NAB SME Business Insights

Cyber security: sources of advice, focus of Investment & use of free training tools.

6 in 10 SMEs rely on IT providers for trusted information or advice.
4 in 5 have invested more in cyber security in the past 12 months -
6 in 10 in software or hardware and 1 in 2 on external IT or
Cyber security experts. But, 4 in 10 were unaware of the availability
of free Government or industry cyber security training tools.

Key findings

Where do SMEs get trusted information or advice about cyber attacks & scams?

Most (6 in 10 or 58%) rely on IT providers or IT support. Around 1 in 3 industry associations (36%) and trusted bank channels such as bank apps or internet banking (34%), around 1 in 4 other business owners or colleagues (28%) and Government bodies such as Australian Cyber security Centre or Scamwatch (23%). Just over 1 in 5 turn to bank public websites (21%), 14% their banker, 10% Telcos, and 2% the police. Only 1 in 50 (2%) said they did not need any information or advice.

- By industry, a much higher number of SMEs in Health (83%) and Business Services (82%) lean on IT providers and IT support, particularly compared to the Construction sector (48%).
- Industry associations were more widely relied upon used in the Finance & Insurance (50%), Business Services (48%) and Hospitality (46%) sectors, and bank messaging in Wholesale (44%), Personal Services (43%) and Construction (41%).
- Reliance on Government was noticeably higher in Finance & Insurance (31%) and bankers in Business Services (19%) and Hospitality (18%). Finance & Insurance relied more on Telcos (19%).

What cyber security measures do SMEs currently have in place to protect themselves?

Around 8 in 10 use antivirus software (82%), keep systems and software updated (79%), back-up systems, data, files and devices (79%), use firewalls and secure Wi-Fi networks (77%). Around 2 in 3 use multi-factor authentication (67%), and 6 in 10 change passwords frequently (57%) and limit user access privileges (55%). 1 in 3 run regular security tests (37%), risk assessments (33%), encrypt key information (32%) or security awareness training (31%). Only 1% do none of these things.

- By industry, noticeably more SMEs in Business Services, Finance & Insurance and Health Services are using antivirus software and keeping systems and software updated, and in Transport & Storage (93%), Health Services (90%), Finance & Insurance (89%) and in Business Services (85%) backing up systems, data, files and devices.
- Changing passwords was much more common in Finance & Insurance and Health, limiting user access privileges in Business Services (77%), and running regular security testing (69%) and carrying out risk assessments (72%) in Finance & Insurance. Finance & Insurance (56%), Health (53%) and Business Services (53%) led the way for encrypting key information, and Finance & Insurance (69%) and Business Services (61%) security awareness training.
- A lower number in Wholesale (26%), Retail (28%), Construction (29%) and Manufacturing (31%) ran regular security testing, in Retail (20%) and Construction (21%) risk assessments, in Manufacturing encrypt key information (15%) and Construction (13%) and Hospitality (14%) security awareness training.

What areas of cyber security have SMEs invested in the last 12 months?

Around 6 in 10 SMEs invested in software or hardware (61%), and 1 in 2 external IT or cyber security experts (50%). Around 3 in 10 invested in staff training (30%) or cyber insurance (28%). Just over 1 in 10 set aside a dedicated budget for cyber security (12%) and 1 in 20 hired or increased the number of staff working in IT or cyber security in house (6%). Almost 1 in 5 had not invested more over the past 12 months (17%).

- Almost twice more SMEs in Finance & Insurance (89%) have invested in software or hardware compared to Retail (48%). Finance & Insurance also were much more active in staff training (83%), particularly compared to Manufacturers (11%).
- Investment in external IT or cyber security experts has occurred most in Finance (69%) and Health (67%) and was lowest in Retail (41%) and Hospitality (43%).
- Almost 1 in 2 SMEs in Finance and Business Services (47%) have taken out cyber insurance, compared to fewer than 1 in 5 in Manufacturing (16%) and Construction (17%). Around 1 in 4 in Business Services (26%) and Finance (22%) had a dedicated budget for cyber security, compared to only 1 in 20 in Wholesale (5%).
- Investment in IT & cyber security staff in house was highest in Business Services (13%) and lowest in Retail (3%). Nearly 3 in 10 (29%) in Manufacturing did not invest more in cyber security in the last 12 months, comparted to 0% among SMEs in Finance & insurance.

What are the barriers to using free Government or industry cyber security training tools?

