2022 Global Digital Trust Insights

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

2022 Global Digital Trust Insights

Organisations know that cyber risks are increasing. More than 60% expect a surge in reportable incidents next year above 2021 levels.

2021 is shaping up to be one of the worst on record for cybersecurity. During the 2020–21 financial year, the Australian Cyber Security Centre received over 67,500 cybercrime reports, an increase of nearly 13 per cent from the previous financial year[1].

Ever more sophisticated attackers are plumbing the dark corners of our systems and networks, seeking — and finding — vulnerabilities. Whatever the nature of an organisation's digital Achilles' heel — an unprotected server, a weakness in remote access or lack of cyber awareness — attackers will use every means at their disposal, traditional as well as ultra-sophisticated, to exploit it.

The consequences of an attack increase as our systems' interdependencies grow more complex. Critical infrastructure is especially vulnerable. The results of an attack go further than financial loss and include the potential for prolonged outages impacting essential services, health, safety and national security[2].

Yet, many of the breaches we're seeing are still preventable with sound cyber practices and strong controls.

[1] ACSC Annual Cyber Threat Report 2020-21
[2] PwC Australia Building Cyber Resilience in Critical Infrastructure

Simplifying cyber

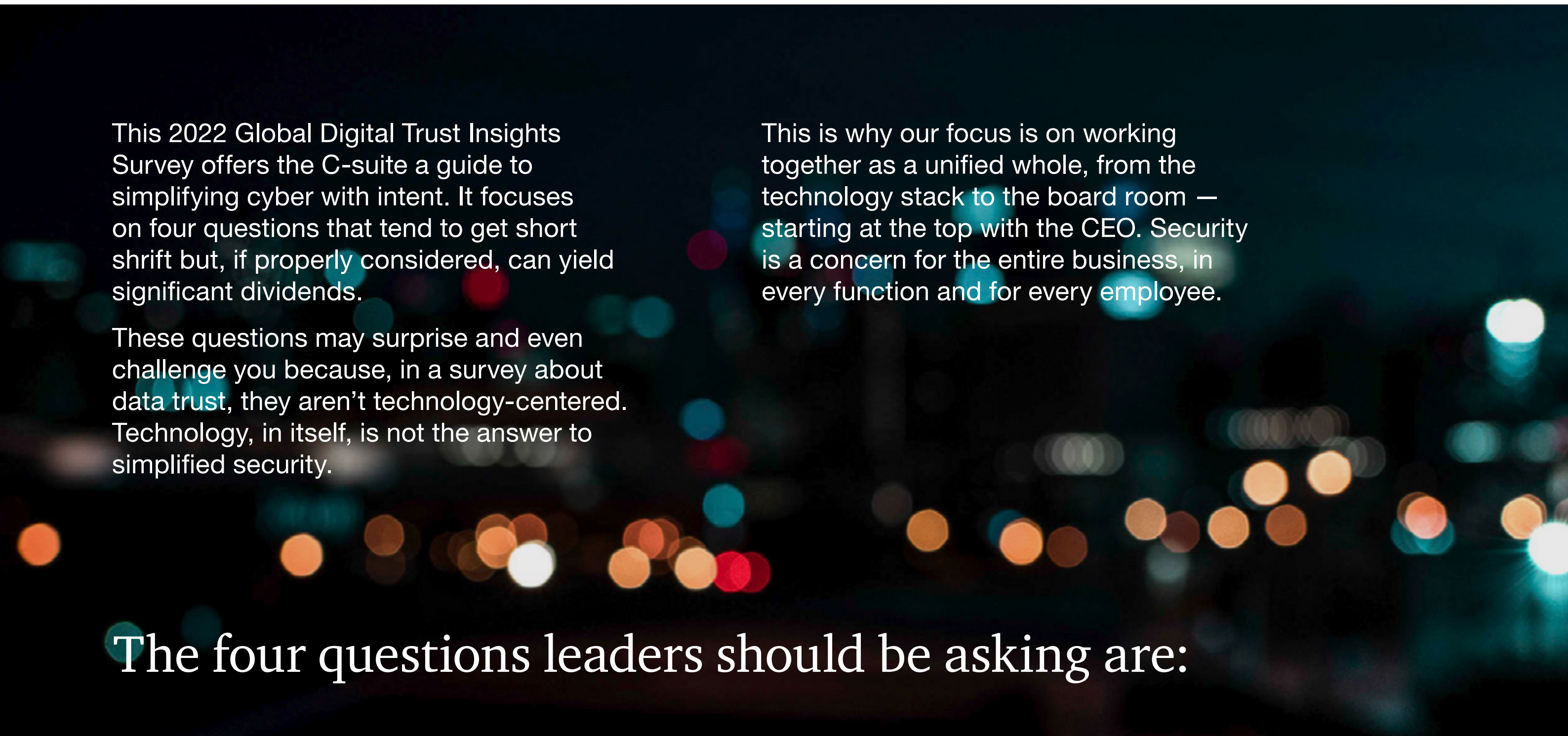
As digital connections multiply, they form increasingly complex webs that grow more intricate with each new technology. Having a smart phone enables us to carry a variety of “devices” — telephone, camera, calendar, TV, health tracker, an entire library of books, and so much more — in our pocket, simplifying our lives in many ways and letting us work on the go.

The Internet of Things lets us perform a myriad of tasks by uttering a simple command, enables factories to all but run themselves, 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? Australian business leaders are sounding the alarm. Some 78% of Australian respondents to our 2022 Global Digital Trust Insights Survey say that unnecessary organisational complexity poses “concerning” cyber and privacy risks.

But because some complexities are necessary, your enterprise shouldn’t streamline and simplify its operations and processes thoughtlessly, but consciously and deliberately.



This 2022 Global Digital Trust Insights Survey offers the C-suite a guide to simplifying cyber with intent. It focuses on four questions that tend to get short shrift but, if properly considered, can yield significant dividends.

These questions may surprise and even challenge you because, in a survey about data trust, they aren’t technology-centered. Technology, in itself, is not the answer to simplified security.

This is why our focus is on working together as a unified whole, from the technology stack to the board room — starting at the top with the CEO. Security is a concern for the entire business, in every function and for every employee.

The four questions leaders should be asking are:

1 How can CEOs make a difference to your organisation?

2 Is your organisation too complex to secure?

3 How do you know if you’re securing your organisation against the most important risks to your business?

4 How well do you know your third-party and supply chain risks?

Can the CEO make a difference to your organisation's cybersecurity?

There appears to be an increasing disconnect between the CEO's view of their cyber engagement and the view of the broader management team.

Multiplying the effect: simplifying moves that get you more results

Strategists and technologists have touted the potential of digital business models to boost business 10x — a promise of exponential returns on digital investments. Likewise, the global results from the survey reveal how simplifying business processes and operations can have a "multiplier" effect on security and privacy.

Here are the four Ps to realising your full cyber potential, as exemplified by the most advanced and most improved organisations, who employ them all.

Principle. The CEO must articulate an explicit, unambiguous foundational principle establishing security and privacy as a business imperative.

People. Hire the right leader, and let the CISO and security teams connect with the business teams. Your people can be vanguards of simplification even as you build "good complexity" in the business.

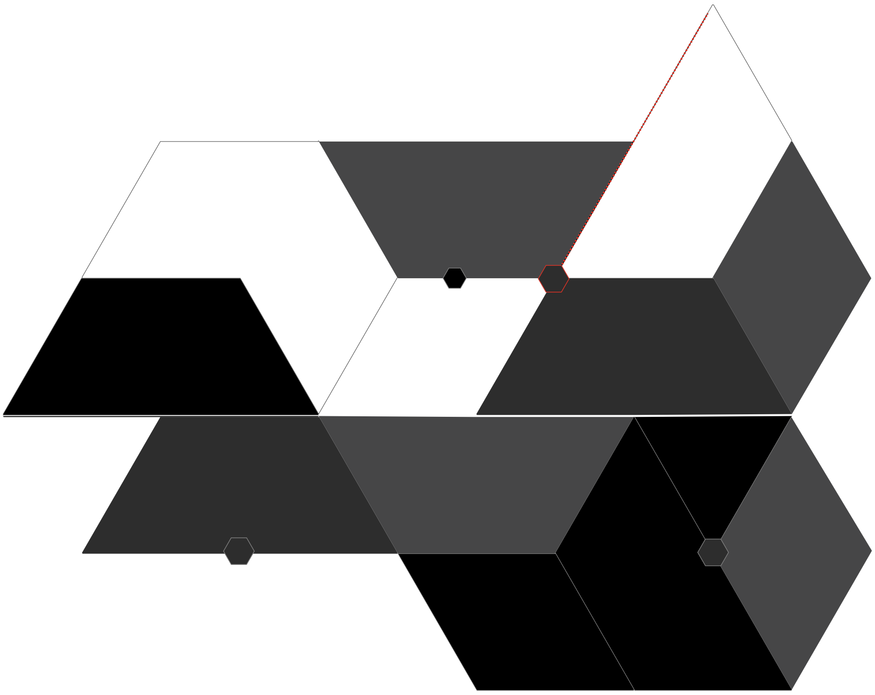
Prioritisation. Your risks continually change as your digital ambitions rise. Use data and intelligence to measure your risks continually, as well.

Perception. You can't secure what you can't see. Uncover blind spots in your relationships and supply chains.

As common-sense as these precepts and practices might seem, our survey would suggest they're not commonplace. Many enterprises continue to struggle amid risky, runaway, befuddling complexity. They use many tech solutions that, too often, do not work together.

Failing to coordinate the work of various functions on resilience and third-party risk management. Failing to create and adhere to processes for dealing with data (governance). Failing to speak in the language of business when talking about cyber, enabling a business outcome rather than a technology solution.

