BUSINESS NSW

SME CYBER SECURITY MANAGEMENT

September 2024

About Business NSW

Business NSW is the peak business organisation for New South Wales representing the needs of 48,000 businesses across the state.

Our purpose is to create a better Australia by maximising the outcomes and potential of Australian businesses. We achieve this by working with businesses spanning all industry sectors including small, medium and large enterprises.

Operating through our network in metropolitan and regional NSW, and with our state chamber partners, Business NSW represents the needs of business at a local, state and federal level. This is why when we speak, the government listens.

Not a member? Add your voice to the conversation today:
businessnsw.com/members/join-business-nsw

Acknowledgement

Business NSW would like to thank all the businesses that have participated in our quarterly Business Conditions Survey. We extend our special gratitude to those who have generously shared their experiences as case studies for this report.

Foreword

When a small to medium business becomes the victim of cyber criminals, the fallout is often devastating. The time and money poured into investigations and beefed-up cyber protections is significant, yet these attacks can also have a lasting impact on the enterprise's reputation, the psychological wellbeing of owners and staff, and the broader economy. And the problem is getting worse. On average, one case was reported every 6 minutes in the financial year 2022-23. The raw number of attacks in Australia – 94,000 – is a 24% increase from the previous year. Cyber experts agree the problem is much worse than that because of widespread underreporting by firms, who are often embarrassed and keen to ensure customers remain loyal.

At a broader economic level, attacks on stevedore company DP World, Latitude Financial, Pizza Hut, Optus, Medibank, Ticketmaster and Ticketek have given business owners and the general public a lesson in what governments have known for a long time – that the problem requires constant diligence and a collective effort.

Business NSW, as the representative of 48,000 businesses in the most populous and economically significant state in Australia, understands the many pressures business owners face, including insurance problems, energy costs, skills shortages and red tape.

This report aims to examine SME experiences of cyber incidents and lessons learnt, put the issue back on the national agenda and offer practical recommendations to business and government. Because when business thrives, we all thrive.

Dan Hunter

Dan Hunter
CEO, Business NSW

TABLE OF CONTENTS

Executive Summary

Cyber attacks can happen in various forms. The most common incidents relate to malware (e.g. ransomware), phishing, man-in-the-middle attacks and Denial-of-Service. The incidence of reported cyber crimes has been increasingly frequent in Australia over the years. On average, one case was reported every 6 minutes in the financial year 2022-23 (ASD Cyber Threat Report 2022-23).

Cyber crimes cost businesses both financially and non-financially. For the financial year 2022-23, the average self-reported financial loss of cyber crimes was $45,965 for small businesses, $97,203 for medium businesses and $71,598 for large businesses (ASD Cyber Threat Report 2022-23). The non-financial impact of cyber crimes includes damage to reputation, customer and supplier relations, and information loss.

Business NSW understands that small and medium-sized enterprises (SMEs) can be particularly vulnerable to cyber attacks. Through several rounds of our quarterly Business Conditions Survey, our research into SME cyber security management has focused on their experience of cyber incidents and their efforts in preparing themselves to withstand cyber attacks.

Key findings from Business NSW analysis:

01 Analysis of concern about cyber security risks by company size found that small businesses were on average the least concerned while medium businesses were the most concerned. However, in relation to preparedness in preventing and withstanding cyber attacks, small businesses were found to be the least prepared and had the widest cyber security risk management gap.

02 34% of small businesses and 43% of medium businesses surveyed by Business NSW reported experience of cyber incidents in the 12 months to August 2023. While outright business system hacking was relatively rare, the occurrence of business accounts (e.g. bank or supplier accounts) being hacked was relatively more frequent.

03 Compared to cyber incidents, more SMEs — 46% of small businesses and 68% of medium businesses — reported encountering online scams. While most of these cases were unsuccessful scam attempts, a small proportion of SMEs did fall victim to online scams (5% of small businesses and 7% of medium businesses) and/or had their company name used by others in a scam (3% of small businesses and 6% of medium businesses).

04 SMEs have invested in cyber security management in various ways. The most common approach was system upgrades, reported by 25% of small businesses and 52% of medium businesses surveyed.

05 The case studies included in this report demonstrate the importance of cyber security management regardless of business size, as SMEs can fall victim to cyber crimes in many ways that have financial and operational consequences.

06 The majority of SMEs (83% of small businesses and 97% of medium businesses) intend to spend on cyber security in 2024. While most of these businesses will at least maintain the same level of expenditure as last year, 22% of small businesses and 15% of medium businesses will reduce spending.

07 The two key barriers to strengthening cyber security of SMEs are the perceived unaffordability and the perceived irrelevance of cyber security to business.

1. Growing cyber security risks

Common forms of cyber attacks

Malware	Remote access trojans (RATs)	Providing a backdoor into a victim's device that allows cyber criminals to do almost anything they like
	Keylogging	Recording which keys a victim presses (e.g. for passwords and credit card details) and sending the information to cyber criminals
	Ransomware	Encrypting private files, preventing access to them, demanding a ransom to restore access to the files and threatening to leak the data on the dark web
Phishing	Fake emails ('Spear phishing' is a targeted form of phishing)	Tricking email recipients into clicking on malicious links or opening attachments to harvest sensitive information
Man-in-the-middle attacks	Alteration of communications between two parties who believe they are directly communicating with each other	Active wiretapping to intercept and selectively modify communicated data to masquerade as one or more entities involved in a communication association
Denial-of-Service (DoS)	Disrupting or degrading online services such as websites and email systems	Directing a large volume of unwanted traffic to consume the victim's network bandwidth, which then limits or prevents legitimate users from accessing the website

Sources: Australian Federal Police; Australian Cyber Security Centre; Computer Security Resource Centre (US Government)

Incidence of cyber crimes in recent years

The number of reported cyber crimes in Australia has been growing in recent years. In 2022-23, a cyber attack was reported every 6 minutes on average. The actual number of cyber attacks is likely to be much higher as the reporting is only compulsory for government agencies. The increasing frequency of reporting indicates greater risk of businesses becoming victims of cyber attacks if they do not implement measures to prevent these.

Figure 1: Number of cyber crimes reported

Financial year	Number of cyber crime reports*	Annual increase	Average frequency of reported cyber crimes
2019-20	59,806	Baseline **	Every 9 min
2020-21	67,500	13%	Every 8 min
2021-22	76,000***	13%	Every 7 min
2022-23	94,000***	24%	Every 6 min

Sources: Business NSW analysis based on data from the ACSC Annual Cyber Threat Report (2019- 2020, 2020-21, 2021-2022) and ASD Cyber Threat Report 2022-23

* *These figures include reports made by the public, businesses, organisations and government agencies. The total number of cyber crimes taken place is most likely to be higher than these figures, as cases are not necessarily reported and therefore not captured in official statistics.*

** *This is the first unclassified report according to the ACSC Annual Cyber Threat Report 2019-20. Hence, no comparison with the previous financial year can be made.*

*** *Approximate values cited in the ACSC Annual Cyber Threat Report 2021-22 and the ASD Cyber Threat Report 2022-23.*

Figure 2 shows that digital-intensive sectors are more likely to be a target of cyber attacks as they involve high-value activities and process large volumes of data.

Figure 2: Share of cyber crimes reported in financial year 2022-23 – top 10 sectors

Ranking	Sector	% of total
1	Federal Government	30.7
2	State and local governments	12.9
3	Professional, scientific and technical services	6.9
4	Education and training	6.7
5	Health care and social assistance	5.9
6	Financial and insurance services	4.7
7	Information, media and telecommunications	4.2
8	Construction	3.4
9	Defence	3.2
10	Retail and trade	3.0

Source: ASD Cyber Threat Report 2022-23

Note: The public sector has obligations to report cyber crimes, which may in part explain the relatively higher proportion of reported cases.

Impact of cyber crimes on business

Generally, the impact of cyber crimes on SMEs is greater than on large businesses, because they do not have the same level of resources to recover as large businesses, and frequently they do not have insurance to help cover financial loss if they fall victims to cyber attacks.

Non-financial impact

- Operational disruptions / productivity loss
- Damage to reputation
- Damage to customer and supplier relations
- Legal and regulatory ramifications
- Data breaches and/or information loss
  - — customer records
  - — employee information
  - — corporate information (e.g. business plans)
- Impact on staff wellbeing (e.g. work-related stress, or reduced work hours while the business has restricted operations during cyber attacks)
- Impact on business owners' wellbeing (especially in the case of SME owners)

Financial impact

In 2022-23, the average reported financial loss was highest for medium businesses. However, small businesses recorded the largest increase (54%) in the average financial loss when compared to 2020-21. SMEs seem to be increasingly attractive targets for cyber criminals.

Figure 3: Average financial loss attributed to cyber crimes reported by businesses in Australia

Business size	2020-21	2021-22	2022-23
Small business	$29,901	$39,555	$45,965
Medium business	$92,400	$88,407	$97,203
Large business	$51,372	$62,233	$71,598

Source: ASD Cyber Threat Report 2022-23

2. SME perspectives

This section presents findings from Business NSW research that shows the SME sector's perception of cyber security risks and their preparedness to prevent or withstand cyber incidents.

Company size classification by Business NSW:

Small = Up to 20 employees
Medium = 21 to 100 employees
Large = 101 or more employees

Concern about cyber security risks

In the survey conducted by Business NSW, businesses were asked how concerned they were about cyber security risks.

While small businesses had the largest proportion (22%) rating their level of concern about cyber security risks at the highest score of 10, they had a similar proportion (21%) giving a rating of 4 or lower.

