SME Cyber Security Behaviour Tracker 2025

September 2025

TRA x NCSC

National Cyber Security Centre

TRA

Background

The National Cyber Security Centre (NCSC) plays a key role in providing information and education around 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 2025.

This research was also conducted in 2024. 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=374 SME IT / operational decision makers was achieved.

Fieldwork ran from the 12th May – 3rd June 2025.

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%.

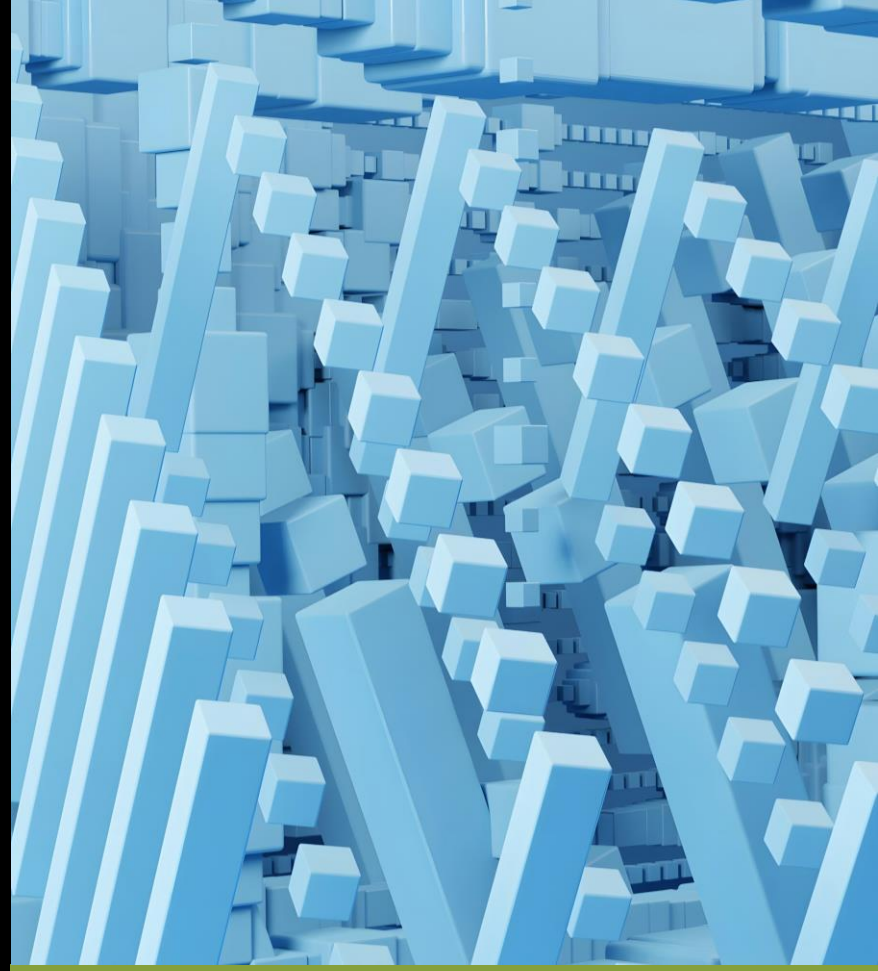
*Full time equivalent (FTE) is a measure of the number of employees that make up the organisation.

Summary of findings

New Zealand SMEs believe cyber security is important, but in reality it's often deprioritised, particularly for the smallest organisations who are grappling with immediate, tangible pressures.

Increasingly, organisations are adopting more preventative cyber security behaviours, but the risk landscape is also evolving fast. In just a year, the proportion of SMEs that have experienced cyber threats has grown significantly. And although preventative behaviours are growing overall, some feel they're 'doing enough already'.