Businesses develop these bad habits in the name of speed, or they accept and assimilate them out of resistance to change. The good thing, however, is that bad habits can be broken. And C-suite champions can help develop new habits, enabling coordination and collaboration among all functions, business and tech, for an organisation that's simply secure.



Make 'simply secure' your business mantra

Cyber has got CEOs' attention, but are they taking action? Ninety-five percent of Australian Chief Executives cited cyber threats as the number one risk to growth - in PwC's 24th Annual Global CEO Survey.

Our findings from the 2022 Global Digital Trust Insights Survey suggest an "expectations gap" for cyber, with CEOs perceiving that they are more involved in, and supportive of, setting and achieving cyber goals than their teams do. A persistent gap can spell disaster if it instills a false sense of security company-wide, given the CEO's leading role in defining an organisation's culture.

How involved are CEOs in cyber?

We asked both CEOs and other C-Suites executives. Among our respondents, CEOs tend to see themselves as more engaged in cybersecurity than others in the organisation perceive them to be.

Our CEO respondents self-identify as engaged and strategic in their approaches to cyber. They indicate that they participate in discussions about the cyber and privacy implications of major operating model changes (ranked 1st) and future strategy (ranked 2nd).

Other executives don't view things in quite the same way. Non-CEOs say their chief executive is more likely to take part in cyber and privacy matters after a company breach, as part of a compliance review or when key metrics of cyber are discussed at a board level.

Executives see CEOs getting involved in cyber when a crisis strikes. CEOs think they are more engaged

	CEO View	Non-CEO View
Reactive CEO		
After a major cyber breach or attack occurs in the organisation	6	1
After a major cyber breach or attack occurs in the industry	3	3
When regulators contact our organisation for cyber incident reporting, matters requiring attention, or enforcement action	5	6
Engaged CEO		
When the key metrics of cyber are discussed at the board level	7	2
When the cyber and privacy implications of M&A activity are discussed	8	5
When the cyber and privacy implications of a major operating model change are discussed	1	7
Strategic CEO		
When the cyber and privacy implications of a new business initiative, whether digital or not, are discussed	4	8
When the cyber and privacy implications of future strategy are discussed	2	4

Question: On which of the following cyber & privacy matters, would you/your CEO become personally involved? Rank them in order.
Base: Australian Non-CEO Respondents: 76; Australian CEO Respondents: 38
Source: PwC, 2022 Global Digital Trust Insights, October 2021.

How much support does the CEO provide CISO leadership?

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

45%

of Australian CEOs said they provide significant support for “ensuring adequate resources, funding and sufficient priority” to cyber while only 30% of non-CEOs agreed that their CEOs do so.

42%

of CEOs say they provide significant help to cyber leadership with embedding cyber and privacy in key operations and decisions of the organisation, while just 36% of non-CEOs agree.

32%

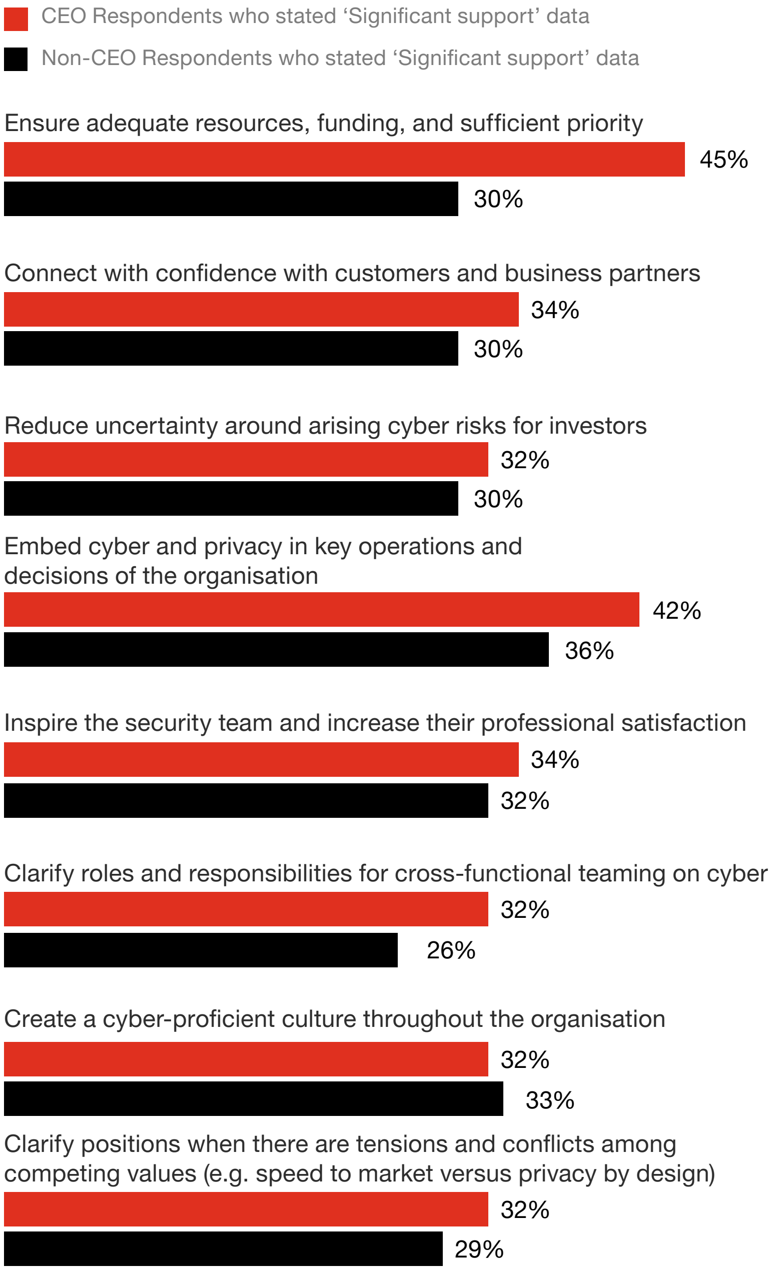
of CEOs say they empower their cyber leadership to clarify roles and responsibilities for cross-functional teaming on cyber, while 26% of non-CEOs say cyber gets that kind of support.

This disconnect is also evident in our global data with similar discrepancies apparent within global organisations.

CEOs matter. The CEO’s engagement and support wield long term importance. Globally, executives in most regions and industries say the most important act for a more secure digital society by 2030 is educating CEOs and boards so they can better fulfill their cyber duties and responsibilities.

It’s time to close the expectations gap between the chief executives and the others in the C-suite regarding the level of CEO involvement and support of cybersecurity. Things seem headed in the right direction: globally, interactions with the CEO on cyber matters have increased significantly in the past two years, according to 46% of our survey respondents.

CEOs believe they give ‘significant’ cyber support, but only 3 in 10 executives agree



Question: What level of support do you/does your CEO provide your cyber leadership to accomplish the following?
Base: Australian Non-CEO Respondents: 76;
Australian CEO Respondents 38
Source: PwC, 2022 Global Digital Trust Insights, October 2021.

CEOs and other executives need to be aligned on the cyber mission

Asked how CEOs frame the cyber mission in their organisation, more than half (61%) of Australian CEOs chose bigger-picture, growth-related objectives, as opposed to narrower, shorter-term expectations.

The responses of non-CEOs were split, with 51% selecting bigger-picture, growth-related objectives. Of the 49% who selected short-term objectives, the highest ranked objective was the response to immediate threats and emerging stronger from disruption (29%).

Cybersecurity's mission is shifting to developing trust and business growth

Bigger picture: growth related framing of mission and expectations	CEO Respondent		Non-CEO Respondent	
	Global	Australia	Global	Australia
A way to establish trust with our customers, with respect to how we use their data ethically and protect their data	18%	11%	20%	21%
A way for our business to compete better and grow, on the basis of trust	15%	29%	13%	8%
A way of operating so the organisation is harder for threat actors to attack	12%	8%	12%	14%
The way to expedite the digital transformation of our organisation	10%	13%	10%	8%

Narrow framing of mission and expectations from security team	CEO Respondent		Non-CEO Respondent	
	Global	Australia	Global	Australia
The way to put controls throughout the organisation to prevent serious cyber disruptions	17%	8%	17%	12%
A way of operating so the organisation responds faster to threats and emerges stronger from disruptions	15%	8%	16%	29%
A cost of doing business and a necessary evil	8%	11%	6%	4%
A way to avoid getting in trouble with regulators	6%	13%	6%	4%

■ Global 🟥 Australia

Question: Which of the following best describes how you/your CEO frames the cybersecurity mission to your organisation?
Base: Australian Non-CEO Respondents: 76; Australian CEO Respondents: 38*; Global Non-CEO Respondents: 2929; Global CEO Respondents: 673
Source: PwC, 2022 Global Digital Trust Insights, October 2021.

Australian CEO’s rate regulatory compliance a priority in the design of their cyber strategies, placing it at number two after enabling growth via the provision of trust. Global CEO’s, on the other hand, ranked it least important. Prioritising regulatory sanctions suggests that these Australian organisations are still focused on compliance-driven cyber programs.

There is an opportunity for CEOs and other executives to mature the dialogue around cyber away from regulatory risk and towards business risk.

The top goals in relation to the changes executives will be making in cyber strategy, people and investments are:

- Improved employee experience
- Less burdensome employee experience in managing risk and compliance
- Expedited launch of new products
- Improved confidence of leaders in our ability to manage present and future threats
- Increased prevention of successful attacks

Management of threats and prevention of attacks is a priority locally and globally. Australian leaders expressed a nuance, putting improved employee experience and its enablers at the top of the list. This might reflect our point-in-time focus on our people and their experience.

How can CEOs make a difference to their organisation's cybersecurity?

