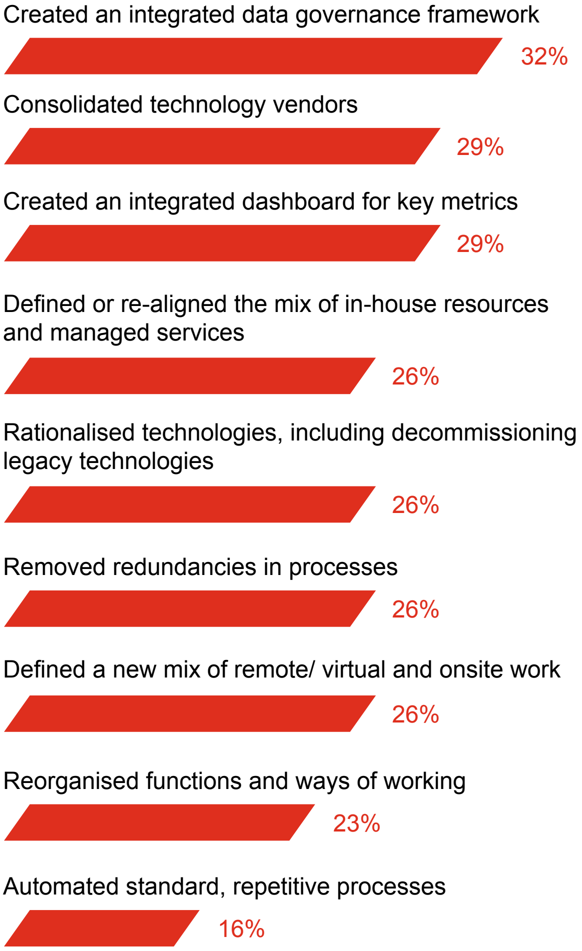
Malaysian trends mirror global's

We see a similar pattern in **Malaysia**. Local organisations have already completed streamlining of their operations in creating an integrated data governance framework (32%), consolidating technology vendors (29%), and creating an integrated dashboard for key metrics (29%).

More and more organisations seek to **reduce reliance on manual processes** that are more prone to human error. We observed that 26% of Malaysian respondents have removed redundancies in processes, and 16% have switched over to a more automated standard, repetitive process.

Increasingly, Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs) are taking a hard look at their tech investments, beyond following trends or pursuing the latest products from tech vendors.

Figure 9: Simplification in organisations: On average, 25% have streamlined enterprise wide over the last two years



Question: In the last two years, to what extent has your organisation streamlined operations in the following ways? Percentage responding 'completed enterprise-wide'. Other potential responses were 'partially completed,' 'just started,' or 'not at all.'
Source: PwC, 2022 Global Digital Trust Insights

Simplifying cybersecurity can be challenging

When asked to prioritise among **nine initiatives** aimed at simplifying cyber programmes and processes, global respondents couldn't choose, allotting near-equal importance to all of them. Chief Information Security Officers (CISOs) who are building layers of control, for defense in depth, are well-intentioned but must guard against introducing more complexity and cost. More controls don't always make a company more secure.

Malaysian organisations allocated an almost equal share of total spending among 9 cyber simplification initiatives, ranging from 9% - 14%, which also reflect similar attitudes to their global counterparts (ranging from 10% - 12%). Moving to the cloud can help simplify business processes and IT architecture, provide flexibility and accelerate innovation. On the flipside, staying stagnant may give rise to complexities resulting from extensive technology options, new architectural approaches, complicated service plans, unused capacity and confusing billing and pricing, especially when the technologies offered are constantly changing.

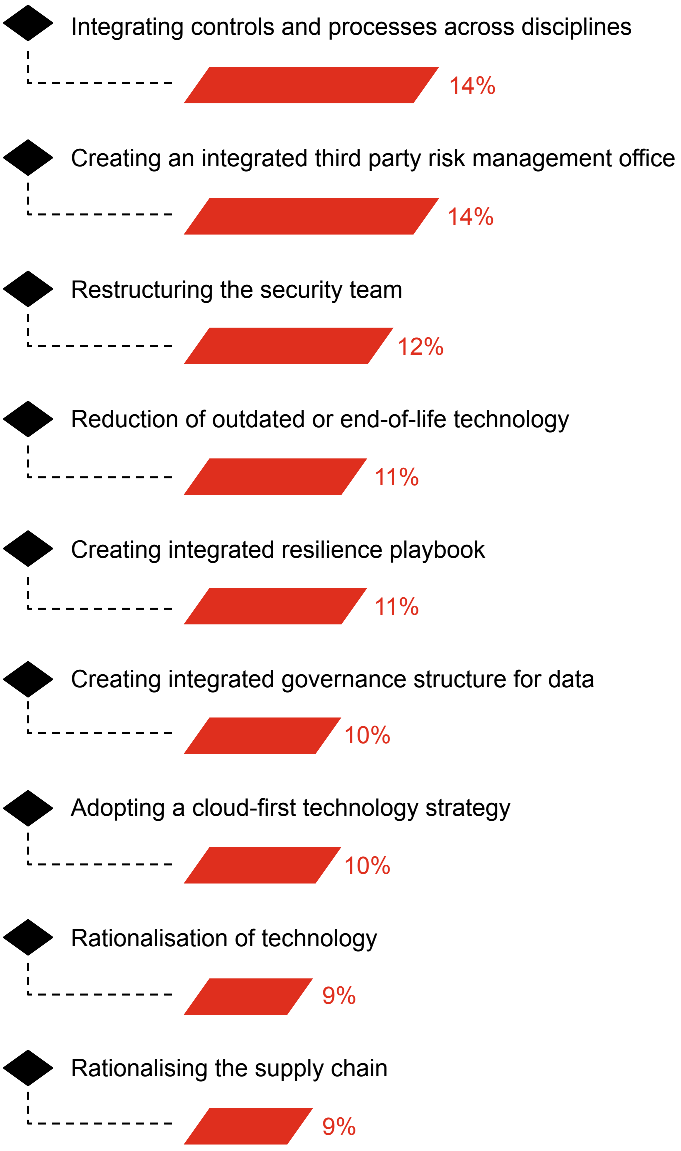
Done right, cloud transformation can be successful

In **Malaysia**, cloud security is among one of the top investment priorities of our local survey respondents, with nearly half of our respondents (48%) having implemented cloud security at scale. While that's encouraging, it's also sobering to note the 6% who are realising benefits from these investments and the 45% who are just starting or planning their investments (refer to page 5 for the diagram).

To simplify cyber, a strong tone from the top is needed to communicate security-minded leadership.

Simplification of cyber spending is spread across several initiatives

Figure 10: Average share of total spending on cyber simplification among Malaysian organisations



Question: In the next two years, what proportion of your cybersecurity spend will your organisation allocate to each of the following initiatives to simplify cybersecurity?
Source: PwC, 2022 Global Digital Trust Insights

Don't overlook moves that can have a significant impact. For example, two moves — deploying two-factor authentication and putting your remote desktop protocol (RDP) behind the firewall — can vastly reduce the risks of phishing, which remains a popular tactic, by itself, and in tandem with malware and ransomware attacks.

Are you securing against the most important risks today and tomorrow?

Size up your risks — using data you can trust — to realise opportunities

Organisational leaders recognise the importance of verifying and safeguarding their business information.

Data infrastructure and data governance rank as the two most needlessly complex aspects of business operations. In our survey, 81% of Malaysian respondents (vs 77% of global respondents) say there is "avoidable, unnecessary levels of complexity" on data infrastructure and more than three-quarters for both Malaysian and global respondents (77%) say the same for governance of data.

More than two-thirds (68% for governance of data, and 81% for data infrastructure) say complexity in these areas poses "concerning" risks to cybersecurity and privacy. Complexity of data can stymie any organisation's ability to effectively use the information it collects and generates.

With the rapid advancement of technology followed by the ever-changing risk environment, it is equally important to build awareness in safeguarding business information via cybersecurity means among the working levels and management levels.

