SME Cyber Security Behaviour Tracker 2026

Published September 2026

TRA x NCSC

National Cyber Security Centre

TRA

Background

The National Cyber Security Centre (NCSC) plays a key role in providing information and education on cyber security to small to medium enterprises (SMEs) in New Zealand.

Using the ‘Own Your Online’ platform, the NCSC aims to improve the cyber resilience of SMEs in New Zealand.

Objectives

Overall objective

Improve cyber understanding and behaviours in the SME market.

Insight objectives

- Understand knowledge and capability when it comes to cyber security.
- Determine current threats, issues and exposure.
- Measure cyber security attitudes (including barriers & motivations to behaviours) and the behaviours themselves.

The approach

Survey

A 15-minute online survey sent out to the SME market (0-49 FTE)* in 2026.

This research has run since 2022.
Comparisons to the previous year are included where applicable.

Content

The survey covered:

- SME demography
- Cyber security motivations and attitudes
- Knowledge
- Cyber security behaviours
- Current threats / issues

Key sample

A total sample of n=373 SME IT / operational decision makers was achieved.

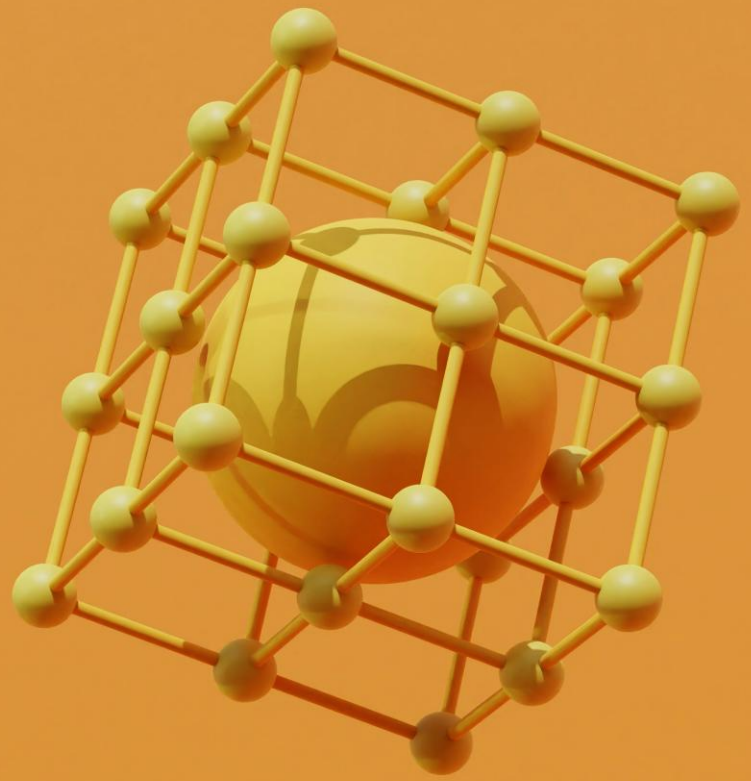
Fieldwork ran from the 21st May – 5th June 2026.

Weighting

The data was post-weighted to ensure it is representative of the New Zealand SME market based on size (FTE) and industry.

The margin of error at the 95% confidence interval is +/- 5.1%.

*Full time equivalent (FTE) is a measure of the number of employees that make up the organisation.

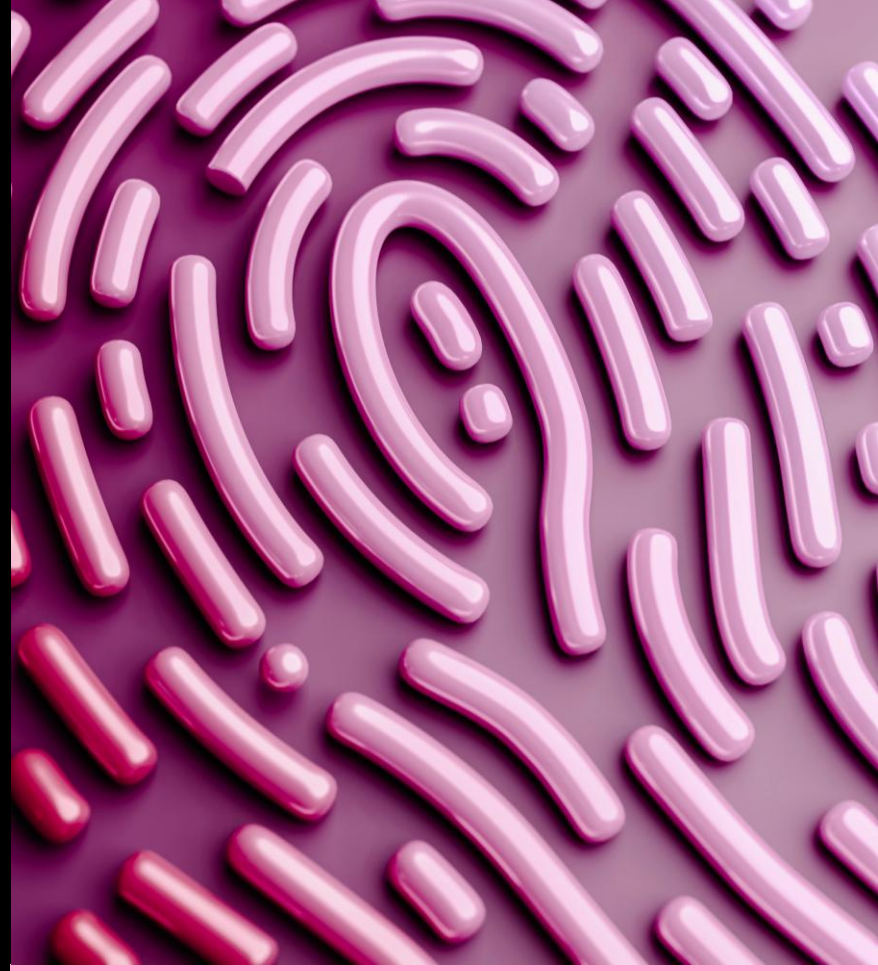


Story in a nutshell

Cyber security remains a critical concern for SMEs, with overall worry and vulnerability increasing as the threat landscape evolves. Emerging AI-related risks add new complexity.