On average, small businesses were the least concerned (with an average score of 6.6) compared to medium businesses (7.1) and large businesses (6.9).

About one in two medium businesses rated their concern with a score of at least 8.

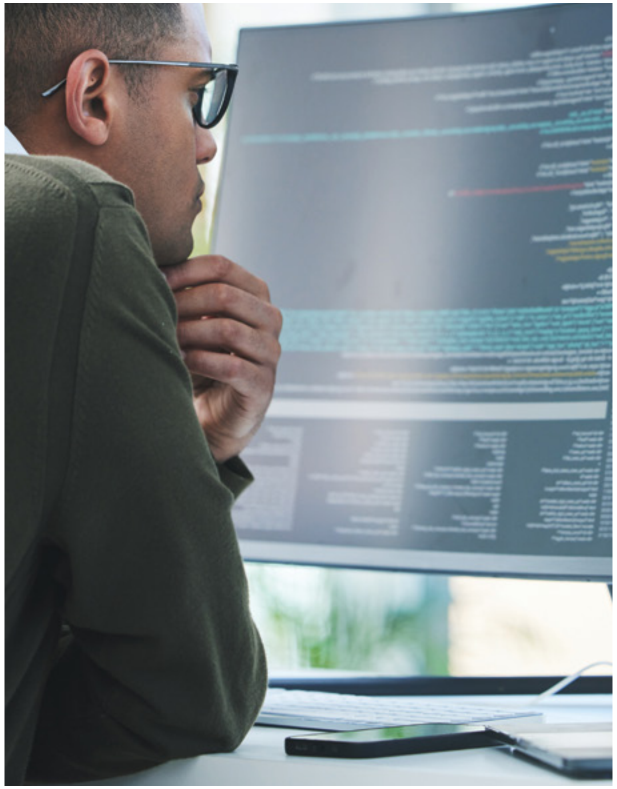
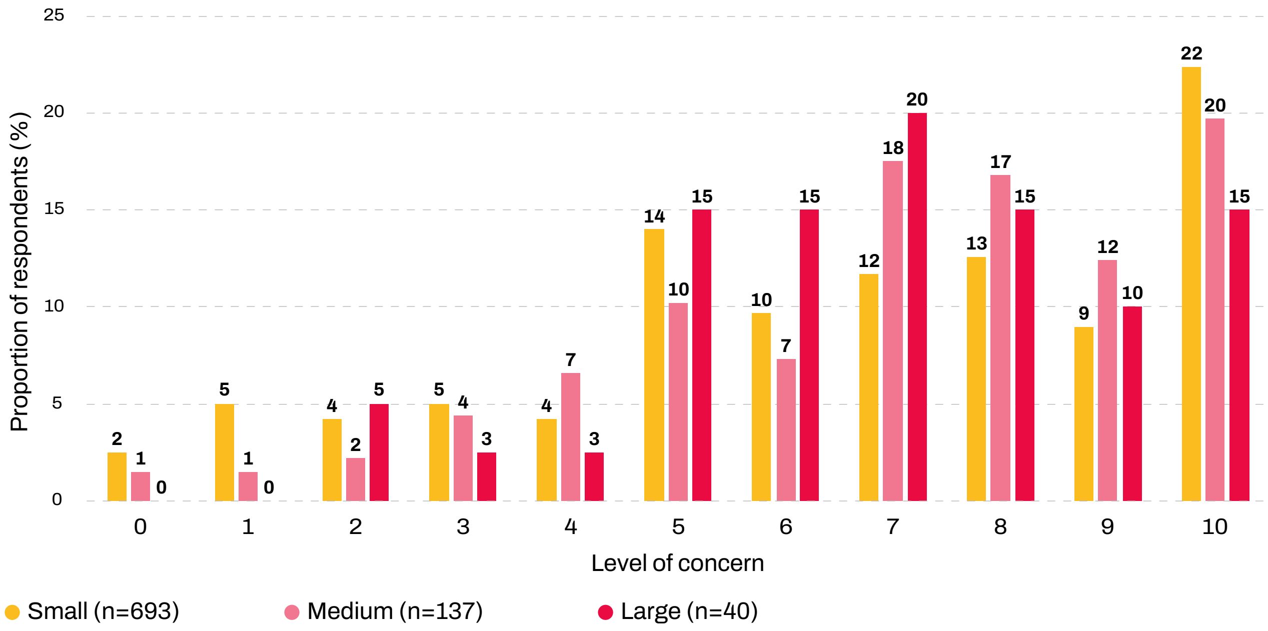


Figure 4: Concern about cyber security risks by company size



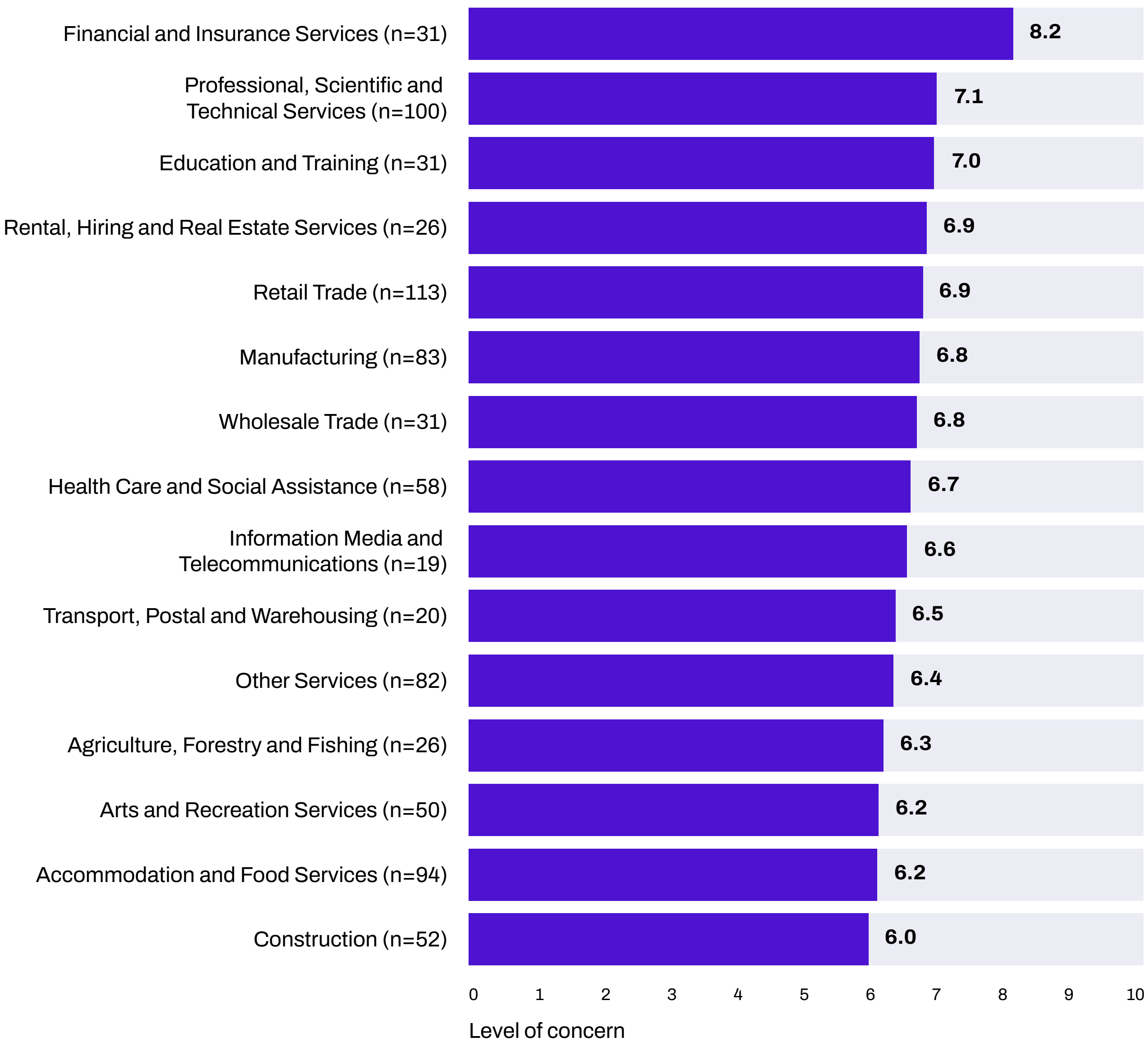
Source: Business Conditions Survey (November 2022), Business NSW

Amongst SMEs, the industry breakdown shows that businesses in the financial and insurance services industry were on average the most concerned about cyber security risks, followed by those in the professional, scientific and technical services industry and the education and training industry.

The construction industry was the least concerned about cyber security risks.

Overall, the ‘white collar’ industries were on average more concerned about cyber security risks than their ‘blue collar’ counterparts. This appears to reflect the different nature of the work, which requires different levels of interaction with digital networks.