Echoing the global findings, in order to avoid complexity, businesses must determine which technology solution will add value to their operations and what kind of risk is being left behind during implementation.

A foundation for data you can trust for better business decisions

Organisations first need to set up that good foundation we call **data trust**: making sure your data is accurate, verified, secure and reliable for business decisions. And when it comes to customer data, you want to make sure customers know they can trust you to keep their information safe from unauthorised eyes.

After crafting your data strategy, governance — the policies, procedures and processes for fulfilling the strategy — should follow immediately.

Concerning levels of data trust practices among Malaysian organisations

In Malaysia, less than a third of local respondents report having mature, fully implemented data trust processes in four key areas: **governance (21%), discovery (23%), protection (27%) and minimisation (32%)** - relatively consistent with global. Among these, data governance scored the lowest (about a quarter stated they had "formal process fully implemented").

Nearly a third of our Malaysian respondents say they have data trust processes in place but are not formalised, and about 10% reported to have no formal data trust processes in place at all.

Securing data from tampering and theft

Only 26%

Malaysian respondents have fully implemented data security technologies including encryption and tokenisation

Turning data into true assets that can increase your revenues is one benefit of good data security — as some leading businesses are discovering. According to the PwC US Trust in Data Survey,* companies with more mature data trust practices tend to be ahead in many respects.

Among the commonalities observed:

- Earned revenues from data monetisation by personalising services, operating more efficiently and better serving their customers
- Strongly agree that higher customer trust leads to demonstrably higher revenue
- Made significant moves in the past year to improve customer and investor trust
- Greater confidence in their third party risk management programme because they monitor their third parties more

*The survey is PwC US' April 2021 snapshot of their Digital Trust Insights Survey.

Data protection is key

Companies can minimise the risk of attacks on data especially crown jewels data (your most critical and most valuable data) by minimising the target.

Govern, discover and protect only the data you need — and eliminate the rest. Drafts, duplicates, superseded data, legacy data and employee personal data are common candidates for elimination. Low-value data not only creates unnecessary risk, it also crowds out or buries your high-value data. Such data could be vulnerable to ransomware attacks.

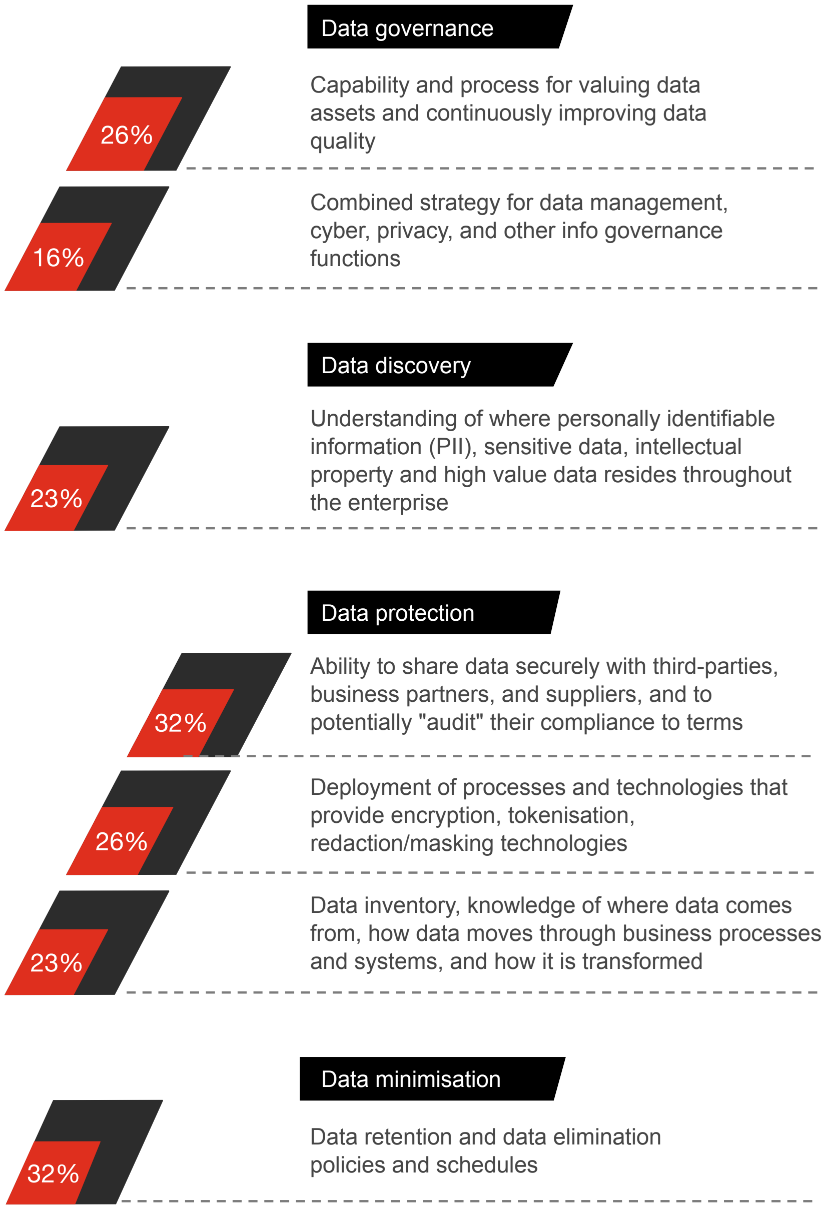
The two-thirds of global organisations that haven't formally implemented data trust practices may be at risk in more ways than one. Effective data governance is important not only for operational resilience but also for compliance with regulations such as the Personal Data Protection Act 2010 ("PDPA"). New, more stringent regulations loom on the horizon as well.

More efforts needed for Malaysian organisations to keep up with industry data trust practices

In comparison with global data, **Malaysia** has a relatively lower scoring overall. Among the four data trust practices, data governance scored the lowest among Malaysian respondents. Clear direction from the leaders has to be defined to set the tone clearly on the data governance strategy.

While data minimisation has the highest average score around the data trust practices adopted by Malaysian respondents (see chart), it only weighted at 32%. This is not a very promising number for data minimisation, but it is evident that nearly one-third of Malaysian companies have a mature data retention and data elimination process in place.

Figure 11: Data trust practices yet to become the norm as observed by the small proportion of Malaysian respondents who have fully implemented formal processes around data trust practices



Data governance

26% Capability and process for valuing data assets and continuously improving data quality

16% Combined strategy for data management, cyber, privacy, and other info governance functions

Data discovery

23% Understanding of where personally identifiable information (PII), sensitive data, intellectual property and high value data resides throughout the enterprise

Data protection

32% Ability to share data securely with third-parties, business partners, and suppliers, and to potentially "audit" their compliance to terms

26% Deployment of processes and technologies that provide encryption, tokenisation, redaction/masking technologies

23% Data inventory, knowledge of where data comes from, how data moves through business processes and systems, and how it is transformed

Data minimisation

32% Data retention and data elimination policies and schedules

Question: How much progress has your organisation made in the past two years?
Only the top two metrics are reported under each category.
Source: PwC, 2022 Global Digital Trust Insights

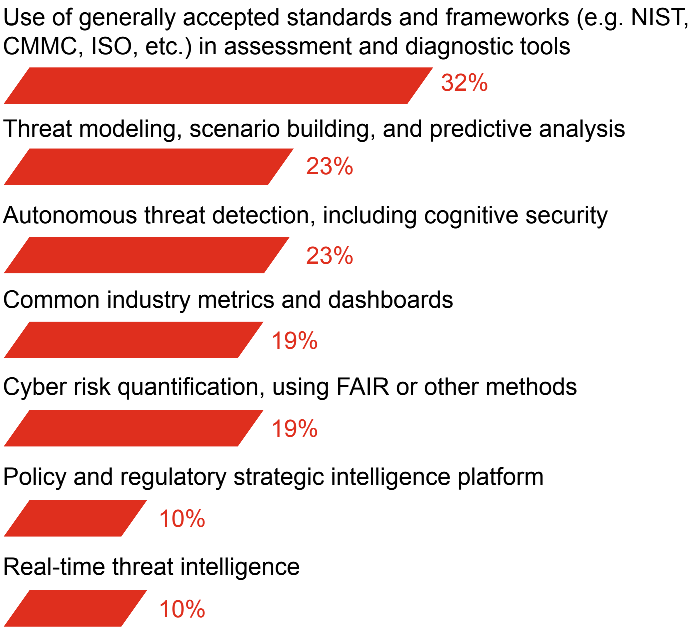
Use insights smartly

Fewer than one in three of our global survey respondents say they've integrated analytics and business intelligence tools into their operating models. These respondents scored lowest in their ability to turn data into insights for cyber risk quantification, threat modeling, scenario building and predictive analysis — all critical technologies for smart cybersecurity decisions.