SME cyber security attitudes



1

When it comes to cyber security, SMEs consider it a highly important issue

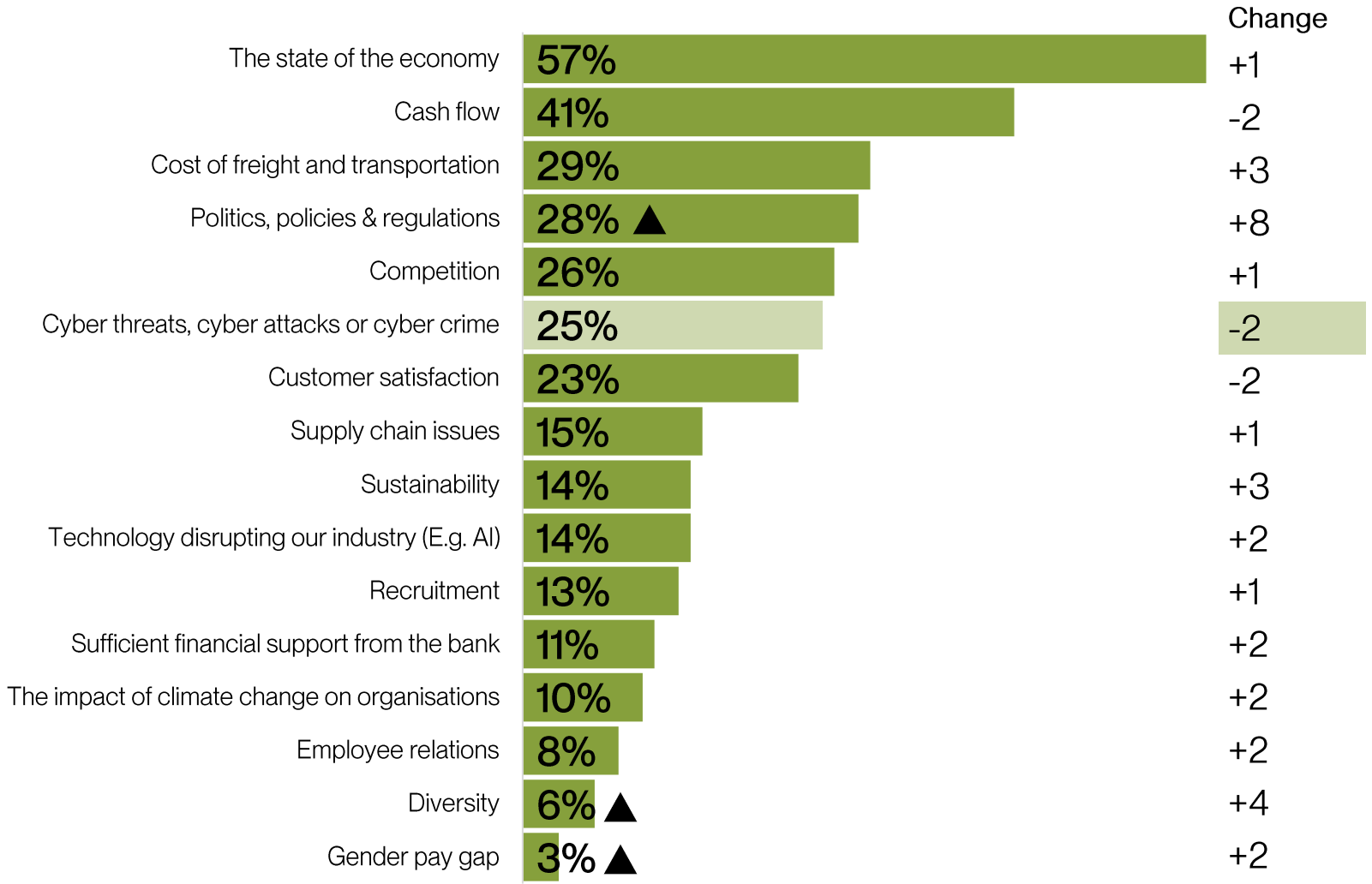
Cyber security beliefs
(Strongly agree / agree)

94%	Cyber security is important for New Zealand
94%	Being cyber safe is something everyone should do at work
94%	We need to take responsibility for protecting our organisation online
94%	It's important that our organisation is protected online

BELIEFS: Please look at the following statements and indicate how strongly you agree or disagree with each of these... (Agree / strongly agree).
Base: Total n=374.

But while cyber security is seen as important, it competes with a long list of other organisational priorities

SME concerns 2025



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: 2025 n=374.