The biggest barrier according to 4 in 10 SMEs overall was lack of awareness they existed (40%). 3 in 10 said they did not know where to find them (31%) and 1 in 4 were time poor (24%). Just over 1 in 10 SMEs had already invested in other cyber training tools (13%), while slightly fewer did not trust them to meet their needs (9%). Only 8% of SMEs said they faced no barriers as they were already using these free tools, while 4% cited "other" barriers for not using them. Around 1 in 10 said using these free tools was not a priority for them.

- Lack of awareness and not knowing where to find these programs were top of mind for most SMEs in most industries. That said, the number unaware ranged from 29% in the Hospitality sector to 45% in Construction, while not knowing where to find them ranged from 23% in Business Services to 47% in Transport & Storage. The number time poor ranged from just 4% in Transport & Storage firms to 19% in Business Services.
- Those that had already invested in other training tools also ranged widely from 27% in Business Services to 4% in Hospitality. Around 1 in 4 (25%) SMEs in Finance & Insurance highlighted lack of trust, compared to 1 in 25 (4%) in Hospitality. Almost 1 in 5 (17%) in Transport & Storage, said it was not a priority compared to 0% in Finance & Insurance.
- Over 1 in 10 in Finance and Business Services (11%) said they already use these free tools compared to just 3% in Manufacturing and Health Services. Nearly 1 in 5 (17%) SMEs in the Construction sector were not worried about a cyber attack on their business, significantly higher than in all other industries.

Cyber security: sources of advice, focus of investment & use of free training tools

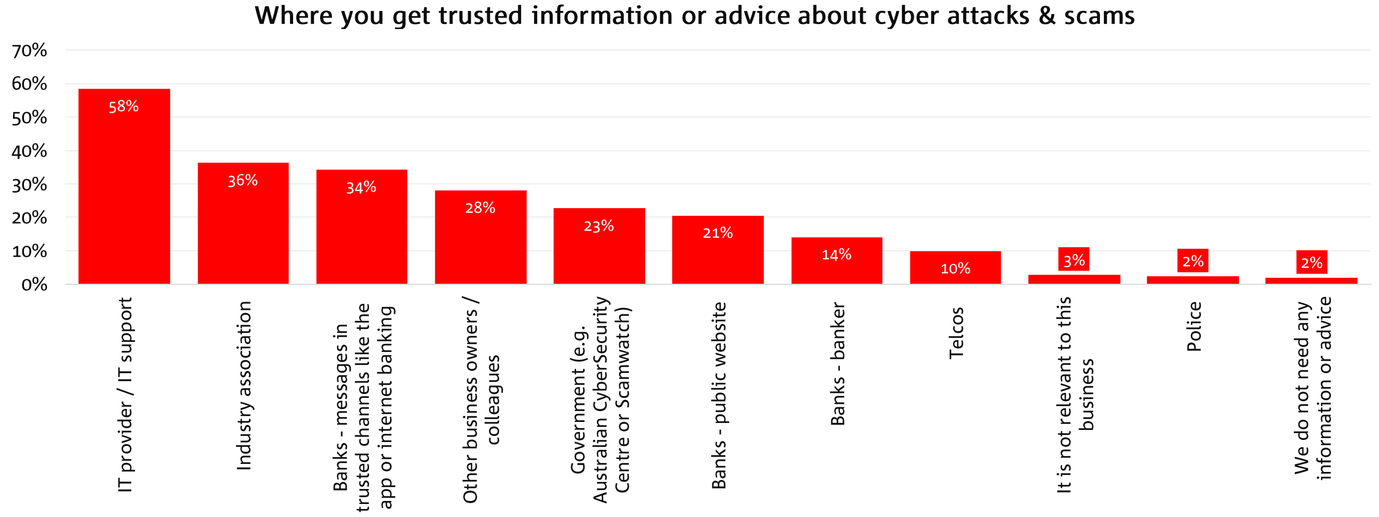
Cyber attacks and scams are an increasingly significant issue in Australia. According to the ACCC's Targeting Scams Report 2023, scam reports increased by 19% to over 601,000 in 2023 (507,000 in 2022), and based on combined data from Scamwatch, ReportCyber, the Australian Financial Crimes Exchange, IDCARE and ASIC, losses totalled $2.74 billion. SMEs have not been immune, with many falling prey - often with significant financial consequences. In 2023, Australian businesses submitted 4,933 scam reports to Scamwatch alone (up 28% from 2022), while the ACCC reported a 23% increase in cybercrime incidents in the last financial year to nearly 94,000. The average cost of cybercrime per report also rose by 14%, with small businesses facing an average cost of $46,000, medium businesses $97,200 and large businesses $71,600. With scams posing an ever increasing threat to SMEs, awareness and proactive measures can help protect their business and finances.