The results of our survey show that **70% of Australian organisations don't get the kind of support they need from their CEO**. The fact is, both the CEO and CISO need to work together better to benefit the company.

CEO: How much should you be involved in your organisation's cybersecurity — without taking on undue burden?

A powerful CEO move: making an explicit statement establishing an imperative for security and privacy organisation-wide.

In some cases, the organisation's mission statement is already implicitly supportive. Many of our global respondents have security and quality as a central theme.

A related CEO imperative: empowering your CISO to carry out the cybersecurity mission, voicing support and providing resources for secure-by-design, secure-by-default processes.

Some may add the CISO to the C-suite. Others may help the CISO communicate more with the board or revamp the enterprise's structure to embed security staff on business teams. Empowering CISOs may also mean giving them the platform to speak outside the organisation to customers about its security and privacy initiatives.

This period of great complexity in the business world demands a third CEO imperative. The CEO must modify certain elements of the company's business and/or operating models to make the company "simply secure" when the security team identifies wasteful habits. For example, in the name of speed, a "get to market first, fix security later" mindset prevails. Companies aren't fully mitigating remote work risks. Business units often buy technologies and contract with third parties autonomously. Cybersecurity is too often an afterthought in cloud adoption or transformation.

By taking action, the CEO reinforces a zero tolerance approach to complexity that gets in the way of security.

CISO: How well do you understand the business? How connected are you with leaders on the business side?

For an organisation that's simply secure, CISOs must move out of the technology trenches and broaden their outreach to learn and support business strategies.

This means aligning with and working alongside leaders at a departmental level, and learning to communicate with the board on cybersecurity in a language that resonates. For some boards or board members that is risk-focussed, others growth and enablement. Less is more and it must be in business terms that non-technical board directors can understand.

This change may require a mindset shift for many CISOs. CISOs interact most frequently with the CIO, Chief Risk Officer and Chief Technology Officer, our survey shows, and least frequently with the chief marketing officer and product management leader.

The CFO also ranks low (9th) on the interactions list. CISOs will need to spend more time with these business partners to begin to speak their language and better understand their business imperatives.

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.

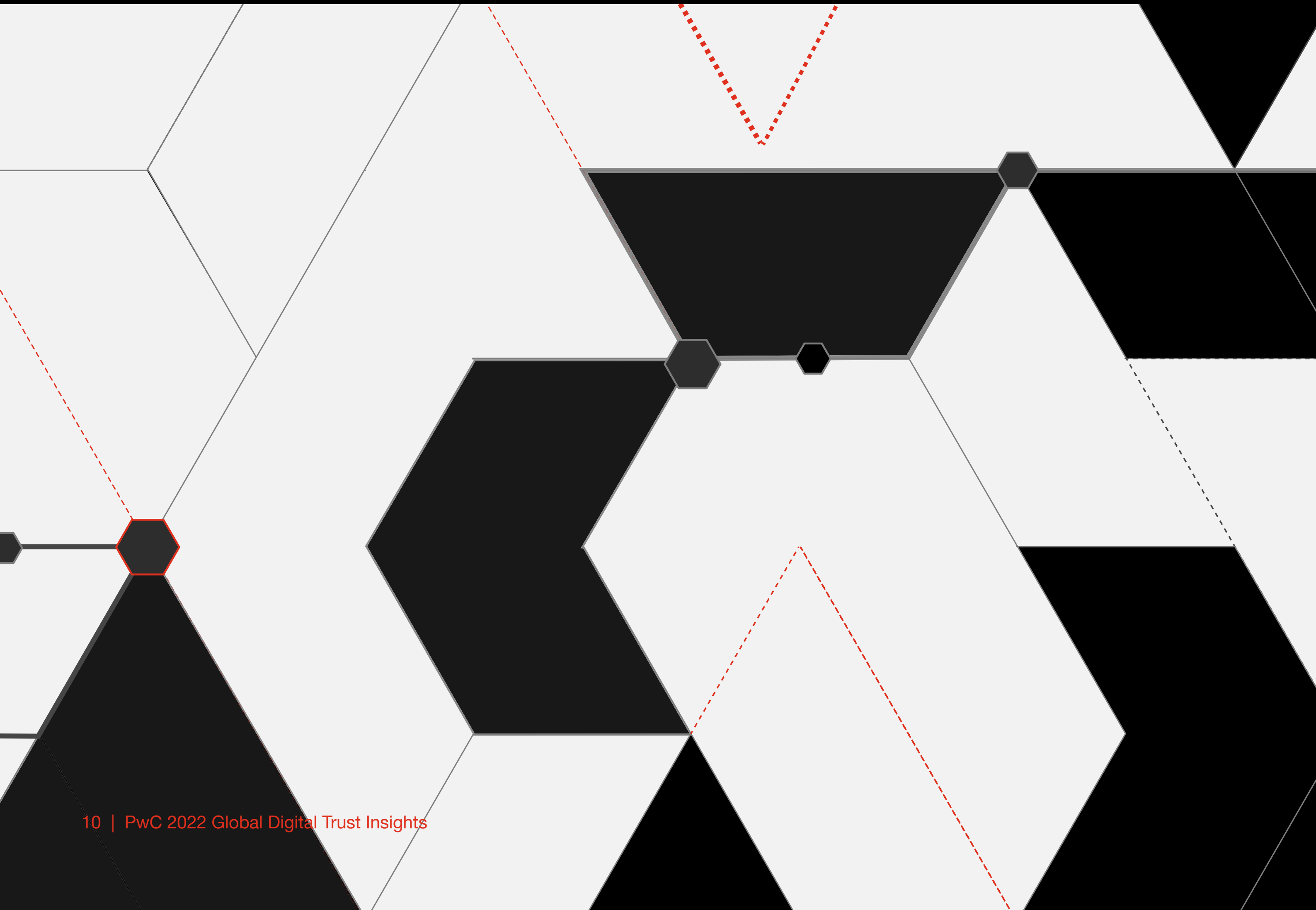
Come to grips with the problems and risks in your business models and change what needs to be changed. You'll have lots of opportunities to follow Peter Drucker's advice: "Management is doing things right; leadership is doing the right things."

For the CISO

Familiarise yourself with your organisation's business strategy.

Build a stronger relationship with your CEO, and keep the dialogue going to help your CEO clear the way for simply secure practices. Speak in a language that aligns with the business.

Equip yourself with the skills you need to thrive in the evolving, expanding role for cyber in business. And reorient your teams, if you haven't already, towards business value and customer trust.



Is your organisation too complex to secure?

78% of Australian respondents say their organisations are too complex.

Be deliberate about simplicity and simplification

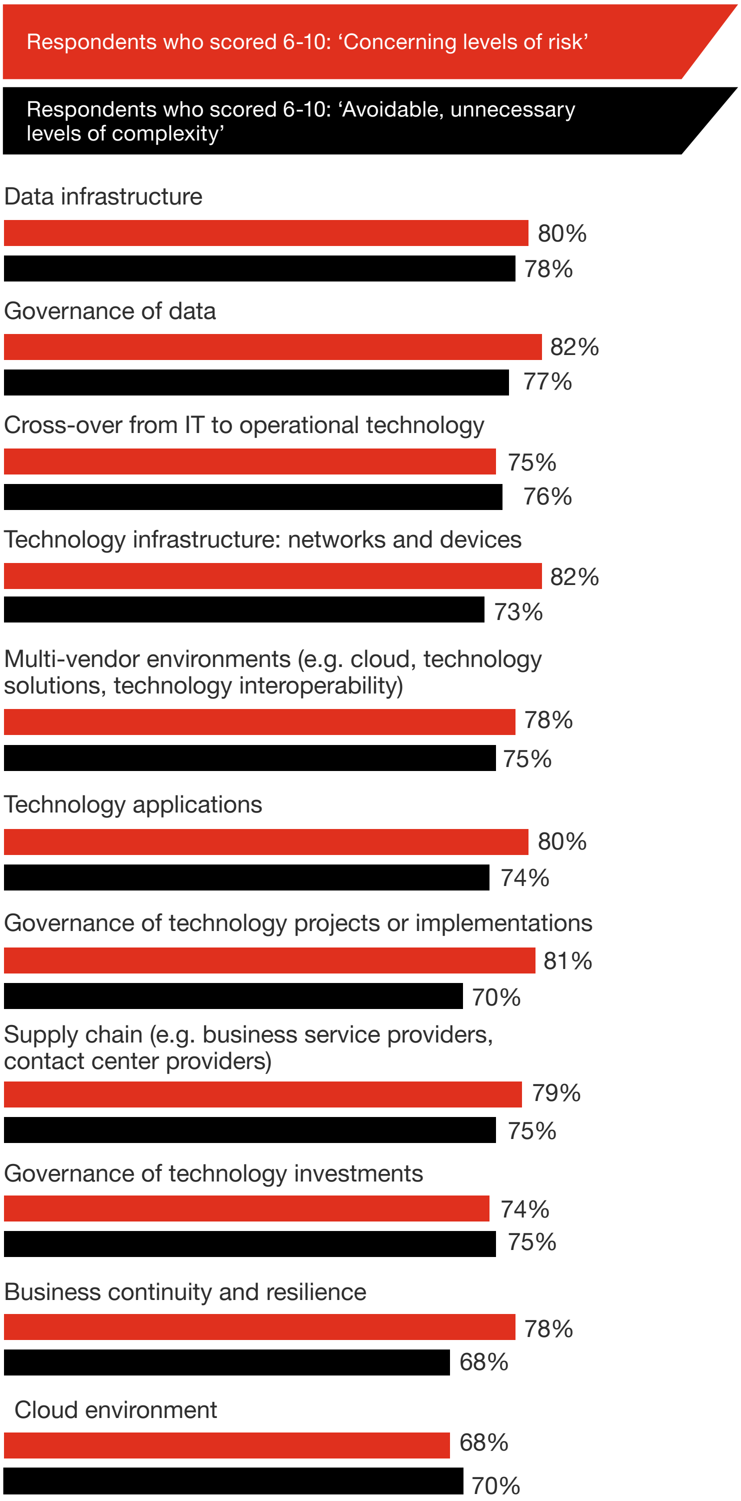
In an overly complex organisation, it's easy for the left hand not to know what the right hand is doing — and the consequences for cybersecurity and privacy can be dire. **Seventy-eight percent of C-suite respondents to our survey**, including CISOs, say their companies are too complex, avoidably and unnecessarily so, and nearly as many say complexity poses "concerning" cyber and privacy risks to their organisations in 11 key areas. This is largely consistent with our global findings.

