Cybersecurity comes of age

Digital Trust Insights Survey 2021
Malaysia report

www.pwc.com/my

Introduction

As the world continues to adapt to new ways of working in a COVID-19 landscape, organisations are ramping up their efforts to embark on digital transformation initiatives. Some are rethinking their cyber strategy in ways they have never done before, and arming themselves with new tools to improve their resilience amidst increasing pressures to build trust among their customers and their wider stakeholders.

PwC's **Digital Trust Insights (DTI) Survey 2021** was conducted among 3,249 business and technology executives globally from July to August 2020. The survey focuses on the recent trends and the next big wave in cybersecurity as automation and new technologies continue to evolve how we operate as businesses.

30 Malaysian respondents comprising C-suites and non-C-suites shared their views on what's next for them in this volatile landscape, including what their concerns are, how they are changing their approaches and thinking, where they are putting their money and how they are upskilling their teams.

From cybersecurity to digital trust

The pandemic has no doubt been an impetus for digital adoption while also presenting significant risks. Organisations realise that using data effectively is critical as a competitive differentiator. They are also cognisant that they need to be better prepared to respond to mounting and increasingly sophisticated cyber threats that are targeted at their data and their digital identities.

Adopting a **cyber-resilient mindset** is crucial. Organisations will need to step up in establishing digital trust and enhancing their cyber-resilience, shifting their focus from pure prevention to proactive monitoring.

A business-driven cyber strategy is the important first step for business and security leaders amid sweeping, rapid business digitisation. This reset not only defines the expanding role of the Chief Information Security Officer (CISO); it also affects the way the organisation sets cyber budgets, invests in security solutions, plans for resilience, and enhances its security posture. It determines whether CISOs may grow to become stewards of digital trust, and whether they are able to lead their organisations securely into the new era with strategies to protect business value and to create it.

With the introduction of the Risk Management in Technology (RMiT) Guidelines by Bank Negara Malaysia (BNM), the role of the CISO is now mandatory in the financial services industry. Under the Guidelines, financial institutions are required to ensure that sufficient authority, independence and resources are given to the CISO to carry out their function in managing technology and cybersecurity risks. Many financial institutions have now formally appointed a CISO.

Organisations from other Critical National Information Infrastructure (CNII) sectors such as telecommunications are amongst those who have similar appointments. Organisations are after all, increasingly recognising that trust is not only an outcome of strong cybersecurity, but a critical asset that needs to be continuously protected and nurtured to help them better withstand the shocks of a volatile landscape.

Key findings

Evolving with the times: COVID-19 changes the game for cybersecurity

The pandemic continues to transform the way we work. According to the Malaysian respondents of our DTI survey, 60% are facing less than 100% capacity and experiencing intermittent closures due to the virus outbreak. Almost half of the survey's global and Asia Pacific respondents are also facing similar situations. 67% of the Malaysian respondents say that accelerated digitalisation for growth is an impact to their industry as they continue to work around the implications to business caused by the pandemic.

1

Cybersecurity is getting more focus among Malaysian organisations.

Businesses are restrategising their cyber budgets to get more out of it. 63% are thinking of a new process of budgeting for cyber spend or investments.

2

Organisations are stepping up to address threats.

Businesses are recognising the threat vectors due to digital transformation. 47% are testing their resiliency to account for more low-likelihood, high-impact events.

3

Investing in every advantage is key to level the playing field with attackers.

New technologies and business models — and the fast pace of adoption — bring new risks. Cybersecurity makes high-speed digital change a lot safer. 70% say they'll adjust their cybersecurity strategy due to COVID-19 to consider cybersecurity and privacy in every business decision.

4

CISOs are evolving to the needs of business

This reset not only defines the expanding role of the CISO, but also calls for new CISO leadership modes. Savvy CISOs are in step with the vision and goals of their enterprise as a whole, not just IT.

5

The cybersecurity talent crunch is concerning.

There is a shortage of cybersecurity professionals yet rising demand for talent. 40% say they need to modernise the organisation with new capabilities.

67%

see the need to accelerate digitalisation for growth

63%

are thinking of a new process of budgeting for cyber spend or investments

70%

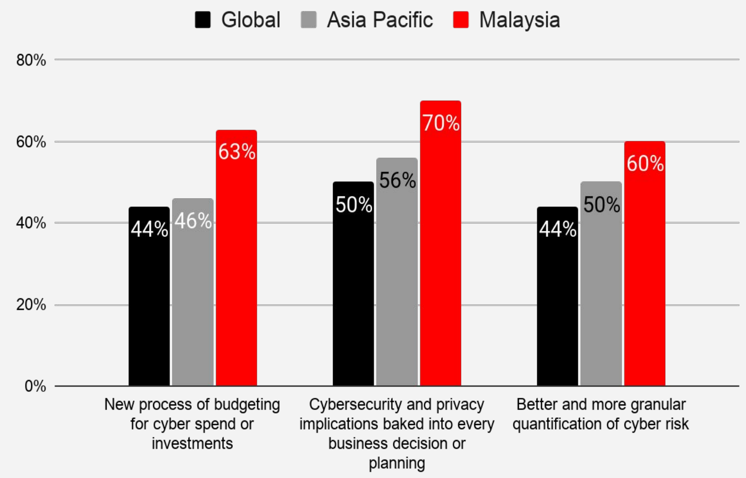
Cybersecurity and privacy implications baked into every business decision

