Ai GROUP
Supporting Australian industry for
150 YEARS
1873-2023

Ai Group Cyber Security Survey 2023

Cyber Readiness in Australian Industry

November 2023

About the Australian Industry Group

The Australian Industry Group (Ai Group) is a peak employer organisation representing traditional, innovative and emerging industry sectors. We are a truly national organisation, and in 2023 we celebrate our 150th year supporting Australian businesses.

Our vision is for thriving industries and a prosperous community. We offer our membership strong advocacy and an effective voice at all levels of government underpinned by our respected position of policy leadership and political non-partisanship.

With more than 250 staff and networks of relationships that extend beyond borders, we have the resources and the expertise to meet the changing needs of our membership. We provide the practical information, advice and assistance members need to run their businesses.

Our deep experience of industrial relations and workplace law, positions Ai Group as Australia's leading industrial advocate.

We listen and we support our members in facing their challenges by remaining at the cutting edge of policy debate and legislative change. We provide solution-driven advice to address business opportunities and risks.

Australian Industry Group contacts for this report

Dr Jeffrey Wilson – Director of Research and Economics
jeffrey.wilson@aigroup.com.au

Colleen Dowling - Senior Research Analyst and Economics Team Leader
colleen.dowling@aigroup.com.au

Contents

Foreword from our CEO

Like many Australians, cyber security is an issue that keeps me up at night. As several recent and high-profile cyber attacks have shown, the concern that a cyber attack could at any time affect your personal or financial security is no longer an academic one.

As the Australian community has become more aware of cyber security, so too has Australian business. Cyber attacks on businesses are increasing at a rapid rate, and can have potentially catastrophic impacts on operational, financial and data security.

Businesses are at the vanguard of Australia's cyber defences. They are often prized targets for cyber criminals – given the data they possess, their financial resources, and their dense relationships with suppliers and customers. But they are also our first line of defence, maintaining the cyber systems that keep criminals out of the Australian digital ecosystem.

The cyber readiness of our businesses will make or break national cyber security.

Ai Group conducted our first Cyber Security Survey in 2023 to better understand how Australian business is responding to this growing threat.

How have cyber incidents impacted business? What cyber defences have they put in place, and where do they get resources and information? How are business leaders approaching cyber investments in a time of broader economic pressures?

This report makes for reading that is both concerning and confidence boosting. Our research shows that cyber incidents now affect around one-in-five businesses annually, with impacts ranging from the disruptive to the destructive. Business leaders report they are highly conscious, and very concerned about cyber security.

However, businesses are also taking decisive action to achieve cyber readiness. Cyber security is now a top-ranked investment priority, and businesses have implemented a wide range of technology- and people-based solutions to protect their data. The majority of small businesses, and almost all medium and large businesses, report confidence in their cyber systems.

Australian business is resilient - while we embrace the opportunities digitisation and increased integration technology bring, we are concious of the increased cyber security risks that come with it. To do so we need to embed cyber security practices into all of our business operations and products across Australian industry.

Innes Willox
Chief Executive Officer
Australian Industry Group

Key findings of the report

1. **Cyber security is now a mainstreamed operational concern for businesses.** Nearly a quarter of a million Australian businesses are estimated to have experienced a cyber security incident in 2020-21. The rate of cyber incidents has tripled since the pandemic, and now affects one-in-five businesses annually.

2. **Australian business leaders are highly attuned to the risks of cyber security.** Two thirds of all businesses report being informed about cyber security, and four-in-five indicate they are somewhat or very concerned about the impacts of cyber attacks on their operations.

3. **Cyber security has become a top business investment priority.** It ranks fifth amongst the investment intentions of Australian business, alongside traditional options like capex, staff training and R&D. Cyber is now viewed as a mainstream business investment, with return-on-investment and cost driving investment decisions.

4. **Businesses have deployed a wide range of capabilities to address identified cyber risks**. Most businesses (82%) use external vendors to access additional cyber capabilities, often as a complement to their in-house resources. Two thirds of small, and over 80% of medium and large businesses, report confidence in the cyber capabilities they have in place.

5. **Medium businesses are the missing middle when it comes to cyber security in Australia.** Medium-sized firms have a similar risk profile to their large peers, but fewer resources to dedicate to cyber. Developing policy and commercial solutions to aid medium businesses is the logical next step in upgrading the cyber security of Australian industry.

6. **The cyber capabilities of staff are as important as technology.** One third of small businesses, and two thirds of medium and large, include staff capabilities as part of their cyber security investments. Ensuring staff are equipped to use technology safely is critical for a holistic cyber security strategy.

1. Executive summary

As digital technology transforms our society and economy, cyber security has become a leading national security concern for Australia. While cyber incidents are an increasing worry for the privacy and security of everyday Australians, they are also a major challenge for our businesses.

We undertook the Ai Group Cyber Security Survey 2023 to understand how Australian industry is approaching cyber issues today. Over two-hundred Australian businesses responded, providing insights on their cyber risk profiles, their capabilities and policies, and the factors shaping their cyber investments.

The Ai Cyber Security Survey 2023 shows that Australian businesses are well informed of the risks of cyber attacks, and have decisively moved from awareness to action.

We find that Australian businesses are conscious, concerned, but moderately confident about cyber security. Cyber has become a top investment priority for business leaders, and the majority of Australian businesses deploy a diverse range of cyber defences sourced from both external vendors and in-house IT teams.

But there is room for an increase in cyber protections across all businesses in the Australian economy. We are only as strong as the weakest link in the national cyber ecosystem.

Cyber attacks on large businesses have been a focus of public, policy and commercial attention – and rightly so, given their data-rich operations and complex supply chain linkages. However, our research shows they also have resources and capabilities to invest in cyber security practices.

Medium businesses appear to be the 'missing middle' when it comes to the national cyber ecosystem. Our research shows they have a similar cyber risk profile to large businesses, but fewer resources to invest in leading-edge security practices.

This is borne out by data from the *Australian Cyber Security Centre*, which found that medium businesses carried the highest average cost per cybercrime, losing over $88,000 compared to over $39,000 for small businesses, and over $62,000 for large businesses[1].

Our research also finds that people are as important as technology when it comes to cyber security. Technology solutions are only as good as the people using them, but the digital capability of some segments of the workforce is concerningly low. With only one-in-three small businesses investing in staff cyber skills, there is need to make workforce investments a greater part of oru cyber defence.

The Ai Group Cyber Security Survey 2023 shows that we have a unique opportunity for Australia to lift the cyber security capability of all businesses, with a focus on our medium-sized enterprises and the digital skills of our workforce.

