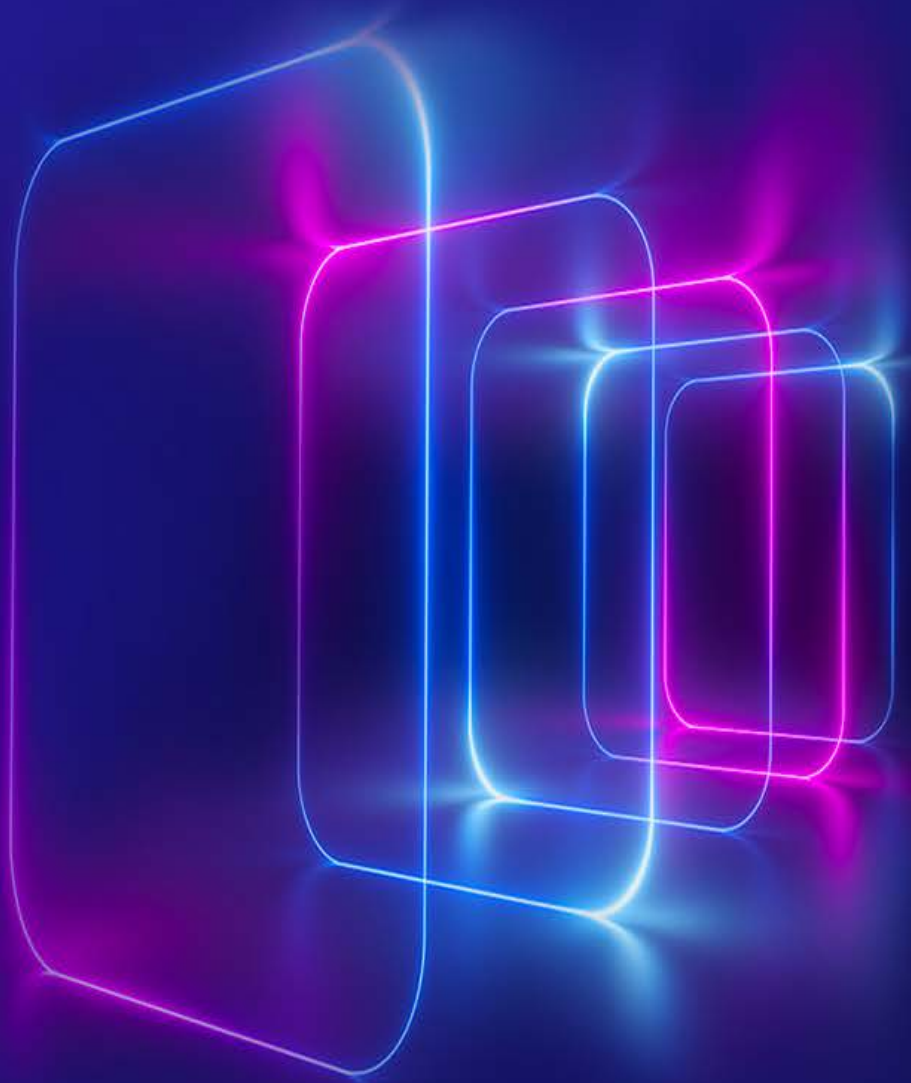
KPMG

KPMG's Australia Cyber Security Insights 2022

Building trust through cybersecurity and privacy



KPMG.com.au

Foreword

Building trust through cyber security and privacy

As Australian businesses continue their widespread digital adoption, it is right and expected that our concerns about cyber security broaden alongside it. I am pleased this is happening at a national level, with the Australian government recognising the critical nature of our industry by identifying cyber security as one of the six sectors vital to the overall long-term health of the Australian economy.

Unfortunately, attacks on businesses continue, with malicious attacks, system faults and human errors being identified as the three primary sources of data breaches in Australia. Despite our technological advances and a 10x increase in controls, we are not winning the battle.

It's one of the reasons KPMG's 2022 Australian Cyber Security Insights report is important. We can better understand and acknowledge our problems by seeking views from a cross-section of Australian businesses. Only then can we look to measure and fix these by **building inherent trust**, ensuring **ethical use of data**, **responding** appropriately to cyber incidents and creating **trusted communities**.

The report delivers some informative insights. With the value of assets such as data, brand repute and customer perception at risk, prevention is a focus for the majority. Most respondents feel the need to increase transparency, manage privacy concerns and implement careful governance and oversight–especially with AI/ML solutions. Organisations also recognise the value of external cyber collaborations, stating they improve their ability to anticipate and recover from cyber-attacks, yet less than half collaborate or share information.

Despite the many challenges, there is opportunity. As people are the weakest chink in our cyber armour, we should pay greater attention to the human element. I believe this can be strengthened by creating a culture of cyber security. If enterprises treat cyber and privacy as a golden thread, it can be woven into business processes and governance-enabling humans to become our strongest defence instead.