In this report, NAB surveyed around 700 Australian SME businesses and asked them where they get their trusted information or advice about cyber security and scams, what cyber security measures they currently have in place, in which areas of cyber security has their business invested in the last 12 months and what are the barriers (if any) to using free Government or industry cyber security training tools to protect their business.

Where SMEs get trusted information or advice about cyber attacks & scams

Small businesses are typically at higher risk of being scammed than larger companies. While large businesses generally have more resources to invest in security measures, small businesses often do not have the same level of protection. This can leave them vulnerable to cyber attacks and scams that can not only have financial consequences, but can also damage business systems, compromise sensitive data and information and lead to reputational damage. For SMEs, this means it is imperative to understand the potential threats and how they could impact their business, and also take steps to protect themselves. But where do Australian SMEs get their trusted information or advice about cyber attacks and scams?

Most surveyed SME's (around 6 in 10 or 58%) relied on IT providers or IT support. Around 1 in 3 got the information or advice they needed from industry associations (36%) and from trusted bank channels such as the app or internet banking (34%), and around 1 in 4 from other business owners or colleagues (28%) and Government such as Australian Cyber security Centre or Scamwatch (23%). Just over 1 in 5 relied on banks' public websites (21%), 14% from their banker, 10% from Telcos, and 2% from the police. Only 1 in 50 (2%) SMEs said they did not need any information or advice.



We also noted some major differences across key states. Around 7 in 10 SMEs in SA relied on IT providers or support, compared to around 6 in 10 in all other states. More firms in VIC and WA (40%) relied on industry associations, and somewhat more in NSW (37%) and QLD (36%) on bank messages in trusted channels. Noticeably more SMEs in NSW also leaned on other business owners or colleagues (32%). More SMEs in NSW (25%) and WA (23%) used banks' public websites, and in NSW and VIC Telcos (12%). Far more SMEs in SA got their information from Government (33%), and in WA the police (11%).

Also apparent was the much lower number of SMEs in QLD that relied on other business owners or colleagues (20%), in VIC (18%) and QLD (19%) on Government, in SA (14%) and QLD (15%) banks' public websites, in SA on bankers (7%), and in WA (6%) and QLD (7%) Telcos - see table below.

Where you get trusted information or advice about cyber attacks & scams: States

	All SMEs	NSW	QLD	SA	VIC	WA
IT provider / IT support	**58%**	57%	60%	70%	59%	57%
Industry association	**36%**	33%	35%	37%	40%	40%
Banks (messages in trusted channels like app & internet banking)	**34%**	37%	36%	30%	31%	31%
Other business owners or colleagues	**28%**	32%	20%	26%	29%	26%
Government (e.g. Australian Cyber security Centre & Scamwatch)	**23%**	27%	19%	33%	18%	25%
Banks (public website)	**21%**	25%	15%	14%	18%	23%
Banks (banker)	**14%**	16%	10%	7%	15%	14%
Telcos	**10%**	12%	7%	9%	12%	6%
Not relevant to this business	**3%**	2%	4%	2%	1%	5%
Police	**2%**	2%	1%	5%	0%	11%
Do not need any information or advice	**2%**	1%	2%	2%	3%	2%

By industry, we noted a much higher number of SMEs in the Health (83%) and Business Services (82%) sectors who leaned on IT providers and IT support, particularly when compared the Construction sector (48%). Industry associations were much more commonly used by SMEs in Finance & Insurance (50%), Business Services (48%) and Hospitality (46%), and bank messaging in trusted channels by SMEs in the Wholesale (44%), Personal Services (43%) and Construction (41%) sectors. Reliance on Government was noticeably higher in Finance & Insurance (31%) and bankers in Business Services (19%) and Hospitality (18%). Noticeably more firms in the Finance & Insurance sector also relied of Telcos for trusted information and advice (19%).

Where you get trusted information or advice about cyber attacks & scams: Industry

	All SMEs	MFG	CON	RET	WHL	TS	FI	BS	PS	ACCOM	HEA
IT provider / IT support	**58%**	52%	48%	52%	55%	53%	69%	82%	71%	50%	83%
Industry association	**36%**	34%	36%	32%	27%	40%	50%	48%	33%	46%	33%
Banks (messages in trusted channels like app & internet banking)	**34%**	39%	41%	29%	44%	20%	25%	34%	43%	18%	20%
Other business owners or colleagues	**28%**	26%	31%	23%	26%	23%	44%	32%	33%	7%	33%
Government (e.g. Australian Cyber security Centre & Scamwatch)	**23%**	16%	22%	15%	16%	27%	39%	32%	33%	21%	30%
Banks (public website)	**21%**	18%	21%	16%	23%	17%	19%	31%	26%	18%	13%
Banks (banker)	**14%**	15%	19%	11%	9%	17%	8%	19%	14%	18%	7%
Telcos	**10%**	5%	15%	3%	13%	7%	19%	10%	12%	7%	10%
Not relevant to this business	**3%**	2%	5%	5%	0%	0%	0%	0%	0%	7%	3%
Police	**2%**	2%	3%	3%	1%	0%	0%	5%	2%	0%	3%
Do not need any information or advice	**2%**	6%	2%	1%	1%	3%	0%	2%	2%	0%	0%