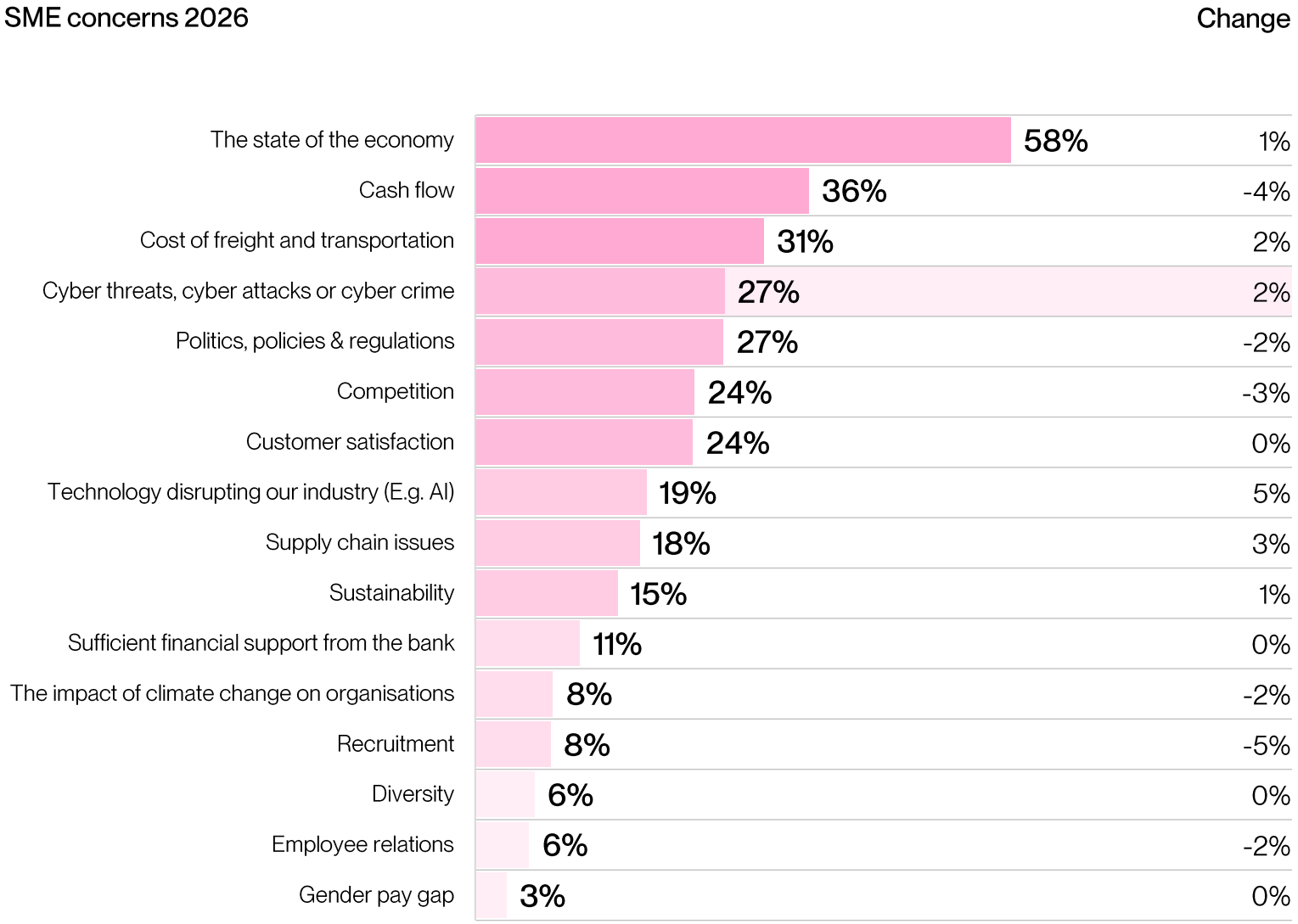
Despite increasing confidence, nearly half of SMEs still feel unprepared. Cyber attacks are becoming more severe, causing financial, data, and reputational impacts, especially for larger SMEs. Motivation remains a barrier; many are still not investing in staff training, highlighting the persistent gap between awareness and action.

The current landscape



1

Overall concern has increased slightly, reflecting ongoing vigilance



▼▲ Significantly lower/higher than the previous wave

LIFE_CONCERNS: From this list of topics below, can you please tell us which (if any) are currently a concern for the organisation you work for?
Base: 2026 n=374, 2025 n=373

Cyber security remains a highly important issue for SMEs

Agree with the following statement (Agree + Strongly Agree)

BELIEFS - Please look at the following statements and indicate how strongly you agree or disagree with each of these?
Base: Total sample n=373

▼▲ Significantly lower/higher than previous wave

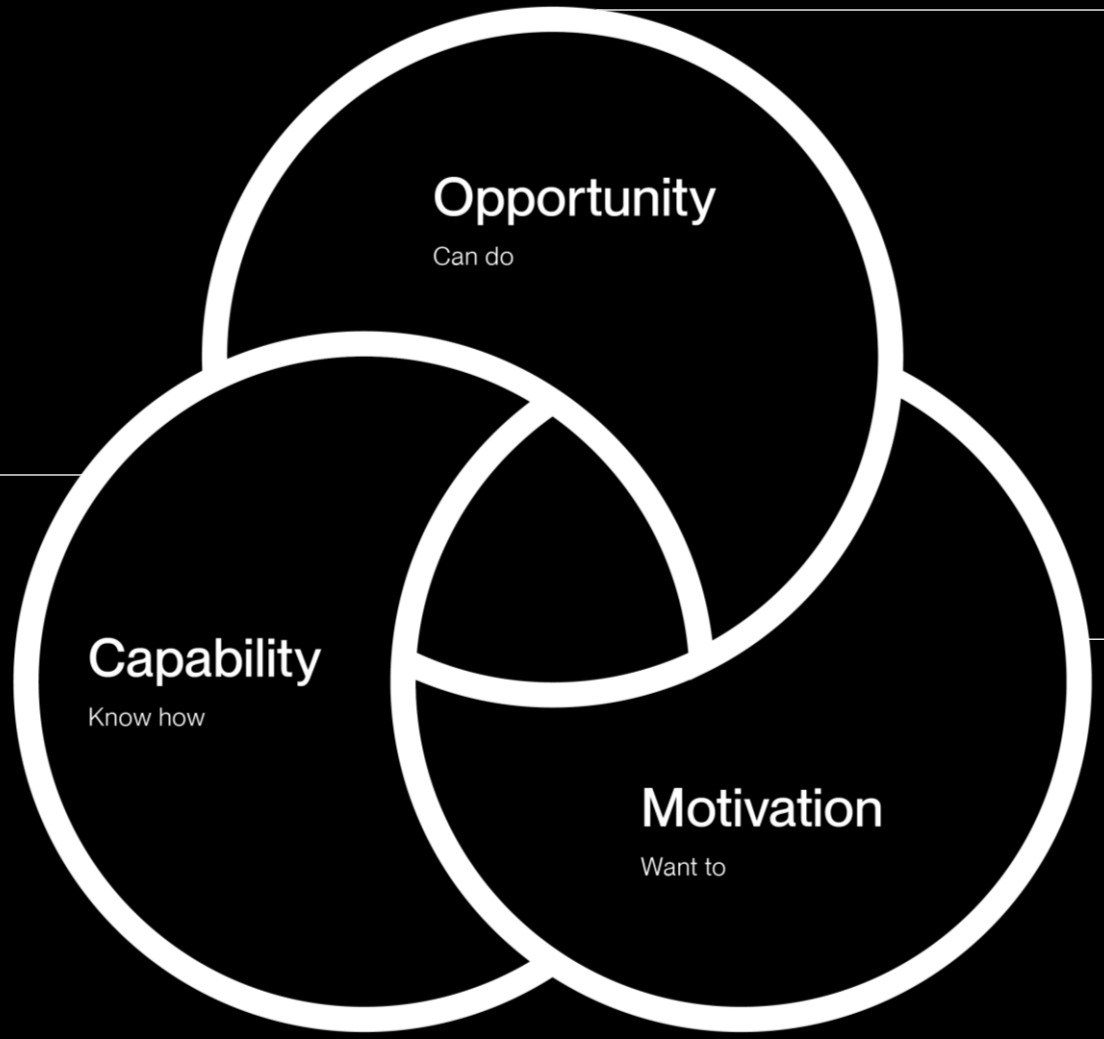
AI risks are emerging as a new concern

Top of mind cyber threats	2022	2024	2025	2026	
Hacking	#1	#1	#1	#1	
Scams, Phishing & Social Engineering	#3	#2	#2	#2	
Data Breaches & Privacy/Security	#2	#3	#3	#3	
Financial Fraud & Banking Security	#4	#4	#4	#5	
Identity Theft & Account Compromise	#5	#5	#5	#5	
AI-Enabled Threats & Emerging Risks	Not evident	Emerging	Growing	#4	New theme that emerges from 2024 and becomes a meaningful concern by 2026, including AI-generated scams, deepfakes and increasingly sophisticated cyber attacks.