[1] https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022 accessed Friday 11 August 2023

2. The impacts of cyber security on Australian businesses

Nearly a quarter of a million businesses affected annually

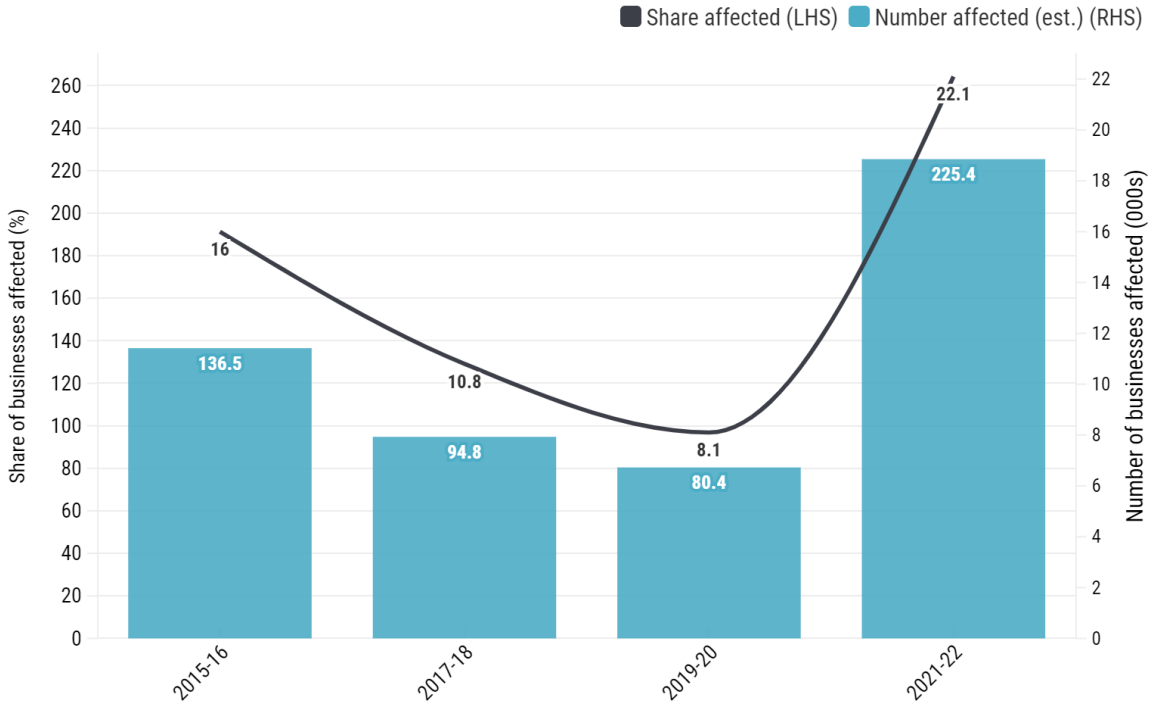
One of the factors driving business attention to cyber security is the fact that cyber incidents are on the rise in Australia. The Ai Group cyber security survey asked businesses about whether they had been affected by a cyber incident and how it affected their operations. Our data complements recent survey data from the Australian Bureau of Statistics (ABS).

Together, the Ai Group and ABS data shows that cyber incidents affecting business are now very common. Both surveys indicate that around one-in-five businesses experienced a cyber incident in the last year.

Given the number of businesses in Australia, this prevalence rate suggests 225,000 businesses now face a cyber security incident every year.

These incidents are also becoming more common (Fig 1). The number of businesses affected had steadily fallen in the years prior to the pandemic, possibly due to growing awareness of cyber issues and improved security practices. But since the pandemic cyber security challenges have surged, with the share of businesses reporting incidents more than tripling to a record 22.1% in 2021-22.

Figure 1: How many businesses are affected by cyber security incidents?

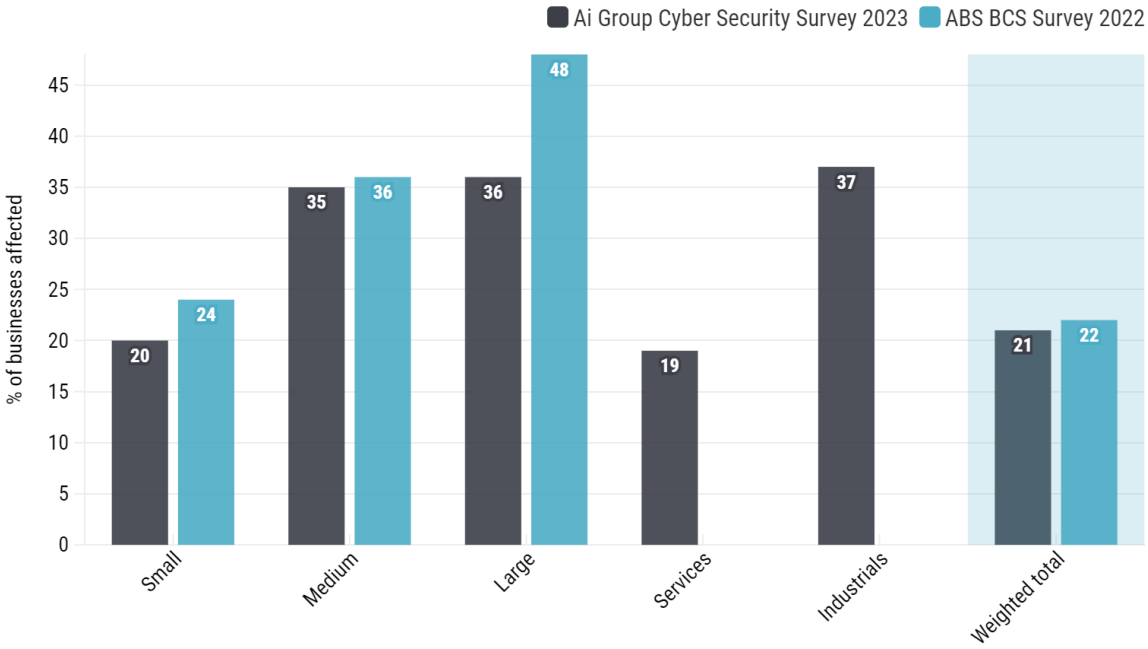


Source: ABS Business Characteristic Survey, ABS Counts of Australian Businesses

Size matters when it comes to being the victim of a cyber-attack (Fig 2). The annual incidence rate rises from one-in-four for small businesses, to one-in-three for medium businesses, and affects nearly half of large businesses.

Ai Group's survey found cyber incidents were almost twice as likely for industrials (37%) than services businesses (19%). This may reflect the larger size of industrial businesses, as well as the greater scope of intellectual property data they possess.

Figure 2: Which type of businesses are affected by cyber incidents?