Martijn Verbree
Cyber Security Australian Lead

Contents

1

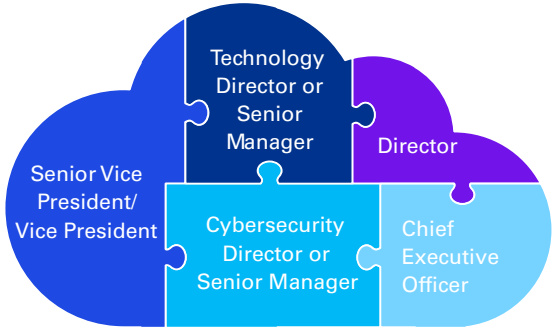
Respondent analysis

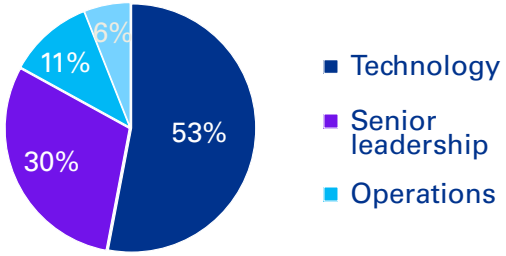
Business sectors of responders

- Financial services
- Life science/ healthcare pharmaceutical
- Technology, media and telecom (TMT)
- Public sector/ government
- Energy and natural resources

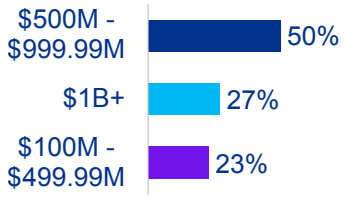
Respondent analysis

KPMG's 2022 Australian Cyber Security Insights report is based on a survey of about 100 respondents from across Australia, understanding their views about building inherent trust, the ethicality of data, responding to cyber incidents and creating trusted communities. The survey covers respondents spanning various industry sectors across firms with varying revenue. It also covers leaders in the field of cyber security and cyber security executives.

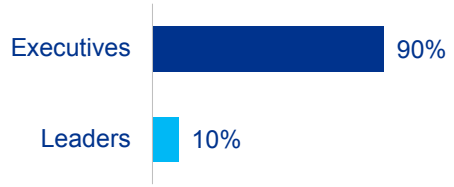




Revenue



Cyber leaders



Source: Cyber Security Insights 2022

2

Australian Cyber Landscape Overview

Increased business growth, cyber incidents and responses.

The Australian Cyber Security Center (ACSC), observed 67,500 cyber crime reports in FY21, a nearly 13 per cent increase from the previous financial year.*

AU $33 billon

Approximate total cybercrime inflicted financial losses.[1]

AU $50,600

Average loss per successful business email compromise.[2]

As a leading economy in the ASPAC, Australia's cyber security concerns have grown alongside the widespread digital adoption across the business landscape. Increased digitisation brings increased risk, and losses businesses face due to cyber incidents. Evidently, in Australia, a cyber crime has been reported approximately every eight minutes, with Queensland and Victoria witnessing the highest proportion of cyber incidents during 2020–21.[1]

The Australian government has been responding with a multi-pronged approach, formalising and implementing the Cyber Security Strategy 2020 and the Ransomware Action Plan and establishing the Industry Advisory Committee (IAC) to monitor the progress on implementing its cyber security strategy.

Cyber attacks in the region have been primarily motivated by attempts to acquire Personally Identifiable Information (PII), which has been the cause of data breaches across most sectors. The increase in AI-enabled cybersecurity, coupled with an acute shortage of cyber experts in Australia, is pushing enterprises to assess their position on cybersecurity and evaluate decisions regarding the funding of cyber security programs/ outsourcing of cybersecurity.[3]

Most prominent cyber security incident types across the Australian landscape[4]

Social engineering attacks

Business email compromise (BEC)

Supply chain compromise

Ransomware threats

Mobile malware

*1 ACSC Annual Cyber Threat Report,

2 International Trade Administration country commercial guide,

3 OAIC notifiable data breaches report

4 OAIC Notifiable data breaches report_Jul-Dec2021

How do enterprises perceive trust?

Digital trust is the confidence stakeholders have in the ability of an enterprise to harness digital technology to protect their interests and uphold societal expectations and values.

Digital trust typically covers security and reliability, inclusive, ethical and responsible use of data, and accountability and oversight.

More than one in three respondents believe increasing trust in the business results in:

- better customer and employee retention,
- stronger commercial relationships with stakeholders, and
- improved profitability.

However, over half do not see information security as a business enabler. Instead, it is viewed as a risk reduction activity or as being shaped by compliance requirements.

As enterprises increase their use of customer data for personalisation, perform multi-channel integrations and create self-serve channels to revamp the customer experience, they increase their cyber risk exposure.

With successful ransomware attacks growing in number, It is evident that **building inherent trust** in their operations, systems and channels by ensuring the **ethical use of data**, establishing cyber **response** mechanisms and creating **trusted communities** is the need of the hour.

Do you agree/disagree with the following statements?

Chart shows percentage of respondents who selected each option in their top three.

Increasing trust across the stakeholder spectrum is emerging as a leading consideration within Australian cyber-risk programs.

Source: 5 OAIC notifiable data breaches report

3

Inherent Trust

Driving digital trust through cyber security culture.