Whereas in **Malaysia**, lesser than one-third of survey respondents stated they have done the necessary analytics and business intelligence integration into their operating models. Among those, policy and regulatory strategic intelligence platform (10%) and real-time threat intelligence (10%) scored the lowest.

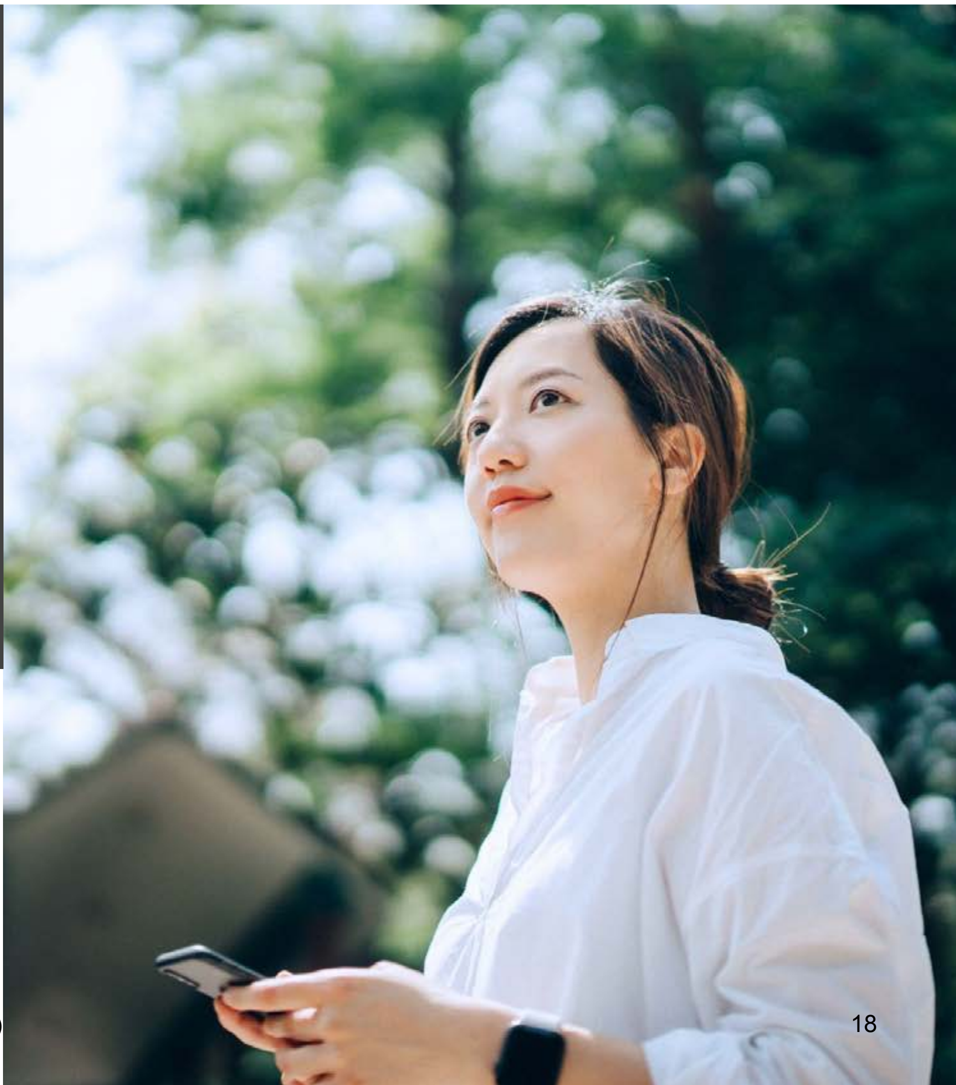
Executives under-utilise data and intel for better decisions and risk management

Figure 12: Percentage of Malaysian organisations who say these are critical to their operating model today



What is a strategic intelligence platform?

A strategic intelligence platform provides insights and connections between different economies, industries and global issues on cybersecurity related topics. This assists the organisation in setting a gold standard in internal cybersecurity frameworks and information & cybersecurity related policies, which are guarded through controls. This further guides employees in adhering to the framework and policies in their daily operations.



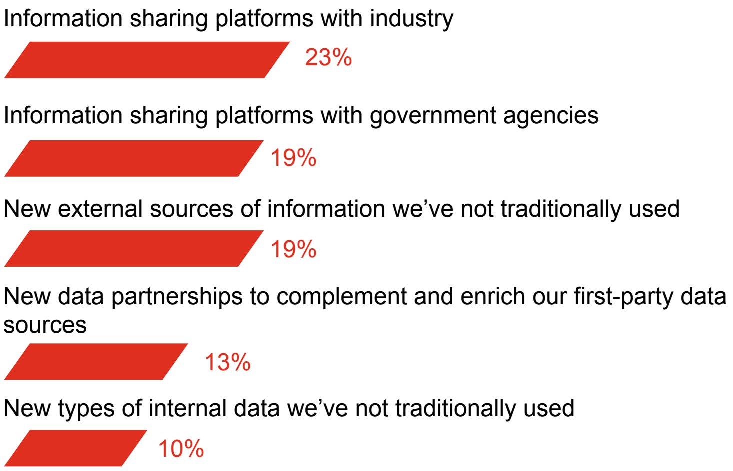
What about operational intelligence?

While business intelligence focuses on decision making at the enterprise and business level, **operational intelligence** optimises the data and information collected, improving performance for competitive gains.