▼▲ Significantly lower/higher than 2024

There is nuance to this picture too:

larger organisations are more concerned about cyber security

SME concerns 2025

	0-5 FTE	6-19 FTE	20-49 FTE
The state of the economy	58%	49%	49%
Cash flow	40%	45%	▼ 27%
Cost of freight and transportation	29%	28%	30%
Politics, policies & regulations	29%	25%	▼ 16%
Competition	26%	36%	24%
Cyber threats, cyber attacks or cyber crime	**25%**	**20%**	**▲ 42%**
Customer satisfaction	23%	29%	33%
Supply chain issues	14%	21%	23%
Sustainability	14%	19%	19%
Technology disrupting our industry (e.g. AI)	13%	12%	▲ 28%
Recruitment	▼ 11%	▲ 29%	▲ 25%
Sufficient financial support from the bank	11%	9%	13%
The impact of climate change on organisations	11%	8%	13%
Employee relations	▼ 7%	▲ 21%	▲ 20%
Diversity	6%	8%	▲ 18%
Gender pay gap	3%	8%	3%

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: 0-5 FTE n=179; 6-19 FTE n=107; 20-49 FTE n=88.
*Full time equivalent (FTE) is a measure of the number of employees that make up the organisation.

▼▲ Significantly lower/higher than other groups

In fact, the mindset towards cyber security is substantially different between organisations of different sizes

In the last year there have been no shifts to how strongly these beliefs are held overall.

BELIEFS: Please look at the following statements and indicate how strongly you agree or disagree with each of these... (Agree / strongly agree).
Base: Total n=374; 0-5 FTE n=179; 6-19 FTE n=107; 20-49 FTE n=88.

TRA NCSC

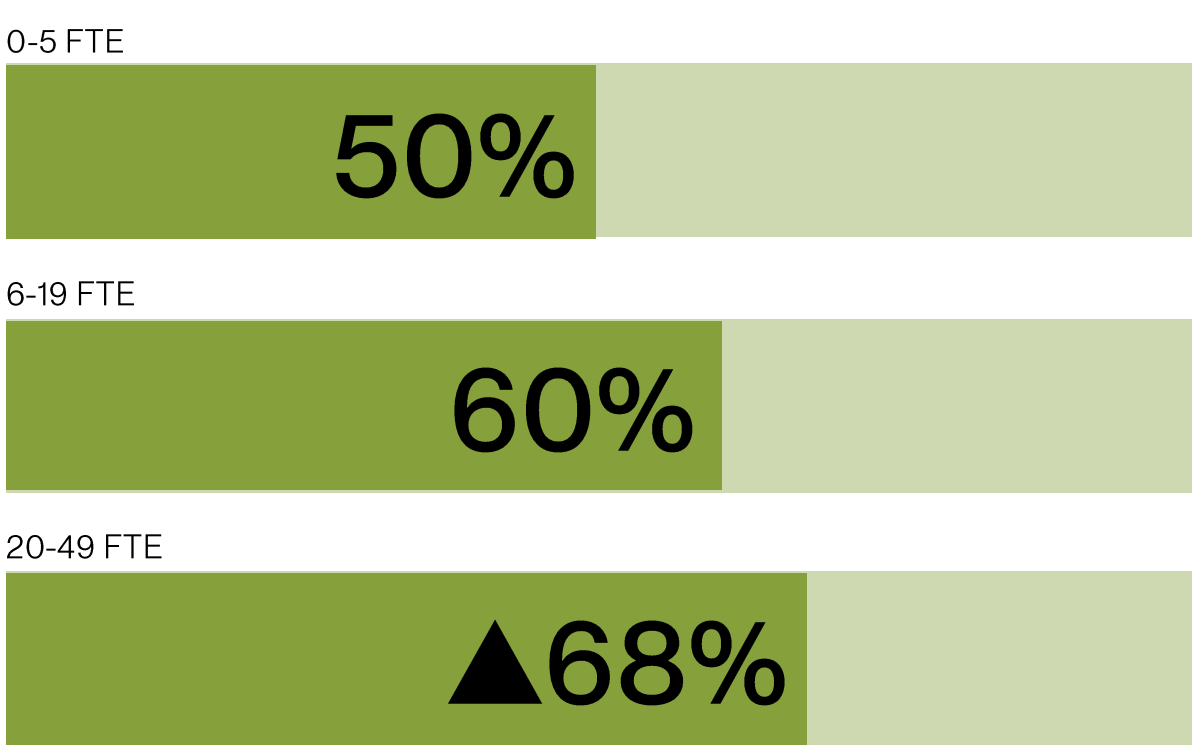
Cyber security beliefs 2025
(Strongly agree / agree)