A lack of local talent increases the complexity of building digital trust.

Data breaches lead to significant downtime, disruption to operations, and impact on business valuation. Enterprises are prioritising resource and budget allocations for cyber security measures and controls to achieve greater data security. However, the increase in employee turnover following 'The Great Resignation' has increased the complexity.

The limited availability of local advanced data security solutions has led many enterprises to outsource data security, increasing exposure and risk of malicious threats. According to the International Trade Administration (ITA), in 2022, Australia has been estimated to spend about AU$2.82 billion importing cyber security solutions, which comprises almost half of its total cyber security spend of AU$6.73 billion.[6]

This raises concerns about the privacy of information and the cost of acquiring such solutions, requiring immediate mitigation.

The contribution of the CISO to building digital trust.

Australian CISOs are proposing various measures to combat cyber threats and ensure data protection.

According to a Proofpoint survey of CISOs, about 75 per cent were focused on strategies that emphasised prevention over detection and mitigation of cyber attacks.

72 per cent felt that businesses needed to be insured against cyber threats to counter events such as ransomware, while maintaining data backups of information of their customers.[7]

CISOs have been urging businesses to adopt a "Zero Trust Policy" to build stakeholder trust. However, they believe their views on cyber security, are sometimes misaligned with their stakeholders. This can lead to serious data security concerns. It is crucial that CISOs and stakeholders work collaboratively to ensure data security.

>1 in 3

respondents indicated that factors such as transparency about how their data is protected, stored and used, and governance mechanisms in place were even more crucial parameters of stakeholder trust than adverse publicity.

30%

respondents felt that handling stakeholder and public communications in the aftermath of cyber attacks, increasing the transparency around data usage and privacy, and promoting cyber security awareness were key action items for CISO teams to pursue.

6 International Trade Administration

7 ProofPoint Voice Of CISO Survey

Note: US$1=AU$0.67369, as on 15 Sept 2022

Make cyber security everyone's responsibility with a strong Cyber Security Culture."

Martijn Verbree
Cyber Security Australian Lead

48%

Respondents were less confident in their organisation's ability to subjectively assess cyber risks.

40%

Respondents felt the need for tailored cyber risk strategies and comprehensive risk modelling for specific scenarios.

30%

Respondents felt that their organisation needed to better quantify its cyber risk.

~1 in 4

Respondents felt that digital trust remained an abstract concept for their enterprise.

Creating a cyber security culture is imperative to effective cyber risk management

Obtaining buy-in across all business levels is crucial to pre-empt cyber attacks, avoid lapses in compliance, reputational damage, and control access to data. Cyber risk programs can help improve an organisation's overall security posture and should extend across the entire value chain, from third-party vendors to employees to the board.

Treating cyber security and privacy as a golden thread woven through an enterprise embeds cyber security into the culture, making it everyone's responsibility.

Employees and vendors can help detect and avoid intellectual property theft, product blueprints theft and protect PII. Boards can ensure the availability of adequate resources and funding to drive effective cyber security measures for mitigating data breaches and avoiding regulatory fines.

CISO teams in Australia are adopting technology such as network detection and response (NDR) to improve vulnerability scanning and patch management, which helps identify high-risk assets, while reducing the possibility of patching delays.

According to a survey by ProofPoint, lack of skills is one of the major concerns for infosec teams, with 76 per cent of Australian CISOs considering human error the biggest cyber vulnerability. Threat trainings for employees are expected to increase the rate of threat detection.[8]

However, many organisations in Australia are still leveraging traditional cyber security infrastructure, which poses a challenge for infosec teams to handle vulnerabilities in time.

4

Ethical Data

Challenges and opportunities to consider

Facing the ethical challenges of AI

Organisations now gather, collect, analyse and disseminate data, relying on technologies such as artificial intelligence (AI)/ machine learning (ML), big data and advanced analytics. This results in personally identifiable information and critical data being subject to risks such as cyber threats, espionage, unethical usage and data leakage. The Australian government has developed the AI Ethics Framework to ensure acceptable and responsible usage of AI algorithms while still recognising the potential of technology to improve productivity and offer more inclusive services across industries.

According to our survey, more than two-thirds of respondents felt the need for monitoring, increasing transparency, managing privacy concerns and implementing careful governance and oversight when adopting AI/ML solutions.

AI has been crucial in defending Australian businesses and the public sector against cyber attacks. Self-learning AI systems are being deployed to protect critical infrastructure. Without historical cyber risk data, they can develop a deep understanding of all elements, including humans and machines, to extend protection against potential attacks.

Such advanced AI systems demand an explainable and trustworthy AI-based cyber security structure to ensure the ethical use of data assets. Accountability for the usage of data acquired during the self-learning process must be fixed along with a provision of consent management systems to ensure the consensual utilisation of data.

80% respondents felt that AI/ML adoption raises unique cybersecurity challenges that must be attended to on priority.

Shows percentage of respondents who agree or strongly agree.