Figure 5: SME concern about cyber security risks by industry



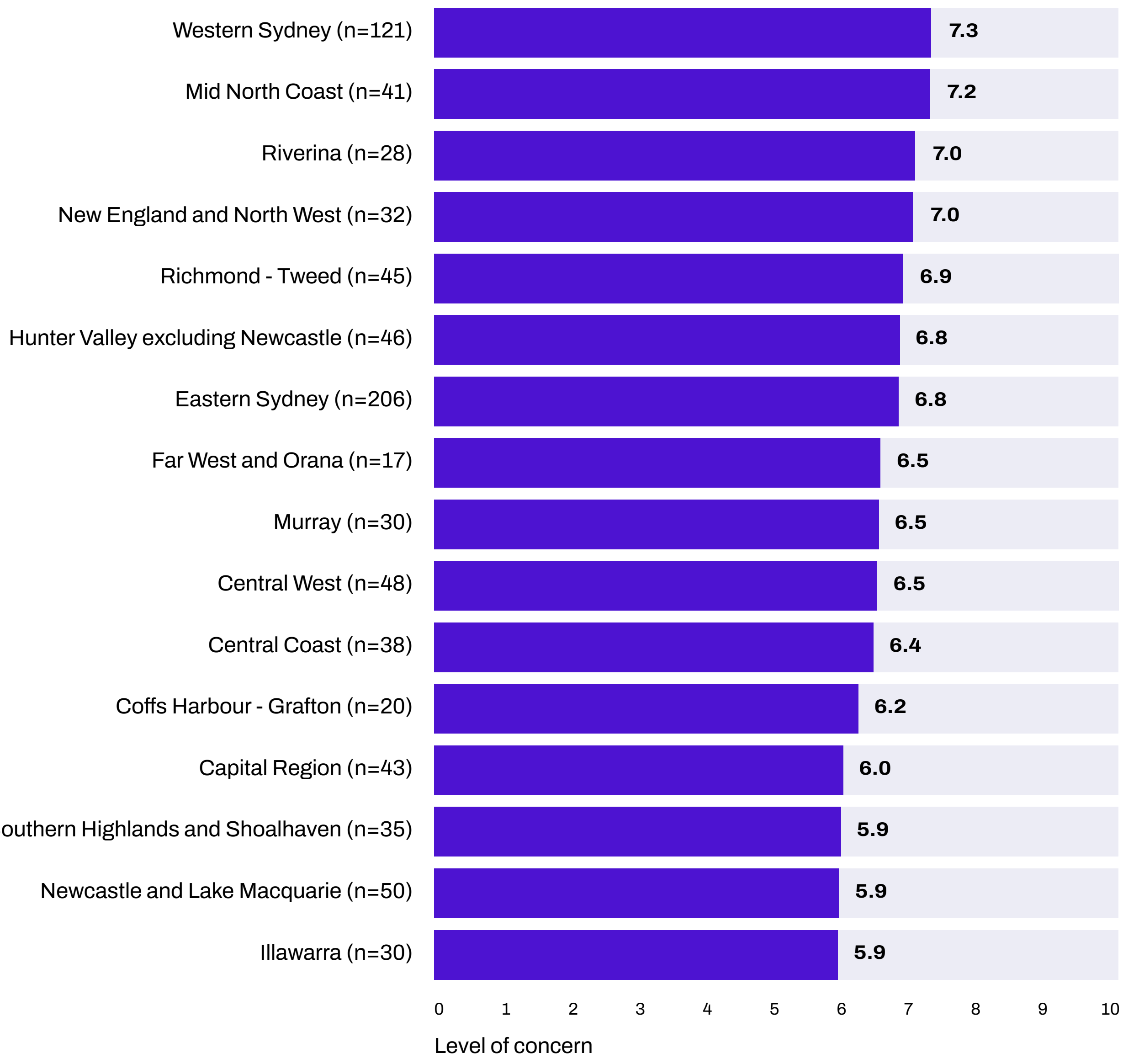
Source: Business Conditions Survey (November 2022), Business NSW

Note: Industries with less than 10 respondents are not included in the graph.

The geographical classification of business is unlikely to influence the level of concern about cyber security risks.

Analysis by region found a range of average scores from 5.9 to 7.3, with metropolitan areas – Western Sydney (7.3), Eastern Sydney (6.8) and Newcastle and Lake Macquarie (5.9) – scattered across the spectrum of average scores.

Figure 6: SME concern about cyber security risks by region



Source: Business Conditions Survey (November 2022), Business NSW

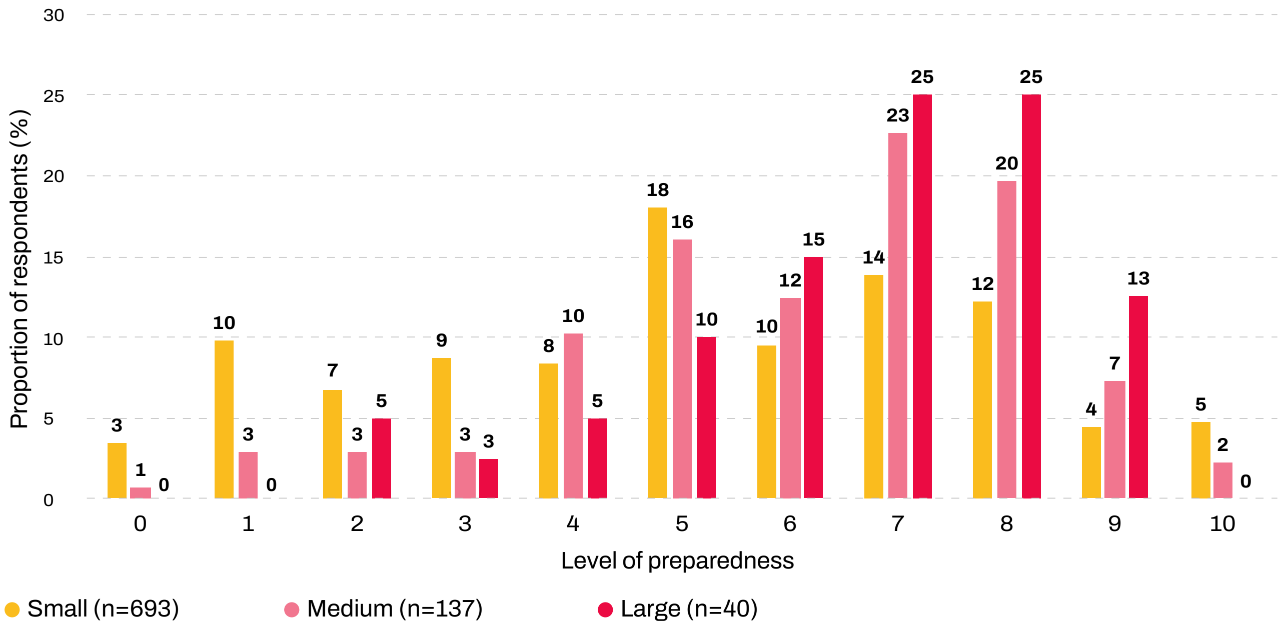
Self-assessed preparedness in preventing and withstanding cyber attacks

Based on self-assessment, small businesses were the least prepared to prevent and withstand cyber attacks (with an average score of 5.1 out of 10) compared to medium businesses (6.2) and large businesses (6.7).

One in five small businesses rated their level of preparedness with a score of 2 or below.

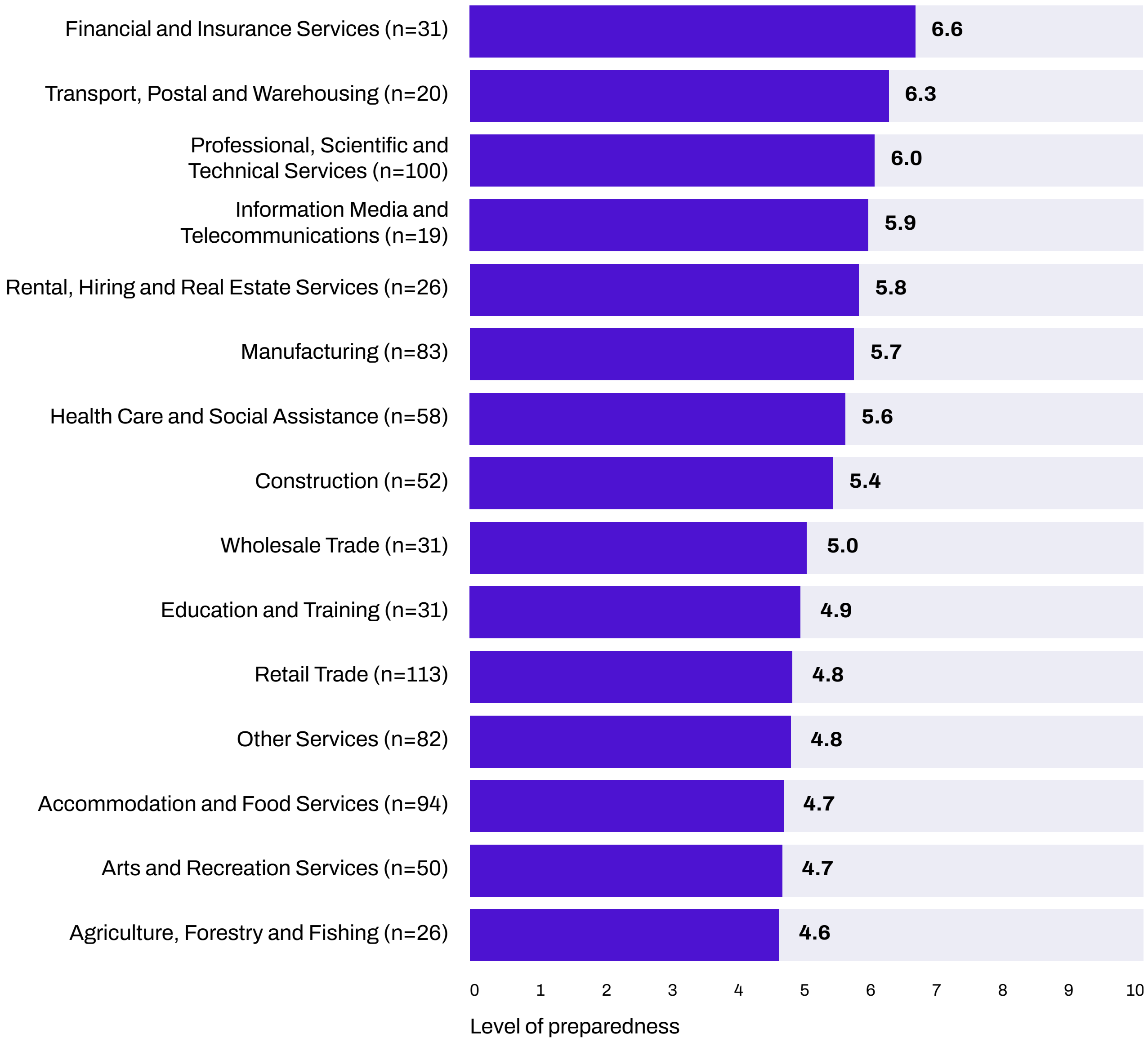
Medium businesses were more confident, with over 50% giving themselves a score of 7 or higher.