Data seems to be a chief point of concern with data governance (82%) and the data infrastructure (80%) ranked amongst the highest areas of "unnecessary and avoidable" complexity.

Technology networks and devices are also highly complex. Digital-native companies — those that exist entirely online — tend to use the newest technologies, which are designed to connect and operate together. Most other companies' technology architectures, which include legacy systems, are more complicated. Mergers with other entities may multiply risks by connecting already complex networks and systems.

Question: 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? **Base**: 114 Australian respondents. **Please note**: Cloud Environment was added as an answer option after survey launch, therefore, has a lower base. **Cloud Environment Base**: Australia=50. **Source**: PwC, 2022 Global Digital Trust Insights, October 2021.

78% of executives report too much complexity in their organisations, leading to 'concerning' cyber and privacy risks.



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.

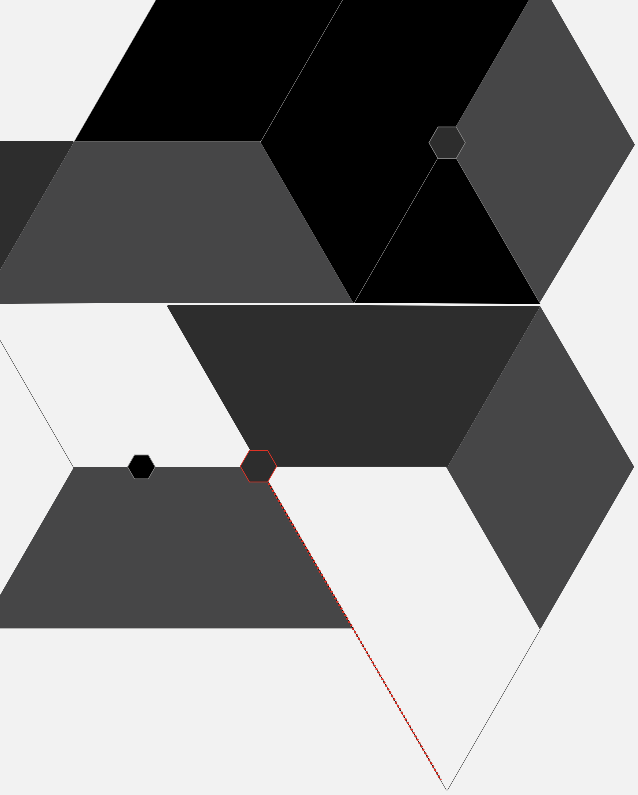
Often companies needlessly keep the sensitive data of people they no longer do business with, making that data available for hackers to steal.

In our article Simplifying cyber, we give examples of 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 whittled the vendor list to two. **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**.

Asked to name the top consequences of operational complexity, our respondents named:

1. Financial losses due to successful data breaches or cyber attacks
2. Lack of operational resilience or inability to recover from a cyber attack or technology failure
3. Inability to innovate as quickly as the market opportunities offer

Complexity not only threatens today's fortunes, in the view of executives, it also prevents organisations from creating new opportunities quickly and pursuing future ones.



The move to simplification

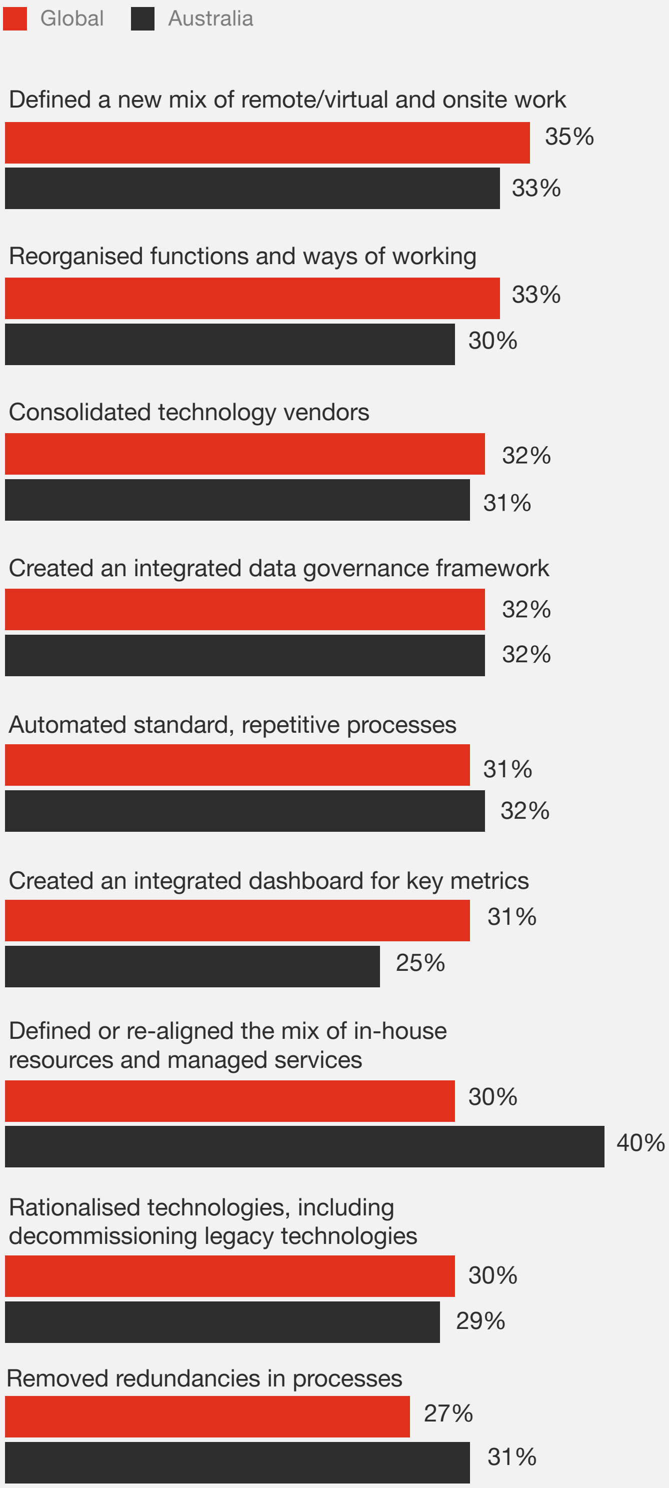
Businesses know the risks of complexity, yet only 31% of our respondents have completed any streamlining of their operations and one-fifth say they've done nothing at all or are just getting started.

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 mighty.

More and more CISOs and CIOs are taking a hard look at their tech investments, no longer just entertaining or chasing the latest products from tech vendors. Globally we're seeing consolidation of tech vendors and applications to reverse the hard-to-manage and risky tangle of disparate and vulnerable software and tech stack.

Simplification in organisations: 3 in 10 have streamlined 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'
Base: Global=3602, Australia=114
Source: PwC, 2022 Global Digital Trust Insights, October 2021.

Simplification of cyber

To be fair, simplifying cybersecurity can be challenging. Even knowing where to begin can be difficult, especially given the attacks hitting businesses on every front.

Asked to prioritise among nine initiatives aimed at simplifying cyber programs and processes, respondents couldn't choose, allotting near-equal importance to all of them. 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.

Moving to the cloud can help simplify business processes and IT architecture, provide flexibility and accelerate innovation. However, runaway complexity can quickly result 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.