80%

AI/ML adoption raises unique cybersecurity challenges which require special attention

74%

AI/ML adoption raises key privacy around how we train AI/ML systems and monitor their performance

77%

AI/ML adoption requires us to be more transparent in the way we communicate how we use AI/ML techniques

67%

AI/ML adoption raises fundamental ethics questions for us which require careful governance and oversight

73%

AI/ML adoption requires safeguards around training AI/ML systems

KPMG perspective: Ethical AI

Organisations know they must become data-driven or risk irrelevance. Many are scaling AI to automate data-driven decision-making, but AI brings new risks to brand and profitability. The technology has the potential to drive inequality and violate privacy, as well as limiting the capacity for autonomous and individual decision-making.

You can't simply blame the AI system itself for unwanted outcomes. Trustworthy, ethical AI is not a luxury, but a business necessity. Growing numbers of business leaders recognise this – but trust is not secured without effort or challenges.

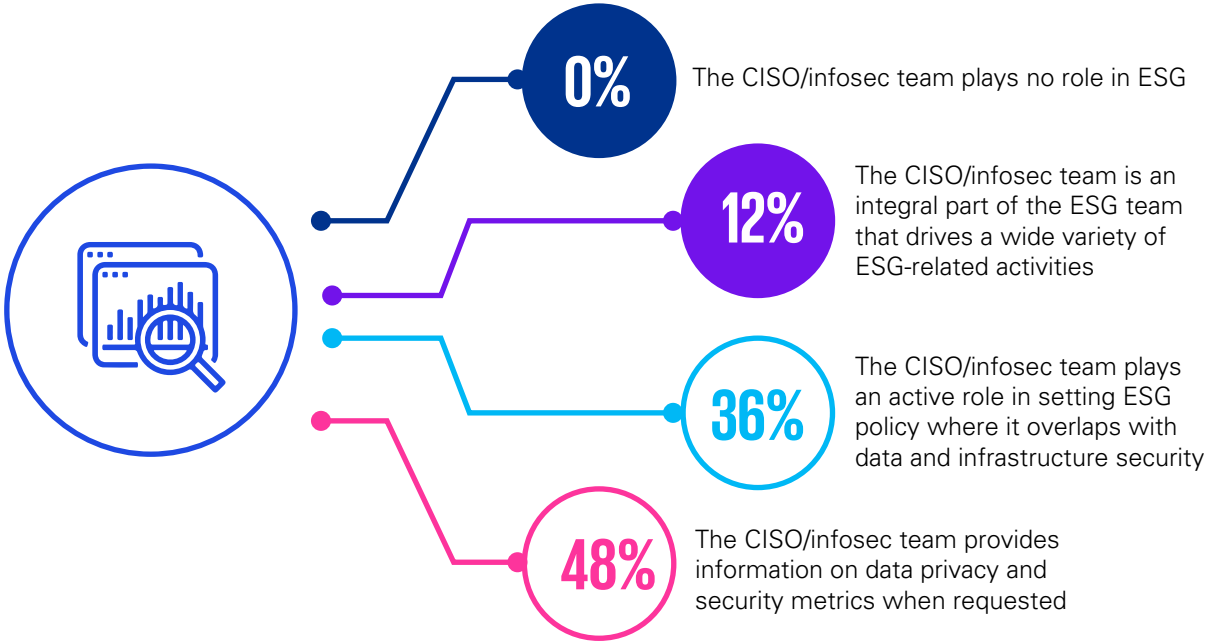
Not least, what is considered ethical and trustworthy in one sector or region may not hold in another.

There is no one-size-fits-all solution and copying existing frameworks is ineffective. Trustworthy AI can only be achieved with a holistic, technology-agnostic and broadly endorsed approach to awareness, AI governance and risk management.

For example, AI impact assessments should involve the right stakeholders to identify risks. AI needs to be aligned with organisational and stakeholder values. Organisations should carefully assess compliance with laws and regulations, as well as AI return on investment. Decisions need to be traceable and auditable. And all these protections must be implemented without impeding innovation.

Most CISOs are only passively involved in ESG policies and activities

Chart shows percentage of respondents who selected one option as their top choice.



Source: KPMG Cyber trust insights 2022

Exploring the link between cyber security and ESG

Enterprises in Australia are cognisant of the relationship between ESG policies and cyber security measures.

Almost all respondents agreed that CISO/infosec teams have a crucial role in ESG.

Yet just 1 in 10 respondents indicated that CISO/infosec teams in their enterprises are an integral part of the core ESG team.

Organisations have been slow to recognise the dependence of ESG on cybersecurity. According to a report by S&P9, intangible assets contribute about 90 per cent of the total asset values of today's organisations. Therefore, a cyber incident can directly affect an enterprise's long-term sustainability, business continuity and value.

Detrimental consequences of cyber attacks, such as fraud caused by leaked PII, can severely damage a business's reputation and erode digital trust. Given the widescale adoption of digital services by governments and healthcare institutions, a cyber attack can have far-reaching consequences for the stability of organisations, communities and, eventually, the government.