"Crime is getting worse and the rise of AI will exacerbate this so that is my biggest concern."
FTE 1-5

"Business currently faces AI complex engineered threats with rapidly evolving methods of obtaining data, putting revenue and operations at risk."
FTE 10-19

Cyber security continues to be seen as highly important and there is increasing nervousness around AI, how can we best support businesses to become more cyber resilient?



Physical opportunity:

Can people do the behaviour in their current environment and context? Do they have timely reminders? Do they have the right tools, equipment and financial capability?

Social opportunity:

Can people do the behaviour in front of their social group, in their culture? Is it socially acceptable amongst their peers?

Physical capability:

Do people know how to do the behaviour physically? Do they have the physical ability?

Psychological capability:

Do people know how to do the behaviour mentally? Do they have the knowledge and mental bandwidth?

Automatic motivation:

Do people want to do the behaviour, instinctually and in the moment?

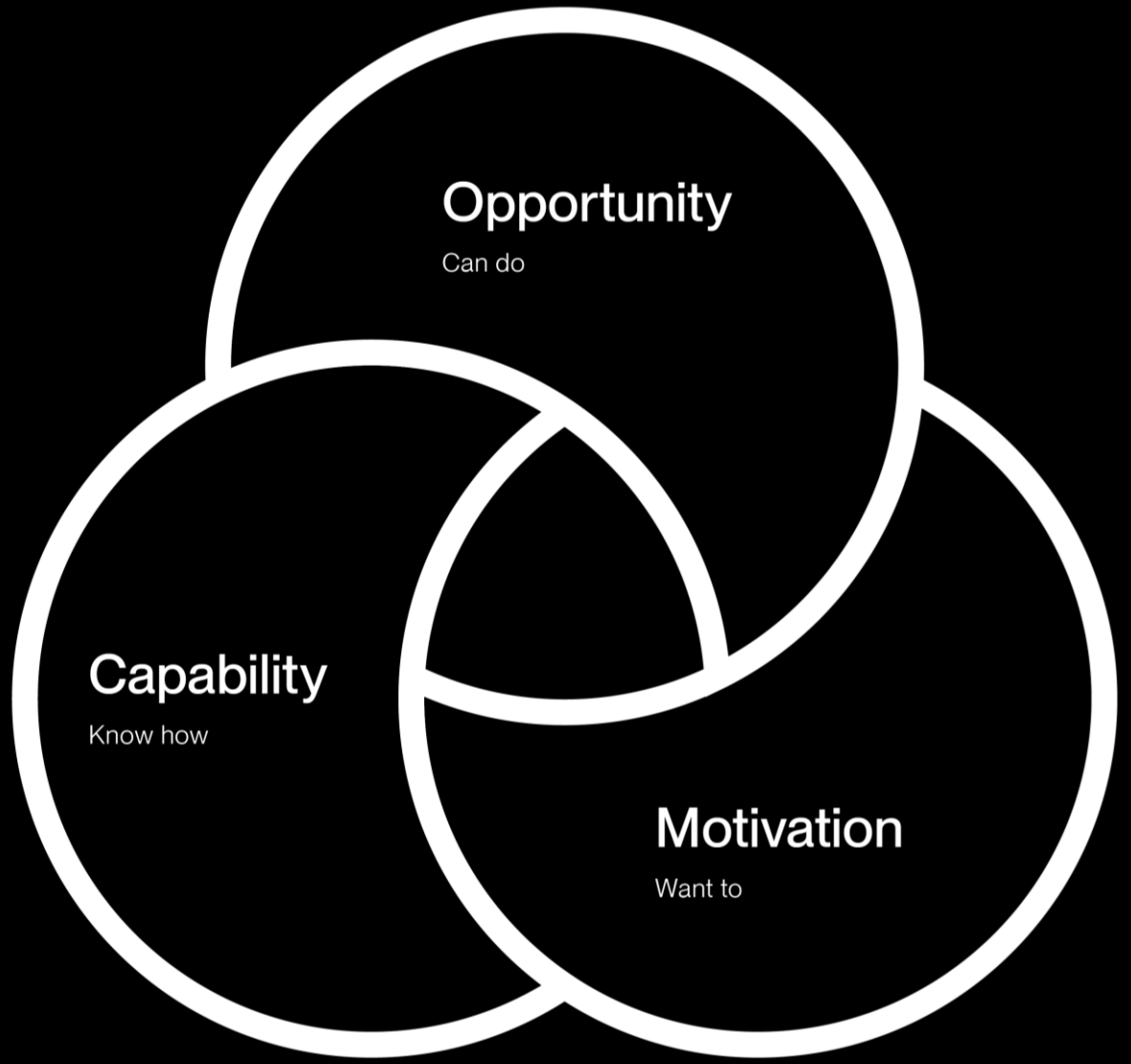
Reflective motivation:

Do people want to do the behaviour, with reasoned reflection and conscious consideration?

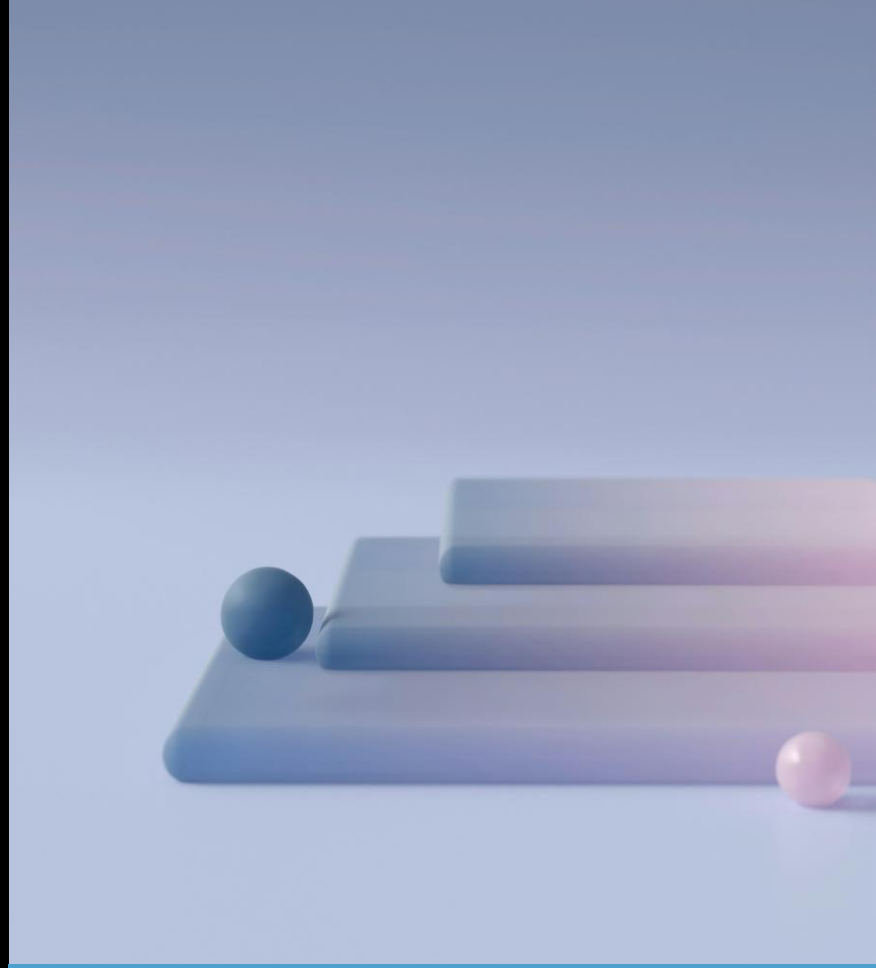
The COM-B Framework allows us to understand what drives behaviour change