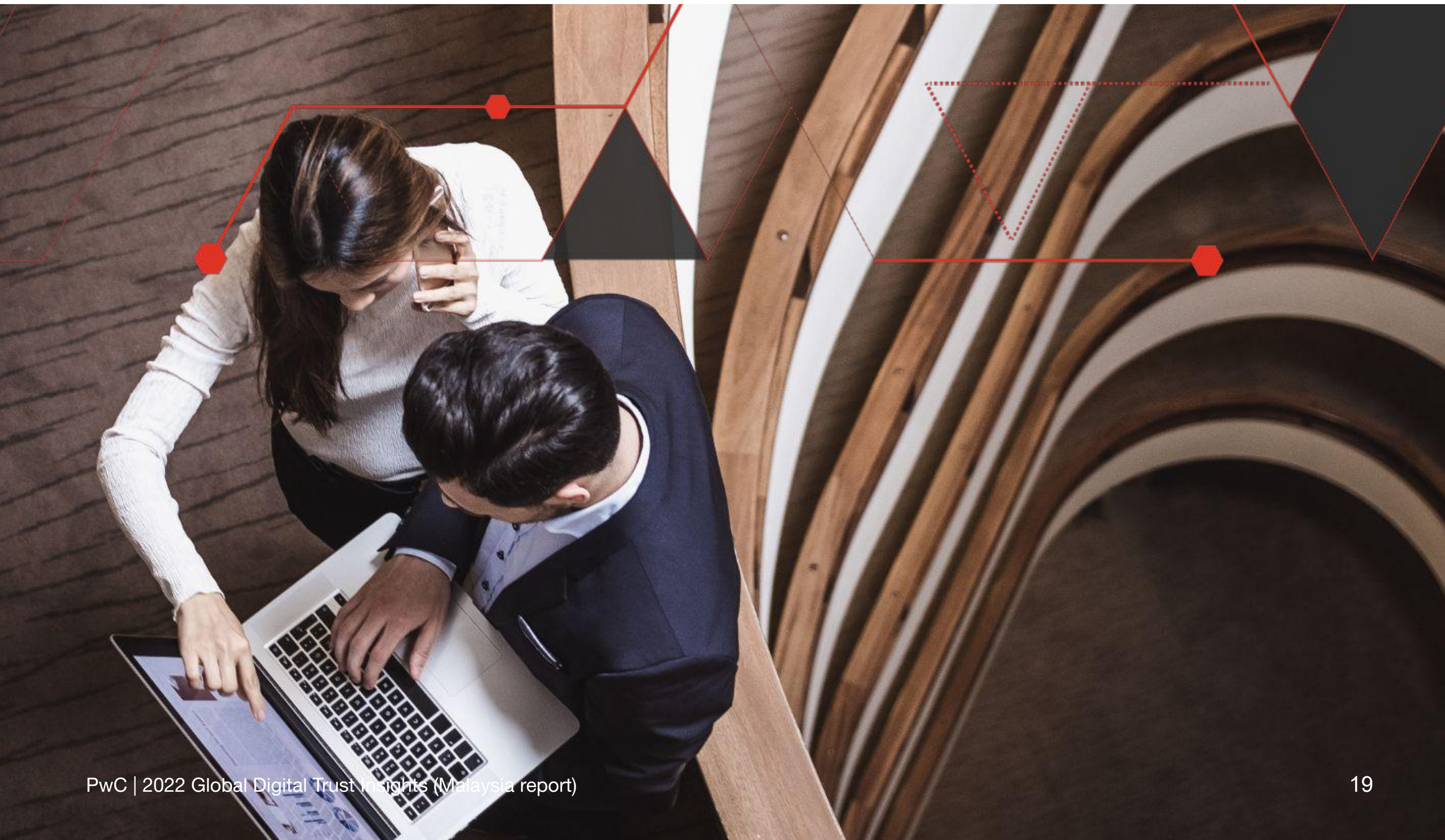
Malaysian organisations are reaping benefits from the following operational intelligence tools and approaches; information sharing platforms with industry (23%), information sharing platforms with government agencies (19%), new external sources of information not traditionally used (19%), new data partnerships to complement and enrich first-party data sources (13%), and new types of internal data not traditionally used (10%).

We observe that those who currently invest in business intelligence and data analytics are mostly predicting an increase in their cybersecurity investments next year, indicating that they recognise the benefits of doing so.

Figure 13: How are Malaysian organisations realising benefits from these tools and approaches?



Questions: To what extent does your organisation use the following tools and approaches when making decisions about cyber investments and responding to cyber risk? What best describes your organisation's plans for using the following tools and approaches for better operational intelligence?
Source: PwC, 2022 Global Digital Trust Insights



Sizing up risks — and opportunities

It's concerning that only 26% of global respondents quantify cyber risks today. The data you use to spot and understand threats, put a dollar figure on risks and prioritise them, and predict cybercrime trends can be a powerful tool for convincing boards and the CEO to invest in your cyber programme.

By the same token, data can help you stay abreast of real-time risks, and adjust security tactics and strategies as the business shifts. Global respondents in five business sectors said the most important reason to quantify cyber risk is “to continuously evaluate our risk landscape and priorities against changing business objectives.”

Malaysian organisations recognise the importance of quantifying risks - is awareness translating into action?

Zooming into the **Malaysian landscape**, respondents ranked “to respond to stakeholder demands to support risk management decisions and performance” as the most important reason to quantify cyber risk (see chart). Similar to the global ranking, executives in Malaysia recognise the importance of protective capabilities after acknowledging stakeholder demands. While awareness is a good start, organisations should consider **operationalising risk quantification**, and incorporating it into their processes.

More often than not, risk management is a crucial element to allow better business decision making, and cybersecurity plays an important role in shaping the future of risk.

Not surprisingly, “to measure the contribution of our security capabilities to risk mitigation” was selected by Malaysian respondents as the third priority to quantify cyber risk. With strong security capabilities, organisation are able to mobilise and adapt quickly amidst any crisis, whilst proper risk mitigation keeps critical operations moving.

Overall, a growing number of global organisations recognise the importance of cybersecurity to business — but many still have a long way to go. Between 37% and 42% of global respondents claim “significant progress” linking cybersecurity to business, while 16% to 18% say they’ve made little or no progress aligning cyber and business goals.

Figure 14: Malaysian executives want to size up their cyber risks in a continually changing risk landscape

	Overall
To respond to stakeholder demands to support risk management decisions and performance	1
To identify and justify improvements to, or transformation in, protective capabilities (including adding personnel)	2
To measure the contribution of our security capabilities to risk mitigation	3
To continuously evaluate our risk landscape and priorities against changing business objectives	4
To help evaluate and communicate risks optimised in line with a defined risk tolerance	5
To provide a basis for allocating limited resources among various security investments	6
To provide quantitative analysis justifying our cyber investment requests	7
To measure and compare various threats and risk events on apples-to-apples basis	8
To provide information on the return on security investments	9

Question: What are your organisation’s most important reasons to quantify cyber risk?
Source: PwC, 2022 Global Digital Trust Insights

The 2022 threat outlook

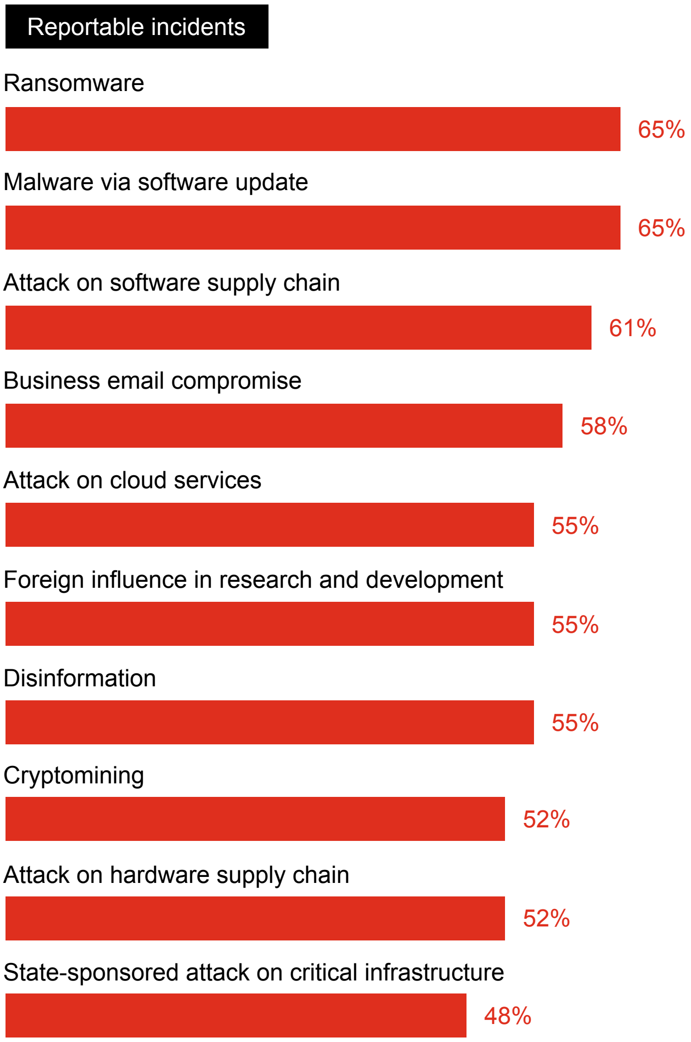
In terms of predictions for the next 12 months. 68% of Malaysian respondents (vs 60% of global respondents) expect an increase in cyber criminals. 48% of Malaysian respondents (vs 53% of global respondents) say nation-state attacks are likely to grow.