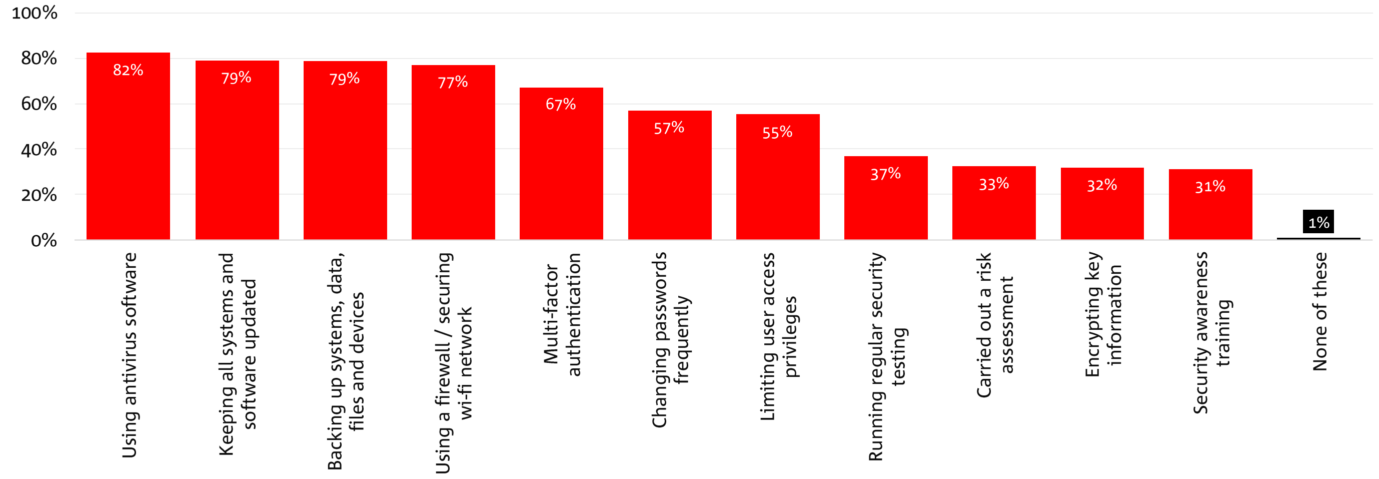
Cyber security measures currently in place

In simple terms, cyber security involves the protection of computer systems connected to the Internet. Entities such as government, business and organisations as well as millions of individuals in Australia rely on these every day.

For SMEs, implementing effective cyber security measures is particularly important as cyber attacks on all businesses - and particularly SME businesses - are becoming more frequent, targeted and complex. This means SMEs need to remain vigilant and continuously monitor their networks against potential attacks.

In this section we explore what cyber security measures SMEs currently have in place to protect themselves. Encouragingly, around 8 in 10 overall said they are using antivirus software (82%), keeping all systems and software updated (79%), backing up systems, data, files and devices (79%) and using firewalls and securing Wi-Fi networks (77%). Around 2 in 3 firms used multi-factor authentication (67%), and about 6 in 10 changed their passwords frequently (57%) and limited user access privileges (55%). Around 1 in 3 run regular security testing (37%), conducted risk assessment (33%), encrypted key information (32%) or conducted security awareness training (31%). Only 1% of SMEs did none of these things.

Cybersecurity measures currently in place



Cyber security measures currently in place: States

	All SMEs	NSW	QLD	SA	VIC	WA
Using antivirus software	**82%**	79%	82%	88%	85%	83%
Keeping all systems and software updated	**79%**	80%	81%	77%	78%	80%
Backing up systems, data, files and devices	**79%**	79%	79%	79%	78%	83%
Using a firewall / securing wi-fi network	**77%**	76%	75%	79%	77%	82%
Multi-factor authentication	**67%**	70%	66%	81%	59%	74%
Changing passwords frequently	**57%**	59%	52%	58%	57%	60%
Limiting user access privileges	**55%**	53%	63%	47%	56%	58%
Running regular security testing	**37%**	40%	41%	40%	30%	35%
Carried out a risk assessment	**33%**	40%	30%	23%	25%	37%
Encrypting key information	**32%**	33%	32%	30%	30%	38%
Security awareness training	**31%**	36%	32%	14%	26%	35%
None of these	**1%**	1%	2%	0%	0%	3%