The COM-B behaviour change model was developed from 19 frameworks of behaviour change identified in a systematic literature review by Professor Susan Michie, Director of the Centre for Behaviour Change at University College London.

The framework stipulates that in order to have effective behaviour change, people require capability, opportunity and motivation. Or as we like to say at TRA, the know how, can do and want to of behaviour change.



How are SMEs currently positioned?



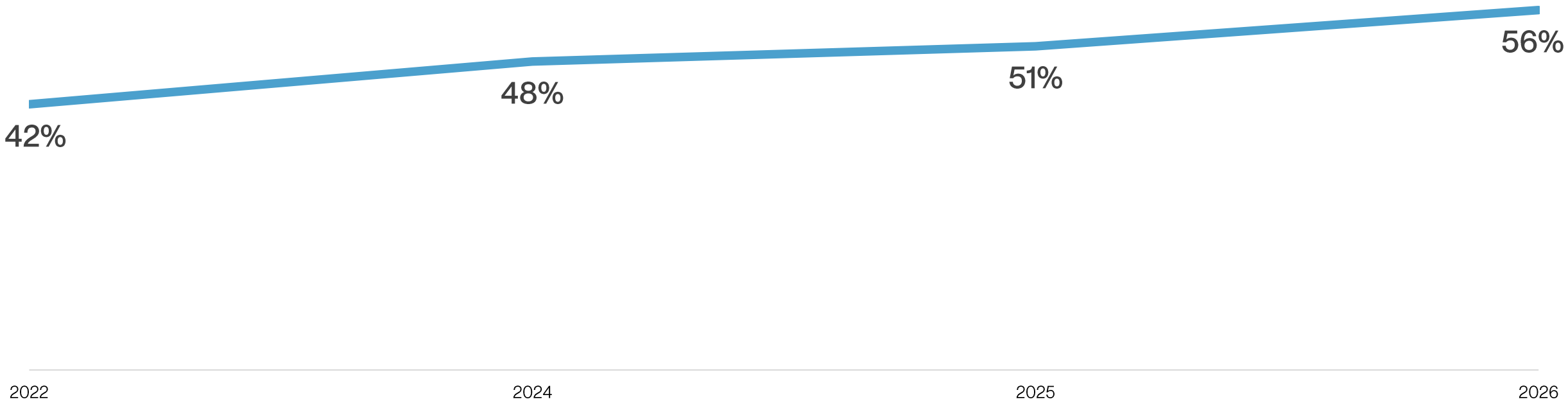
2

SMEs gradually feel better prepared to prevent attacks

But nearly half still don't feel prepared – this is driven by 0-5 FTE.

SME Preparedness over time

▲75% for 20-49 FTE

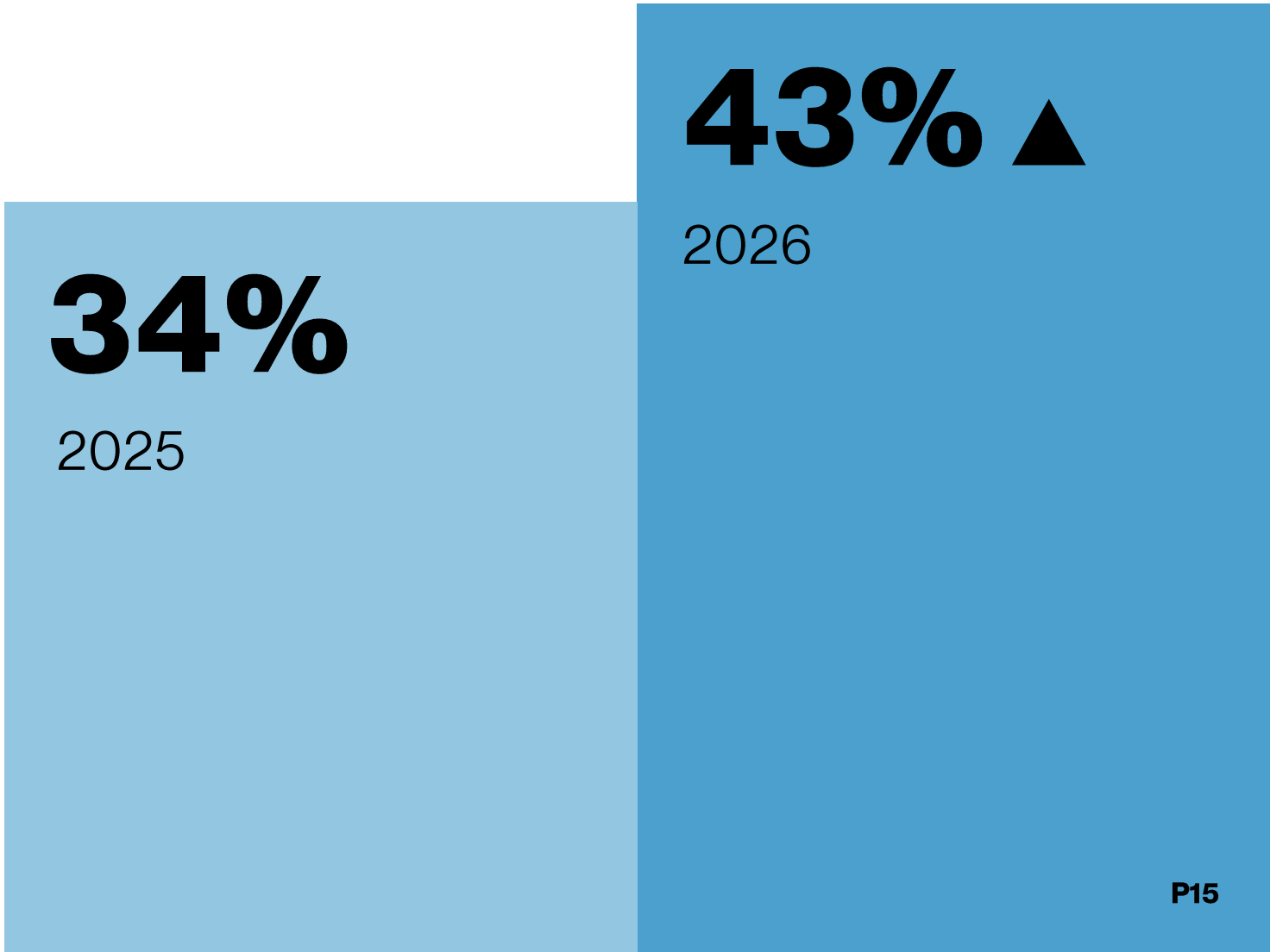


How prepared is the organisation when it comes to preventing a cyber security breach?
Base: Total sample n=373