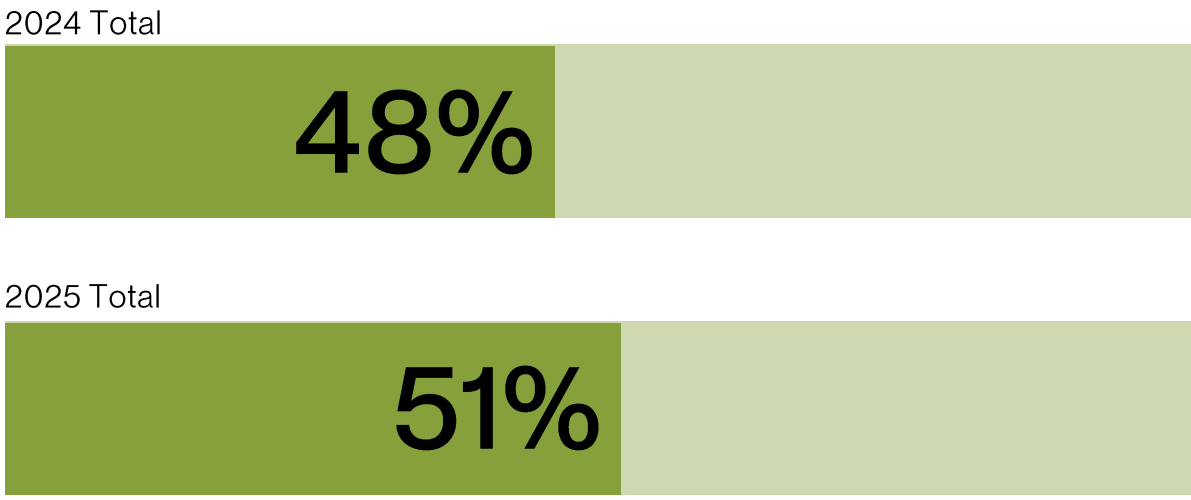
	Total	0-5 FTE	6-19 FTE	20-49 FTE
Our organisation is alert to the possibility of cyber attacks	79%	▼ 78%	▲ 91%	82%
Cyber threats, attacks and crimes affect organisations like ours	64%	64%	72%	75%
Our organisation is doing enough to keep safe and secure online	64%	63%	73%	77%
New Zealand organisations think that the actions they take can prevent cyber attacks and crime	63%	▼ 62%	▲ 75%	▲ 78%
Cyber security is one of our top priorities for our organisation right now	52%	▼ 51%	▲ 66%	▲ 76%
New Zealand organisations know what to do to stop cyber attacks and crimes	36%	▼ 33%	▲ 64%	▲ 61%
It's unlikely a cyber security incident would happen to our organisation	35%	34%	46%	42%
Our organisation is vulnerable to cyber attacks	34%	▼ 32%	▲ 51%	▲ 54%

▼▲ Significantly lower/higher than other groups

With cyber security a lower priority, small organisations feel less prepared in preventing cyber security breaches

Cyber security preparedness 2025





There have been no significant changes at the total level, however larger organisations are less prepared compared to 2024 (-15).

PREPARED: How prepared is the organisation when it comes to preventing a cyber security breach?
Base: 2024 n=349; 2025 n=374; 0-5 FTE n=179; 6-19 FTE n=107; 20-49 FTE n=88.

▼▲ Significantly lower/higher than other groups

[UNCLASSIFIED]

With Kiwi organisations experiencing cyber security so differently, how can we better meet them on their cyber journey?

Cyber security behaviours

2

28% of organisations have taken new cyber security actions in the past six months

This level is consistent across organisation size and industry.

New cyber security actions in the last 6 months

29% 2024

28% 2025

NEW_BEHAV: In the past six months, has your organisation taken any new actions to keep yourself more secure online?
Base: 2024 n=349; 2025 n=374.