Most SMEs in all states use antivirus software, keep all systems and software up to date, back-up systems, data, files and devices and use firewalls and secure Wi-Fi networks as defences against cyberattacks. The survey also found significantly more SMEs in SA relied on multifactor authentication (81%) than other states, particularly VIC (59%). Limited user access privileges were much more common in QLD (63%), but far less so in SA (47%). Around 4 in 10 (40%) SMEs in NSW carried out risk assessments, compared to only 1 in 4 in SA (23%) and VIC (25%). Fewer firms in VIC also ran regular security testing (30%) than in other states, whereas a much higher number in WA encrypted key information (38%).

Cyber security measures currently in place: Industry

	All SMEs	MFG	CON	RET	WHL	TS	FI	BS	PS	ACCOM	HEA
Using antivirus software	**82%**	79%	81%	75%	82%	83%	92%	94%	81%	79%	93%
Keep systems & software updated	**79%**	76%	70%	76%	83%	67%	92%	92%	83%	79%	90%
Backup systems, data, files & devices	**79%**	76%	75%	77%	77%	93%	89%	85%	69%	75%	90%
Use firewall / securing wi-fi network	**77%**	73%	71%	71%	81%	83%	89%	87%	71%	86%	87%
Multi-factor authentication	**67%**	65%	62%	58%	69%	67%	81%	79%	76%	61%	80%
Changing passwords frequently	**57%**	48%	55%	46%	51%	43%	83%	71%	67%	57%	83%
Limiting user access privileges	**55%**	50%	50%	42%	48%	73%	69%	77%	62%	50%	70%
Running regular security testing	**37%**	31%	29%	28%	26%	43%	69%	50%	43%	43%	57%
Carried out a risk assessment	**33%**	29%	21%	20%	30%	33%	72%	53%	33%	29%	53%
Encrypting key information	**32%**	15%	25%	23%	27%	40%	56%	52%	36%	36%	53%
Security awareness training	**31%**	18%	13%	26%	23%	37%	69%	61%	48%	14%	50%
None of these	**1%**	2%	2%	2%	0%	0%	0%	0%	0%	0%	0%

By industry, noticeably more SMEs operating in the Business Services, Finance & Insurance and Health Services sectors were using antivirus software and keeping systems and software updated, and in Transport & Storage (93%), Health Services (90%), Finance & Insurance (89%) and Business Services (85%) backing up systems, data, files and devices.

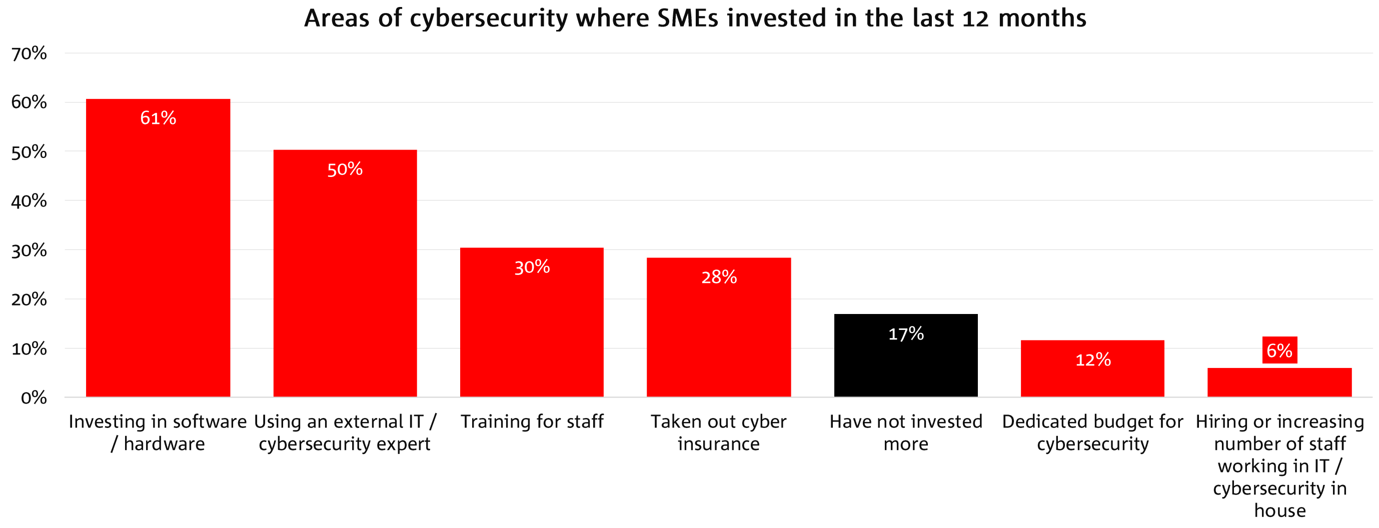
Changing passwords frequently was much more common in the Finance & Insurance and Health Services (83%) sectors, limiting user access privileges in Business Services (77%), and running regular security testing (69%) and carrying out risk assessments (72%) in Finance & Insurance. SMEs in Finance & Insurance (56%), Health (53%) and Business Services (53%) also led the way for encrypting key information, and in Finance & Insurance (69%) and Business Services (61%) security awareness training.