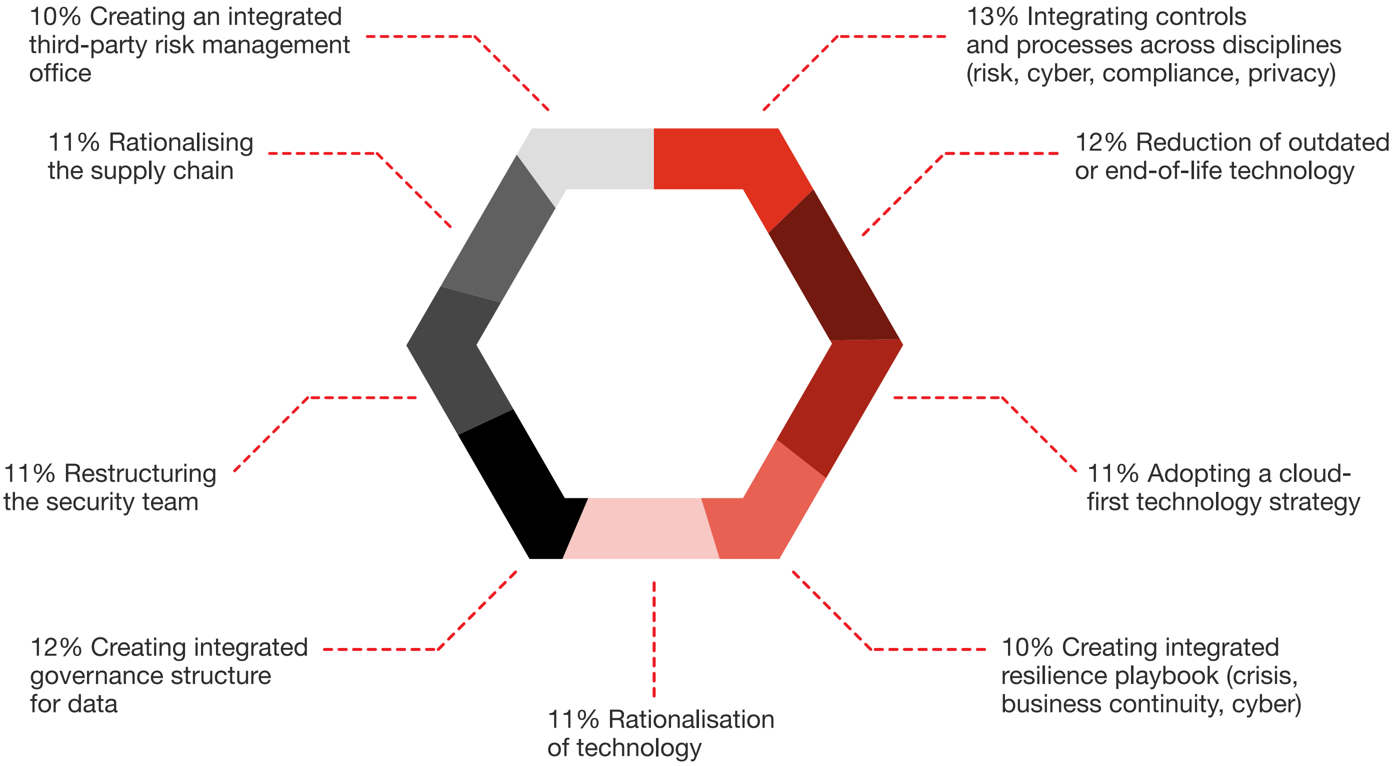
Done right, however, cloud transformations can be secure, efficient, and successful. The cloud opportunities for Australian organisations are material, particularly given we are coming off a relatively low base.

Only 17% of Australian organisations report realising benefits from cloud security investments. **Thirty-two percent** haven't fully benefited from cloud security investments and **49% are just starting** or planning their cloud security investments.

Whether or not you're using the cloud to simplify, minimising and combining your tech stack and processes may feel like a bold move. Doing so requires asking hard questions and maintaining a keep-it-simple mindset. To get there, your organisation will need security-minded leadership starting at the very top.

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 from phishing resulting in credential theft, which remains a popular tactic, by itself, and in tandem with malware and ransomware attacks. Don't forget that simplifying, minimising or removing unnecessary complexity can also result in efficiencies and operational cost savings.

Simplification of cyber: spending is spread across several initiatives



Question: In the next two years, what portion of your cybersecurity spend will your organisation allocate to each of the following initiatives to simplify cybersecurity? **Base**: 114 Australian respondents. **Source**: PwC, 2022 Global Digital Trust Insights, October 2021.

Takeaways

For Operations and Transformation Leaders

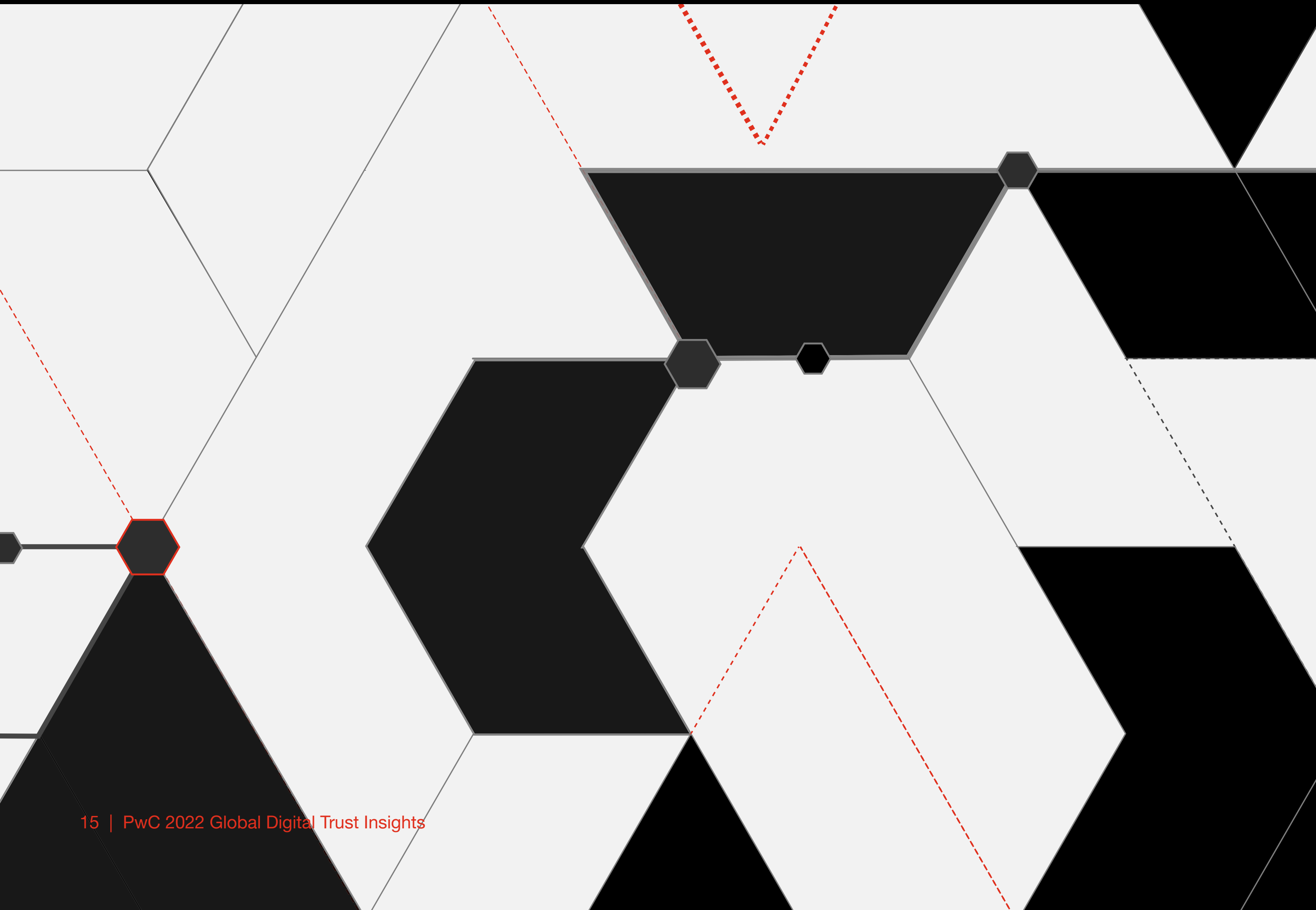
Ask: what's the cyber plan for that? You can ignite major changes — operational and cultural — simply by asking this one question of every business executive in charge of a transformation or new business initiative. By placing cybersecurity front and centre, you can avoid the unnecessary and costly complexities you may see now, when it's an afterthought.

Include the CISO and security teams early in cloud migration and adoption, mergers and acquisitions, and other organisational initiatives. That way, every executive at the helm of a major business initiative will be able to readily answer the cyber-plan question.

For the CISO and CIO

Dare to subtract. Left on their own, technology and data tend to multiply, divide, and conquer efficiency and security. Whittle down excess with security goals in mind: assess your data stores and eliminate everything you don't need now; move your disparate apps and solutions into a cloud environment for easier management; and consolidate, remove and automate where you can.

Also, rethink your tech and cyber investment processes. Focus first on simplifying where benefits are greatest for the whole organisation.



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

Fewer than 1 in 3 organisations use available data and intelligence when making decisions.

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

Organisational leaders recognise the importance of verifying and safeguarding their business information. Asked to frame the cybersecurity mission, the number-one response (29%) from non-CEOs was, "A way of operating so the organisation responds faster to threats and emerges stronger from disruptions." In contrast, **only 8% of Australian CEOs** selected this as the way they framed the cyber mission in their organisation.

Data governance **(82%)** and technology infrastructure (networks and devices) **(82%)** rank as the two most needlessly complex aspects of business operations in our Australian survey. On top of this, **about three-quarters** say complexity in these areas poses "concerning" risks to cybersecurity and privacy. Complexity of data can stymie any organisation's ability to protect that data and effectively use the information it collects and generates.

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 and verified and secure so you can rely on them 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.)

Just over a third of respondents report having mature, fully implemented data-trust processes in four key areas: governance, discovery, protection and minimisation. **Nearly one fifth of our respondents** say they have no formal data-trust processes in place at all.

Only about one-third of organisations report having a full, formal data governance program — a surprisingly low number. Once you've crafted your data strategy, governance — the policies, procedures and processes for fulfilling the strategy — should follow immediately.

Securing your data from tampering as well as theft is also critical to success, yet **just over one-third of respondents** report having in place fully implemented, formal data security processes including encryption and secure data-sharing **(39%)**. Verifying and protecting the integrity of your data is essential as well.

Only 32% of Australian organisations believe they have mapped all their data, meaning they know where it comes from, where it goes and how it is used.

And, only 38% believe they have mature data minimisation processes.

Data is the asset attackers covet most. Your companies can minimise that risk by minimising the target. You must 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.

The 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 including local privacy, information security and critical infrastructure laws, and international obligations including Europe's General Data Protection Regulation (GDPR). New, extensive and more stringent regulations loom on the horizon in Australia as well.

When asked for information about their data — what you're keeping and what you're doing with it — organisations should be able to answer this quickly and accurately. If it's a regulator or key customer doing the asking, the wrong answer could have significant ramifications.

Data trust practices have yet to become the norm.

Percentages who say they have fully implemented formal processes around these data trust practices.