Figure 7: Self-assessed preparedness to prevent and withstand cyber attacks by company size



Source: Business Conditions Survey (November 2022), Business NSW

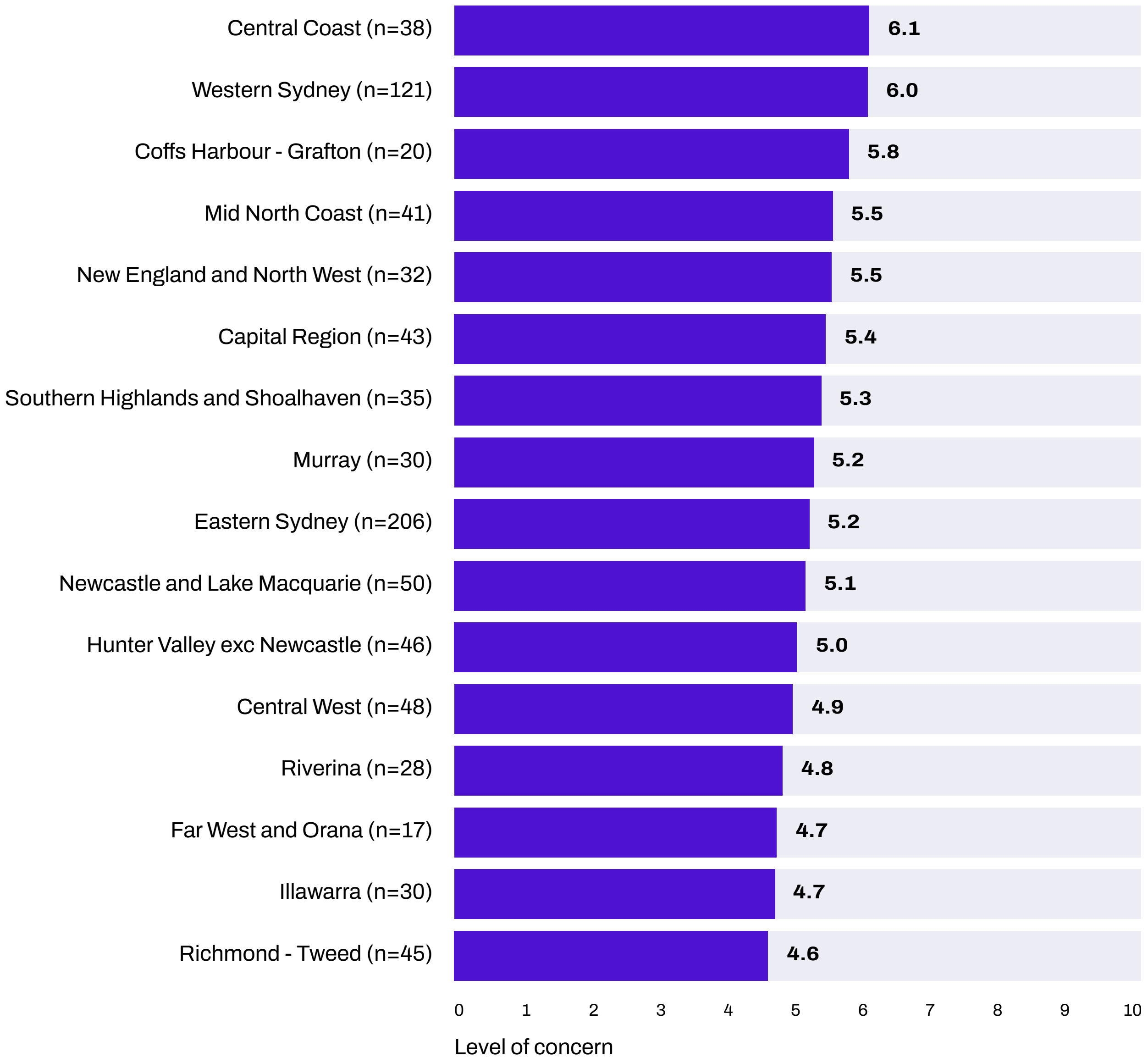
Figure 8: Self-assessed preparedness to prevent and withstand cyber attacks by industry



Source: Business Conditions Survey (November 2022), Business NSW

Note: Industries with less than 10 respondents are not included in the graph.

Figure 9: Self-assessed preparedness to prevent and withstand cyber attacks by region



Source: Business Conditions Survey (November 2022), Business NSW

Cyber security risk management gap

The ‘cyber security risk management gap’ captures the difference between business concern about cyber security risks and the level of preparedness to prevent and withstand cyber attacks.

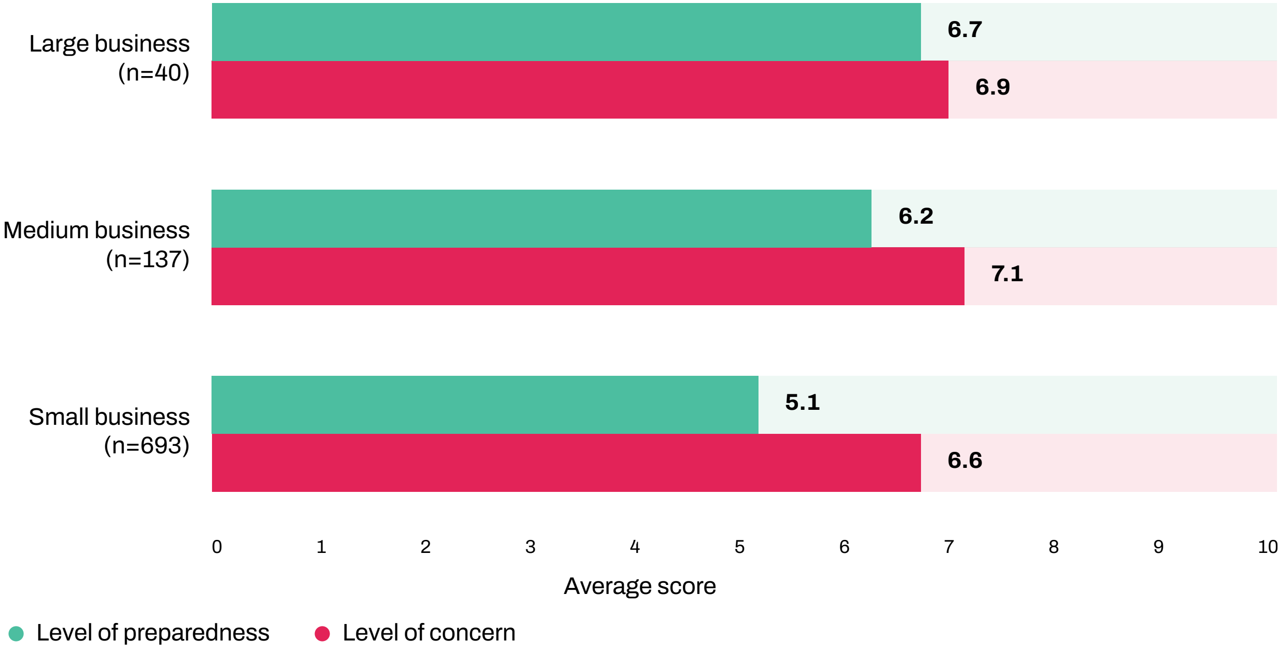
SMEs have a larger cyber security risk management gap than the large businesses, making them more vulnerable to cyber attacks. Digital security incidents can result in sizeable costs and non-financial losses as discussed in Section 1.

Large businesses had the narrowest gap, given the average concern score of 6.9 and the average preparedness score of 6.7.

This was followed by medium businesses with an average concern score of 7.1 and an average preparedness score of 6.2.

Although small businesses were the least concerned about cyber security risks (6.6), they were also the least prepared to deal with cyber attacks (5.1). This relatively wide gap warrants attention.

Figure 10: Cyber security risk management gap



Source: Business Conditions Survey (November 2022), Business NSW

3. SME experiences

Cyber attacks are a constant threat to SMEs. Greater reliance on digital technology increases SME exposure to cyber security risks and likelihood to become a victim of cyber crime.

This section draws on Business NSW research and explores SME experiences with cyber incidents and online scams.