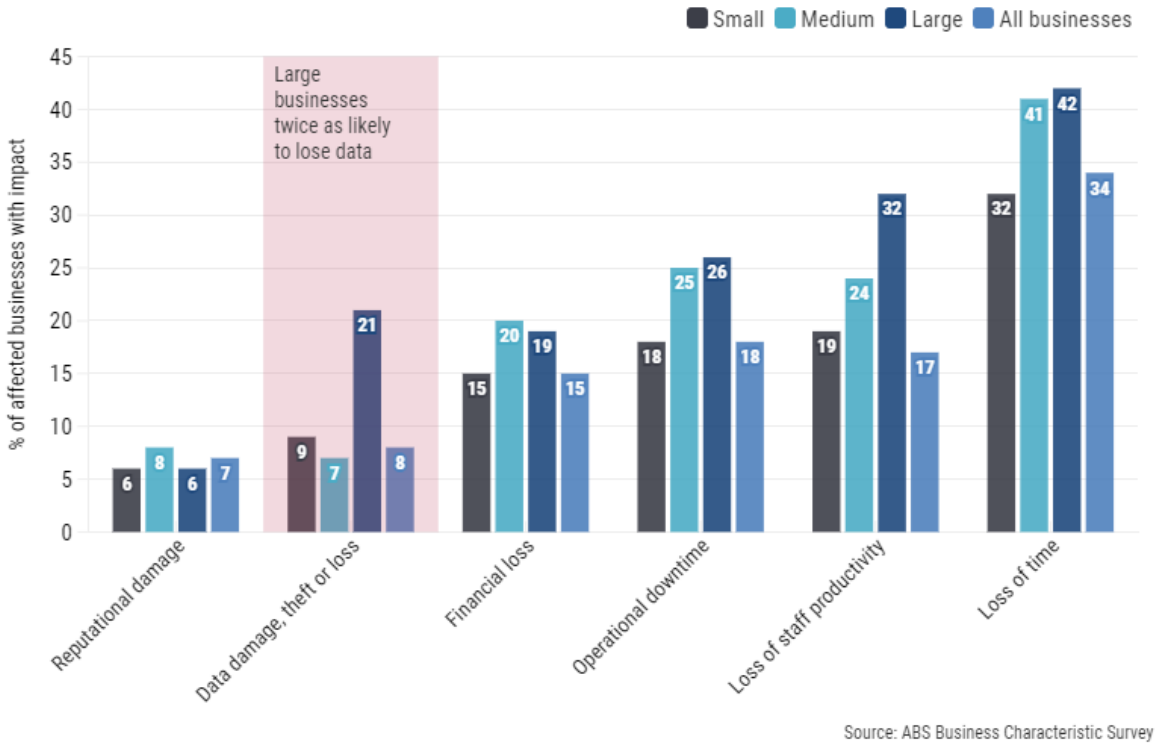


Source: Ai Group Cyber Security Survey, ABS Business Characteristic Survey • ABS survey asked whether businesses were affected by any incident, whereas Ai Group survey limited to incidents that disrupted operations

The impact of these cyber incidents was far from trivial. According to ABS data, 55% of businesses experiencing a cyber incident suffered an impact as a result of it. The impacts included (Fig 3):

- The most common was **loss of time**, which impacted 34% of incident-affected businesses.
- **Operational downtime** (18%) and **loss of staff productivity** (17%) were also common outcomes from a cyber incident.
- A more serious outcome was **financial loss**, impacting 15% of affected businesses. This is likely to reflect costs incurred during incident recovery.
- The least common outcome was **reputational damage**, with only 7% affected.
- **Damage, theft or loss of data** occurred for 8% of impacted businesses. However, the ultimate impact of data loss is likely to be larger, as data theft can expose information of other businesses as well.

Figure 3: What were the impacts of a cyber incident?



Source: ABS Business Characteristic Survey

Across the various impacts of a cyber incident, small businesses were generally less affected than their peers. Impact rates are broadly similar for medium and large businesses.

However, one notable outlier was data loss impacts, which were experienced by large businesses at more than double the rate (21%) of small and medium. Given the number of large businesses, this implies that approximately 950 suffered a cyber incident that led to data loss in 2021-22.

This data suggest that cyber threat actors are preferentially targeting medium and large businesses, with a specific focus on large businesses for the purposes of data theft. This is likely due to the greater quantity of data these businesses hold, the broader range of customers and suppliers they engage, and the interdependent structure of their digital systems. These features mean the implications of a attack on larger businesses has much greater impact for everyone in the economy.

3. Business views on cyber security

Conscious, concerned, and moderately confident

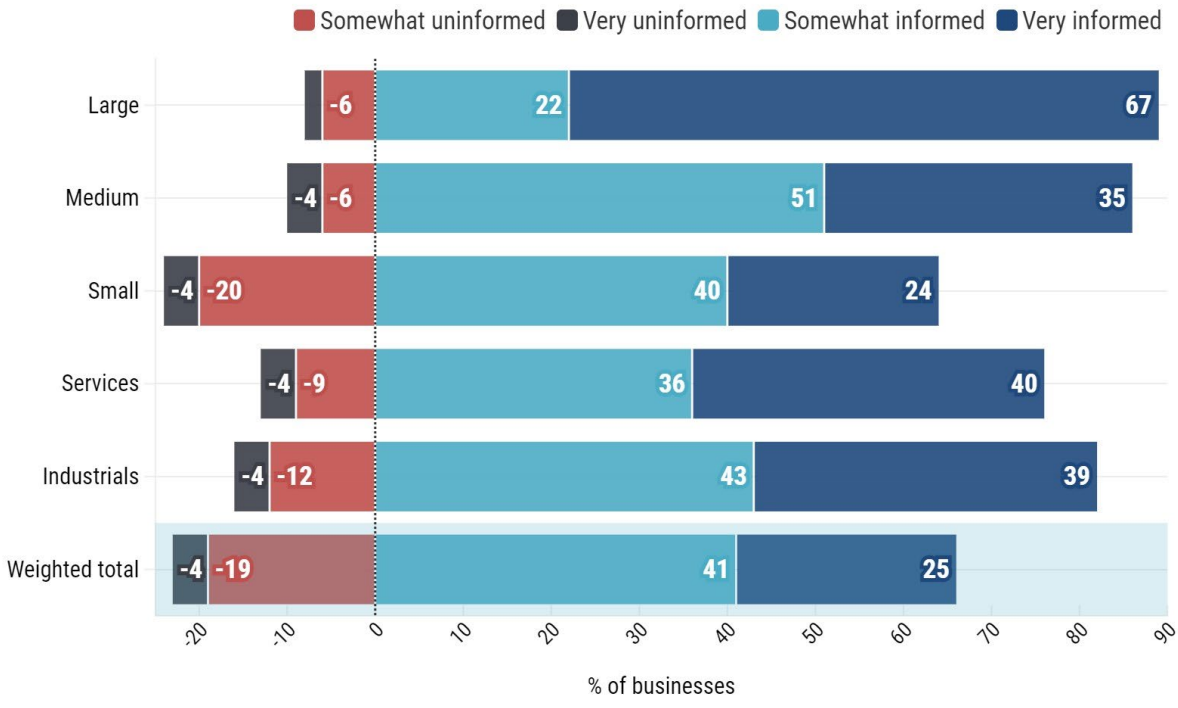
The importance of cyber security is now widely recognised by business leaders. As cyber incidents become more common – and public debate of their consequences grows – businesses have become very attune to cyber risks.

The Ai Group cyber security survey found that businesses are very conscious of cyber issues, quite concerned about them, and moderately confident in their capabilities to respond.

Overall, **two-thirds of businesses report they are somewhat or very informed** about the nature of cyber security issues (Fig 4). Only 23% describe themselves as uninformed. Large businesses are more likely to be cyber informed than small businesses, and industrials are slightly ahead of services.

This data shows that the majority of businesses in every category consider themselves cyber informed, and only a minority of predominantly small businesses are not. This speaks to the attention that cyber security issues now command amongst Australian business leaders and decision makers.

Figure 4: How informed are businesses about cyber security?