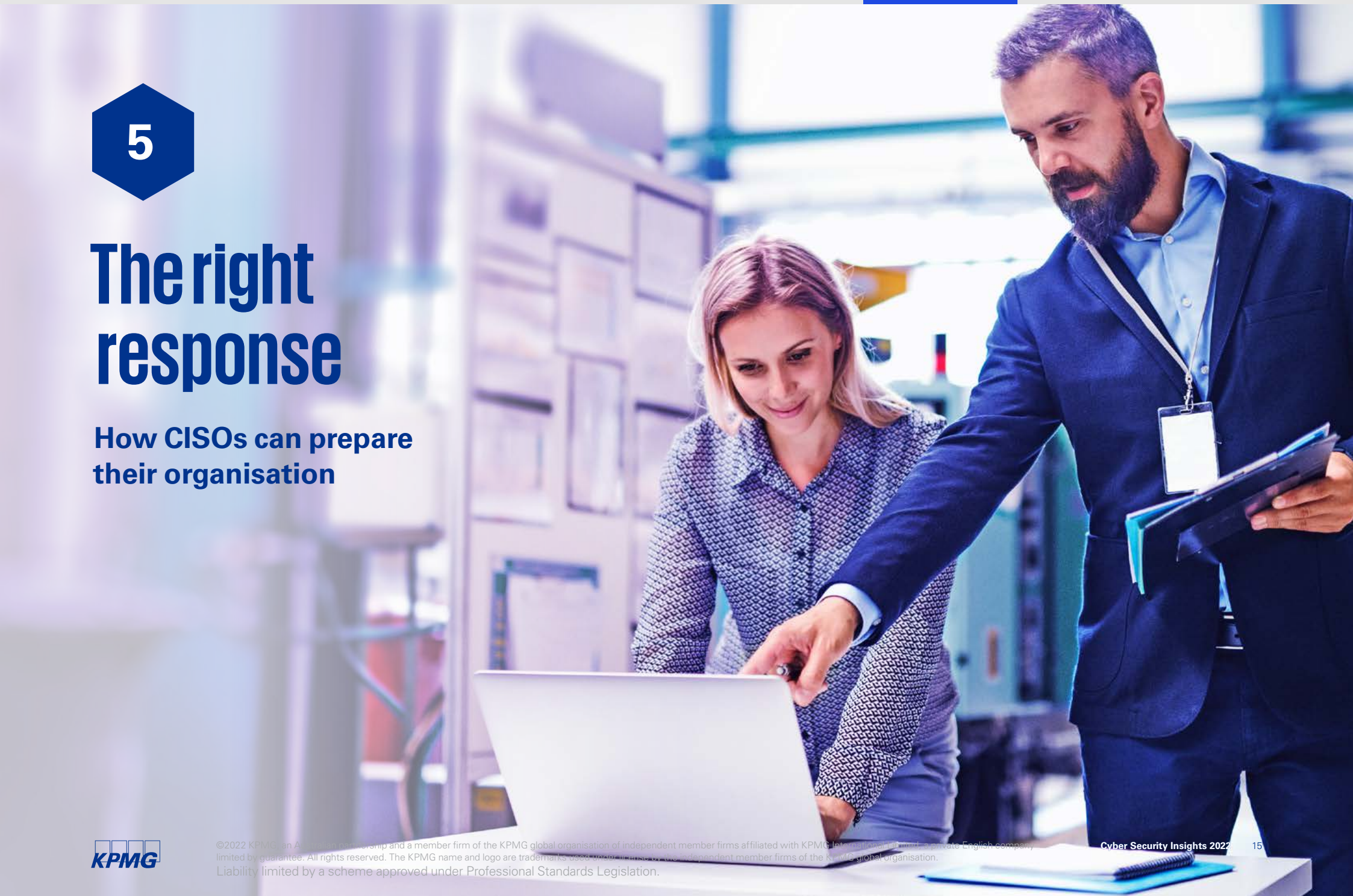
Only about 36 per cent of respondents felt that CISO teams were equipped to play an active role in setting ESG policy where it overlaps with data and infrastructure security.

However, as the link between cyber security and ESG deepens, it is crucial that CISO teams proactively engage with designated ESG stakeholders to achieve long-term business sustainability.

5

The right response

How CISOs can prepare their organisation



Identifying the data crown jewels, a factor in fortifying cyber defence

Organisations in Australia must examine their cyber response strategy to gain technical expertise and plug the gap as soon as a cyber incident is detected, demanding an Incident Response Plan (IRP) to be put in place. The ACSC provides a comprehensive cyber incident response plan offering guidance to organisations to produce a robust IRP, using a tailored fit-to-purpose approach.

Multiple sectors are utilizing IRPs to both prevent and respond to adverse events. In case of a security breach, severity and type of the incident is assessed followed by its containment to avoid any further loss from it.

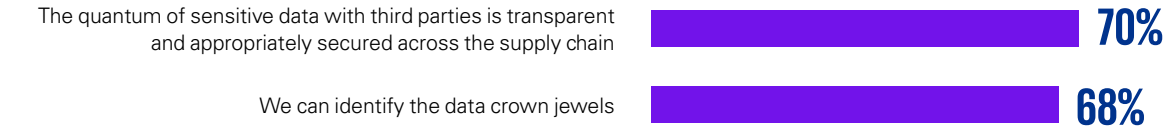
A successful response to an incident concludes with a meeting that involves the CISO, board and other relevant stakeholders to collaboratively build an understanding of the flaws in their cyber risk efforts and to deliberate on future strategies to prevent a replay or repeat attacks.