35%	Knowledge of the data inventory, where data comes from, how data moves through business processes and systems and how it has been transformed (protection)
38%	Data retention and data elimination policies and schedules (minimisation)
39%	Ability to share data securely with third-parties, business partners, and suppliers, and to potentially "audit" their compliance to terms (security measures, disposition, appropriate usage) (protection)
39%	Deployment of processes and technologies that provide encryption, tokenization, redaction/masking technologies across sensitive data environments (protection)
32%	An understanding of where personally identifiable information (PII), sensitive data, intellectual property and high value data resides throughout the enterprise (discovery)
34%	Capability and process for valuing data assets and continuously improving data quality (governance)
35%	A combined strategy for data management, cyber, privacy, record retention functions and other information governance functions (governance)

Question: For each of the following, please rate how mature your organisation's data trust practices are. Percentages are for the response 'formal process, fully implemented'
Base: 114 Australian respondents.
Source: PwC, 2022 Global Digital Trust Insights, October 2021.

Use it or lose out

Chances are good that neither you nor your competitors are letting data inform your cyber risk management. Fewer than one in three of Australian respondents say they've integrated analytics and business intelligence tools into their operating model. These respondents scored lowest in their ability to turn data into insights for autonomous threat detection.

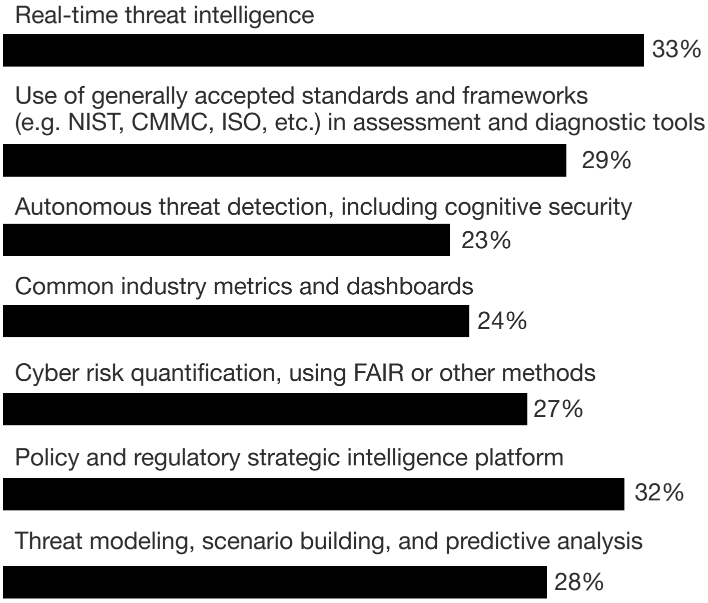
Many entities fail to benefit from today's advanced intelligence tools and approaches.

New types of internal data, data from new external sources, new data partnerships and information-sharing platforms can be important sources of business intelligence, but just over a quarter of respondents say they're reaping benefits from these tools.

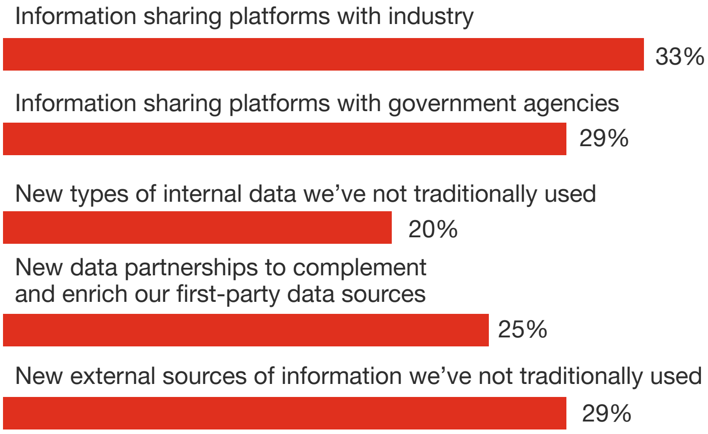
The other remaining organisations are missing out. Businesses predicting an increase next year in their cybersecurity spending are often the same enterprises whose operational models use business intelligence and data analytics. Data can not only help you spend your cyber budget wisely, it can also help you get more to work with.

To what extent does your organisation use the following tools and approach executives under utilise data and intel for better decisions and risk management.

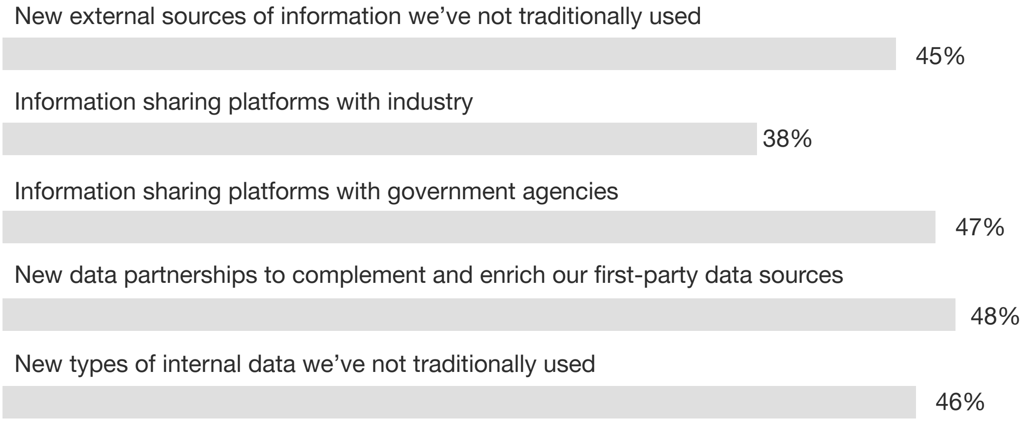
Respondents who stated ‘Integral to our operating model’:



Respondents who stated ‘Realising benefits/critical to our decision making’:



Respondents who stated ‘Implemented but not critical to our decision making’:



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? **Base**: 114 Australian respondents. **Source**: PwC, 2022 Global Digital Trust Insights, October 2021.

Sizing up risks and opportunities

“In today’s system-of-systems world, cybersecurity can no longer be treated as a ‘too-hard-to-measure’ problem,” the US Cybersecurity and Infrastructure Security Agency argues. Still, as we saw above, only **27% of Australian organisations 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 empowering boards and the CEO to invest in a cyber program. On the other hand, if an organisation is having trouble getting the funding needed for cyber, they need to do a better job of quantifying the cybersecurity risk.

By the same token, data can help you stay apprised of real-time risks, and adjust security tactics and strategies as the business shifts.

Enterprise leaders recognise that risks are always in a state of flux and that data is the tool that lets them monitor and measure changes.

Sizing up risks is also important for sizing up opportunities and linking cyber-threat narratives to business narratives that the C-suite and boards can understand. A growing number of organisations recognise the importance of cybersecurity to business — but many still have a long way to go. Less than half of respondents **(between 36% and 47%)** claim “significant progress” linking the two.

The 2022 threat outlook

Our respondents do make predictions about the next 12 months. **Sixty-six percent** expect an increase in cybercrime; **70% say nation-state attacks are likely to grow.** The interconnectivity inherent in the Internet of Things tops the list of anticipated vulnerabilities. But the type of attack could take almost any form, in our respondents’ minds. Breaches via software supply chains **(72%)** narrowly edged out state-sponsored attacks on critical infrastructure **(69%)** and ransomware **(68%)** as most likely to see increases, and a long line of other attack types scored between **56%** and **67%.**

Takeaways

For the CFO

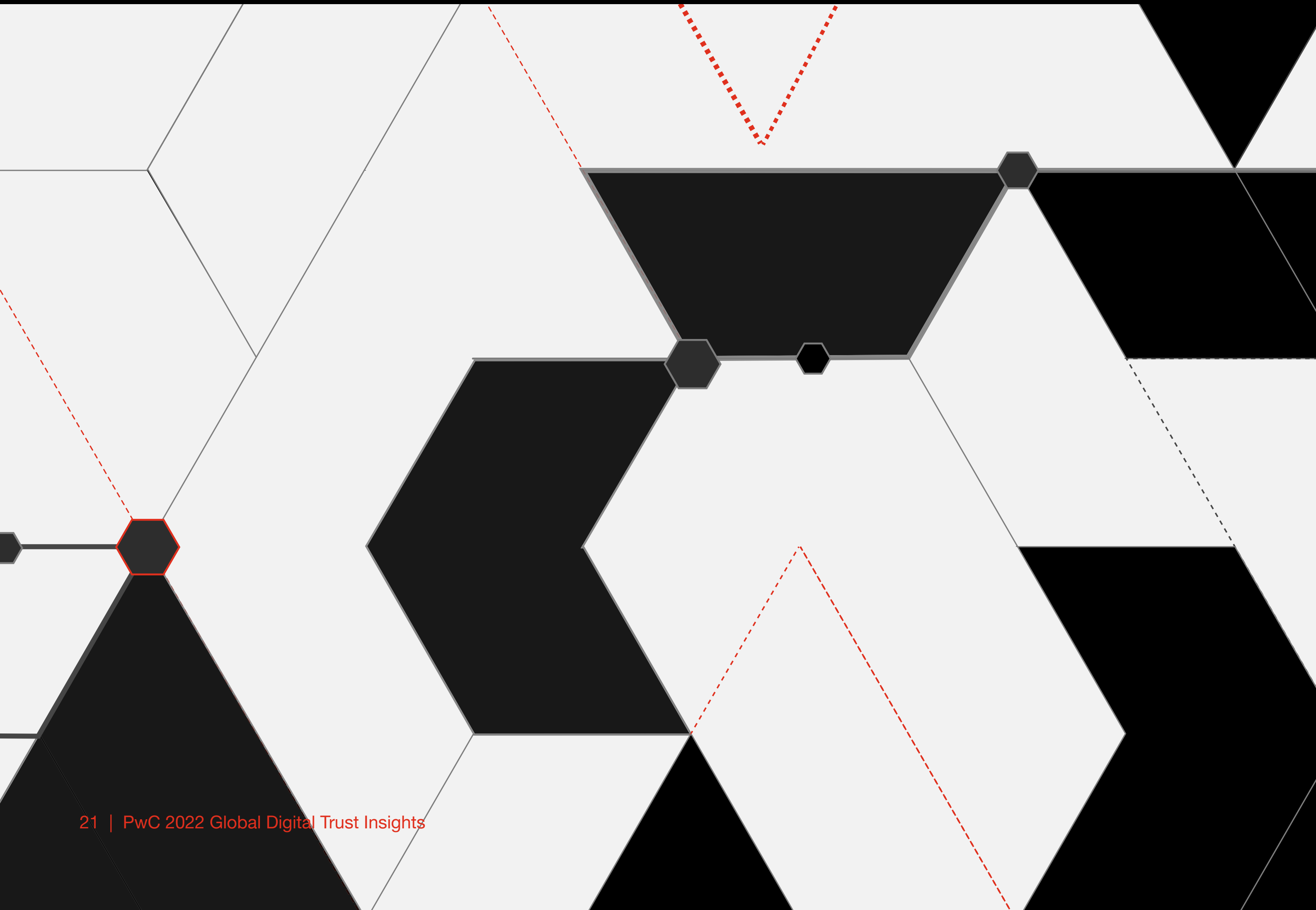
Work with the CISO in taking a risk-based approach to cyber budgeting that ties to business objectives