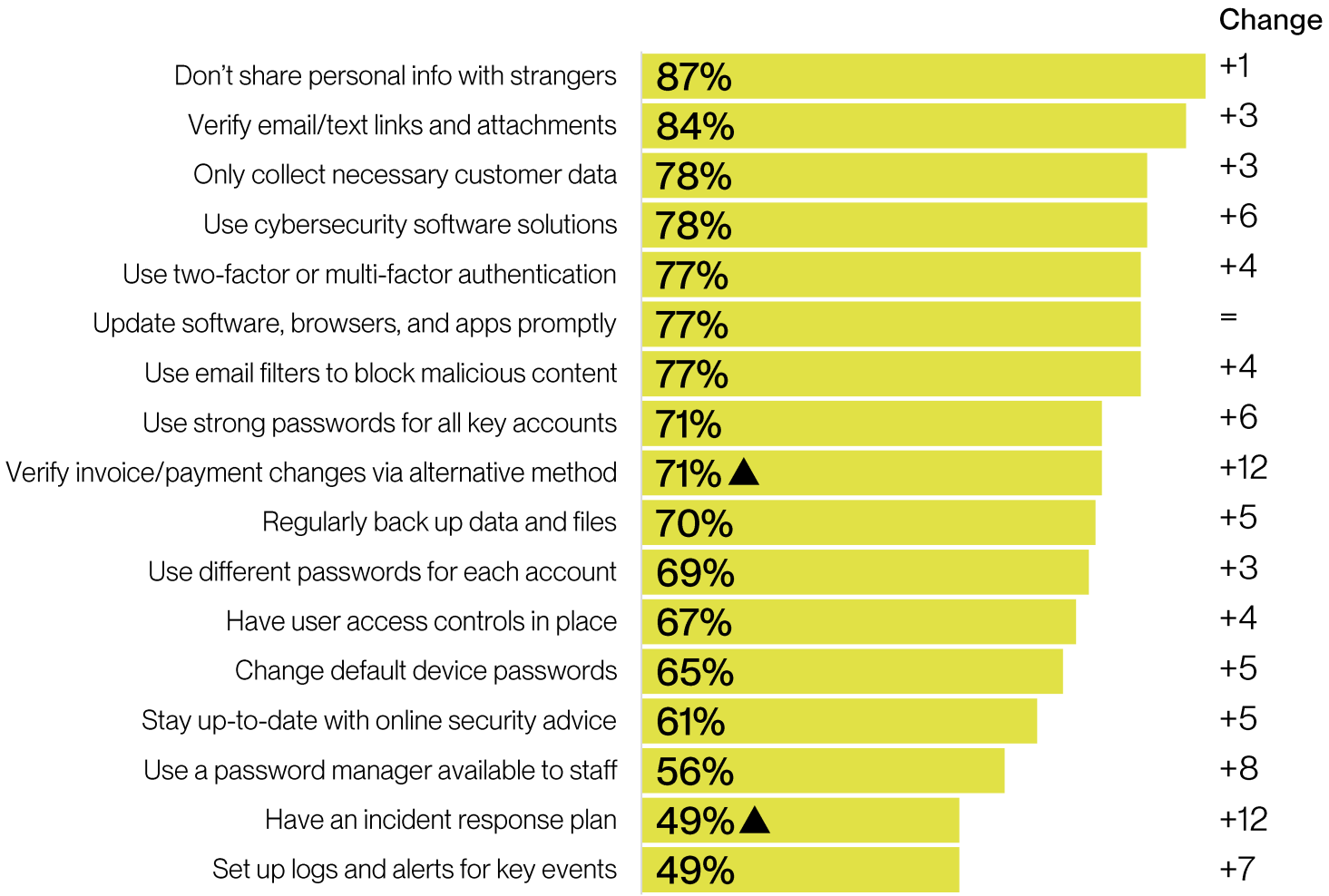
There has been an increase in the total number of preventative actions organisations are taking

Verifying payment changes via an alternative method and having an incident response plan have become more common.

Organisations with 0-5 FTEs verify links and attachments within emails more often than larger organisations (+11).

CYBER_ACTIONS2_NEW: From this list of cyber security measures, can you please tell us how often the organisation you own or work for currently does them? (Actions taken: always / almost always).
Base: 2024 n=349; 2025 n=374.