Mobile, the Internet of Things, and cloud top the list of anticipated targets for both Malaysian and global respondents.

But the type of attack could take almost any form, in our respondents' minds, and often, these incidents are linked. For global respondents, cloud service attacks (22%) narrowly edged out ransomware (21%) and cryptomining (21%) as most likely to see significant increases. Notably, 56% of global respondents expect a rise in breaches via their software supply chain, with 19% eyeing significant increases.

Among the **Malaysian respondents** (see chart), 65% expected a surge in ransomware attacks. A similar proportion expect a significant increase in malware incidents via software updates. Respondents also expect that attacks on software supply chain (61%) and business email compromise (58%), are likely to grow. Aligned with these expected attacks, nearly 60% - 70% of local respondents see an increase of threat actors among cyber criminals, competitors, and third-parties or contractors in 2022.

Figure 15: Malaysian executives expect a surge in attacks and reportable incidents



Questions: How do you expect a change in reportable incidents for these events in your organisation? How do you expect threats via these vectors/actors to change in 2022 compared to 2021?
Source: PwC, 2022 Global Digital Trust Insights

Organisations can do more to protect yourselves from potential ransomware attacks.

- Understand your business priorities and risk appetite
- Up your cybersecurity game to protect critical assets
- Engage a suitable technology enabler (i.e. MFA-VPN, robust patching and vulnerability management, antivirus and IPS-IDS, etc.)
- Incorporate plans to manage critical data as part of the Disaster Recovery Plan (i.e. online and offline strategy, robust restore procedure, etc.)
- To Pay or Not To Pay - Design a response strategy when a ransomware attack occurs

Source: PwC, Ransomware: four things you need to know about the new dangers — and what you should do

4

How well do you know the risks posed by your third parties and supply chain?

Shrink the large blind spot hiding the risks in your business relationships

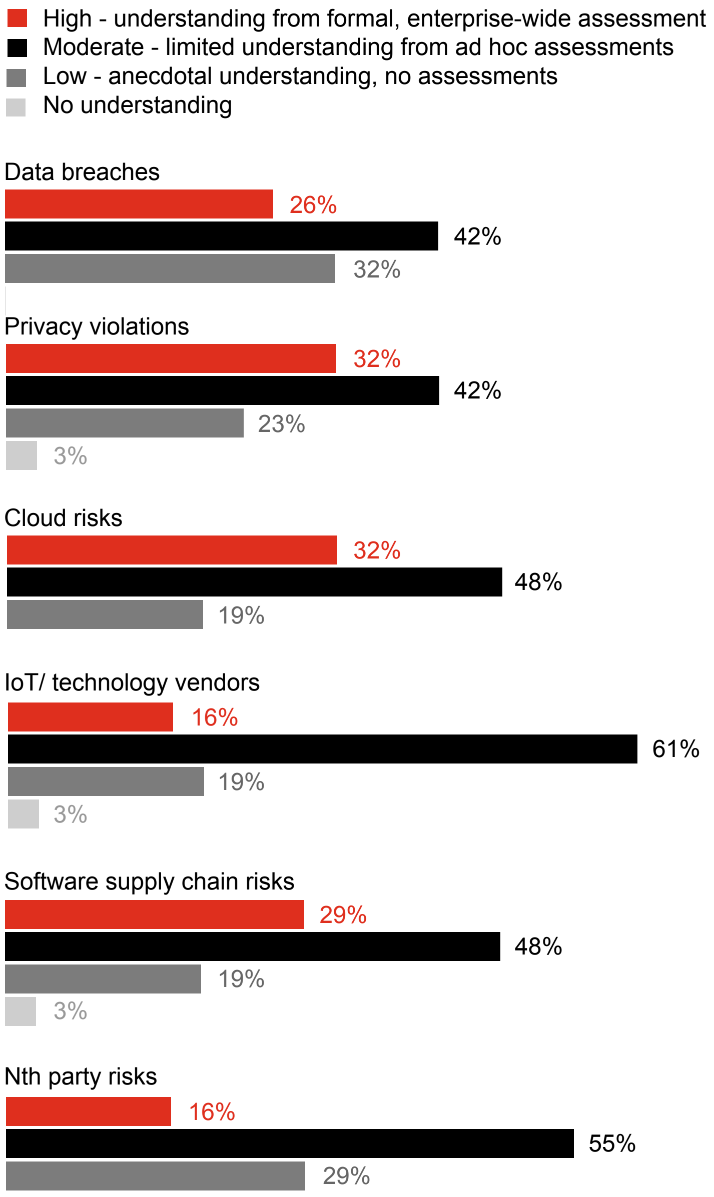
You can't secure what you can't see. Most respondents to our survey seem to have trouble seeing their third party risks — risks obscured by the complexities of their business partnerships and vendor/supplier networks.

Globally, organisations are increasingly starting to expand treatment of external party risks, also known as "nth-party" risks, expanding to include risks posed by the suppliers of their suppliers and so on. However, the more complex the network of third parties, the harder it becomes to see the risks buried within.

Understanding cyber and privacy risks: Malaysian organisations have a long way to go

Third party risk has become an unavoidable topic even among **Malaysian organisations**. Based on the data, Malaysian companies generally have insufficient understanding of the cyber and privacy risks arising from software supply chain vendors. Only 29% of respondents have a high level understanding of these risks, even though 61% of Malaysian companies expect an increase in reportable incidents on software supply chain attacks (see Figure 15, page 21). Also, there is more than a quarter (26%) with low or no understanding of privacy violations.

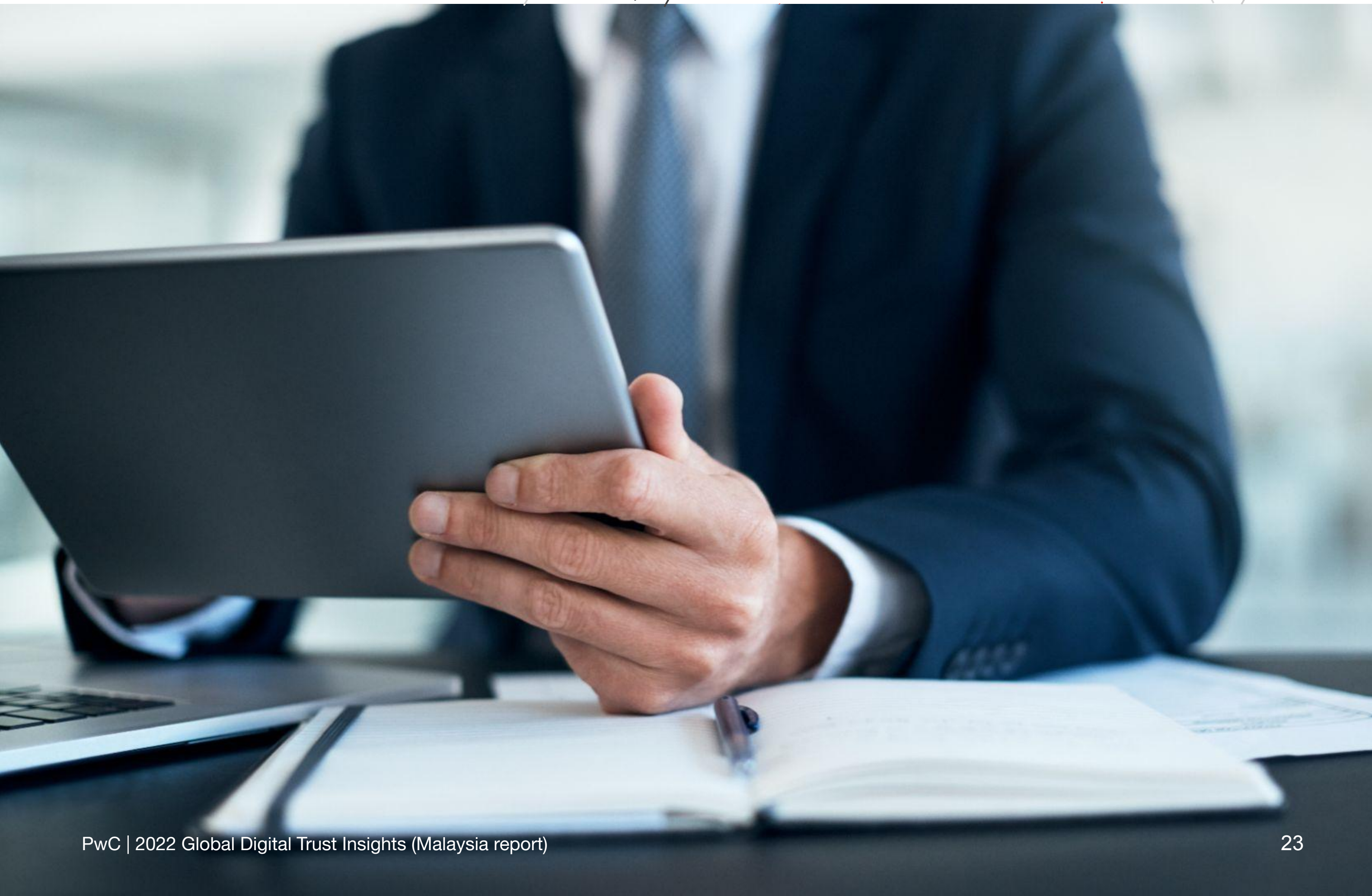
Figure 16: Malaysian organisations have a large blind spot to risks arising from third parties and the supply chain