1 Cybersecurity is getting more focus among Malaysian organisations

Boost in cybersecurity consideration and spending due to digital acceleration

We observed that organisations in Malaysia responded positively on the following key changes, ahead of their peers globally and in Asia Pacific:

- Change in budgeting process for cyber
- Embedding security and privacy in every business decision
- More granular quantification of cyber risk



Q: Which of the following changes are most likely to be impacts of the COVID-19 experience on cybersecurity in your industry?

A need for change in the budgeting process

Significant changes in the budgeting process for cyber spend or investments among Malaysians could be attributed to a few reasons. They are compelled to accelerate digitalisation for growth. Coping with customer demands, which are growing in complexity as the pandemic persists, may also be one of the main factors fueling this shift in priorities. Organisations fear that they may lose out if they don't evolve in these volatile times.

Organisations in Malaysia are also more cognisant of the security and privacy risks from digitalisation, along with the need to keep up with increasing regulations around technology and cybersecurity risks.

1 Cybersecurity is getting more focus among Malaysian organisations (cont'd)

Boost in cybersecurity consideration and spending due to digital acceleration (cont'd)

Embedding security and privacy in every business decision

These trends may explain why a significant proportion of Malaysian organisations have indicated an increased appetite to embed security and privacy implications in every business decision or during planning. It further shows that organisations in Malaysia are starting to consider having a longer term strategic risk-based investment in security as they will then be better positioned to handle threats.

This also demonstrates a shift from cybersecurity to digital trust (a custodian role which could be well placed for CISOs to take on, as CEOs and boards increasingly turn to CISOs to help improve their resilience and create business value).

As a comparison, the respondents to a 2018 PwC Malaysia survey in collaboration with the Asian Institute of Chartered Bankers (AICB) on Building a Cyber Resilient Financial Institution, revealed that 40% of security spending is still primarily driven by compliance and regulatory requirements. As our Digital Trust Insights survey shows, organisations in Malaysia have started to realise the need for cyber spending beyond compliance.

More granular quantification of cyber risk

With confidence lagging in the process used to fund cybersecurity, executives say it's time for an overhaul. Executives can do more with less, but to do so they need to quantify cyber risks more granularly or richly, and use the information to make smart choices that protect the business's security, privacy, and cash flow.

2 Organisations are stepping up to address threats

Global outlook on emerging threats

The digitisation of business operations leading to dependencies on technologies, have exposed corporations to various digital or cyber attacks - some are new and unknown to the organisations. We asked executives to rank the likelihood of cyber threats affecting their industry, and the impacts on their organisations, over the coming year.