About one-third of respondents felt that CISOs lacked confidence around identifying their organisation's data crown jewels and were not completely aware of the quantum and security of sensitive data across the supply chain.

An effective cybersecurity strategy demands prioritisation of organisational assets in line with the financial and operational outcomes of a potential breach. CISO teams must also focus on securing critical pathways that may lead an attacker to the crown jewels. ACSC provide a list of eight mitigation strategies to assist organisations in securing their systems and crown jewels against a range of adversaries.

80% of respondents felt CISOs are confident that cybersecurity measures offered competitive advantage over other firms in their industry.

How confident would your CISO be if responding to the following questions from the board of directors?



> To keep organisations safe in Australia, businesses need to have a proactive approach to how they plan for and respond to a security incident'

Paul Black
Cyber Security
Incident response & Intelligence Lead

An influential CISO can be the key to great cyber risk management

Australian organisations are now focused on securing digital assets and pre-emptively combating threats. A factor in the success of these efforts is the CISO's relationship with the board. **About half of the respondents felt that boards see information security as a necessary cost rather than a long-term competitive advantage.**

CISOs must choose a platform-based approach to optimise security while minimising security sprawl to ensure the endpoints' security under resource limitations.

Three in five respondents feel that the relationship between the board and CISO is characterised by high trust and consultation. Only two in five felt that the CISO had adequate authority and accountability for implementing cyber security.

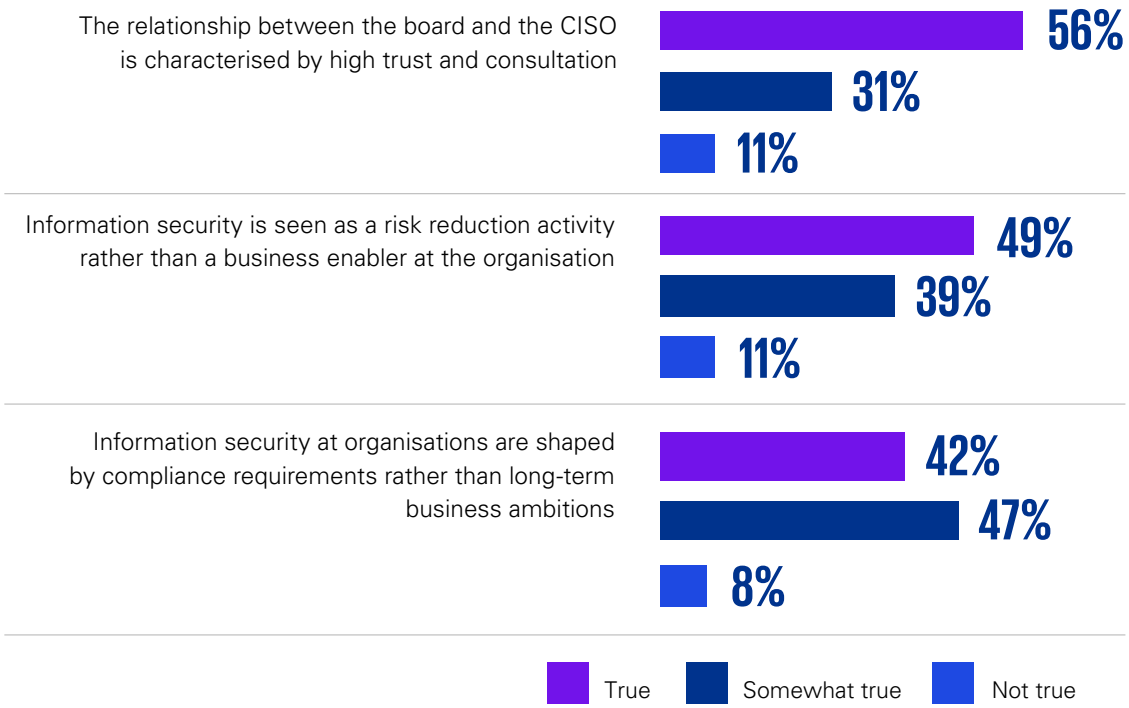
CISOs must build a strong working relationship with the board and find common ground–enabling enterprise-wide security measures such as

- purple teaming,
- attack surface management,
- zero-trust networks,
- managed detection and response (MDR),
- security orchestration and
- automated response (SOAR)
- to be deployed effectively.

Risk assessment and cyber security investments are distinct decisions for two in five respondents. There is also a view that risk modelling is based on assumptions about threats and vulnerabilities, with about **one in three highlighting that their organisation faces challenges in quantifying cyber risks**. CISOs can better manage these difficulties by developing preemptive external cybersecurity partnerships.

Which of the following statements relating to the relationship to the relationship between the CISO and the board of directors are true ?