Question: What is the level of understanding within your organisation of the cyber and privacy risks arising from your third parties or suppliers across the following areas?
Source: PwC, 2022 Global Digital Trust Insights

Fewer than half of global respondents — 30% to 46% — say they've responded to the escalating threats that complex business ecosystems pose. The ones that have responded seem to be focusing their efforts primarily on today, perhaps at the expense of tomorrow.

It's worth referring to the previous (2021) global report Building digital trust: The partnership of leadership and operations for a retrospective look at past sentiments. In the global survey, nearly half of last year's respondents said in the past year alone, they experienced significant disruptions due to third parties, including but not limited to software supply chain disruptions (47%), cloud breaches (45%), third party platform exposures and outages and downtime (41%), data exfiltration (39%). And yet the trend of new third party dependencies seen last year continues to gather steam.



Addressing third party risks

When asked how they're minimising their **third party risks**, global respondents gave largely reactionary answers: auditing or verifying their third parties' or suppliers' compliance (46%), sharing knowledge with third parties or helping them in some other way to improve their cyber stance (42%), and addressing cost- or time-related challenges to cyber resilience (40%).

Only one top response — that they are refining criteria for onboarding and ongoing assessments (42%) — could be considered proactive, offering benefits over the long term. Globally, publicly listed organisations (47%) were significantly more likely to claim this step.

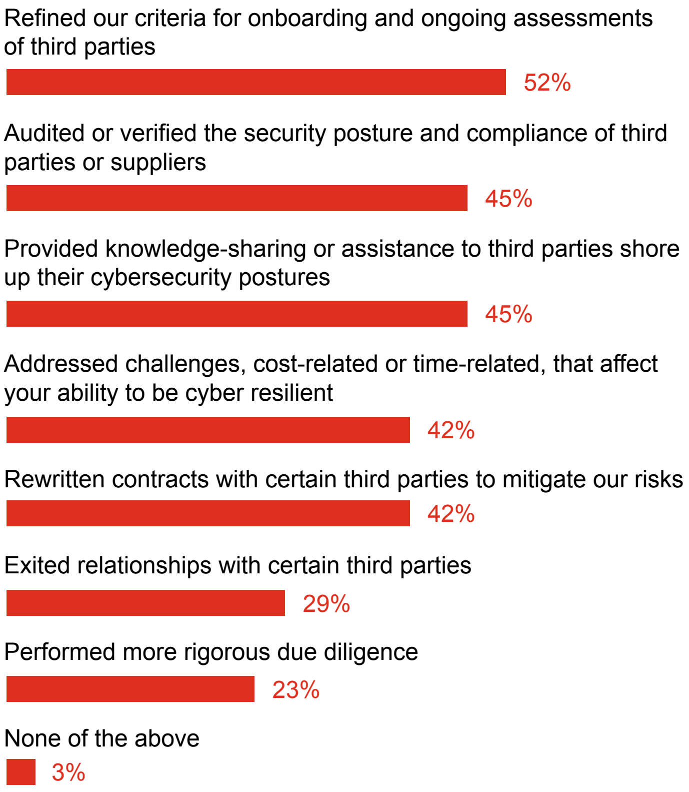
Malaysian respondents are aligned with their global peers in their response to third party risks

The landscape in **Malaysia** is pretty similar, For the past 12 months, most organisations refined the criteria for third party security assessments (52%), while 45% helped the third parties shore up their cybersecurity postures via knowledge sharing.

45% of organisations validated the security posture and compliance of third parties or their suppliers. On the other hand, just over a quarter of organisations also opted to exit relationships with certain third parties (29%) to minimise third party risks.

Still, nearly half have taken no action on their third party risk management. They've not refined their third party criteria (48%), not rewritten contracts (58%), nor increased the rigour of their due diligence (77%).

Figure 17: An encouraging proportion of Malaysian respondents have opted to revise their third party risk management processes and practices



Question: Has your organisation done any of the following actions in the past 12 months to minimise third party or supplier risks in your ecosystem? Check all that apply.
The three lasting actions are: refining criteria for third party assessments, rewriting contracts, and performing more rigorous due diligence.
Source: PwC, 2022 Global Digital Trust Insights.

Simplifying the chain

Evidently, dependence on third parties continues to rise. The “transaction” costs within the enterprise of establishing multiple nodes of partnerships (where risks are hidden) have gone down, thanks to the ubiquity and lower costs of digital interactions via APIs.

Today’s trending cyber-attack target may be the most nefarious one yet: your **supply chain of trusted vendors, suppliers and contractors**. A mere software update could be used against unsuspecting victims. The payoff is ransom payments to cybercriminals, valuable intelligence to nation-states or training data sets for AI models to competitors.

No organisation is immune to supply chain attacks

An organisation could be vulnerable to a supply chain attack even when its own cyber defences are good, with attackers simply finding new pathways into the organisation through its suppliers.