For the CISO

Build a strong data trust foundation: an enterprise-wide approach to data governance, discovery, protection and minimisation. Create a roadmap from cyber risk quantification to real-time cyber risk reporting.

Don’t stop at cyber risks. Tie the cyber risks to overall enterprise risks and, ultimately, to effects on the business.

With a fuller accounting of cyber risks, identify what works in your business model and where you might need to simplify.



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

At best, only 40% say they thoroughly understand their third-party cyber and privacy risks.

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

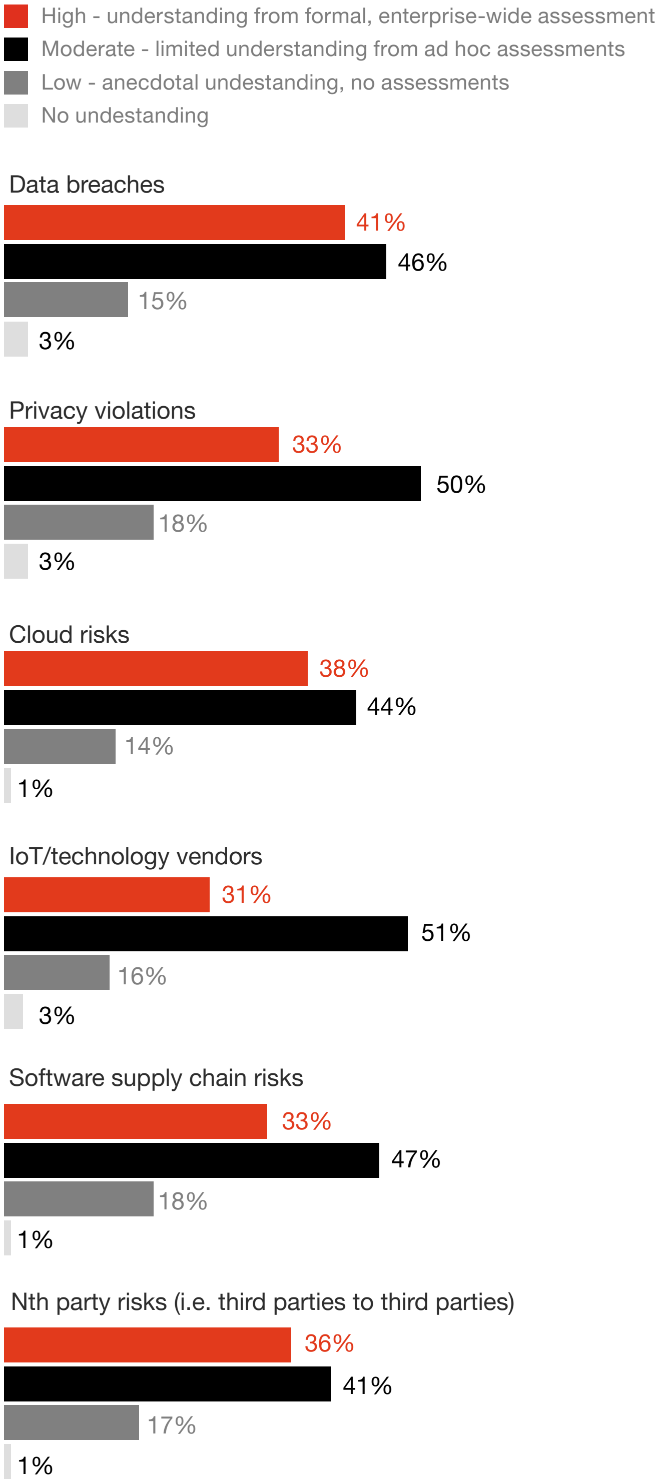
You can’t secure what you can’t see, and most respondents to the PwC 2022 Global Digital Trust Insights Survey seem to have trouble seeing their third-party risks — risks obscured by the complexities of their business partnerships and vendor/supplier networks.

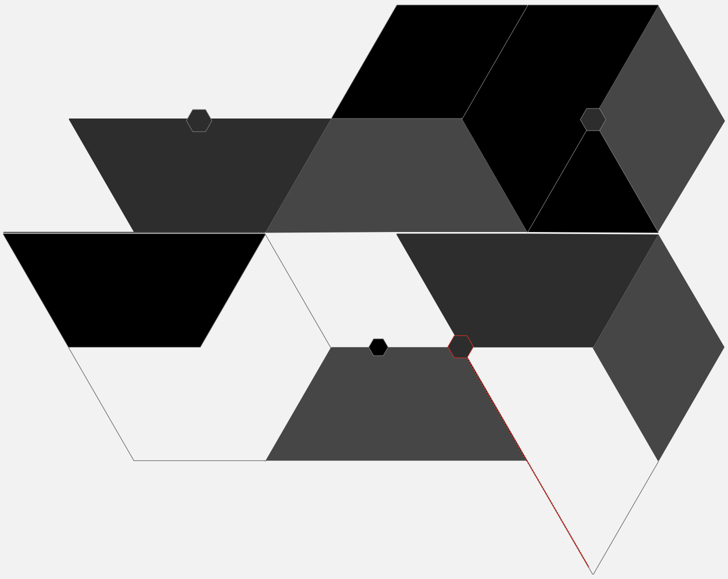
Only 41% of survey respondents say they thoroughly understand the risk of data breaches through third parties, using formal enterprise-wide assessments. Nearly one-fifth have little or no understanding at all of these risks — a major blind spot of which cyber attackers are well aware and willing to exploit.

Among our respondents, 72% expect an increase in reportable incidents in 2022 from attacks on the software supply chain, but only 33% have formally assessed their enterprise’s exposure to this risk. Sixty-five percent expect a jump in attacks on cloud services, but only 38% profess an understanding of cloud risks based on formal assessments.

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?
Base: 114 Australian respondents.
Source: PwC, 2022 Global Digital Trust Insights, October 2021.

Organisations have a large blind spot to risks arising from third parties and the supply chain





Around half of all respondents 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.

Asked how they're minimising their third-party risks, they gave largely reactionary responses: auditing or verifying their suppliers' compliance (54%), addressing cost- or time-related challenges to cyber resilience (46%), and rewriting contracts with certain third parties to mitigate risks (42%).

Still, more than half have taken no actions that promise a more lasting impact on their third-party risk management. They've not refined their third-party criteria (61%) and not increased the rigor of their due diligence (61%).

Simplifying the chain

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 cost of digital interactions.

Today's trending cyber-attack target may be the most challenging one yet: your supply chain of trusted vendors, suppliers and contractors. The weapon? A process many have taken completely for granted: the software update. The payoff? Ransom payments to cybercriminals, valuable intelligence to nation-states or training data sets for AI models to competitors. Over the past decade, vendors and hijacked updates accounted for 60% of software supply chain attacks and disclosures, according to The Atlantic Council. The European Union Agency for Cybersecurity (ENISA) predicted in a July 21, 2021 report that supply chain attacks would quadruple in 2021 over the number of 2020 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. That's because 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.

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

Public-private collaboration

Visibility also means seeing which challenges others face and what they are doing to meet them. Collaboration can be an important part of your cyber-business ecosystem. This point has been emphasised in recent times by the Australian Signals Directorate and the need for threat intelligence sharing is critical. But much more needs to be done.

Fewer than one-third of survey respondents (28%) said their public-private collaboration efforts are "very effectively" helping them achieve their cyber goals. Currently in Australia, intelligence sharing between organisations limited to small select groups, and then large organisations such as the Financial Services Information Sharing and Analysis Center (FS-IAC).

More needs to be done to enable wide-spread sharing. The Australian Cyber Security Centre is working towards solutions to improve sharing levels and ease, for example CTIS (their sharing platform) and other close hold sharing communities. Australian organisations need to be encouraged to establish industry sharing groups that are informal in nature and allow free flow of information without fear of repercussions.