At the same time they feel increasingly vulnerable

Our organisation is vulnerable to cyber attacks

This is driven by mid to large SMEs (6-19 FTE (55%) and 20-49 FTE (59%))



▼▲ Significantly lower/higher than the previous wave

Please look at the following statements and indicate how strongly you agree or disagree with each of these?
Base: Total sample 2026 n=373, 2025 n=374

Knowledge of cyber threats has remained broadly stable

Knowledge of cyber threats

	2024	2025	2026
Scam calls	89%	88%	84%
Phishing	76%	71%	73%
Malware	74%	70%	69%
Data Breach	77%	71%	61% ▼
Invoice Scam	69%	63%	59%
Unauthorised Access	69%	57% ▼	56%
Ransomware	70%	61% ▼	55%
Impersonation Scam	59%	65%	54% ▼
Business Email Compromise	50%	46%	51%
Unauthorised Transfer	48%	44%	47%
DDoS (Distributed Denial-Of-Service-Attack)	32%	30%	27%
Insider Threat	22%	26%	27%

From this list of cyber threats, attacks and crime, can you please tell us which (if any) you are aware of?
Base: Total sample 2026 n=373, 2025 n=373, 2024 n=349

▼▲ Significantly lower/higher than the previous wave

Larger SMEs are experiencing more attacks

Experienced Cyber Threats by FTE size

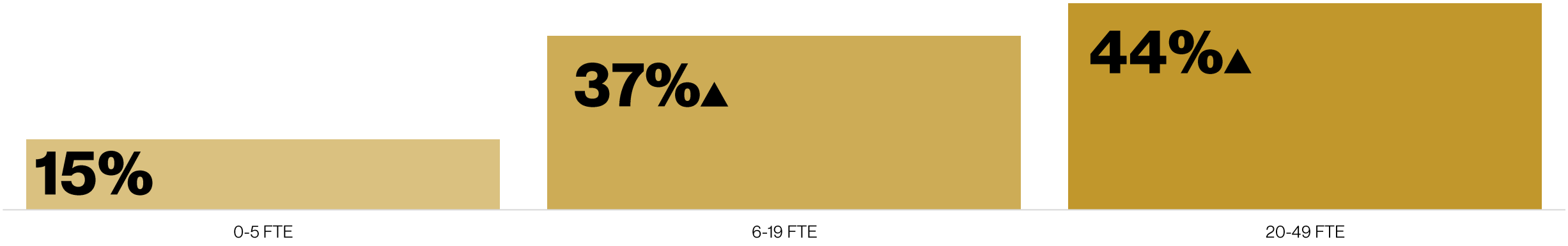
	Total	0-5 FTE	6-19 FTE	20-49 FTE
Any attack	53%	52% ▼	65%	76% ▲
Scam calls	34%	34%	32%	38%
Phishing	22%	22%	18%	38% ▲
Impersonation Scam	7%	6%	11%	11%
Invoice Scam	8%	8%	9%	9%
Malware	7%	7%	7%	18% ▲
Unauthorised Access	7%	7%	8%	6%
DDoS (Distributed Denial-Of-Service Attack)	1%	1%	5%	4%
Unauthorised Transfer	3%	3%	5%	7%
Business Email Compromise	5%	5%	4%	4%
Ransomware	3%	3%	3%	3%
Data Breach	3%	3%	9%	7%
Insider Threat	1%	1%	2%	7% ▲

From this same list of cyber threats, attacks and crimes, can you please tell us which (if any) you have personally experienced in the past six months?
Base: 0-5 FTE n=166, 6-19 FTE n=134, 20-49 FTE n=73

▼▲ Significantly lower/higher than other groups

And the severity of those attacks is also increasing among mid to large SMEs

Severity of Attack (Total moderate to severe impact)



Q. Can you please rank how much of an impact the cyber threat, attack or crime had on the organization?
Base: 0-5 FTE n=179, 6-19 FTE n=107, 20-49 FTE n=88

▲ Significantly higher than 2025

Larger SMEs are also experiencing more consequential attacks in terms of stress, damage and financial loss

NET Effect of cyber attack

20-49 FTE did not over index in any effects of cyber harm in 2025.

	0-5 FTE	6-19 FTE	20-49 FTE
It took up our time	67% ▼	60%	49%
It was stressful	49%	56%	60% ▲
It impacted our mental wellbeing	32%	23%	30%
Lost productivity / impacted operations	29%	35%	37%
It was embarrassing	25%	31%	42%
We lost information or data	13%	29%	41%
It damaged our device/s	13%	24%	43% ▲
None of the above / prefer not to answer	12%	8%	8%
It damaged our reputation with customers or suppliers	11%	26%	28%
We lost money or had to pay money	9% ▼	24%	32% ▲

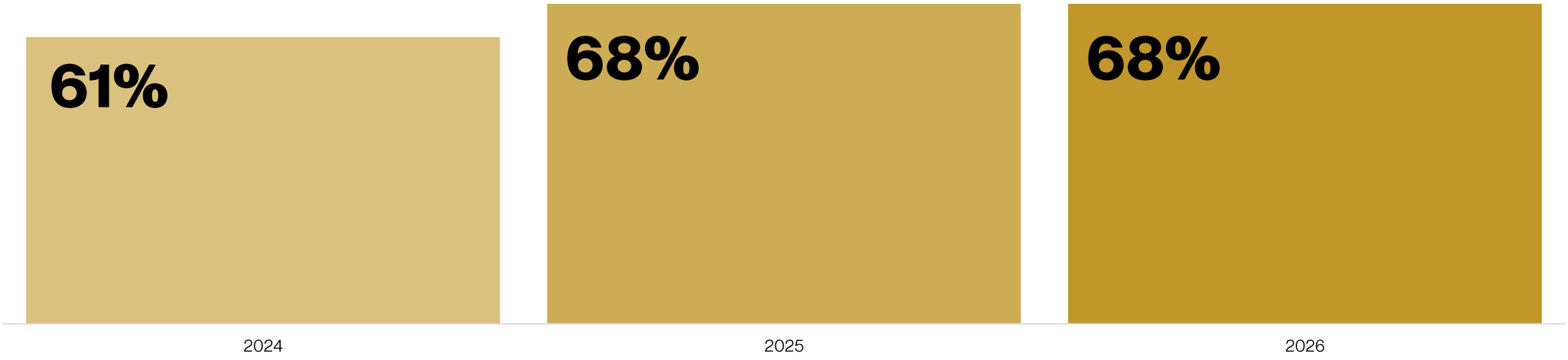
Q. Regarding the cyber threats, online security attacks and crimes your organisation experienced, in what way was your organisation affected?
Base: Experienced a cyber threat, FTE 0-5 n=53, FTE 6-19 n=72, FTE 20-49 n=46

▼▲ Significantly lower/higher than the previous wave

While attacks are becoming more severe and consequential, reporting has plateaued

NET Reported/disclosed the cyber attack

20-49 FTE (87%) were significantly more likely to report their attack.