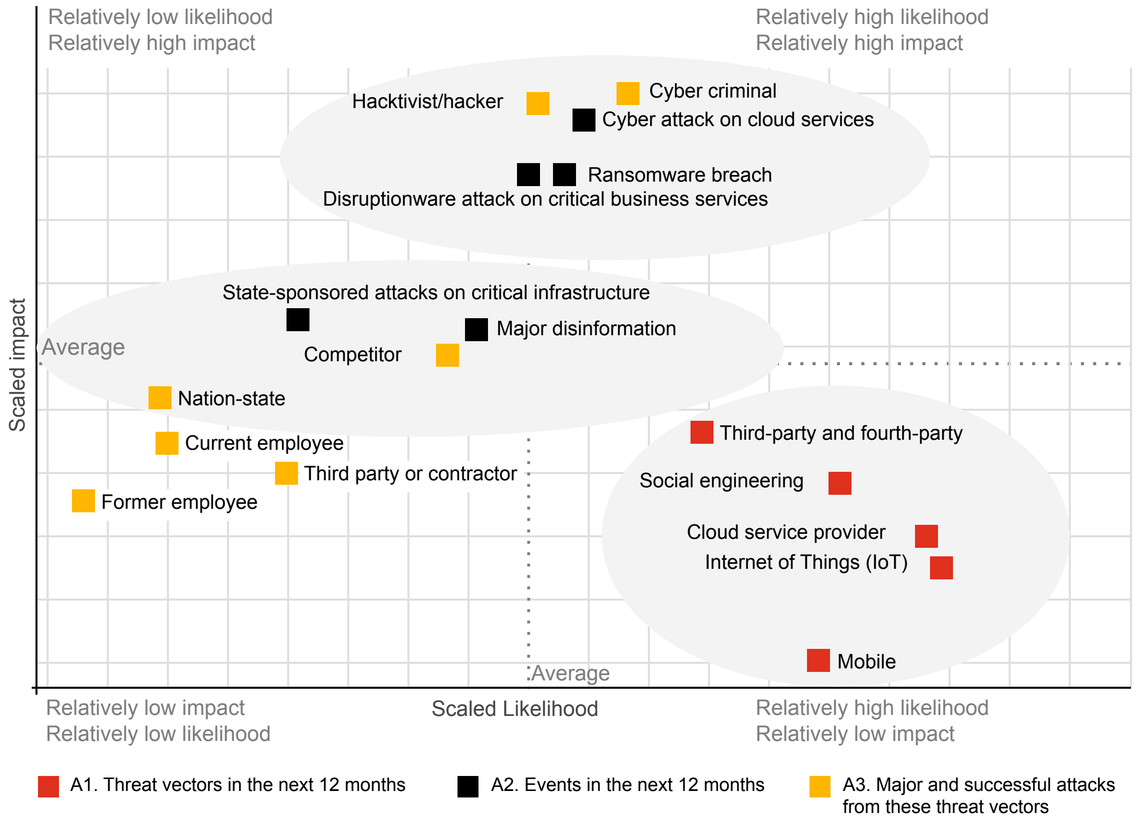
Among the global respondents, IoT and cloud service providers top the list of 'very likely' threat vectors (mentioned by 33%), while cyber attacks on cloud services top the list of threats that will have 'significantly negative impact' (reported by 24%).

More and faster digitisation means an increase in digital attack surface and potential for harm to the business. Globally, respondents say that the most likely to occur in the next year and potentially the most damaging, are attacks on cloud services, disruptionware affecting critical business services (operational technology), and ransomware.

Q: In your view, what is: (a) the likelihood that these threat vectors are going to affect your industry in the next 12 months, and (b) the extent of impact, if it were to happen, on your organisation?

Q: In your view, what is: (a) the likelihood of these events occuring in your industry in the next 12 months, and (b) the extent of impact, if it were to happen, on your organisation?

Q: In your view, what is: (a) the likelihood of a major and successful attack from these threat actors in your industry in the next 12 months, and (b) the extent of impact, if there was a successful attack, on your organisation?



Note: Respondents who have selected 'Don't Know' for Likelihood OR 'Impact Unknown at this time' for Impact have been excluded from this analysis to ensure that the same base is used on both scales.

Outlook on emerging threats in Malaysia

Cloud services is the next big switch (and concern)

Among Malaysian respondents, 77% indicated that there is a high likelihood that cyber threat vectors would stem from cloud service providers. 70% of survey respondents say that it is likely that cyber attacks on cloud services would occur in the next 12 months in which 70% agree that the impact is expected to be significantly negative.

This is concerning considering the increasing trend towards dynamic, nimble, integrated cloud systems. 83% of the local respondents are rapidly moving their operations as well as security to the cloud. And 93% of Malaysian respondents agree[1] that moving more services and infrastructure to the cloud is foundational for the next generation of business solutions for their organisation.

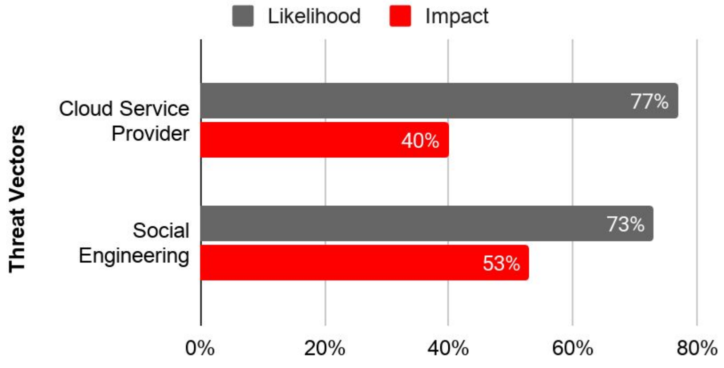
With the increasing implementation of cloud services by the financial services industry, BNM expects financial institutions (FIs) to conduct a comprehensive risk assessment on the cloud services and deployment model to understand its underlying security risks prior to adoption. The Risk Management in Technology (RMiT) Guidelines by Bank Negara Malaysia (BNM) took effect in January 2020, and it is applicable to all FIs licensed with Bank Negara Malaysia.