Experience of cyber incidents and online scams

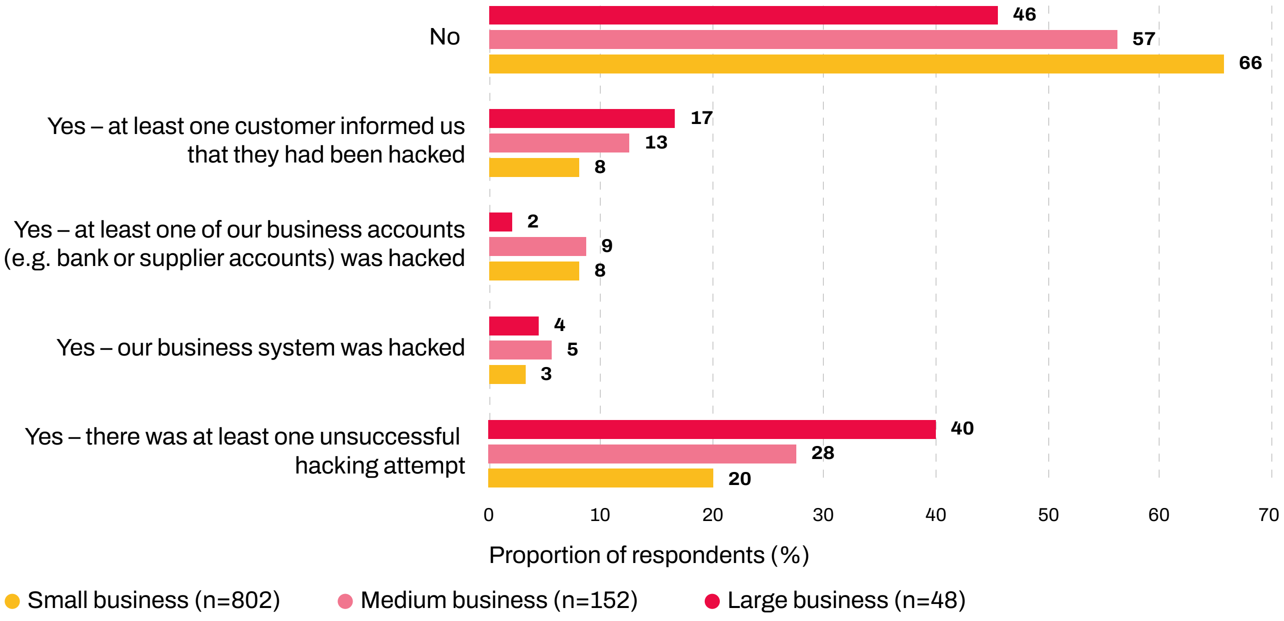
34% of small businesses and 43% of medium businesses surveyed by Business NSW reported experience of cyber incidents in the 12 months to August 2023.

The most common experience was unsuccessful hacking attempt, which was reported by 20% of small businesses and 28% of medium businesses.

While outright business system hacking was relatively rare (experienced by 3% of small businesses and 5% of medium businesses), the occurrence of business accounts being hacked was more frequent (experienced by 8% of small businesses and 9% of medium businesses).

Apart from businesses' own encounter with cyber incidents, their customers' cyber security woes can also have flow-on effects. The survey found that 8% of small businesses and 13% of medium businesses had at least one customer informing them of being a hacking victim.

Figure 11: Experience of cyber incidents in the 12 months to August 2023



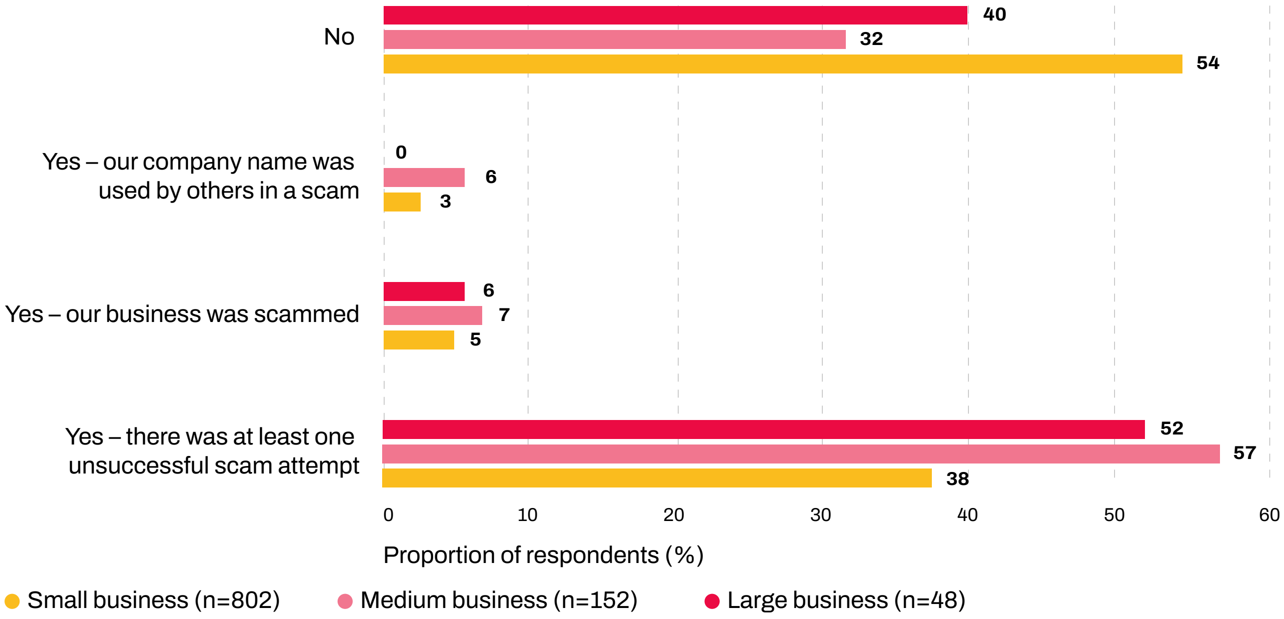
Source: Business Conditions Survey (August 2023), Business NSW

Note: Multiple 'Yes' selections were permitted in the survey to capture the whole range of experiences.

Compared to cyber incidents, online scams appear to have affected more SMEs, with 46% of small businesses and 68% of medium businesses reporting experiences with online scams in the 12 months to August 2023.

The majority of these cases were unsuccessful scam attempts. However, some SMEs did fall victim to online scams. Some impact would have been more direct, such as the case for 5% of small businesses and 7% of medium businesses that were scammed. Some impact would have been less direct, as in the case for 3% of small businesses and 6% of medium businesses that had their company name used by others in a scam.

Figure 12: Experience of online scam in the 12 months to August 2023



Source: Business Conditions Survey (August 2023), Business NSW

Note: Multiple 'Yes' selections were permitted in the survey to capture the whole range of experiences.

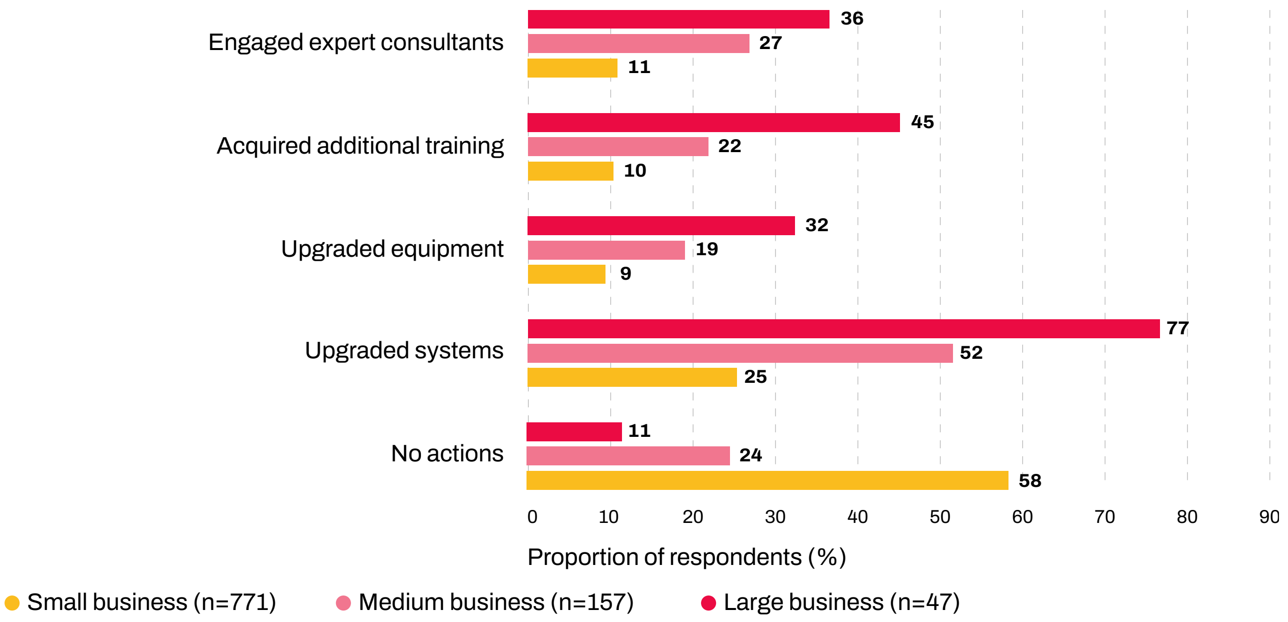
Cyber security management

SMEs tend to have less comprehensive and sophisticated cyber security management than large businesses. This is due to reasons such as limited awareness of cyber security risks and ability to fund cyber security management.

A survey conducted by Business NSW in mid-2023 found that 42% of small businesses and 76% of medium businesses have invested in cyber security management in various ways. The most common approach was system upgrades (consistent with large businesses), reported by 25% of small businesses and 52% of medium businesses surveyed.

For large businesses, the second most common approach was training. However, for SMEs, it was engagement of expert consultants. This difference likely reflects the lack of in-house expertise within SMEs.

Figure 13: Steps taken to enhance cyber security for business



Source: Business Conditions Survey (June 2023), Business NSW

Note: Multiple selections were permitted in the survey to capture the whole range of experiences.