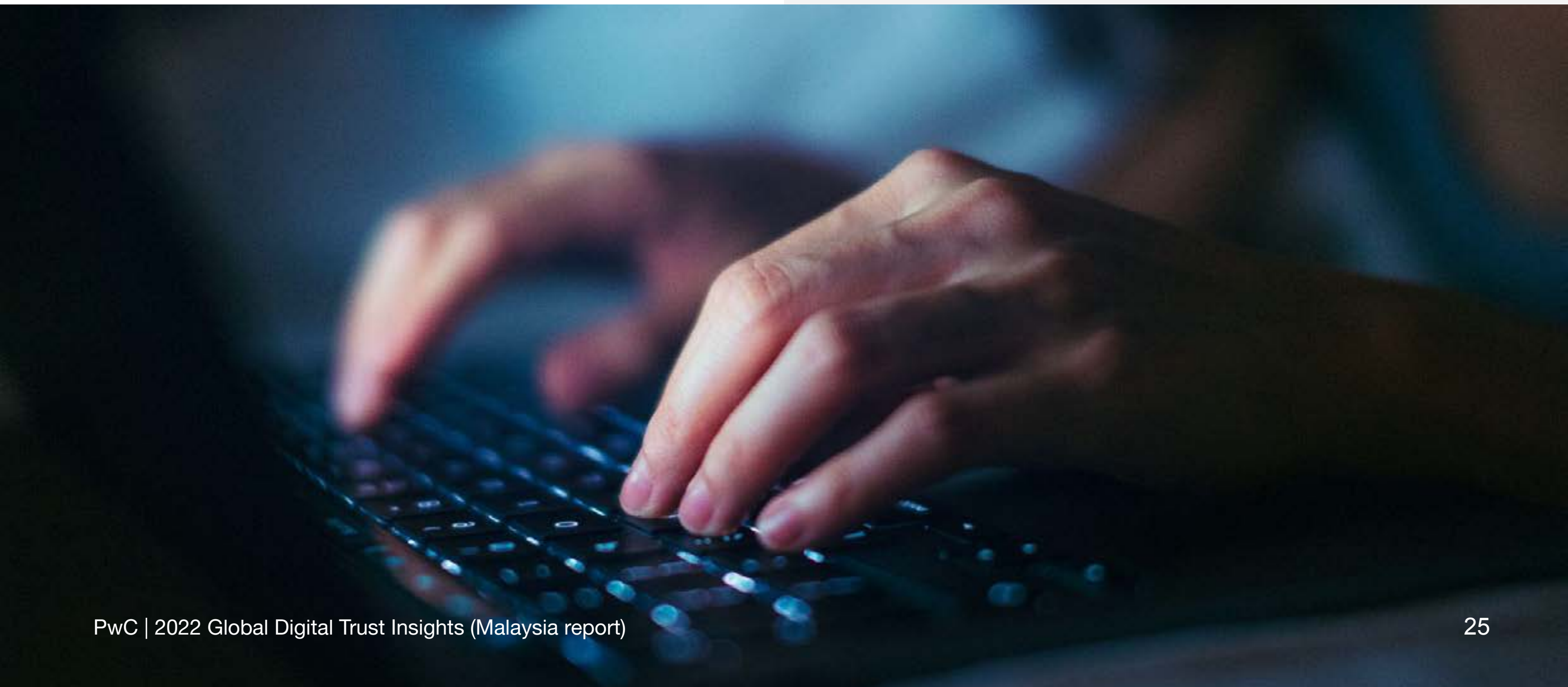
Detecting and stopping a software-based attack can be very difficult, and complex to unravel. Every component of any given software depends on other components such as code libraries, packages and modules that integrate into the software and are necessary for its operation.

As reported in our latest global Digital Trust Insights research, the organisations that had the best cyber outcomes over the past two years have consolidated tech vendors as a simplification move.

Paring the number of tech and other third parties reduces complexity and increases your ability to know how secure they are. One benefit is that different functions (procurement, risk managers, fraud team, legal, security) can better understand their roles in protecting their supply chains from cyber disruptions. And with fewer vendors to monitor, your organisation can more efficiently keep an eye on their security practices.

It is key to have visibility into the web of third party relationships and dependencies. Top cybersecurity companies integrate solutions (real-time threat intelligence, threat hunting, security analytics, vulnerability management, intrusion detection and response) on broad platforms.

And often, vendors have multiple points of access within the organisations. Allowing them access to critical data at the wrong level can inadvertently expose the organisation to risks.



Public-private collaboration

Visibility also means seeing which challenges others face and what they are doing to meet them. Collaborators can be an important part of your cyber-business ecosystem.

Malaysian respondents did not deviate too much from the global average in this regard. Organisations increasing their cyber budgets in 2022 were significantly likely to say they have achieved these goals effectively:

- Share knowledge about new threats, approaches, and solutions in my peer set
- Activate public-private sector relationships for more effective responses to a cyber attack on our organisation
- Promote broader awareness and upskilling of workforce

Public-private collaboration can be crucial in addressing third party risks. From regulatory compliance to information sharing, third party risk management comes with high risks and is often a highly regulated area.

Setting up an information sharing platform with stakeholders, especially with government agencies, encourages active interactions with regulators on third party risk related topics.

Figure 18: Collaborators are an important part of secure ecosystems. More effective public-private collaboration is needed before, not just after, attacks.

Goals for public-private collaboration

1 Share knowledge about new threats, approaches, solutions and best practices in my peer set

2 Activate public-private sector relationships for more effective responses to a cyber attack on our organisation

3 Promote broader awareness and upskilling of workforce

4 Provide input to government and policymakers on proposed rules and regulations

5 Demonstrate avoidance of tangible financial losses

Questions: Thinking about your most significant public-private collaboration mechanism, what are your organisation's goals with public-private collaboration? And in the past year, how well has your organisation achieved each of those goals you mentioned?
Source: PwC, 2022 Global Digital Trust Insights

Key Takeaways

For the CEO

- Frame cybersecurity as important to business growth and customer trust — not just defence and controls — to create a security mindset organisation-wide.
- Demonstrate your trust in and steadfast support for your CISO.
- Come to grips with the problems and risks in your business models and change what needs to be changed.

For the CFO & COO

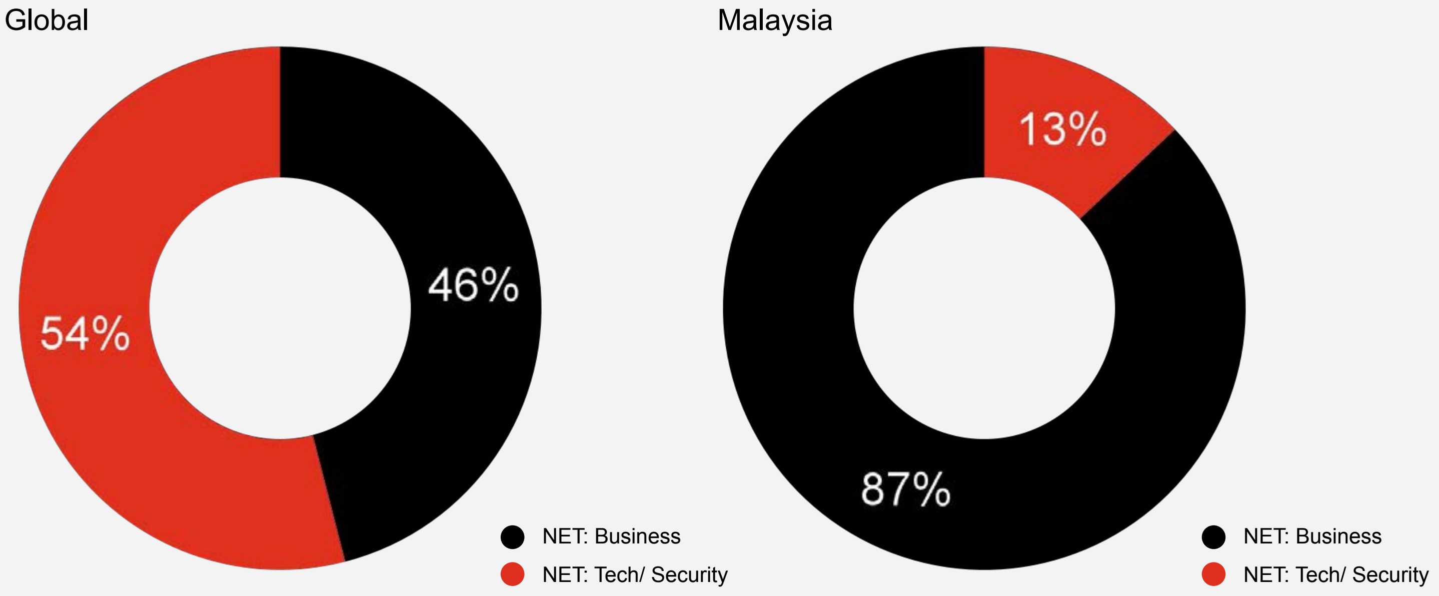
- Work with the CISO in taking a risk-based approach to cyber budgeting tied to business objectives.
- Focus on building a more mature information governance practice. Ask yourself these three questions: Which key data provides a competitive edge for your organisation? Where is the data located? Who has access to the data?