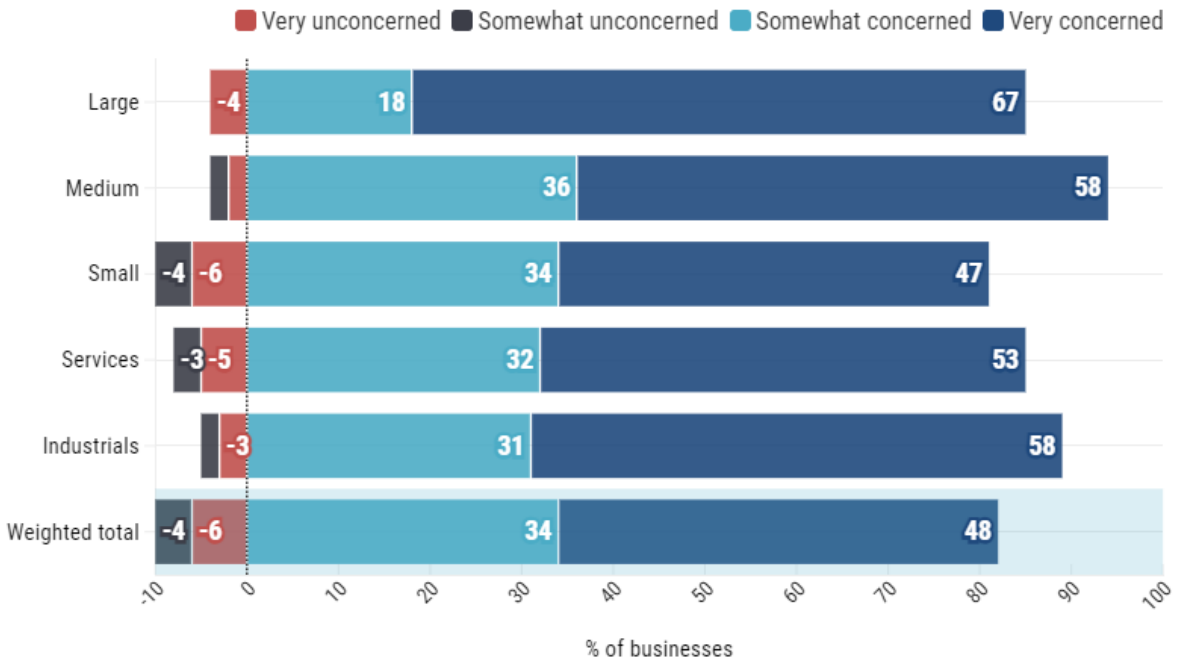
Source: Ai Group Cyber Security Survey

In an environment of increasing cyber threats, high levels of cyber awareness are naturally associated with very high levels of cyber concern. Across all businesses, some **82% are either somewhat or very concerned about cyber security risks**, while only 10% are unconcerned (Fig 5).

Despite their differing risk profiles, industrial and services businesses report similar levels of cyber concern. This indicates that cyber security is now recognised as issue that can affect any business, and is not only considered a problem for industries which are commonly perceived as high risk (such as banking, telecommunications and infrastructure).

Surprisingly, medium-sized businesses report higher levels of cyber concern (94%) than either their large (85%) or small (81%) peers. This may reflect the fact that medium businesses are sizeable enough to face heightened risks of a cyber incident, but lack the scale to address those risks in the way a large business can.

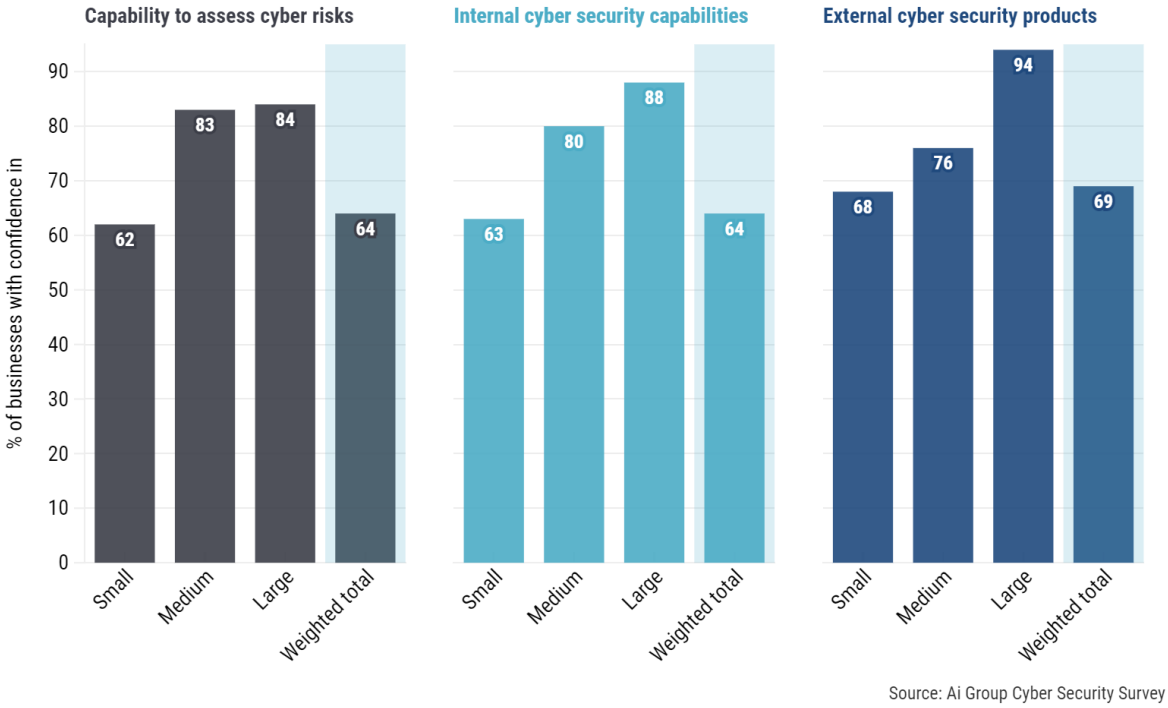
Figure 5: How concerned are businesses about cyber security?



Source: Ai Group Cyber Security Survey

However, while the majority of businesses are cyber concerned, this does not mean they lack confidence. The Ai Group cyber security survey asked businesses about their confidence in three elements of their cyber systems: their capacity to assess risk, their in-house systems and practices, and the products they deploy from external vendors (Fig 6).

Figure 6: How confident are businesses in their cyber systems?



The results show a **moderately high level of business** confidence in dealing with cyber risks:

- Around two-thirds of small businesses, and most medium and large businesses, have **confidence in their ability to assess cyber risks.**
- Similar proportions of businesses have confidence in their **in-house capabilities** to adequately address identified risks.
- Confidence in **external cyber security solutions** was slightly higher than for in-house capabilities amongst large and small businesses.

Overall, this data shows that Australian businesses are well-advanced in their thinking about cyber security issues. The majority of businesses report being informed about the nature of risks, and while being appropriately concerned also display confidence in the internal and external systems they use to manage risk.

The principal cleavage in cyber thinking lies between small businesses and their larger peers. While approximately two thirds of small businesses report being cyber-informed and confident, in all the indicators they lag behind medium and large businesses.

This is unsurprising, as it reflects the resource constraints facing small businesses. But it also points to the importance of providing small businesses straightforward and cost-effective options to address cyber risks.