4. Case studies of cyber incidents

This section provides case studies of cyber incidents encountered by SMEs in NSW. Each case study not only details the experience of the victim, but also highlights the common vulnerability of the SME sector and serves as a reminder of the importance of cyber security management regardless of business size.

Case study 1: phishing and man-in-the-middle attack

WHAT HAPPENED?

In February 2023, a book-keeping business in regional NSW fell victim to a business email compromise. The business paid nearly $50,000 from a client's account after receiving a falsified request to change the bank account for one of the client's suppliers.

The email requesting the change appeared to be legitimate and the business did not verify this request. However, the bank account was controlled by cyber criminals. The business realised that it became a victim to a cyber crime when the client inquired about delays in payment to the supplier.

The business immediately contacted the bank to which the payment was made, the Cyber Crime Squad, and NSW Police. The Police investigation concluded in January 2024, with findings that the cyber attack was done by international cyber criminals that have been active for the past four years.

IMPACT ON BUSINESS

The impact of this incident on the business was significant. The business had to cover the financial loss because it was their responsibility to check whether the payment was made to the correct account and their insurance did not cover this type of breach. In addition, the business had to dedicate resources and 50 hours of staff time towards the investigation process. The staff member who handled this fraudulent transaction also suffered a nervous breakdown.

LESSONS LEARN

- The business has switched to an email provider that they believe offers better cyber security.
- The business has tightened their payment procedures to ensure verification processes are in place. A dedicated staff member has been assigned the responsibility to check bank accounts details (if different from record) with clients before making any payment.

Case study 2: ransomware attack

WHAT HAPPENED?

A restaurant in regional NSW was attacked by ransomware. The cyber criminals gained access to the restaurant's main server and blocked the restaurant's access to their own system. The business owners were requested to pay a ransom to have the block removed.

IMPACT ON BUSINESS

No ransom was paid. The estimated losses due to the incident were between $2,500 and $3,000. The restaurant shut its door for several hours to have the system reinstalled and user files restored from their cloud backup. The staff were paid their full wages that day while the restaurant had significantly reduced revenue. Also, they had to manage disgruntled customers whose bookings could not be honoured. It was an extremely stressful period for the general manager of the restaurant and the team.

LESSONS LEARN

- The restaurant has strengthened its IT security settings so that no device could be accessed remotely without authorisation.
- Following a security review by an external IT company, an additional virus and malware protection software was installed.
- Additional backup software has been installed and this software is regularly updated.

> “*We have outlaid a lot of money to get additional security. It's frustrating that even a restaurant needs really high level and expensive security measures these days due to how prevalent these sorts of incidents are.”*

Case study 3: malware attack

WHAT HAPPENED?

A coffee shop relied on Facebook for marketing purposes. They had around 8,000 followers.

Cyber criminals accessed the coffee shop's Facebook account and changed their Facebook password as well as the password of their business email account.

IMPACT ON BUSINESS

The number of customers visiting the coffee shop dropped dramatically during the attack because the business owner was unable to communicate with customers to promote events and offers. The business owner had to create a new Facebook account and a new email address to re-establish communication with customers.

LESSONS LEARN

- The business owner is now more alert to cyber security risks, being more mindful of phishing emails and not responding to calls with no caller ID.

Case study 4: proactive approach to cyber security

WHAT HAPPENED?

A medical consultancy business is proactive in managing its cyber security to protect clients' data and its systems and information. The cyber security of the business systems is managed by an external company. The business uses multi-factor authentication to prevent unauthorised access to their accounts. In addition, the company regularly trains their staff in cyber security using Business NSW products. The business owner advised that these products convey information on threats and cyber security management that is easy to understand. The two-minute videos are based on real-life examples and staff really enjoy watching them.

IMPACT ON BUSINESS

The staff participation rate in the cyber security training sessions is 100%.

As a result, staff members became more interested and aware of cyber security threats and their role in preventing incidents. Staff members use the acquired knowledge to apply cyber security measures to protect the business as well as their IT systems and information.

Other comments direct from SMEs

> *“There is a daily onslaught of email and SMS attempts to get us sucked in. This takes time, effort and vigilance to sort out the crap from the actual real sales leads and supplier interactions and eats into productivity at a time when I can least afford it.”*
>
> Retail Trade

> *“Our ATO BAS accounts were compromised and BAS refunds were obtained by changing our tax agent to the scammer’s bogus account and then generating refunds to a bogus account. A total of $185k was taken.”*
>
> Professional, Scientific and Technical Services

5. SME planned investment in cyber security in 2024

Amid rising cost-of-living and cost-of-doing-business, businesses (especially SMEs) have to be cautious with discretionary spending decisions for 2024.

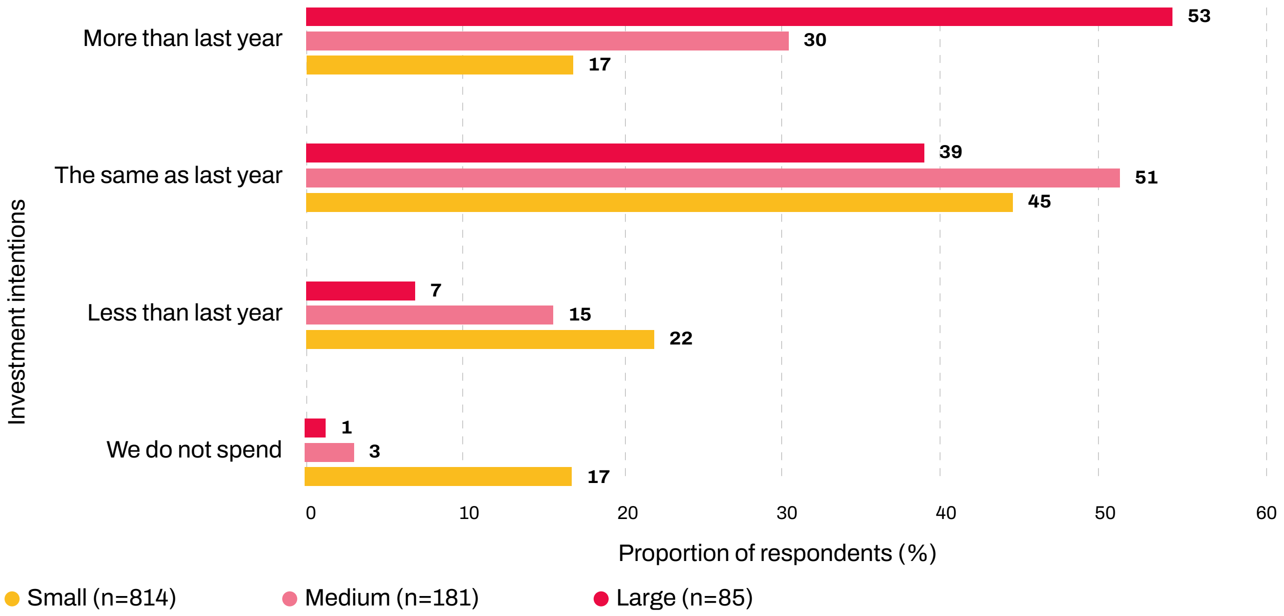
SME investment intentions

The majority of SMEs (83% of small businesses and 97% of medium businesses) intend to invest in cyber security in 2024. While 45% of small businesses and 51% of medium businesses plan to maintain the same level of expenditure as last year, 17% of small businesses and 30% of medium businesses plan to increase their spending on cyber security.

In light of the growing number and sophistication of cyber attacks, it is worth noting that some SMEs may not be sufficiently prioritising investment in cyber security management. For instance:

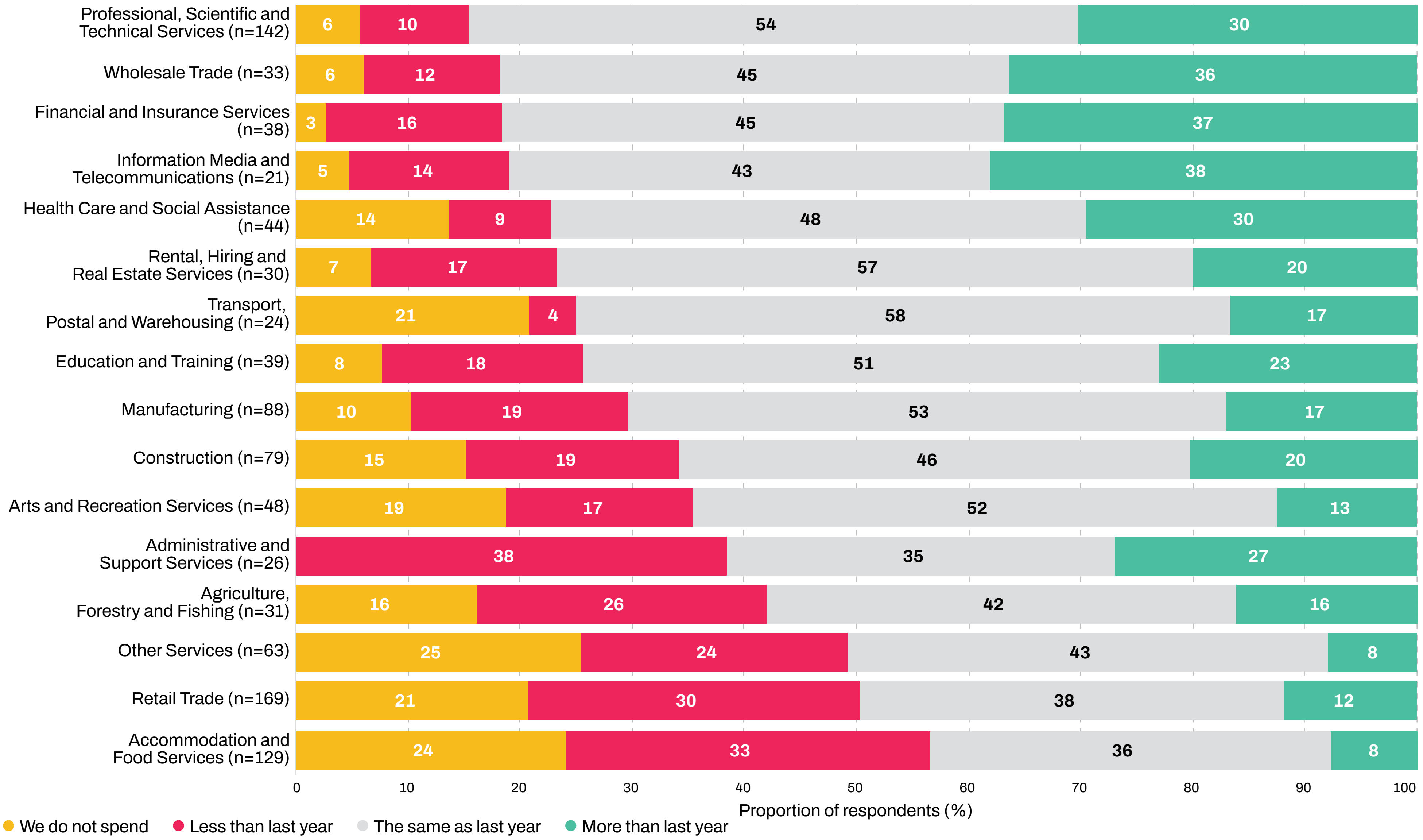
- 17% of small businesses do not intend to spend on cyber security; and
- 22% of small businesses and 15% of medium businesses intend to spend less than last year.