Malaysian sentiments

Q: In your view, what is:

(a) the likelihood that these threat vectors are going to affect your industry in the next 12 months, and

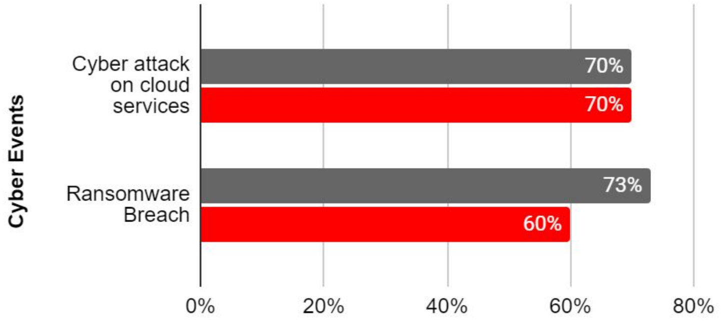
(b) the extent of impact, if it were to happen, on your organisation?



Q: In your view, what is:

(a) the likelihood of these events occurring in your industry in the next 12 months, and

(b) the extent of impact, if it were to happen, on your organisation?



[1] Respondents who 'agree' comprise those who stated 'strongly agree' and 'somewhat agree' in their answers.

2 Organisations are stepping up to address threats (cont'd)

Outlook on emerging threats in Malaysia (cont'd)

Widespread ransomware and phishing campaigns

Over the last 6 months, we saw a spike in cybersecurity incidents with significant impact on organisations already dealing with the challenges posed by the pandemic.

COVID-19 themed phishing and spear-phishing attacks were targeted at employees to steal user credentials and confidential data. Perpetrators were exploiting the popularity of COVID-19 related news and headlines to lure unsuspecting victims. Ransomware attacks compromising remote services (or work from home set-ups) which led to successful data exfiltration are also amongst the top threats affecting organisations both globally and in Malaysia.

Based on our survey, 73% of local respondents indicated that a **ransomware breach** would be likely to occur in their industry in the next 12 months, with 60% expecting such incidents to have a significantly negative impact.

Recent events involving **data leakages and breaches** of databases of sensitive information such as full names, ID numbers, addresses i.e. information classified as Personally Identifiable Information (PII) on local organisations, further substantiate such concerns.

With COVID-19 as a possible event demonstrating how businesses can be halted overnight, is your business resilient to these threat vectors?

82.5%

increase in cybersecurity incidents during the Movement Control Order (MCO) in 2020 compared to the same period in 2019 (18 March - 7 April 2020)

Source: CyberSecurity Malaysia

Building resilience for any threat scenario

Based on our survey, all Malaysian respondents (and 76% of respondents globally) agreed with the statement, “Assessments and testing if done right, will help in targeted investments in cybersecurity.” So it makes sense that organisations in Malaysia should plan to increase resilience testing to ensure that if a disruptive cyber event happens, their critical business functions will stay up and running.

Recent high profile cybersecurity attacks further prove that no organisation can be spared from cyber breaches. It is critical for organisations to be able to respond to, and recover from breaches as it is to be able to prevent them.