4. Cyber practices in Australian businesses

More investment needed in medium businesses

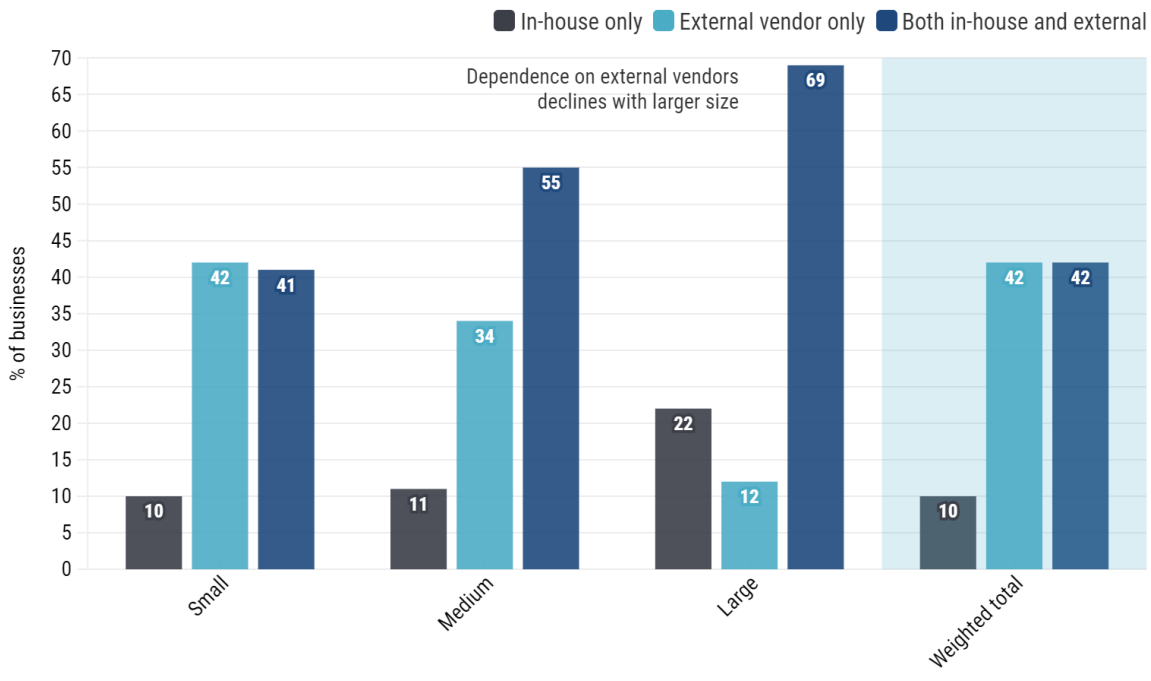
With cyber awareness high and incidents becoming more common, businesses have responded by deploying a wide range of tools to address cyber security risks.

When it comes to sourcing cyber capabilities, very few businesses try and go-it-alone. 82% of businesses bring in help from external vendors, either a standalone cyber provider or to augment their in-house IT teams. This is extremely valuable in ensuring business leaders have access to the expertise, knowledge and technology that keeps pace with quickly evolving cyber threats.

There is also evidence of a natural maturation in cyber capabilities as a business grows. Small businesses rely heavily on external vendors for cyber security. But as they grow to medium size, they start building up their own capabilities and reduce sole dependence on external vendors. By the time a business achieves large scale, additional resources enables the in-house team to take greater control.

This data suggests we should think about cyber readiness as a "pathway" businesses advance along, with the mix of external and in-house sourcing changing as they grow.

Figure 7: Where do businesses source their cyber capabilities?

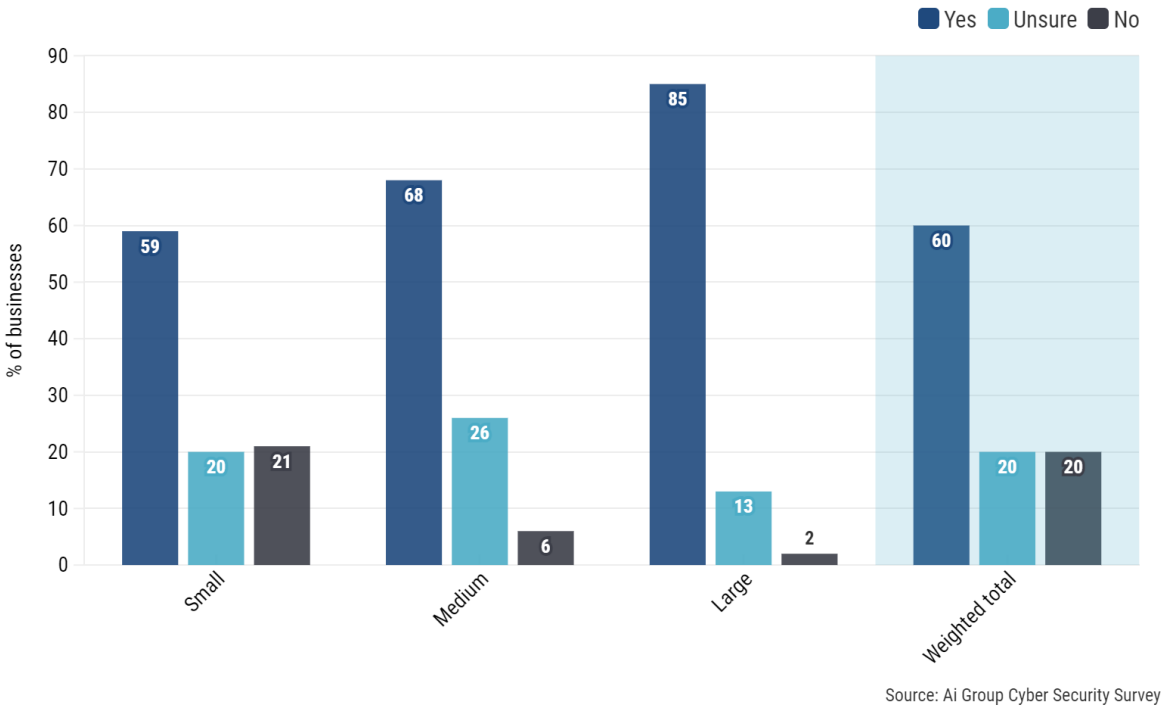


Source: Ai Group Cyber Security Survey

The reliance on external providers reflects the fact that many businesses need help and advice on cyber security matters (Fig 8). Overall, **60% know where to get information on cyber security** – a similar number to those reporting they are cyber aware and cyber confident. But 20% don't know where to get information, and another 20% are unsure. As companies get larger, their ability to access information improves.

While it is reassuring that the majority of businesses know where to get information, there remains a significant number of small businesses facing knowledge gaps. Even amongst large companies 13% report being unsure, which speaks to the challenge businesses face in finding reliable cyber security information.

Figure 8: Do businesses know where to get cyber security information?



Source: Ai Group Cyber Security Survey

Which specific cyber security practices are businesses currently employing? The Ai Group cyber security survey examined the utilisation of common cyber security practices (Fig 9), and the deployment of the ACSC's *Essential Eight* mitigation strategies (Fig 10):