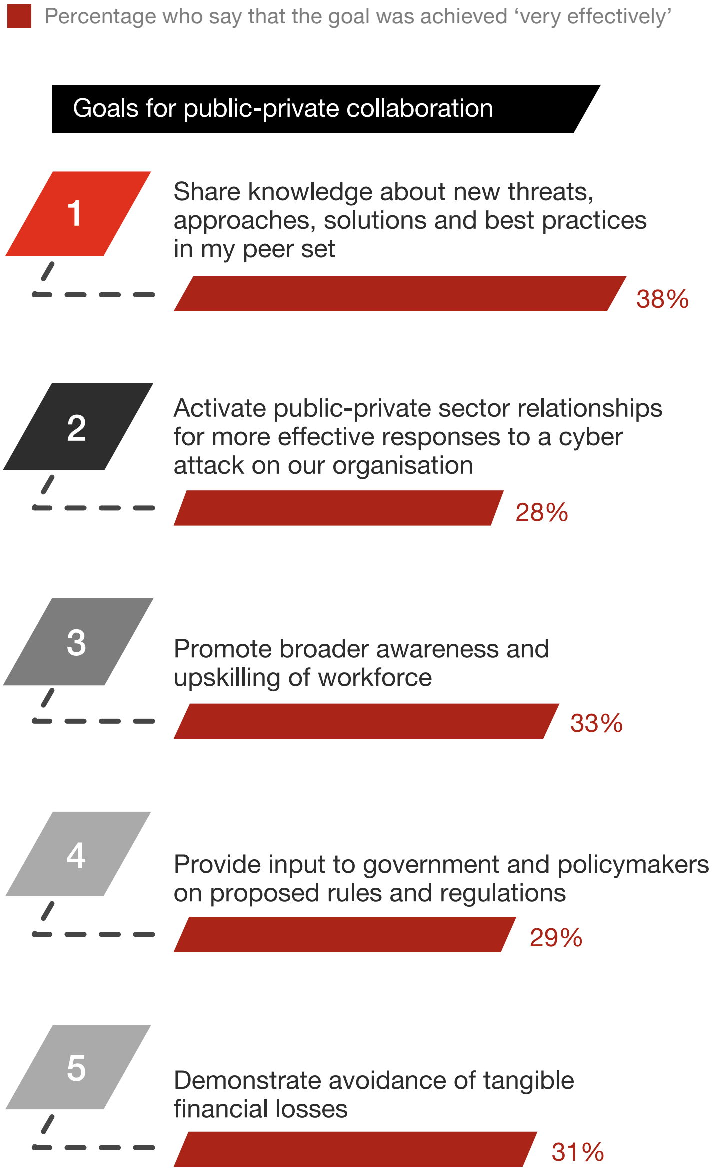
When looking at our global data, those who've had the best cybersecurity outcomes over the past two years, were 34x more likely to have achieved their public-private collaboration goals "very effectively." Organisations increasing their cyber budgets in 2022 were also significantly likely to say they have achieved these goals "very effectively":

- Share knowledge about new threats, approaches, and solutions in my peer set (38%)
- Demonstrate avoidance of tangible financial losses (36%)
- Activate public-private sector relationships for more effective responses to a cyber attack on our organisation (33%)
- Promote broader awareness and upskilling of workforce (32%)

When it comes to influencing governments and policymakers on proposed rules and regulations, smaller companies perceive that they are less effective than larger ones. This is a global issue with small and medium sized businesses concerned about their ability to effect change.

Collaborators are an important part of secure ecosystems.

More effective public-private collaboration is needed before, not just after, attacks.



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?
Base: 114 Australian respondents**.**
Source: PwC, 2022 Global Digital Trust Insights, October 2021.

Takeaways

For the COO and the supply chain executive

Map your system, especially your most critical relationships, and use a third-party tracker to find the weakest links in your supply chain.

Scrutinise your software vendors against the performance standards you expect. Software and applications that your company uses should undergo the same level of scrutiny and testing that your network devices and users do.

After a fuller accounting of your third-party and supply chain risks, identify ways to simplify your business relationships and supply chain. Should you pare down? Combine?

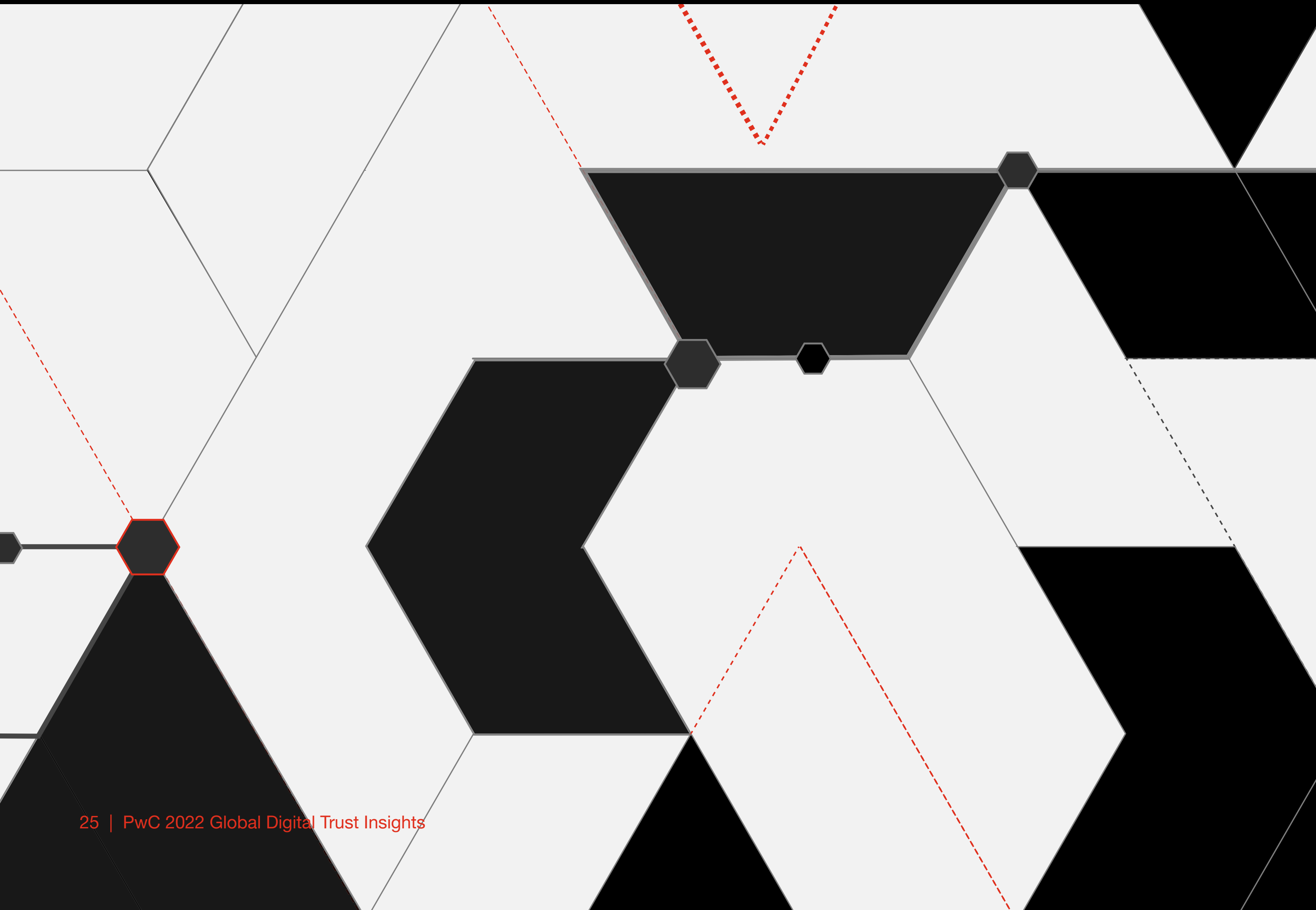
For the CRO and CISO

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.

Strengthen your data trust processes. Data is the target for most attacks on the supply chain. 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.



About the survey

The 2022 Global Digital Trust Insights is a survey of 3,602 business, technology, and security executives (CEOs, corporate directors, CFOs, CISOs, CIOs, and C-Suite officers) conducted in July and August 2021. Female executives make up 33% of the sample.

Sixty-two percent of respondents are executives in large companies ($US1 billion and above in revenues); 33% are in companies with $US10 billion or more in revenues.

Respondents operate in a range of industries: Tech, media, telecom (23%), Industrial manufacturing (22%), Financial services (20%), Retail and consumer markets (16%), Energy, utilities, and resources (8%), Health (7%), and Government and public services (3%).

Respondents are based in various regions: Western Europe (33%), North America (26%), Asia Pacific (18 %), Latin America (10 %), Eastern Europe (4%), Middle East (4%), and Africa (4%).

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

Australian respondents

The total number of respondents from Australia was 114 executives (38 CEOs and 76 corporate directors, CFOs, CISOs, CIOs, and C-Suite officers).

Of the Australian respondents, 53% were business executives while 47% were technology and security executives. Female executives made up 46% of the sample.

Seventy-nine percent of Australian respondents are executives in large companies ($US1 billion and greater in revenues); 21% are in companies with less than $US1 billion.

Respondents operate under various ownership structures: 49% of Australian respondents are from privately owned companies. Of those, 13% of respondents are from family run companies, 54% of respondents are from companies backed by private equity, 16% of respondents are from partnerships, 16% of respondents are from owner-managed companies and 2% of respondents accounted for 'Other' structures. With the remaining 51% consisting of publicly listed companies (46% of respondents) and G&PS (4% of respondents).

Contact us

Michael Cerny
Partner
michael.cerny@pwc.com

Nicola Nicol
Partner
nicola.nicol@pwc.com

Cameron Whittfield
Partner
cameron.whittfield@pwc.com

Peter Malan
Partner
peter.malan@pwc.com

Rick Crethar
rick.crethar@pwc.com