3 Investing in every advantage is key to level the playing field with attackers

Improve the management of cybersecurity risks

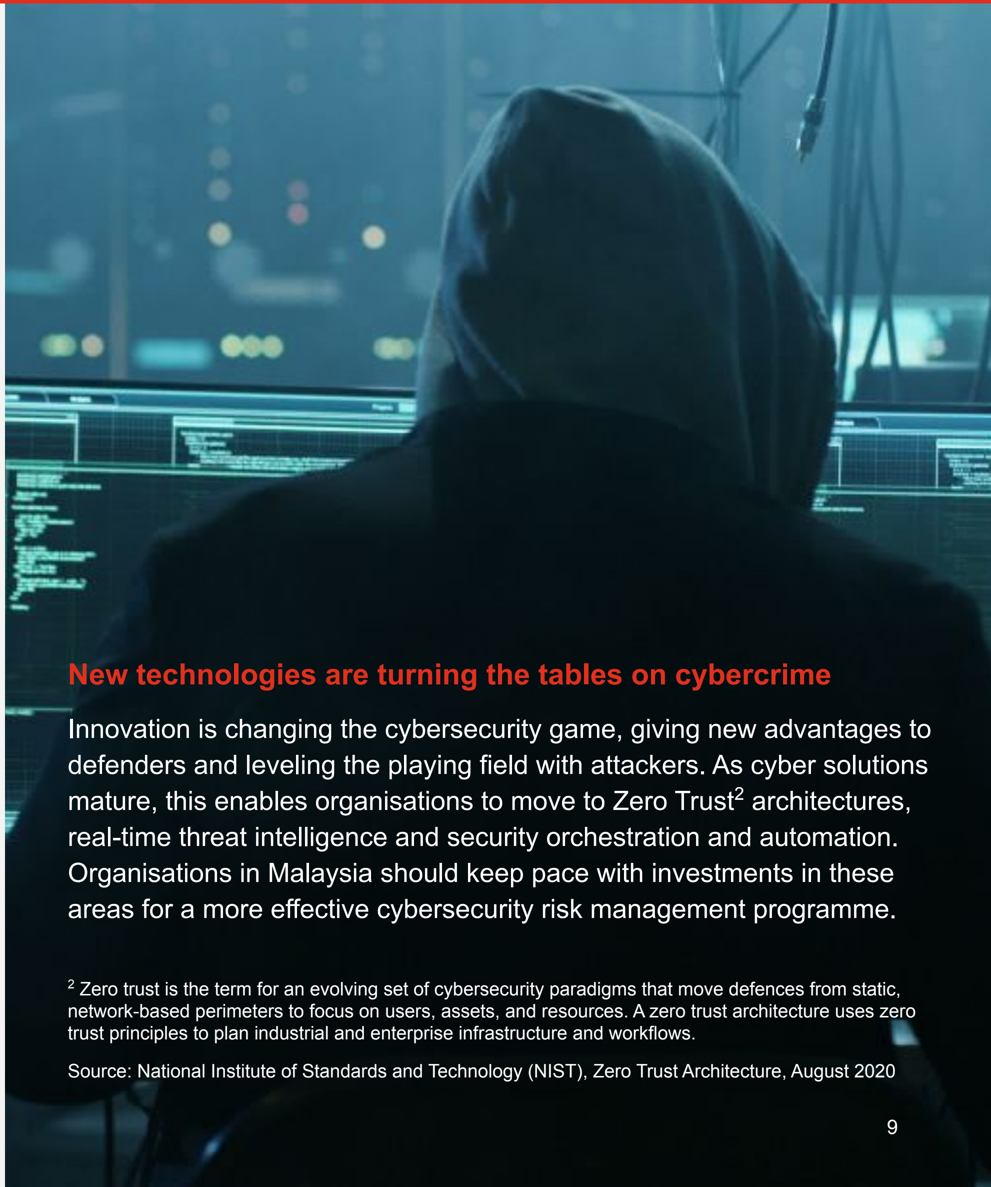
Good cyber hygiene is critical in staving off these threats. We are seeing early switchers embracing new solutions more quickly than they typically would, in adjusting to the new normal.

Early switchers are setting the trend for other players in the market and have taken advantage of the developments of an array of cyber solutions. But, more importantly, they're investing in the classic digital transformation trifecta — **people, processes, and technologies** — to close the wide lead that attackers have long held. These early switchers are already benefiting from some of these new practices.

Our survey indicates that organisations in Malaysia are most likely investing in the following areas that are expected to lead to improvements in managing cybersecurity risks:

People	▶ Improve the security function's skills set ▶ Cybersecurity team to collaborate more with the business side in delivering business outcomes
Capabilities and processes	▶ Better quantify cyber risks ▶ Unify the reporting across the organisation on cyber risks
Technology	▶ Invest in advanced technologies to improve the effectiveness of their organisation's cyber defence and security detection capabilities ▶ Reduce the cost of cyber operations via automation, rationalisation and/or other solutions

Q: To what extent is your organisation investing in the following ways to improve the management of cybersecurity risks in your organisation over the next 2 years? (Respondents who stated "Realising benefits from implementation")



New technologies are turning the tables on cybercrime

Innovation is changing the cybersecurity game, giving new advantages to defenders and leveling the playing field with attackers. As cyber solutions mature, this enables organisations to move to Zero Trust[2] architectures, real-time threat intelligence and security orchestration and automation. Organisations in Malaysia should keep pace with investments in these areas for a more effective cybersecurity risk management programme.

[2] Zero trust is the term for an evolving set of cybersecurity paradigms that move defences from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture uses zero trust principles to plan industrial and enterprise infrastructure and workflows.

Source: National Institute of Standards and Technology (NIST), Zero Trust Architecture, August 2020

4 CISOs are evolving to the needs of business

CISOs need to play encompassing roles

Beyond the financial services industry, the expansion of the Information Security function in recent times has also paved the way for more Malaysian organisations to appoint a CISO.

As organisations embark on initiatives to strengthen their information security posture in these volatile times, they look to the CISO to provide clear leadership and strategic decisions while nurturing innovation.

According to the survey, the skills of a CISO which makes a difference to the business are:

- Strategic insights/ability
- Ability to make data-driven decisions / take smart risks
- Ability to recognise and nurture innovation

An increased reliance on the CISO role post-pandemic

According to a separate PwC pulse survey which polled the first responses to the COVID-19 pandemic, 141 security and information leaders were in agreement that CISOs and CIOs were on the frontlines as C-suite executives shaped crisis plans, especially with the sudden shift to large scale remote work and the acceleration of digitisation in new or previously untested areas.