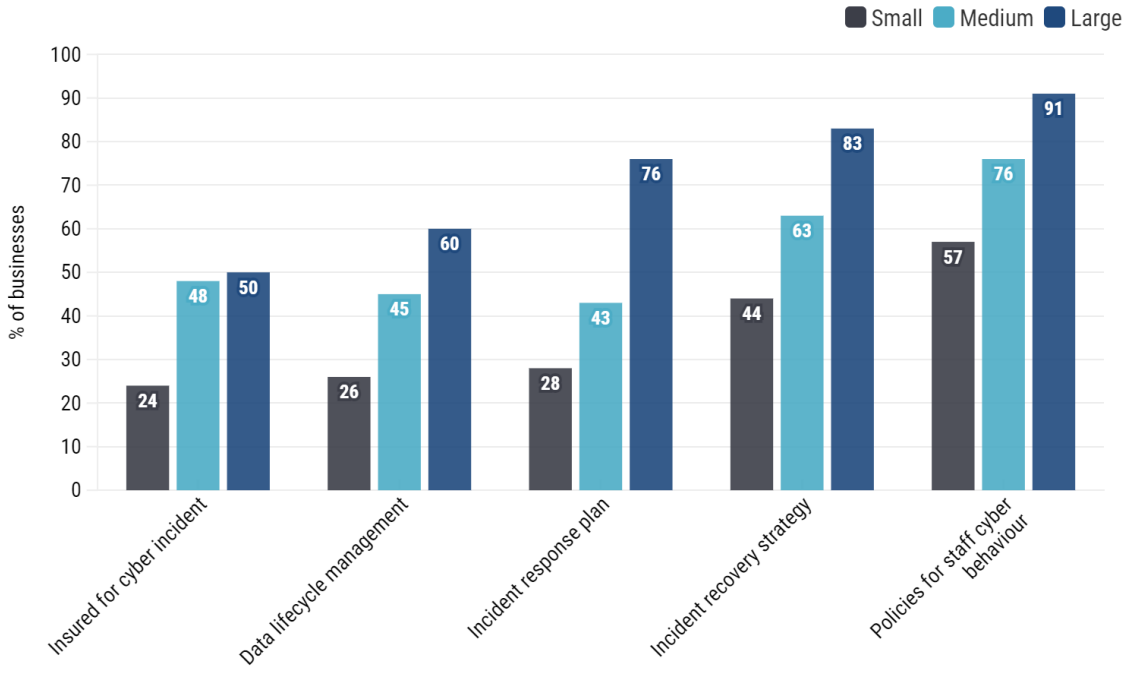
- The most common cyber practice across all business sizes are **policies to assist staff to practice good cyber security behaviours**. Most (91%) large businesses have developed policies to assist staff, falling to just over half (57%) of small businesses.

- **Incident recovery strategies** are also common, deployed by 83% of large and 44% of small businesses. However, businesses are less likely to have an **incident response plan**, held by 76% of large and only 28% of small businesses.

- Large businesses are more likely than medium or small to have a **data lifecycle management strategies,** with 60% of large firms reporting they have one, compared to 26% of small businesses.

- **Cyber security insurance** is the lowest priority. Only half of large and medium, and one-quarter of small businesses, are insured for a cyber incident, with the value of insurance for incidents not yet a convincing investment.

Figure 9: What cyber practices do businesses employ?



Source: Ai Group Cyber Security Survey

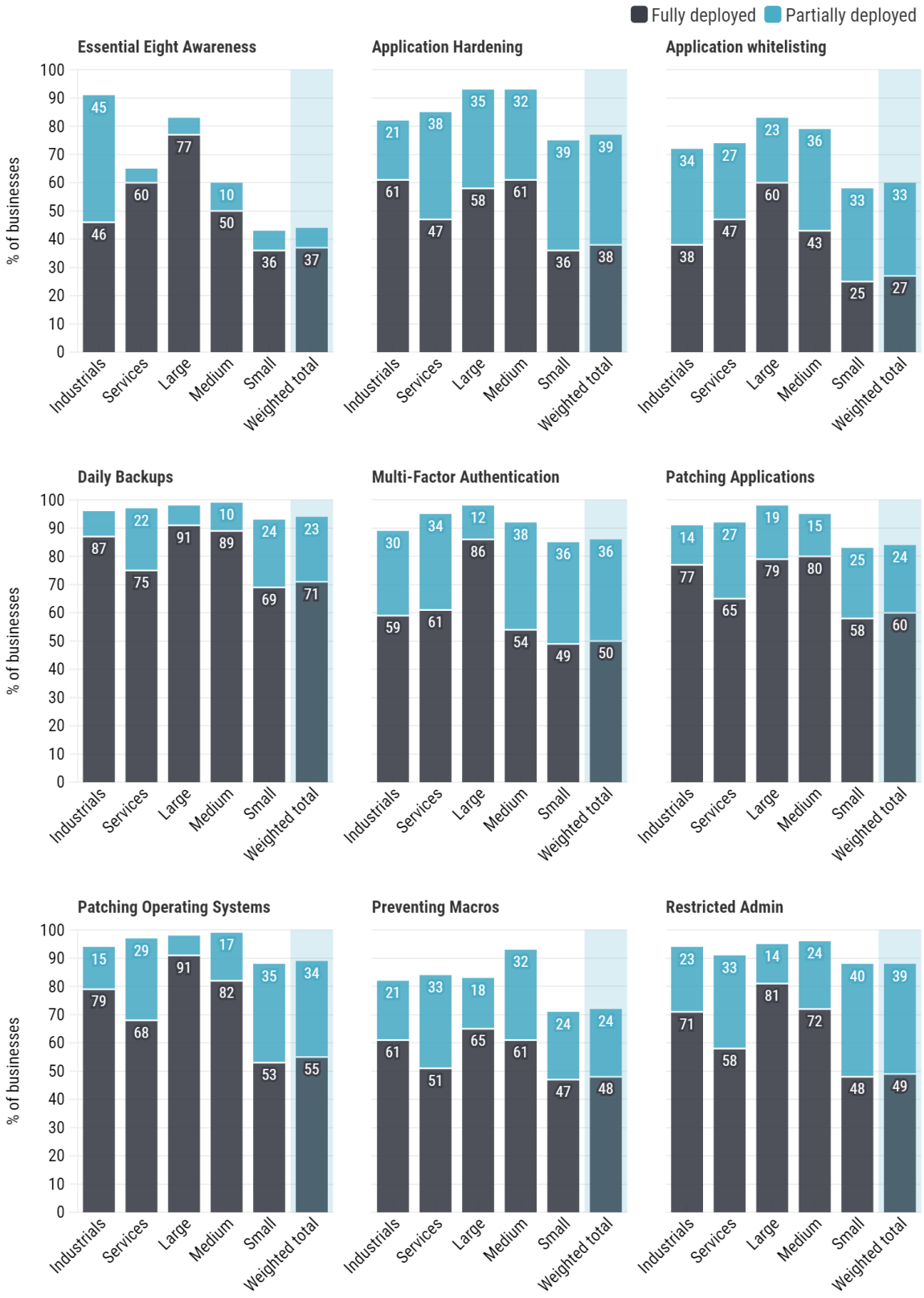
Data on **Essential Eight deployment rates** tells a similar story (Fig 10). Nearly all businesses have deployed the more straightforward mitigation strategies – such as daily backups, O/S and application patching, restricted administrative privileges and two-factor authentication. But deployment rates fall to around two-thirds for more technically challenging actions, such as macro blocking and application hardening and whitelisting.

This data points to a gap in the cyber security practices of Australia's medium businesses. They have similar attributes to large businesses in terms of the data they hold, their levels of digitisation, and the density of connections to external parties. Medium and large businesses also face cyber incidents at roughly similar rates.

Yet there is a gap between the cyber practices of medium and large businesses. Medium businesses are less likely than large peers to employ all of the key cyber security practices and Essential Eight strategies. This means medium businesses have lower cyber defences than their large peers, despite facing similar risk profiles.

That medium businesses are a particular point of exposure is borne out by data from the Australian Cyber Security Centre. It found medium sized businesses had the highest average cost per cybercrime, losing over $88,000 compared to over $39,000 for small businesses, and over $62,000 for large businesses. This indicates that there is considerable room for more uptake of cyber secure practices for medium sized enterprises.