Also evident was the comparatively lower number of SMEs operating in the Wholesale (26%), Retail (28%), Construction (29%) and Manufacturing (31%) sectors running regular security testing, in Retail (20%) and Construction (21%) carrying out risks assessments, in Manufacturing encrypting key information (15%) and in Construction (13%) and Hospitality (14%) doing security awareness training.

Areas of cyber security where SMEs invested in the last 12 months

Research suggests many small businesses think they are not a target of cybercriminal activity, with many also overlooking the critical importance of safeguarding their digital assets and investing in cyber security. This oversight can lead to vulnerabilities, putting their business operations reputation at risk. As the threat of cybercrime continues to evolve and grow, it is increasingly important for SMEs to invest in cyber security. In this section, NAB explores the areas of cyber security (if any) Australian SMEs have invested in the last 12 months.

Around 6 in 10 SMEs overall said they invested in software or hardware (61%) in the last 12 months, and 1 in 2 in using an external IT or cyber security expert (50%). Around 3 in 10 invested in staff training (30%) or took out cyber insurance (28%). Just over 1 in 10 invested in a dedicated budget for cyber security (12%) and 1 in 20 hired or increased the number of staff working in IT or cyber security in house (6%). Almost 1 in 5 however said they had not invested more over the past 12 months (17%).



Areas of cyber security where SMEs invested in the last 12 months: States

	All SMEs	NSW	QLD	SA	VIC	WA
Investing in software / hardware	**61%**	60%	58%	56%	67%	52%
Using an external IT / cyber security expert	**50%**	53%	58%	49%	44%	48%
Training for staff	**30%**	33%	27%	26%	28%	37%
Taken out cyber insurance	**28%**	31%	32%	23%	24%	23%
Have not invested more	***17%***	***15%***	***19%***	***21%***	***13%***	***28%***
Dedicated budget for cyber security	**12%**	13%	7%	9%	12%	14%
Hiring or increasing staff working in IT / cyber security in house	**6%**	5%	9%	0%	5%	9%

Cyber security investment priorities over the last 12 months differed across the main states. Around 2 in 3 SMEs in VIC invested in software or hardware (67%), but this fell to just 1 in 2 in WA (52%). Investment in using an external IT or cyber security expert was most widespread in QLD (58%) and least so in VIC (44%). Investment in staff training was noticeably higher for SMEs in WA (37%) and NSW (33%) and taking out cyber insurance in QLD (32%) and NSW (31%).

Around twice as many SMEs in WA (14%), NSW (13%) and VIC (12%) invested in a dedicated cyber security budget than in QLD (7%). but around twice as many in QLD and WA (9%) invested in hiring or increasing staff working on IT or cyber security in house than in NSW and VIC (5%), with no SMEs in SA undertaking this investment in the last 12 months (0%).

The number of SMEs who said they did not invest more in the last 12 months was highest in WA (28%) and lowest in VIC (13%).

Areas of cyber security where SMEs have invested in the last 12 months: Industry

	All SMEs	MFG	CON	RET	WHL	TS	FI	BS	PS	ACCOM	HEA
Investing in software / hardware	**61%**	50%	64%	48%	53%	60%	89%	77%	55%	64%	73%
Using an external IT / cyber security expert	**50%**	47%	50%	41%	39%	63%	69%	58%	60%	43%	67%
Training for staff	**30%**	11%	22%	24%	22%	27%	83%	39%	50%	32%	43%
Taken out cyber insurance	**28%**	16%	17%	20%	23%	40%	47%	47%	43%	36%	43%
Have not invested more	**17%**	29%	19%	22%	16%	7%	0%	10%	17%	11%	17%
Dedicated budget for cyber security	**12%**	8%	8%	7%	5%	10%	22%	26%	17%	14%	17%
Hiring / increasing staff working in IT / cyber security in house	**6%**	6%	5%	3%	5%	10%	6%	13%	5%	4%	7%

By industry, almost twice as many SMEs in the Finance & Insurance sector (89%) invested in software or hardware than in Retail (48%). Finance & Insurance firms were also by far most active in the last 12 months investing in staff training (83%), particularly when compared to Manufacturers (11%). Investment in external IT or cyber security experts was most widespread in Finance & Insurance (69%) and Health Services (67%), with this investment lowest in Retail (41%) and Hospitality (43%).