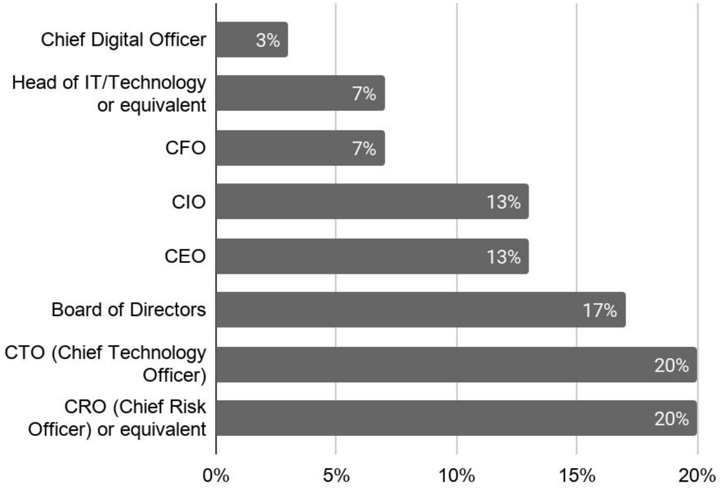
Leading corporations through strategic steering of digital roadblocks and threats amidst the pandemic, CISOs demonstrated the importance of having vigilant, innovative and focused leadership for the information security function of a corporation. Having shown that a CISO plays an essential role in the C-suite amid the crisis, the CISO is looked upon as the transformational leader in using the current landscape as a springboard in enhancing digitalisation by navigating between critical and strategic investments into technology.

As mentioned in the pulse survey, a majority of CISOs interacted more frequently with their CEOs (65%) and the boards (50%) during the crisis. The increased reliance on the CISO role in recent times has also led to a potential change in the corporate governance structure of organisations. Corporate governance should include the CISO as an influential leader within a corporation, often seated amongst the ranks of other C-suite members.

The dilemma of the CISO reporting structure

With regards to the introduction of the CISO to the governance structure, only 13% of our survey respondents say that their CISO (or Cybersecurity leader) reports to the CEO, whereas 40% of respondents continue to have the CISO reporting to the CTO, CIO or Head of IT collectively.

Clearly, organisations in Malaysia are still behind their peers globally and in Asia Pacific, where the CISO has taken on a more strategic leadership role in an organisation and become the steward of digital trust.



Q: To whom does the CISO/cybersecurity leader directly report?

5 The cybersecurity talent crunch is concerning

The cybersecurity talent crunch is concerning.

Unsurprisingly, talent management and upskilling plays an important role in today's cybersecurity landscape for long term gains in the future. 40% of Malaysian respondents are aspiring to modernise their organisation with new capabilities and 30% are progressing to invest in improving the security function's skills set.

Talent management

With the increase in demand for advancements in security measures and cybersecurity preventive and detective controls, comes an increase in demand for the governance required in managing the cybersecurity or information security function of a corporation.

64% of Malaysian respondents say that an increase in the headcount of the cybersecurity team is to be expected in the next 12 months.

With this anticipated increase in headcount, surges in demand for cybersecurity talents can be observed in the recruitment scene. While there is a growing demand for talents to support cybersecurity functions in organisations, it is concerning to note the acute cybersecurity talent shortage in the market.

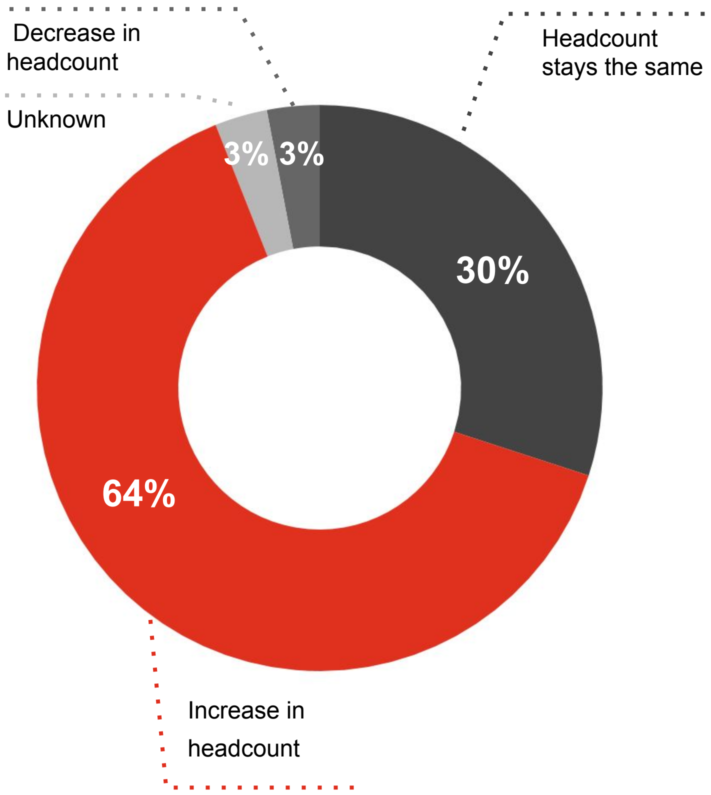
Upskilling and training

Executives are naturally seeking more technologically skilled and digitally equipped new hires. 67% of respondents have expressed that skills such as data management, and security intelligence (also 67%) are highly sought after. Data analysis is the next highest skill set in demand (63%), followed by knowledge and experience in cloud solutions (60%).