Figure 14: Intentions to spend on cyber security in 2024 compared to past year by company size



Source: Business Conditions Survey (March 2024), Business NSW

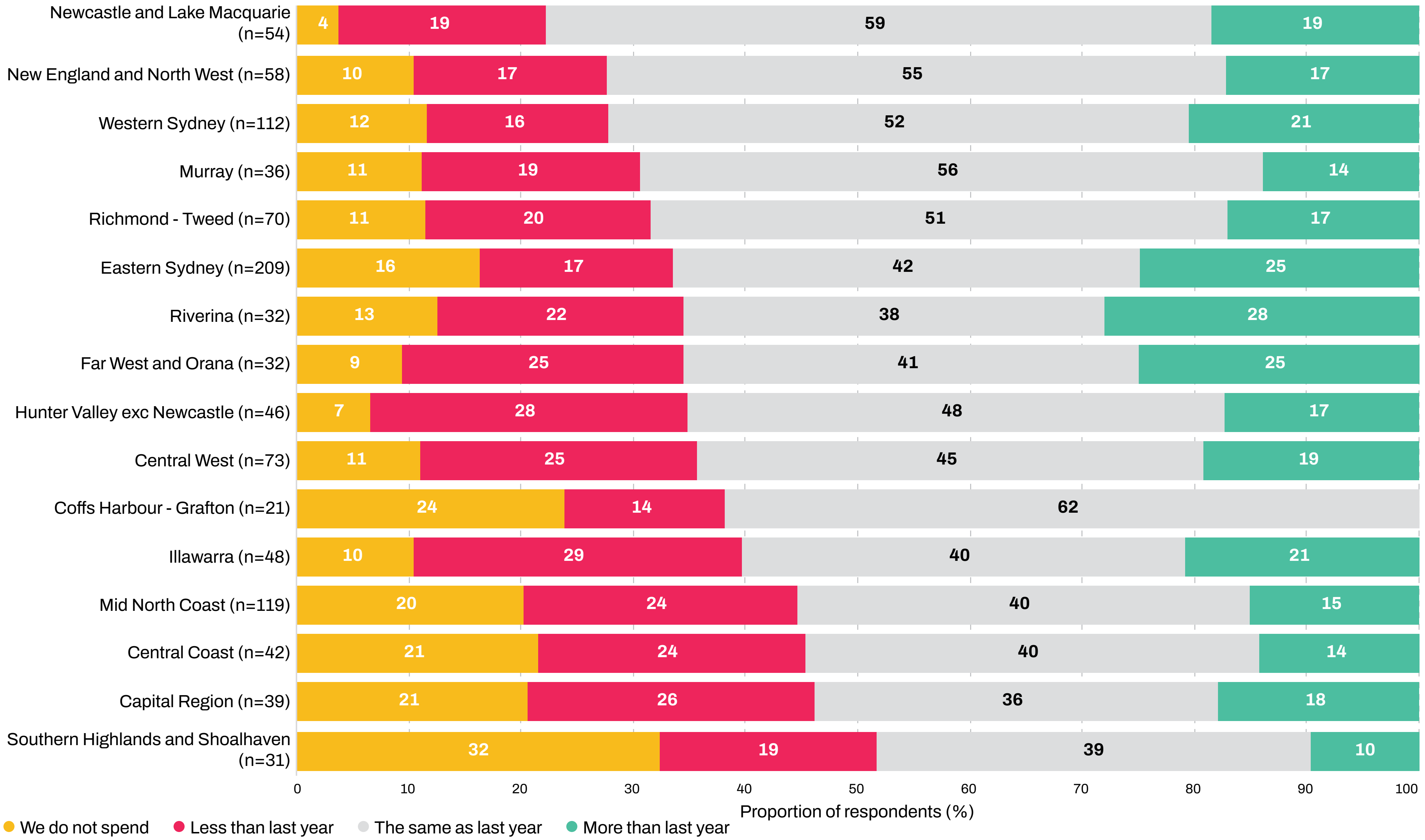
Figure 15: SMEs’ intentions to spend on cyber security in 2024 compared to past year by industry



Source: Business Conditions Survey (March 2024), Business NSW

Note: Industries with less than 10 respondents are not included in this graph.

Figure 16: SMEs' intention to spend on cyber security in 2024 compared to past year by region



Source: Business Conditions Survey (March 2024), Business NSW

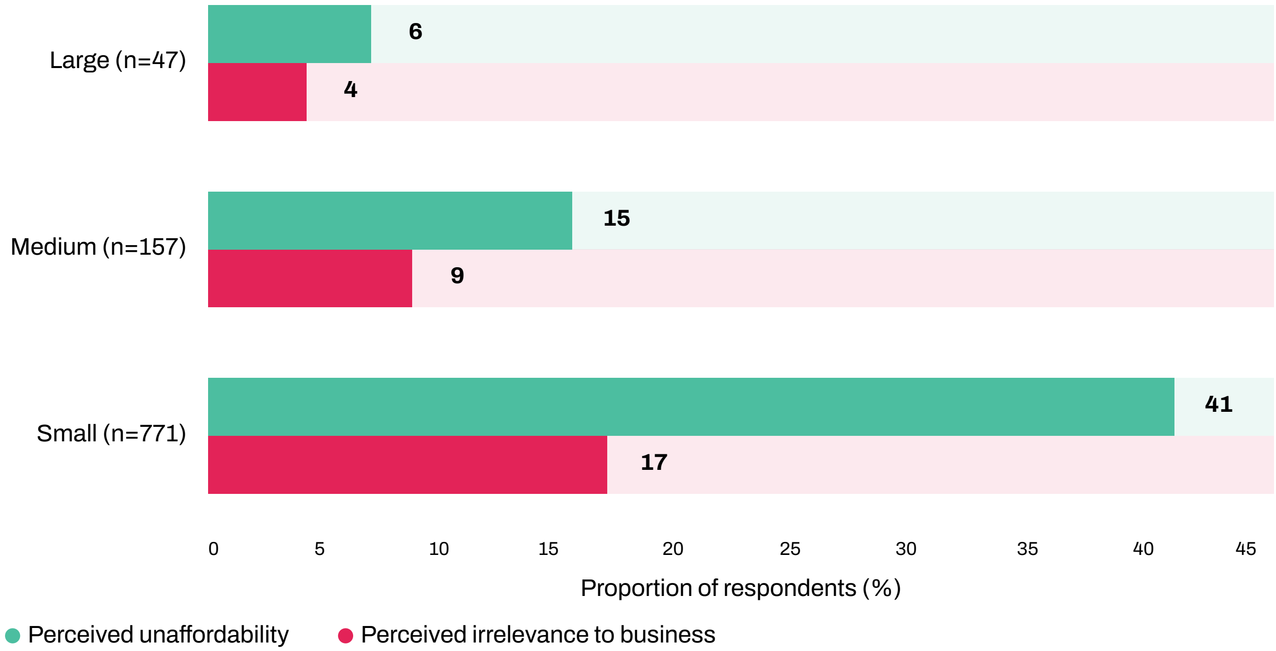
Barriers to strengthening cyber security of SMEs

While the majority of SMEs intend to invest in cyber security in 2024, there are two key barriers – perceived unaffordability and irrelevance to business – that may influence their actual investment.

Research by Business NSW has found that in the 12 months to May 2023:

- 41% of small businesses and 15% of medium businesses had taken no actions to enhance cyber security as they could not afford it; and
- 17% of small businesses and 9% of medium businesses had taken no actions to enhance cyber security as they considered it not relevant to their business.