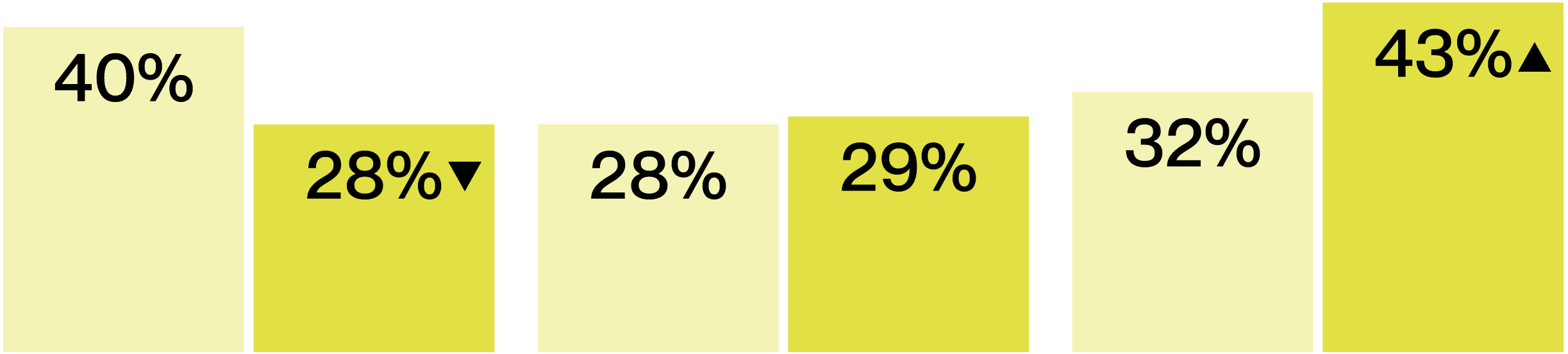
Cyber security actions taken 2025
(always / almost always)



▼▲ Significantly lower/higher than 2024

Growth in preventative actions isn't just coming from those already taking actions; the 'Cyber Compelled' group has grown

The proportion that fits in the bracket of organisations that take the highest number of preventative actions has significantly grown in 2025, while the 'Capable' group that takes the fewest actions, has decreased.



The Cyber Capable
Less than 10 preventative actions taken

The Cyber Compliant
10-14 preventative actions taken

The Cyber Compelled
15+ preventative actions taken

CYBER_ACTIONS2_NEW: From this list of cyber security measures, can you please tell us how often the organisation you own or work for currently does them?
Base: 2024 n=349; 2025 n=374.

▼▲ Significantly lower/higher than 2024

SMEs are motivated to take action due to the perceived relevance of cyber security

Motivators for organisations taking the following cyber security actions (always / almost always)

	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
The safety and security of our information online is important to us	**57%**	**57%**	**66%**
We understand that cyber security is our responsibility	**62%**	**57%**	**53%**
We know how to do the right thing to keep secure online	38%	52%	50%
We find it easy to be secure online	37%	40%	35%
It does not take long to implement cyber security measures to be secure online	34%	37%	36%
We're worried about cyber security breaches happening to us	34%	30%	37%
We are regularly reminded to implement cyber security measures	30%	36%	29%
We're forced to use cyber security measures like long passwords, two factor authentication already	31%	23%	21%
Other organisations do this	7%	9%	9%

WHY_MOTIVATORS: For behaviours where you answered always or almost always, please tell us what motivates your organisation into doing those. (always / almost always).
Base: NCSC priority actions taken always / almost always n=262-270.

TRA NCSC

As for barriers, a perception of already doing enough can hinder further actions

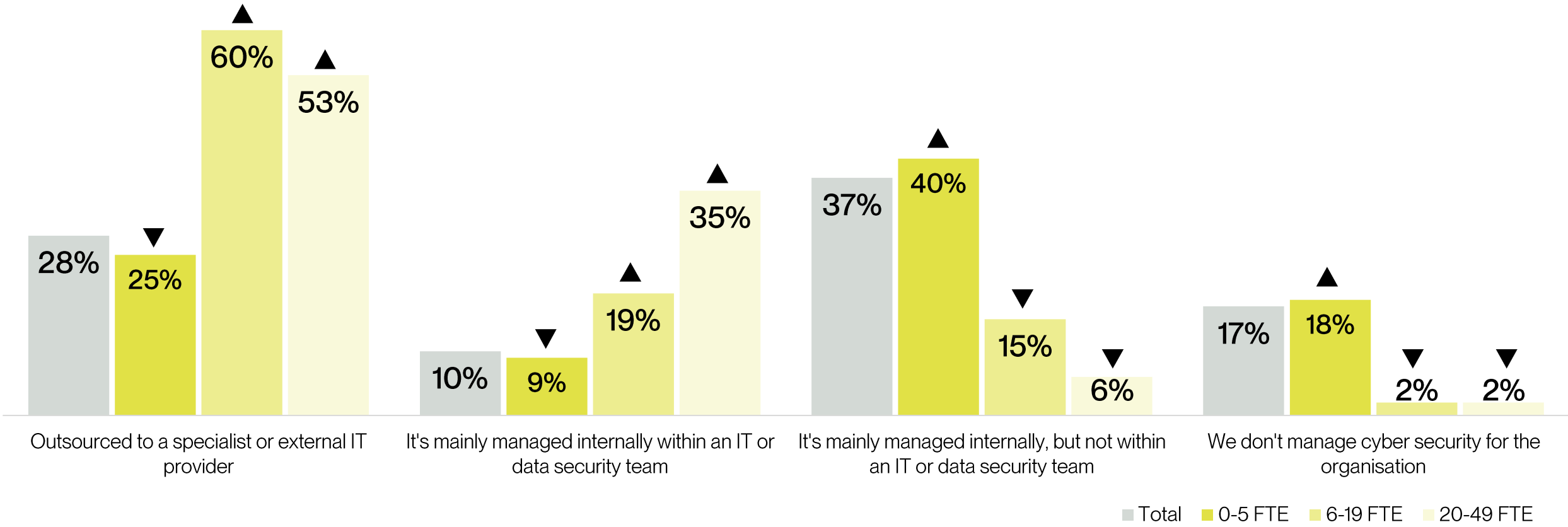
Barriers for organisations not regularly taking the following cyber security actions