Almost 1 in 2 SMEs in the Finance & Insurance and Business Services sectors (47%) took out cyber insurance, compared to less than 1 in 5 in Manufacturing (16%) and Construction (17%). Around 1 in 4 in Business Services (26%) and Finance & insurance (22%) invested in a dedicated budget for cyber security, compared to only 1 in 20 in Wholesale (5%). Investment in staff working on IT and cyber security in house was highest in the Business Services sector (13%) and lowest in Retail (3%). Nearly 3 in 10 (29%) in the Manufacturing sector did not invest more in cyber security in the last 12 months. No SMEs in Finance & insurance did not invest more (0%).

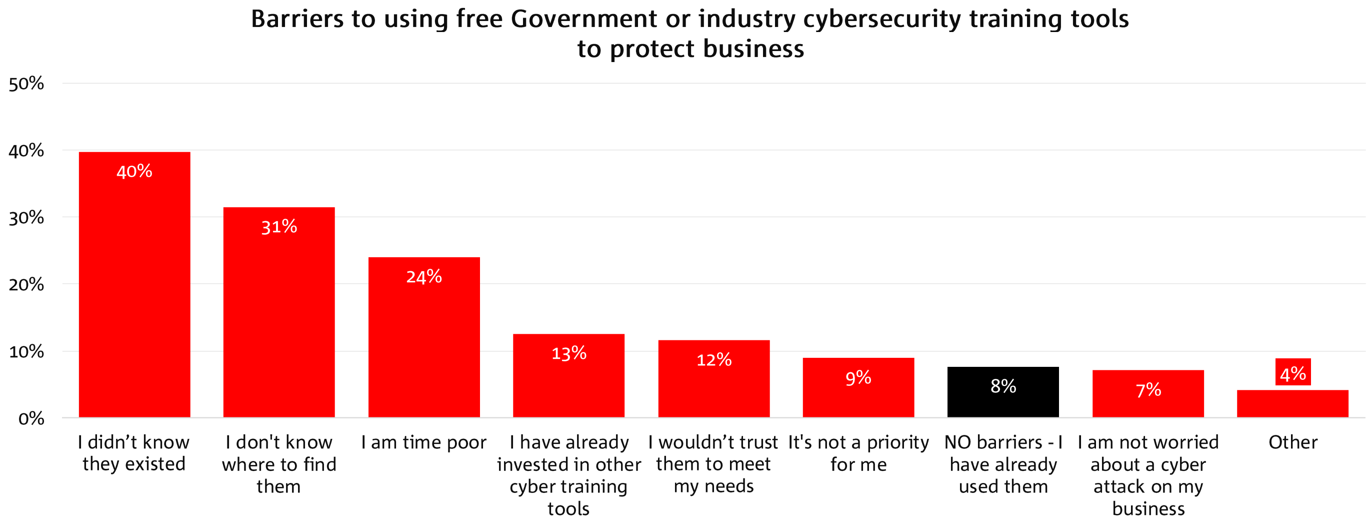
Barriers to using free Government or industry cyber security training tools

There are a number of free Government or industry cyber security training tools available to Australian SMEs. Australian SMEs are also set to get more personalised support to help prevent and recover from cyber attacks under the Government's Small Business Cyber Resilience Service which will help SMEs by providing free, tailored, person-to-person support during and after a cyber attack to develop and implement a specific plan to improve their cyber security. This service builds on the Cyber Wardens Program (a short course funded by the Government to protect small businesses from daily online threats) and is a key part of the 2023–2030 Australian Cyber Security Strategy.

In this section, we establish what barriers (if any) do Australian SMEs identify to using free Government or industry cyber security training tools to protect their business.

The biggest barrier to using these free tools according to 4 in 10 SMEs overall was that they were not aware they existed (40%). In addition, around 3 in 10 said they did not know where to find them (31%). Around 1 in 4 SMEs were hampered from using them because they were time poor (24%) - see chart below.