For the CRO, CISO & CIO

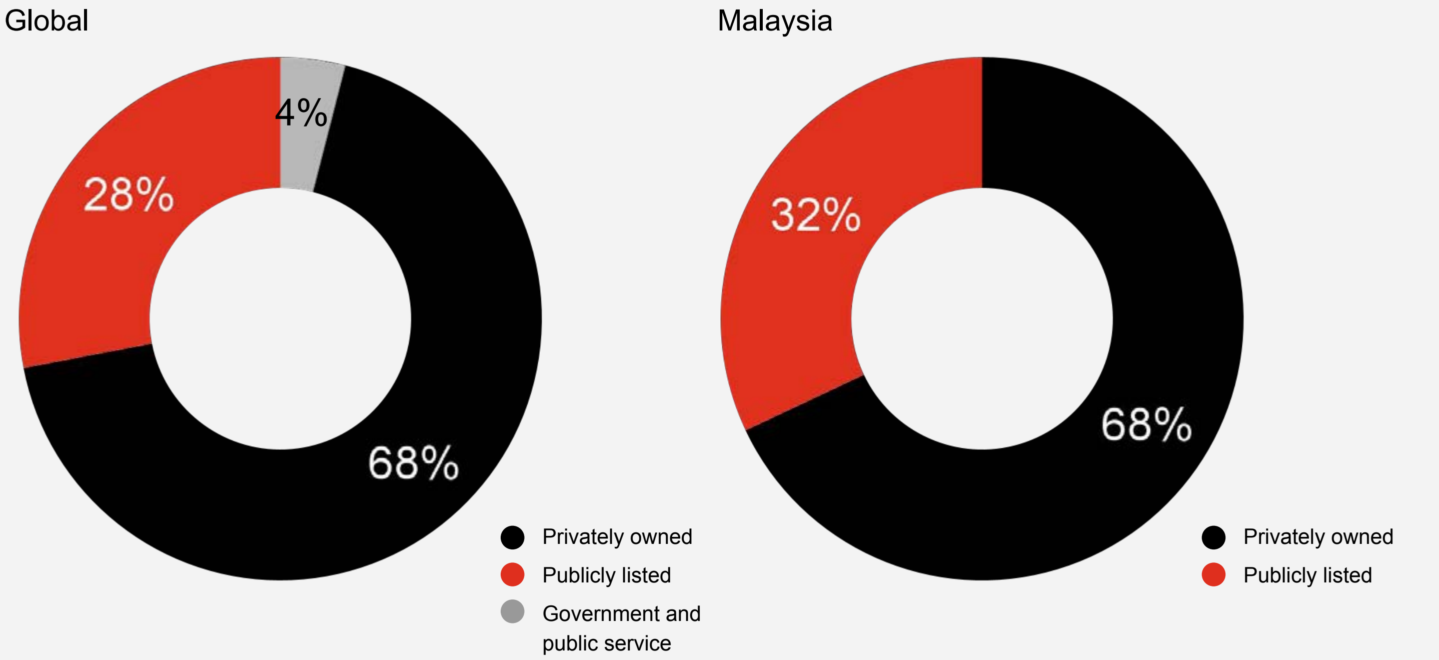
- Whittle down excess with security goals in mind: move your disparate apps and solutions into a cloud environment for easier management; and consolidate, liquidate, and automate where you can.
- Rethink your tech and cyber investment processes. Focus first on simplifying where benefits are the greatest for the whole organisation.
- Build a strong data trust foundation: an enterprise-wide approach to data governance, discovery, protection and minimisation.
- Create a roadmap to include priorities from cyber risk quantification to real-time cyber risk reporting.
- With a fuller view of cyber risks, identify what works in your business model and where simplifications are needed.
- Build up your technological ability to detect, resist and respond to cyber attacks via your software, and integrate your applications so you can manage and secure them in unison.
- Establish a third party risk management office to coordinate the activities of all functions that manage your third party risk areas. Data trust and good third party risk management go hand in hand.
- Educate your board on the cyber and business risks from your third parties and supply chain.

Demographics

Job Title

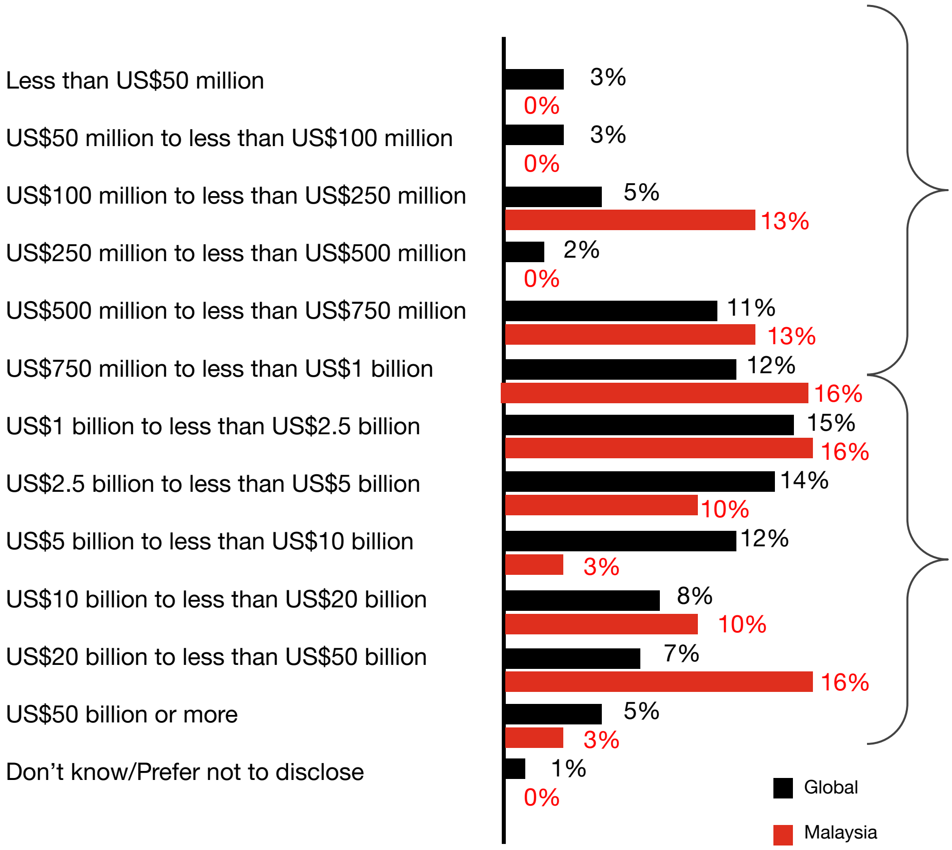


Organisation ownership



Demographic

Revenue



NET: Less than US$1 billion

Global: 37%

Malaysia: **42%**

NET: Greater than US$1 billion

Global: 62%

Malaysia: **58%**

Gender

Male

Global: 66%

Malaysia:

74%

Female

Global: 33%

Malaysia:

26%

About the survey

The 2022 Global Digital Trust Insights is a survey conducted in July and August 2021 among 3,602 global business, technology, and security executives (CEOs, corporate directors, CFOs, CISOs, CIOs, and C-Suite officers). 633 were Asia Pacific respondents and 31 were from Malaysia.

The Global Digital Trust Insights Survey is formally known as the Global State of Information Security Survey (GSISS). PwC Research, PwC's global Centre of Excellence for market research and insight, conducted this survey.

Contact us

Elaine Ng

Partner, Risk Assurance Leader
PwC Malaysia
+603 2173 1164
yee.ling.ng@pwc.com

Clarence Chan

Director, Digital Trust & Cybersecurity
PwC Malaysia
+603 2173 0344
clarence.ck.chan@pwc.com

Alex Cheng

Senior Manager,
Digital Trust & Cybersecurity
PwC Malaysia
+ 603 2173 0647
alex.ct.cheng@pwc.com

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.