Although technical acumen is highly sought after, social skills (including critical thinking) and business enablers (such as analytical skills and project management) are also in demand. Analytical skills are sought after by 80% of respondents, project management skills by 57% of respondents, and critical thinking by 73% of respondents.

This demonstrates the need for a healthy balance of soft, technical and digital skills, as well as a growth mindset to continuously make learning and relearning part of the individual's DNA, in order to succeed as a cybersecurity professional in the current landscape.

External hires are not the only option for recruitment given the shortage of such talents globally. Corporations should encourage internal upskilling of their employees, promoting from within to form competent cybersecurity teams. Enhancing work flexibility and encouraging collaborative and innovative thinking can further incentivise internal upskilling.



Q: How is headcount for your cybersecurity team changing in the next 12 months?

Key takeaways

1

Increase and rethink cyber spending

Organisations are starting to think beyond just complying with rules and regulations. Expansion in cybersecurity spending is essential to align with longer term strategic risks in the overall enterprise or business unit to build a better cybersecurity posture.

2

Fundamentals of data management

Demand for privacy and data protection are propelling organisations to step up in delivering consistent system performance, and improve their data management capabilities by embedding security and privacy in every business decision. As we head into 2021, organisations should reexamine their cybersecurity approaches to future-proof their data management strategy.

3

Transformational leadership

Bold and decisive leadership is necessary for innovation and transformation to take place. CISOs play an essential role in steering the organisation through digital roadblocks and threats, with their experience and foresight. They are able to lead critical digital shifts in business operations with their deep understanding of the organisation's vision.