Chart shows percentage of respondents who selected each option in their top three.



Source: KPMG Cyber trust insights 2022

6

Trusted Community

The power of collaboration and partnership

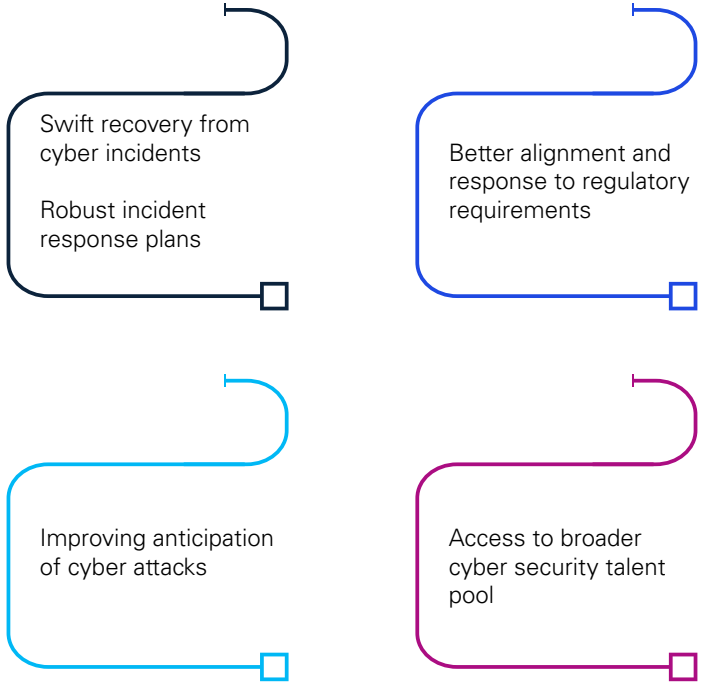
Trusted community as a shared ecosystem for cyber security

Growing cyber incidents have made organisations think ahead for proactively responding and pre-empting cyber threats. One effective way to achieve these outcomes is through developing strategic cybersecurity partnerships. Collaboration can provide the missing skill sets and technology organisations need, improving their ability to combat the increasing sophistication of bad actors, navigate talent shortages, and access pooled cyber resources.

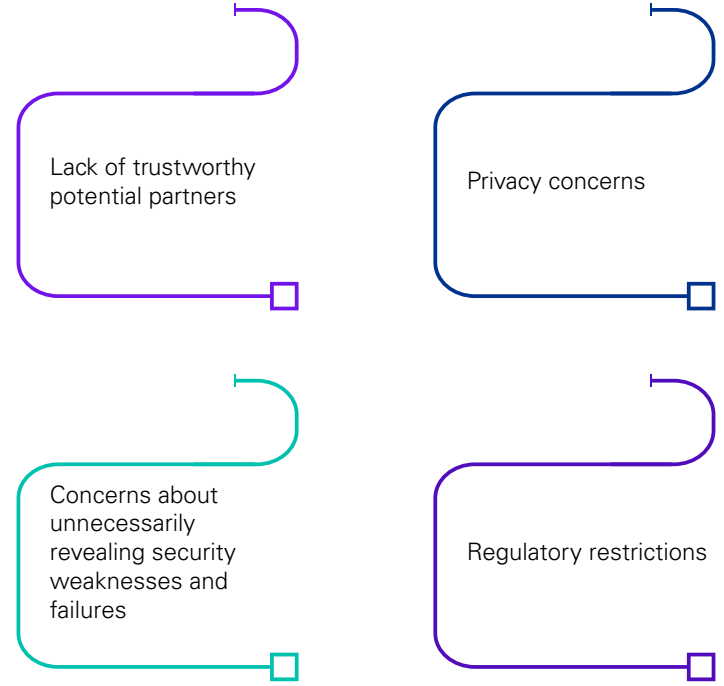
According to the survey, about **three in four respondents highlighted the need for collaborating with extended stakeholders, such as suppliers and customers, as vital to ensuring an organisation's cyber security.**

Yet, more than half of the respondents felt a lack of visibility around vulnerabilities in procurement and the supply chain. They would want their organisations to approach cybersecurity collaborations with greater zeal.

Key benefits of collaboration with trusted communities



Key barriers to collaborating with trusted communities



Source: KPMG Cyber trust insights 2022

Cyber collaborations: an Australian lens

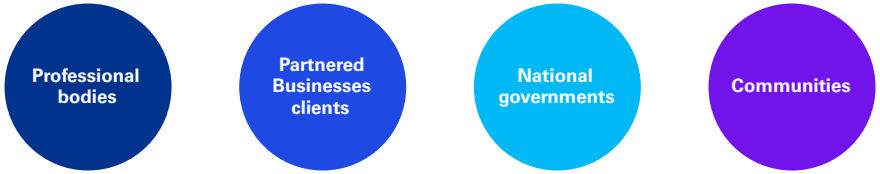
Significant national programs are emerging in Australia, driven by public-private partnerships among federal and state governments and industry. The ACSC operates a partnership program through its Joint Cyber Security Centers (JCSCs) network. The ACSC Network includes cyber security professionals across government, industry, academia, and the research sector to share insights and collaborate on common threats and opportunities.