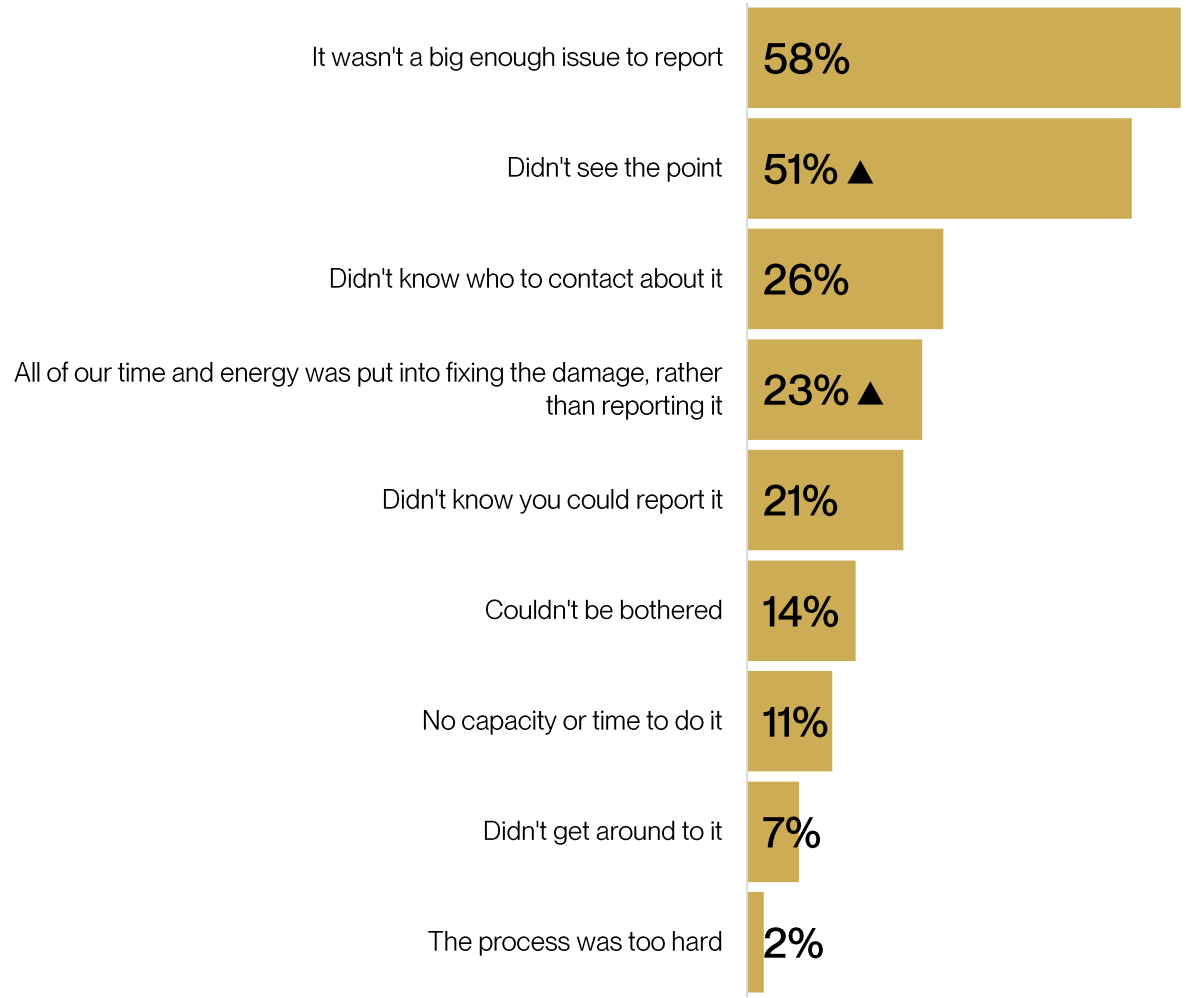


Q. Can you please tell us which actions were taken as a direct result?
Base: Experienced a cyber threat 2022 n=113, 2024 n=169, 2025 n=194, 2026 n=223

▲ Significantly higher than 2025

And lack of motivation to report is increasingly evident

Reason for no report



▼▲ Significantly lower/higher than previous wave

You said that the organisation you own or work for had experienced at least one type of cyber threat, attack or crime but did not report it. Which of the following reason/s best describes why it wasn't reported?
Base: Experienced a personal attack, but didn't report it 2025 n=44, 2026 n=41

Preventative action taken is stable over time

Preventative action taken
(Always + almost always)

	2024	2025	2026
We update software, browsers and apps to the latest version	77%	77%	79%
We use cyber security software solutions	72%	78%	78%
We regularly back up our data and files to a separate and secure location	65%	70%	77%▲
We use email filters to block malicious content	73%	77%	77%
We verify links and attachments within emails or text messages	81%	84%	76%
We only collect customer data that is absolutely necessary	75%	78%	75%
We use two-factor or multi-factor authentication on all main accounts	73%	77%	74%
We use strong passwords for all key accounts and systems	65%	71%	69%
We use different passwords for each account and system	66%	69%	67%
We verify any changes to invoices and payment processes or details	59%	71%	66%
We have user access controls in place	63%	67%	63%
We change default password settings on devices	60%	65%	62%
We use a password manager and make one available to staff	48%	56%	57%
We have an incident response plan in place	37%	49%	50%
We set up logs and alerts for when key events or changes occur	42%	49%	50%