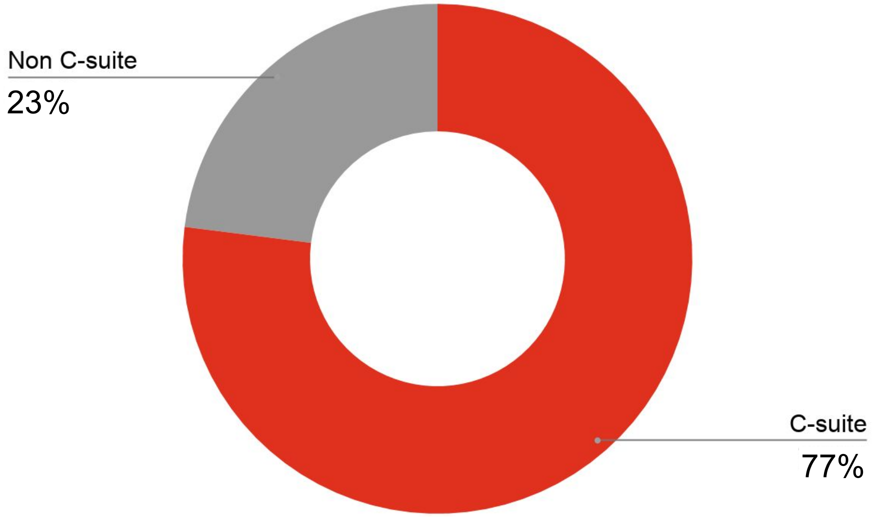
4

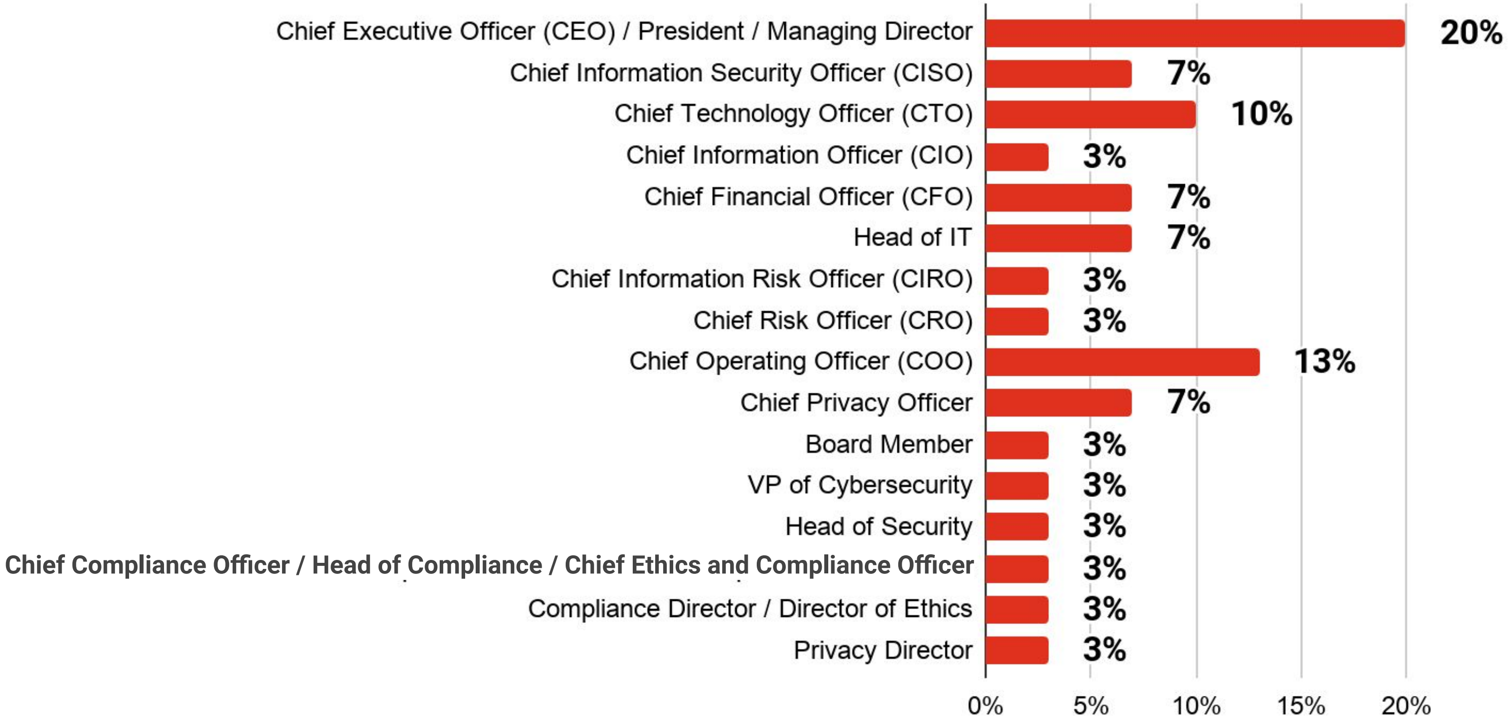
Upskill from within

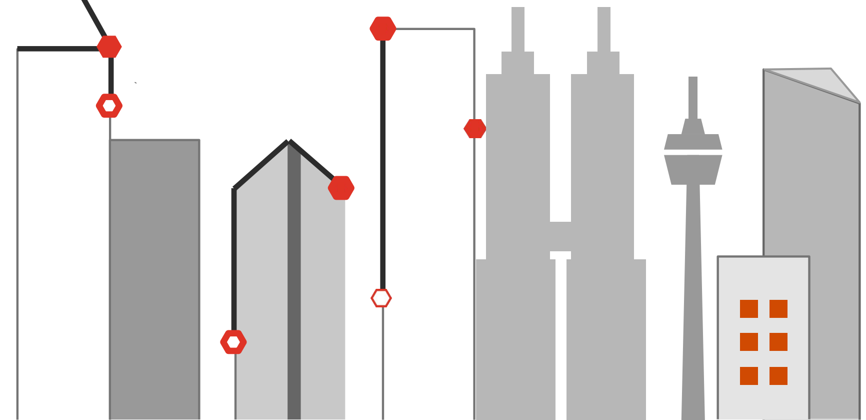
Cybersecurity talent shortage is evident globally. Companies are urged to train and reskill their existing talents to equip them with both technical and business acumen. This is the way forward in future-proofing their security teams.

Respondent breakdown

Malaysia







Respondent breakdown

Global Respondents by Sector

22%	Technology, Media & Telecommunications
20%	Retail and Consumer
19%	Financial Services
19%	Industrial Manufacturing
8%	Healthcare
8%	Energy, Utilities and Resources
4%	Government/ Public Services

Note: Breakdown by sector for Malaysian respondents isn't available.

Contacts

Elaine Ng
Partner, Risk Assurance Leader
PwC Malaysia

+03 2173 1164
yee.ling.ng@pwc.com

Clarence Chan
Director, Digital Trust & Cybersecurity
PwC Malaysia

+03 2173 0344
clarence.ck.chan@pwc.com

Josephine Phan
Partner, IT Risk Assurance
PwC Malaysia

+03 2173 0715
josephine.phan@pwc.com

Alex Cheng
Senior Manager, Digital Trust & Cybersecurity
PwC Malaysia

+03 2173 0647
alex.ct.cheng@pwc.com