Just over 1 in 10 SMEs cited the fact they had already invested in other cyber training tools (13%), while slightly less because they would not trust free cyber security training tools to meet their needs (9%). Only 8% of SMEs said they faced no barriers as they were already using these free tools, while 4% cited "other" barriers for not using them. But around 1 in 10 SMEs said using free Government or industry cyber security training tools was not a priority for them.



Responses did not vary materially across the main states, with most SMEs in all states indicating the main barriers to using these free training tools were that they did not know they existed, did not know where to find them or were time poor (particularly in SA). Other areas where SMEs looked different included the somewhat higher number in WA who said it was not a priority for them (14%), in QLD where significantly more indicated they were not worried about a cyber attack on their business (12%) and in VIC and WA who said it was not a priority (11%) - see table below.

Barriers to using free industry or Government cyber security training tools to protect your business: State

	All SMEs	NSW	QLD	SA	VIC	WA
I didn't know they existed	**40%**	40%	42%	40%	39%	38%
I don't know where to find them	**31%**	32%	28%	30%	34%	31%
I am time poor	**24%**	24%	20%	33%	22%	29%
I have already invested in other cyber training tools	**13%**	13%	15%	9%	10%	14%
I wouldn't trust them to meet my needs	**12%**	10%	14%	19%	9%	14%
It's not a priority for me	**9%**	10%	7%	7%	6%	14%
There are no barriers - I have already used them	**8%**	7%	5%	2%	11%	11%
I am not worried about a cyber attack on my business	**7%**	5%	12%	2%	7%	9%
Other	**4%**	4%	5%	5%	3%	5%

Barriers to using free industry or Government cyber security training tools to protect your business: Industry

	All SMEs	MFG	CON	RET	WHL	TS	FI	BS	PS	ACCOM	HEA
I didn't know they existed	**40%**	40%	45%	41%	39%	37%	36%	35%	38%	29%	43%
I don't know where to find them	**31%**	32%	30%	30%	35%	47%	28%	23%	33%	39%	30%
I am time poor	**24%**	23%	26%	23%	22%	40%	22%	19%	24%	25%	20%
I have already invested in other cyber training tools	**13%**	11%	11%	10%	9%	13%	19%	27%	10%	4%	13%
I wouldn't trust them to meet my needs	**12%**	8%	12%	10%	9%	10%	25%	10%	17%	4%	20%
It's not a priority for me	**9%**	15%	11%	7%	5%	17%	0%	8%	10%	14%	7%
There are no barriers - I have already used them	**8%**	3%	8%	6%	8%	7%	11%	11%	7%	14%	3%
I am not worried about a cyber attack on my business	**7%**	11%	17%	10%	0%	7%	0%	0%	0%	4%	3%
Other	**4%**	8%	2%	2%	5%	10%	8%	5%	2%	4%	3%

Industry responses were more varied, though unawareness and not knowing where to find these programs were top of mind for most SMEs in most industries. That said, the number unaware of the existence of free training tools ranged from 29% in the Hospitality sector to 45% in Construction, and not knowing where to find these programs from 23% in Business Services to 47% in Transport & Storage. The number of SMEs that said being time poor was a barrier also ranged widely from just 4% in Transport & Storage firms to 19% in Business Services. Those that had already invested in other cyber training tools also ranged widely from 27% in Business Services to just 4% in Hospitality.

Around 1 in 4 (25%) SMEs in the Finance & Insurance sector highlighted lack of trust in the ability of these free programs to meet their needs as a barrier, compared to 1 in 25 (4%) in the Hospitality sector. For almost 1 in 5 (17%) in Transport & Storage, it was not a priority whereas no firms in the Finance & insurance sector said it was not a priority (0%).

Over 1 in 10 SMEs in the Finance & insurance and Business Services sectors (11%) said they already use these free cyber security training tools compared to just 3% in Manufacturing and Health Services. Nearly 1 in 5 (17%) SMEs in the Construction sector were not worried about a cyber attack on their business, significantly higher than in all other industries - see table above.

Contact the authors

Dean Pearson
Head of Behavioural & Industry Economics
Dean.Pearson@nab.com.au
+61 (0) 457 517 342

Robert De Iure
Director Behavioural & Industry Economics
Robert.De.Iure@nab.com.au
+61 (0) 477 723 769

Important Notice

This document has been prepared by National Australia Bank Limited ABN 12 004 044 937 AFSL 230686 ("NAB"). Any advice contained in this document has been prepared without taking into account your objectives, financial situation or needs. Before acting on any advice in this document, NAB recommends that you consider whether the advice is appropriate for your circumstances.

NAB recommends that you obtain and consider the relevant Product Disclosure Statement or other disclosure document, before making any decision about a product including whether to acquire or to continue to hold it.

Please click **here** to view our disclaimer and terms of use.