Q. Can you please tell us how often the organisation you own or work for currently does them
Base: Total sample n=373

▼▲ Significantly lower/higher than the previous wave

Motivation remains the major barrier to action

Barrier to preventative action

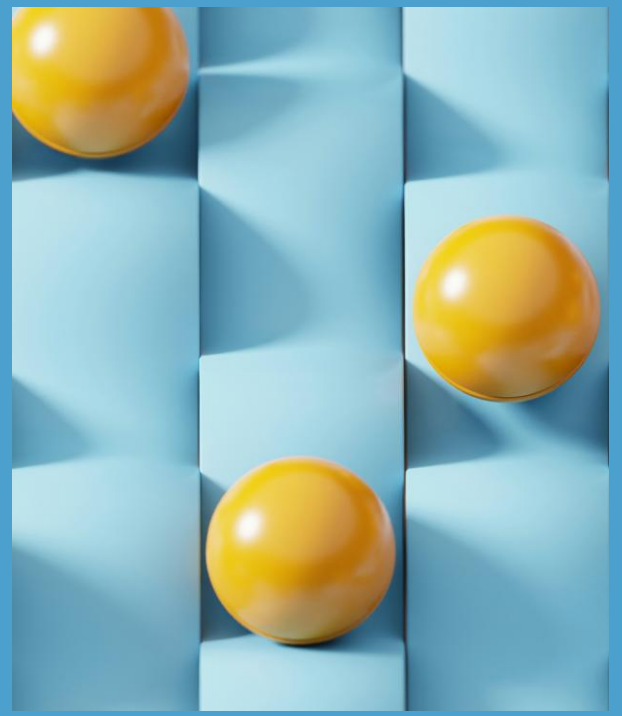
	We use two-factor or multi-factor authentication on all main accounts	We update software, browsers and apps to the latest version	We regularly back up our data and files to a separate and secure location
NET: Motivation	56%	60%▲	52%
We feel we are already doing enough to protect ourselves against cyber threats	26%	28%	21%
We don't want to / We can't be bothered	15%	13%	24%▲
We're not worried about cyber security incidents happening to us	9%	8%	4%
We don't know why it's important	6%	22%▲	5%
The safety and security of our information online is not that important to us	6%	3%	9%
We would be protected by government agencies or banks if a cyber security breach happened to us	6%	6%	2%
NET: Opportunity	29%	48%	42%
We keep forgetting to	17%	32%	24%
It costs too much	13%	24%	19%
Other organisations don't do this	0%▼	6%	1%
NET: Capability	26%	21%	40%
We don't know how to do it / it's too complicated	19%	9%	21%▲
We don't know what to do	11%	7%	11%
We don't have time	6%▼	9%	15%

What is stopping your organisation from doing that action?
Base: Not using two factor n=99, not updating software n=79, not backing up data to a separate location n=93.

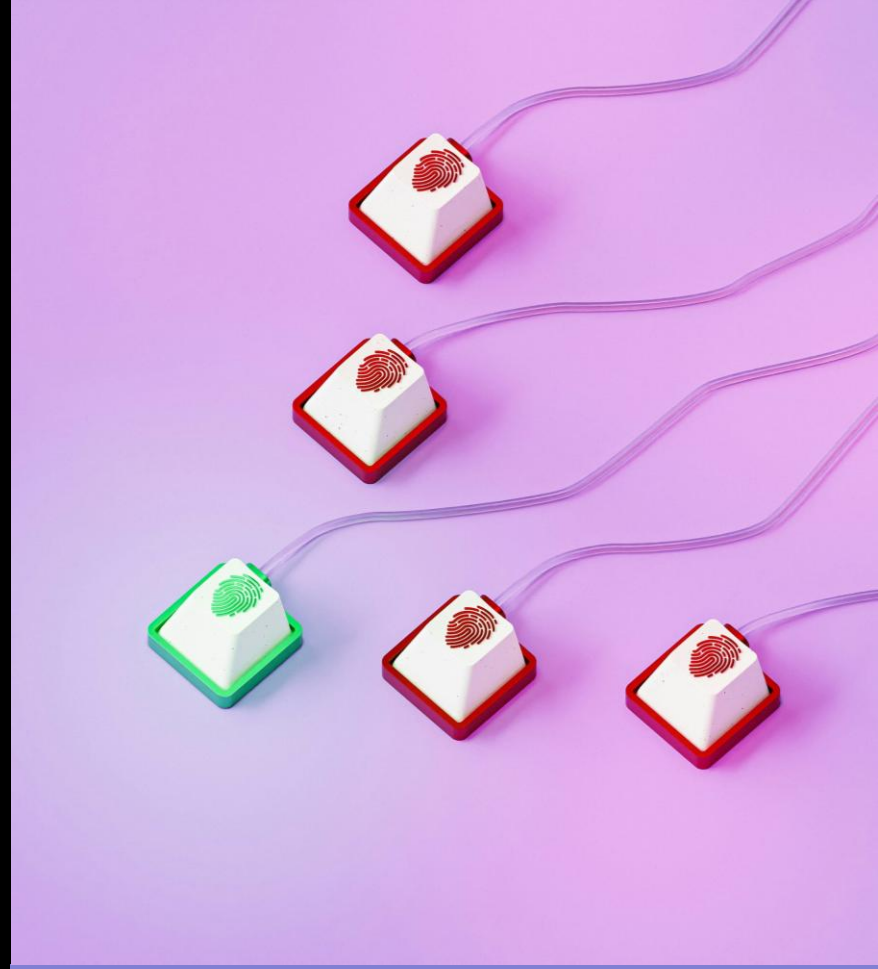
Implication

Businesses remain vulnerable to increasingly sophisticated threats

SMEs increasingly recognise the importance of cyber security and feel better prepared than in previous years. However, vulnerability is also rising, cyber attacks are becoming more harmful, and the adoption of key protective behaviours has largely plateaued.