Figure 10: Which Essential Eight practices have businesses deployed?



Source: Ai Group Cyber Security Survey

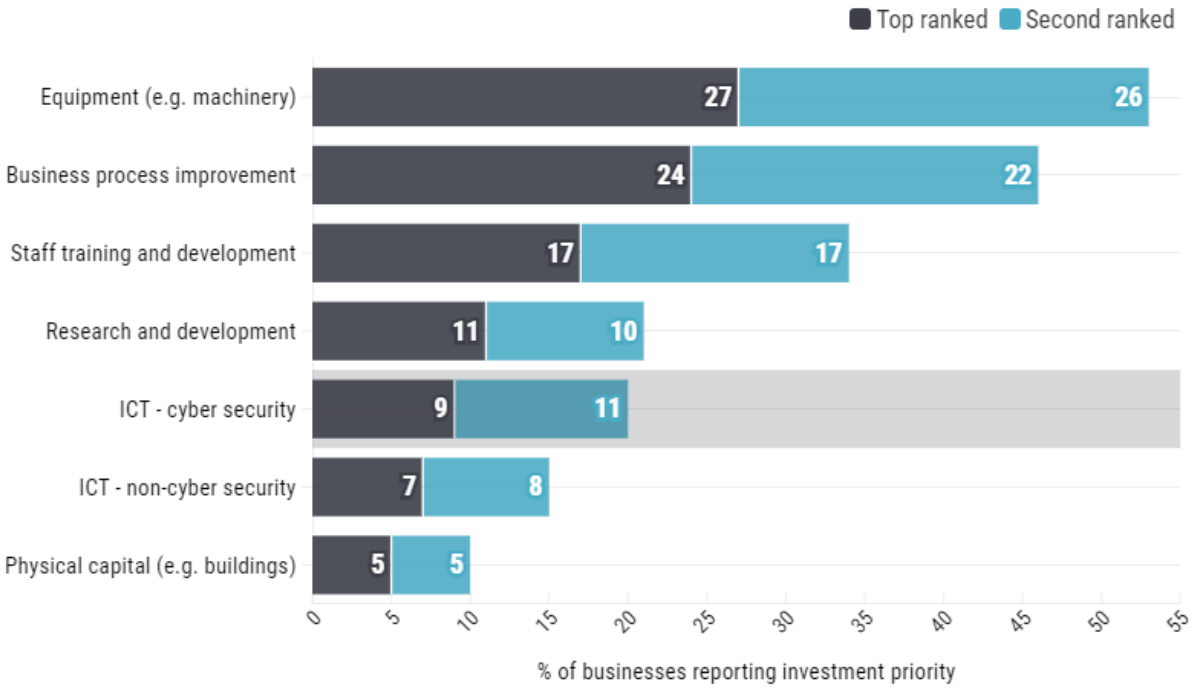
5. Cyber security investment priorities

Cyber is now a mainstreamed investment decision

One of the major cyber security questions asked by business concerns investment decisions: What are the right investments – in people and technology, in-house capabilities and external technologies – to address their unique cyber risk profile?

The Ai Group cyber security survey found that cyber security was the **fifth highest ranking investment priority** of Australian business, with 20% declaring it their top or second priority for the current year (Fig 11). Cyber security is ranked almost as highly as research and development, and sits ahead of non-cyber ICT and capex investments.

Figure 11: Where does cyber security rank in business investment priorities?

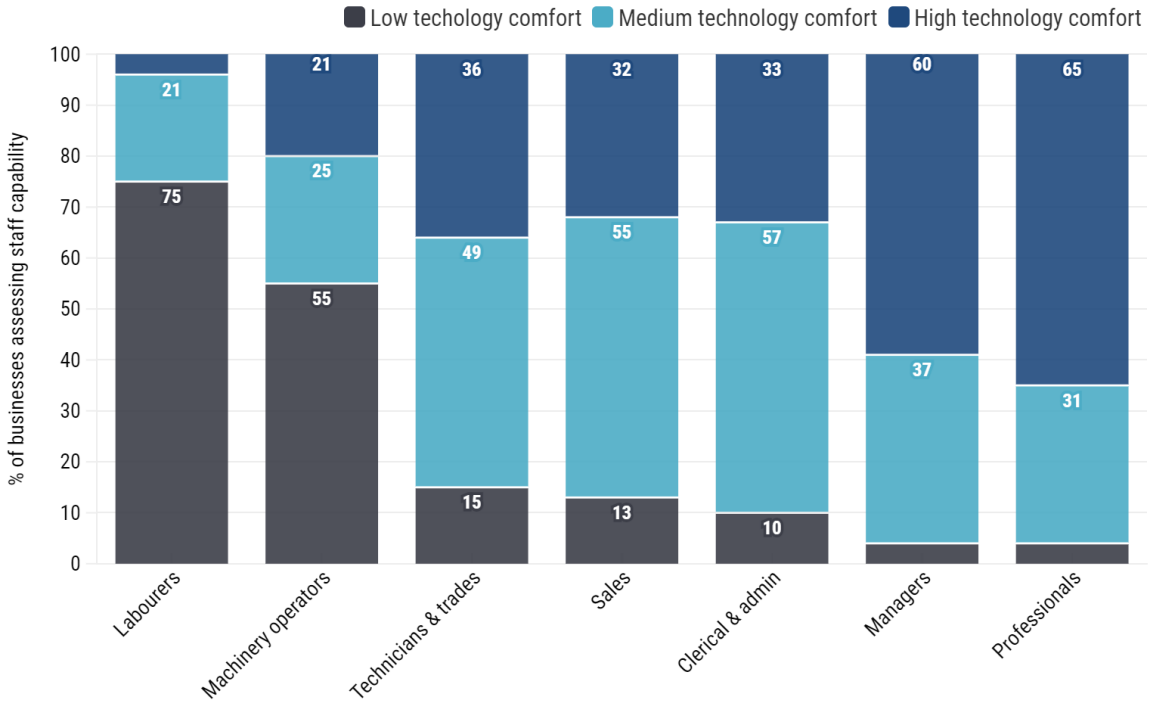


Source: Ai Group Cyber Security Survey

An important – if often overlooked – cyber security investment is in **staff technology training**. While technology solutions play a key role in cyber security, how employees use that technology is equally important to security outcomes. This is particularly relevant for segments of the workforce that have lower technology skill levels, who are more likely to engage in insecure digital behaviours.

Businesses report that **workforce comfort with technology** is lowest amongst trade and technical roles (Fig 12). 75% of businesses indicate low technology capability amongst labourers, and 55% in machinery operators. However, even in the highest skill occupations, only two-thirds of businesses considered their workforce highly comfortable with technology. This speaks to the importance of making investments in people, and not only technology, as part of a complete cyber security strategy.

Figure 12: How comfortable with technology is your workforce?