Threat intelligence platforms such as the Cyber Threat Intelligence Sharing (CTIS) and digital identity management frameworks such as Trusted Digital Identity Framework (TDIF) have been established for facilitating shared cyber security efforts.

However, according to our survey, **Australian organisations must work on improving collaborations with peer companies in the same sector, local/city governments and NGOs working towards cyber security.** By extending the golden thread through establishing trusted communities, organisations can meld together security systems, secure data processing, and their cyber response to create a truly holistic cyber security ecosystem.

Based on the analysis of the KPMG survey, respondents from Australia, consider the following as key stakeholder groups for forming trusted communities

Top four sought-after collaborations for enhancing cyber security



Key takeways

Key takeaways

- Create a cyber security culture by treating cyber and privacy as a golden thread. When these are woven into business processes and governance, it becomes everyone's responsibility.
- Cyber risk programs can help improve an organisation's overall security posture. They should extend across the entire value chain to pre-empt cyber attacks, avoid lapses in compliance, protect against reputational damage, and safeguard against data theft.
- Tackling concerns around the ethical use of data is crucial to protecting consumer privacy and building trust with stakeholders.
- Advanced technologies such as AI and MI increase the risk of PII exposure to cyber threats. These technologies must be carefully monitored and managed to ensure the ethical use of data and algorithms, especially as the link between cyber security and ESG deepens.

- Influential CISOs can ensure a more effective cyber response within their organisation.
- For the board to recognise cyber security as a long-term competitive advantage, their relationships with the CISO need to have high confidence, trust and consultation, with CISOs accountable for implementing cyber security.
- Strategic cyber collaborations can fill the missing gaps in defence for organisations.
- Sharing cyber intelligence and mitigation strategies with trusted partners creates an ecosystem of cyber security. It allows organisations to benefit from improving their ability to anticipate and recover from cyber-attacks.

Methodology and acknowledgments

About the KPMG Australian Cyber Security Insights Report 2022

The KPMG 2022 Australian Cyber Security Insights Report is segmented from the Australian data researched and featured in KPMG Cyber trust insights 2022 Global survey, conducted by KPMG International between May and June 2022. It surveyed 1,881 executives and interviewed five corporate leaders from across the world to explore the role that cybersecurity and privacy play in building and maintaining trust.

A significant proportion of the sample surveyed is composed of senior leadership, board or C-suite members. All respondents have annual revenues over US$100M, 45 per cent have annual revenues over US$500M, 23 per cent have revenues over US$1B and 7 per cent have revenues over US$5B.

About KPMG

KPMG can help you create a resilient and trusted digital world – we work across sectors and industries to embed cyber security in organisantial culture, even in the face of evolving threats, by giving confidence to pursue growth ambitions while building trust with clients, investors and partners.

KPMG cybersecurity professionals can offer a multidisciplinary view of risk, enabling you to carry security throughout your organisation, so you can anticipate tomorrow, move faster and get an edge with secure and trusted technology.

Because bold growth shouldn't be a security risk

No matter where you are on your, cyber security journey, KPMG has expertise across the continuum – from the boardroom to the data center. Security is a shared responsibility model, owned by everyone and we work with you to assess your cybersecurity alignment to your business priorities, helping you develop advanced solutions, assist with implementing them, advise on monitoring ongoing risks and help you respond effectively to cyber incidents.

KPMG professionals harness constantly evolving technologies that can connect and power businesses forward – building trust and creating and protecting value, while bridging the gap between past and future. We help businesses be cyber safe from the inside out.

Contacts

Martijn Verbree
Cyber Security Australian Lead
E: mverbree@kpmg.com.au

Mitra Minai
Cyber Security Health and Victoria Government Lead
E: mitraminai@kpmg.com.au

Gergana Winzer
Cyber Security Mid-Market Lead
E: gwinzer@kpmg.com.au

Gordon Archibald
Cyber Security Futures and Technology Lead
E: garchibald@kpmg.com.au

Matt O'Keefe
Cyber Security ASPAC Lead
E: mokeefe@kpmg.com.au

Natasha Passley
Cyber Security Financial Services Lead
E: npassley@kpmg.com.au

Greg Miller
Cyber Security Critical Infrastructure Reforms Lead
E: gmiller3@kpmg.com.au

Ian Gray
Cyber Security Government Lead
E: igray@kpmg.com.au

Stuart Mort
Cyber Security Technology Lead
E: stuartmort@kpmg.com.au

Kate Marshall
Cyber Security Law Lead
E: katemarshall@kpmg.com.au

Danny Flint
Cyber Security Identity and Access Management Lead
E: dflint@kpmg.com.au

Paul Black
Cyber Security Incident Response and Intelligence Lead
E: paulblack1@kpmg.com.au

Angela Pak
Cyber Security Operational Technology Lead
E: apak@kpmg.com.au

Kelly Henney
Cyber Security Privacy and Data Protection Lead
E: khenney@kpmg.com.au

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

KPMG.com.au

November 2022. 9555883381CYBER