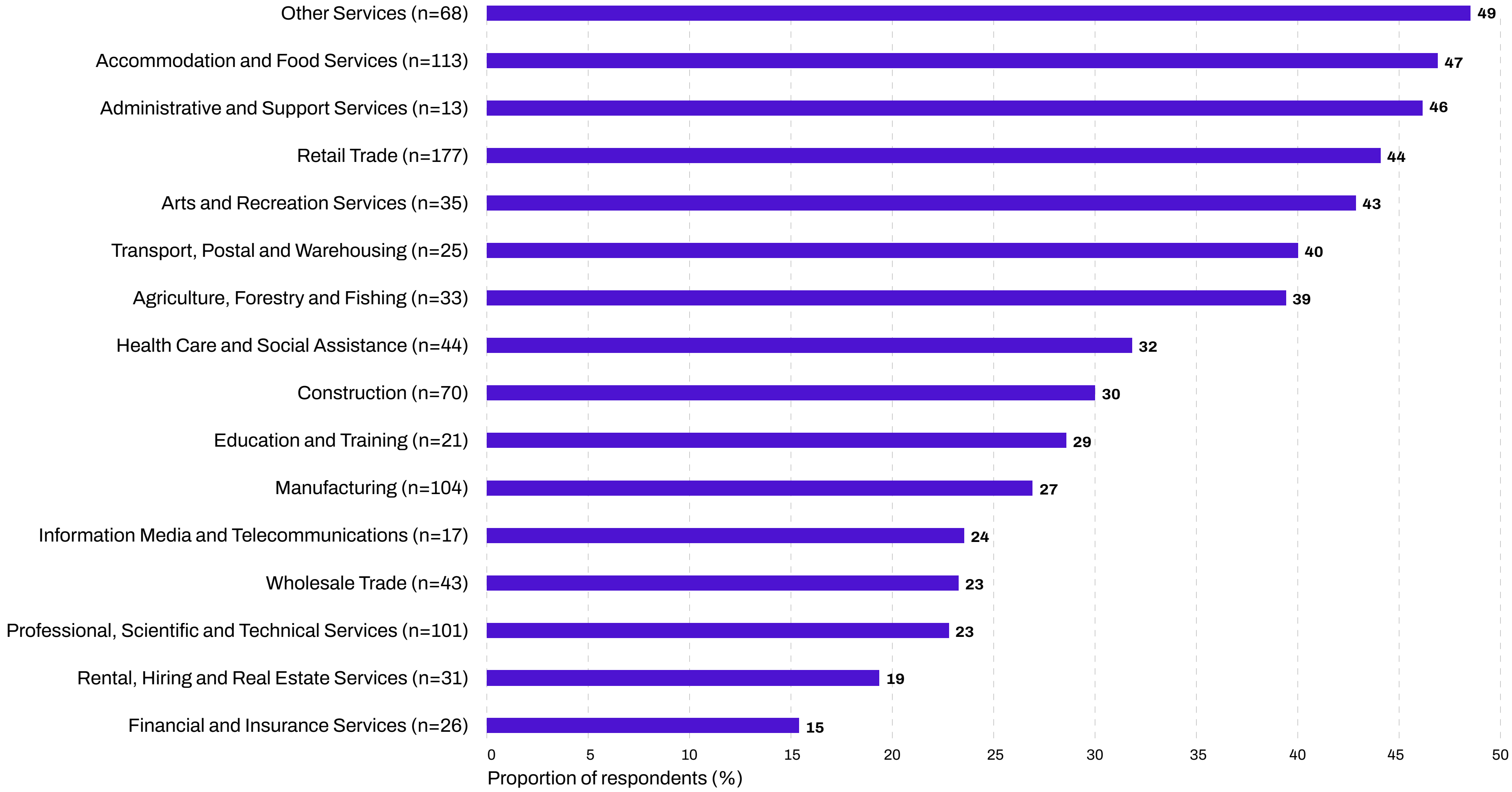
Figure 17: Barriers to investment in cyber security by company size



Source: Business Conditions Survey (June 2023), Business NSW

Note: The answers were not mutually exclusive. Some businesses cited both reasons for not investing in cyber security.

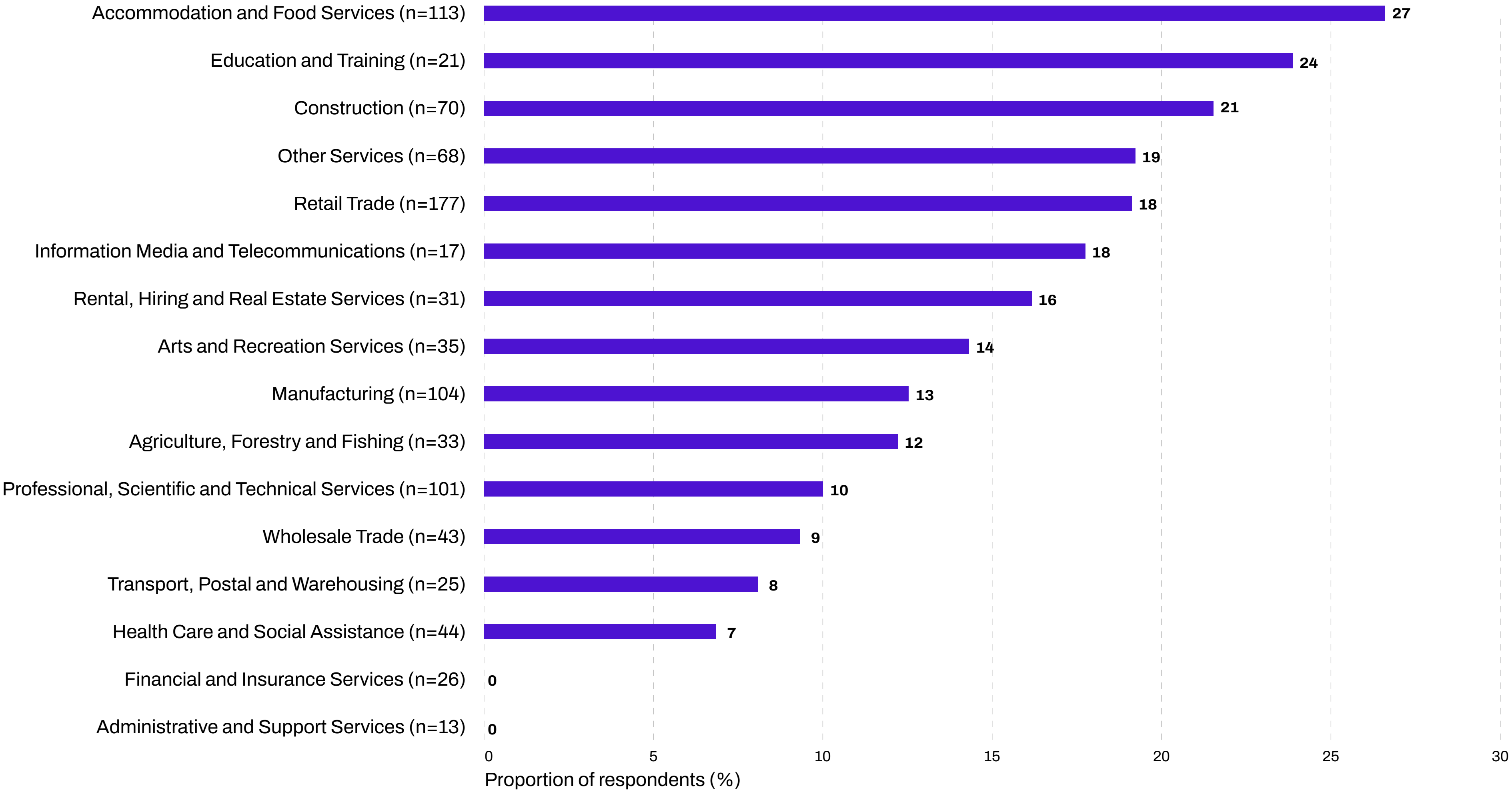
Figure 18: Proportion of SMEs that have not taken any action because they could not afford to invest in cyber security



Source: Business Conditions Survey (June 2023), Business NSW

Note: Industries with less than 10 respondents are not included in the graph.

Figure 19: Proportion of SMEs that have not taken any action because they perceived cyber security to be irrelevant to their business



Source: Business Conditions Survey (June 2023), Business NSW

Note: Industries with less than 10 respondents are not included in the graph.

Recommendations

To improve cyber security in the SME sector, which also protects the broader community, both Federal and NSW governments have a role to play. Reflecting on the SME needs identified in our research, Business NSW recommends the following:

- The Federal Government provides a 20% deduction bonus on all cyber security related expenditure to enable businesses to invest in cyber security.
- The NSW Government expands the Service NSW Business Bureau's role to include guidance on cyber security for businesses.
- The Federal and NSW governments continue to review current small business focused cyber initiatives to understand their take-up and efficacy.
- The Federal and NSW governments – together with relevant industry leaders and membership organisations – combine to support SMEs and ensure their cyber security.

To strengthen your cyber security, individual SMEs are recommended to implement the following core measures at a minimum:

Secure your accounts

- turning on multi-factor authentication
- using strong passwords or phrases
- using different passwords per system
- managing shared accounts
- Implementing access controls

Protect your devices and information

- updating your software and operating systems
- backing up your information
- using security software
- hardening your website
- wiping old equipment before disposal

Prepare your staff

- educating employees
- preparing an emergency plan and incident response plan
- staying informed

For more guidance, businesses can access the Australian Cyber Security Centre website.

CONTACT

Ben Pike
Executive Manager, Marketing & Media
Ben.Pike@businessnsw.com

Dr Sherman Chan
Chief Economist
Sherman.Chan@businessnsw.com

Not a member?
Add your voice to the conversation today:
businessnsw.com/members/join-business-nsw

© Business NSW 2024