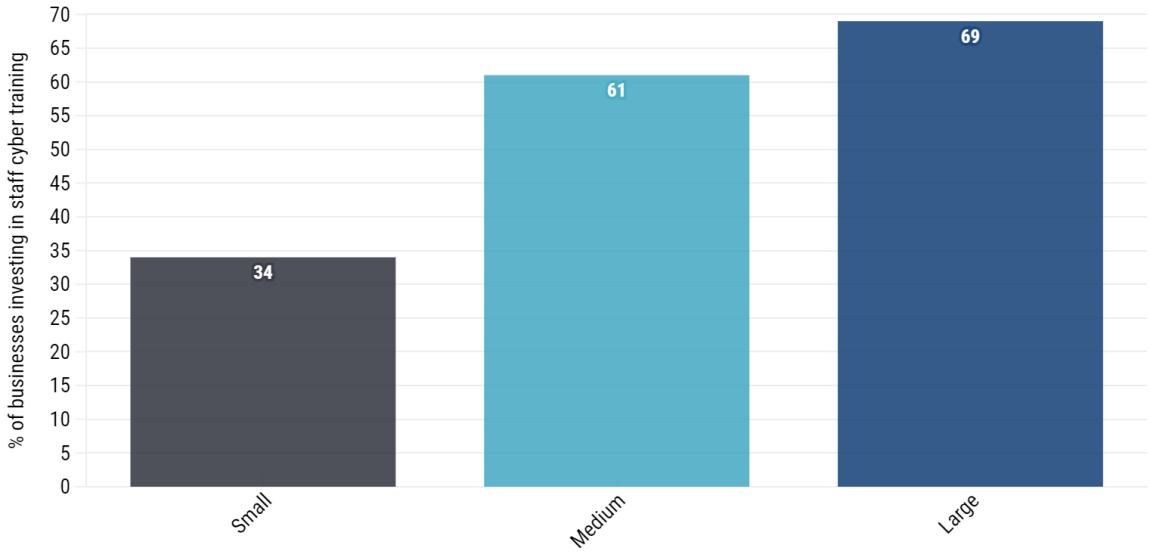


Source: Ai Group Cyber Security Survey

Encouragingly, many businesses are investing in staff cyber training, but size plays a key role (Fig 13). 69% of large and 61% of medium businesses report investing in staff cyber training, but the number falls to only 34% for small businesses.

While small businesses are less likely to have technology demands that necessitate higher levels of technology skills training, they are also the largest group of businesses. There is an obvious need to increase staff cyber training in small businesses, to ensure a holistic approach that combined technology- and people-oriented solutions.

Figure 13: Do businesses invest in staff cyber training?



Source: Ai Group Cyber Security Survey

What factors explain how businesses choose to invest in cyber security capabilities? The Ai Group cyber security survey found that businesses treat cyber investments in much the same way as any other investment decision (Fig 14):

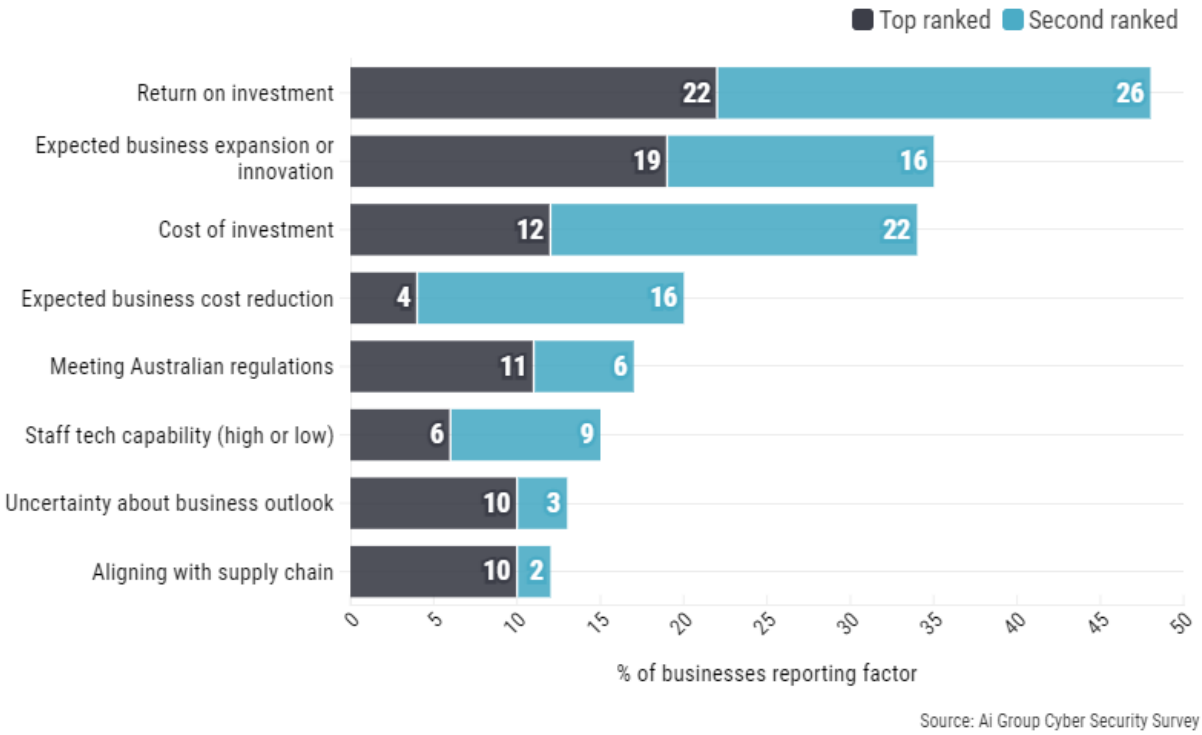
- Around half of businesses ranked **return on investment** (48%) as a top influence on their cyber investment decisions. This is normally the highest ranked factor in business investment surveys, and reflects that cyber security is now viewed as a mainstream business consideration.

- **Expected business expansion or innovation** was the next most influential (35%), and the **cost of cyber investment** came a close third (34%). Like return on investment, these are standard investment decision criteria and shows businesses are trying to balance costs against growth opportunities.

- Factors external to the business – such as **meeting Australian regulations** (17%) or **aligning with supply chain** (12%) – were comparatively low ranked as factors shaping cyber investments. This indicates that 'compliance' is not a major factor driving cyber investments, with business instead focused on how cyber capabilities can contribute to business operations and security.

- **Uncertainty about the outlook** (13%) also received a relatively low rank. As the survey was taken at a time of considerable uncertainty regarding the business environment in Australia, this suggests that cyber investments have been somewhat ring-fenced from business cycle factors.

Figure 14: What factors influence business cyber investments?



Source: Ai Group Cyber Security Survey

About the Ai Group Cyber Security Survey

Ai Group conducted the inaugural *Cyber Security Survey* in June and July 2023. We asked leaders in Australian businesses their thoughts regarding cyber security information that was available and whether they could find it, their cyber security capability, confidence in the skills of their workforce and systems, who they prioritise for training, what decisions they make about investment and how they make them.

Over two hundred private-sector businesses across Australia participated in the survey. Collectively, these businesses employed 52,000 people (258 people in each business on average).

All Australian states, and private sector industries, are represented:

- The **industrials grouping** contributed the highest proportion of respondents (63%) and is an aggregate of manufacturing, construction, mining and defence.
- The **services grouping** includes IT, communications & media services; transport, post & storage services; wholesale trade; retail trade; finance & insurance; real estate & property services; professional services; and administrative services.

Data presented in this report is weighted by employment size (based on ABS estimates from counts of Australian businesses) in order to adjust for the characteristics of the sample.

Ai Group Cyber Security Survey 2023	Small	Medium	Large	Industrials	Services	Total
Number of survey respondents	71	85	50	130	76	206
% of survey respondents	35%	41%	24%	63%	37%	100%
Size weighting	93.73%	5.82%	0.44%	-	-	100%

www.aigroup.com.au