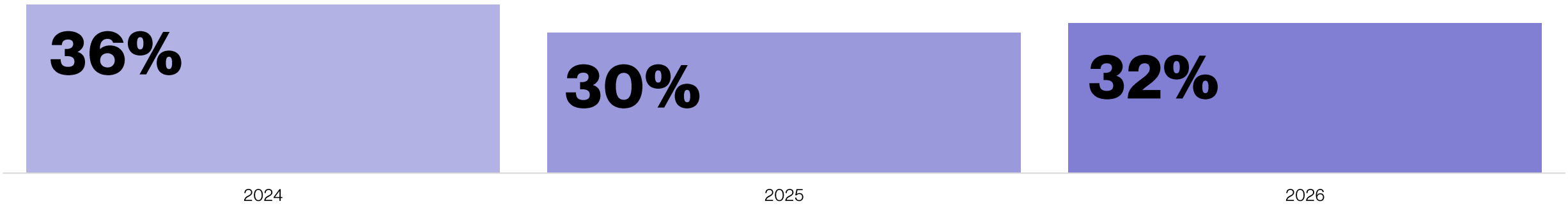
Information and support



3

Still a third are taking no action to upskill staff

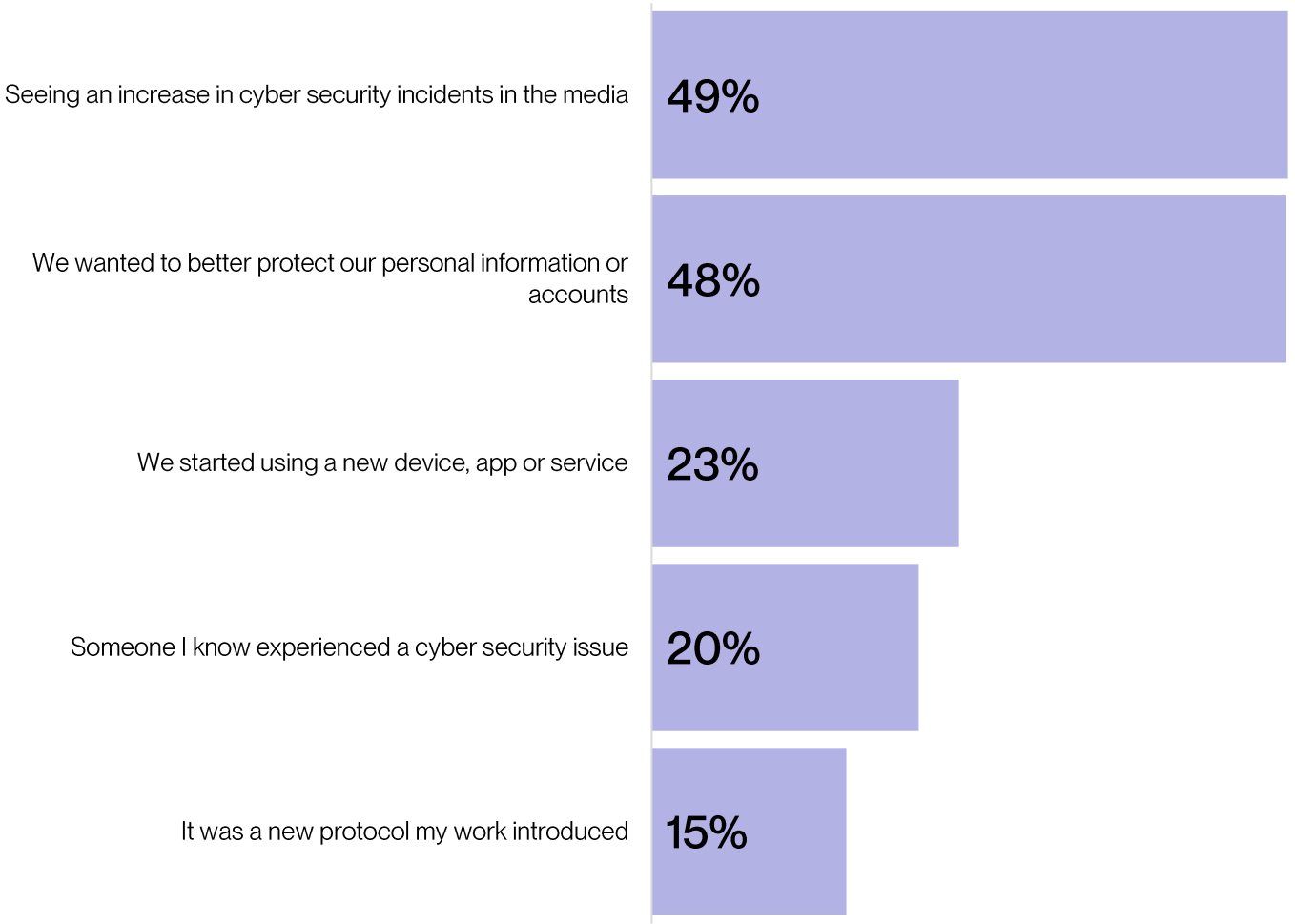
% of SME's taking no action to upskill/train staff for cyber security purposes



Please tell us which (if any) of the following are used to upskill staff & maintain cyber security?
Base: Total sample 2026 n=373, 2025 n=373, 2024 n=349

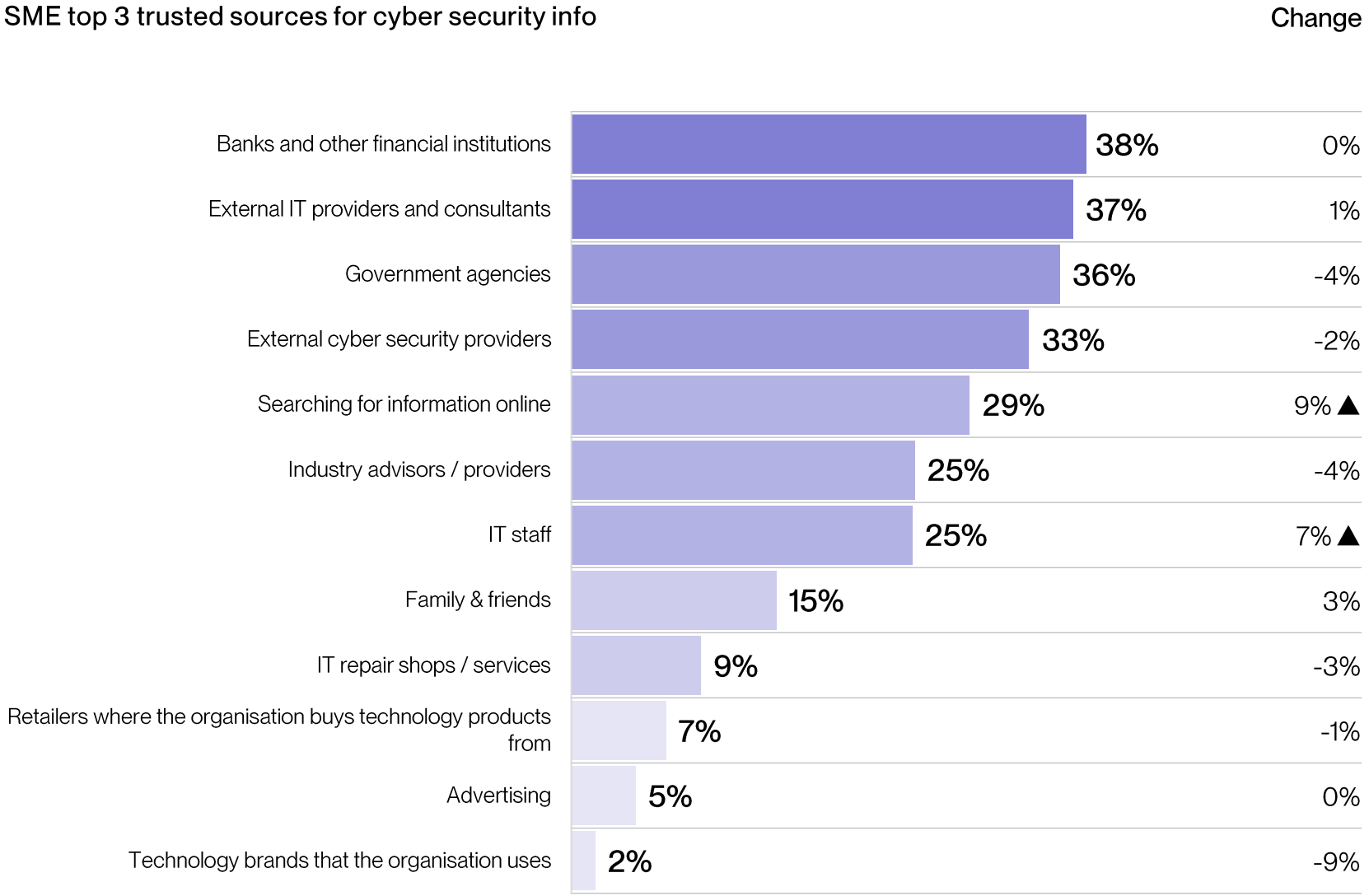
Media exposure is driving new cyber security action

Prompted a new cyber security behaviour



Q. What prompted your organisation to start using these behaviours?
Base: Started a new cyber security behaviour in the last six months n=160

Online information is increasingly a trusted source



▼▲ Significantly lower/higher than the previous wave

And from that same list of information sources, please rank the top three most trusted sources for the organization
Base: Total sample 2026 n=373, 2025 n=373

TRA

New Zealand

Level 4, Quay Building,
106-108 Quay Street,
Britomart, Auckland 1010

+64 9 377 8129

Melbourne

The Commons,
54 Wellington St,
Collingwood VIC 3066

+61 406 482 715

Sydney

The Commons,
285A Crown St,
Surry Hills NSW 2010

+61 405 604 226