	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
We feel we are already doing enough to protect ourselves against cyber threats	**33%**	**23%**	**32%**
We keep forgetting to	11%	18%	24%
We don't have time	11%	11%	15%
We don't know how to do it / it's too complicated	22%	4%	10%
We don't want to / We can't be bothered	17%	7%	5%
It costs too much	9%	9%	11%
We don't know what to do	14%	9%	5%
We don't know why it's important	6%	8%	9%
We're not worried about cyber security incidents happening to us	11%	5%	4%
We would be protected by government agencies or banks if a cyber security breach happened to us	4%	3%	10%
The safety and security of our information online is not that important to us	7%	2%	8%
Other organisations don't do this	5%	3%	4%

WHY_BARRIERS: For behaviours where you answered sometimes, rarely, or never, please tell us what is stopping your organisation from doing that action. (sometimes / rarely / never).
Base: NCSC priority actions taken sometimes / rarely / never n=101-108

Many larger SMEs lean on IT teams or external providers, while smaller ones are more likely to manage it informally or not at all

Cyber security management

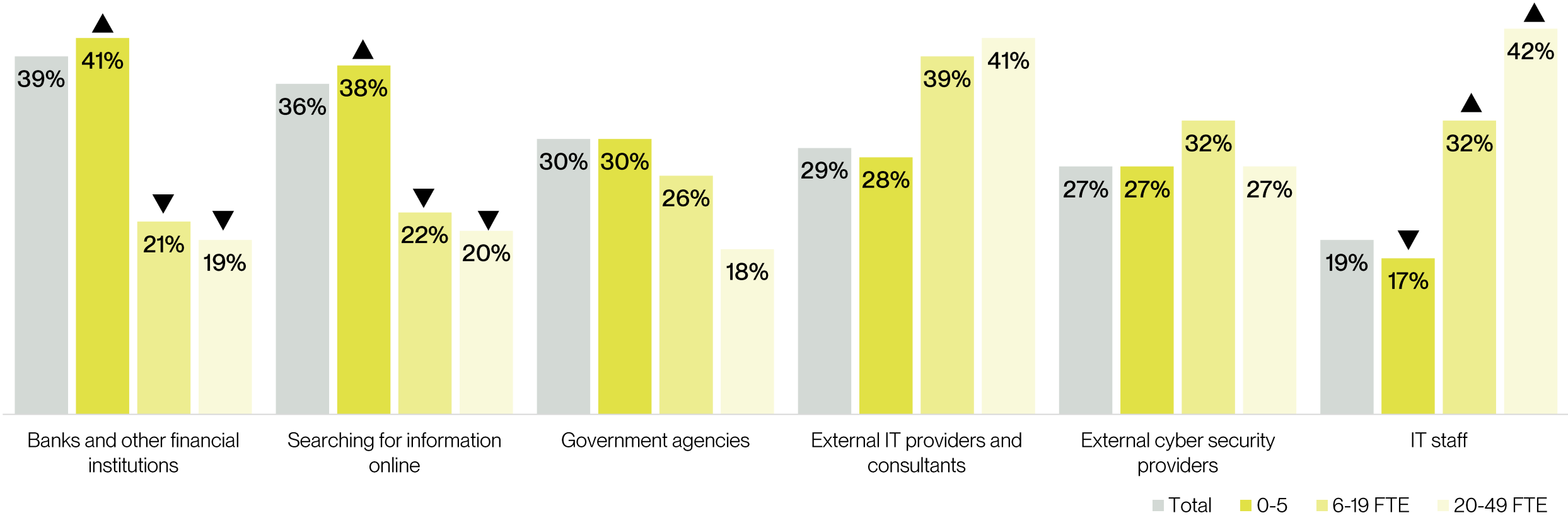


IT_TEAM: Which best describes how the organisation's cyber security is managed?
Base: 2025 n=374; 0-5 FTE n=179; 6-19 FTE n=107; 20-49 FTE n=88.

▼▲ Significantly lower/higher than other groups

The sources for cyber advice also differ by size, with banks or online searches more likely for smaller SMEs

Sources of Information and advice



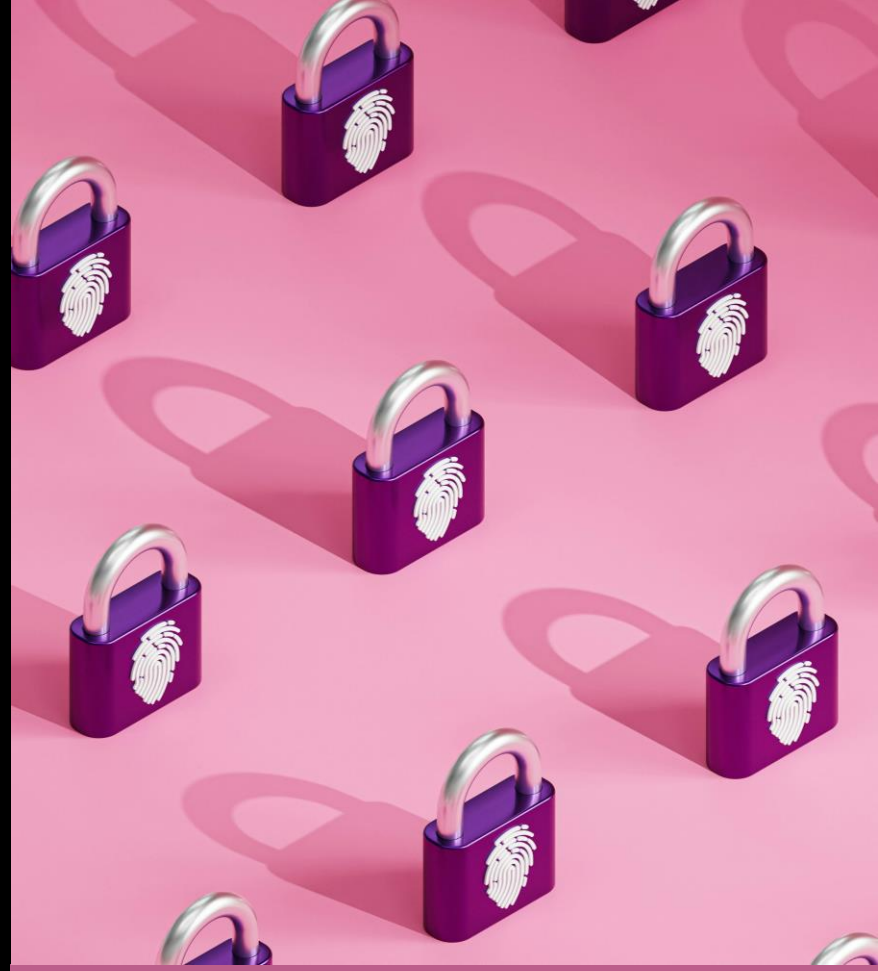
INFO_SOURCE: Where does your organisation currently get cyber security information and / or advice from?
Base: 2025 n=374; 0-5 FTE n=179; 6-19 FTE n=107; 20-49 FTE n=88

▼▲ Significantly lower/higher than other groups

Influencing further shifts in behaviour is likely to happen via different channels for smaller and larger SMEs

- Positively, organisations are increasingly taking preventative actions in 2025, and the proportion that fall in the ‘Cyber Compelled’ group of organisations has grown.
- However, some are at a point of complacency or confusion about what else needs to be done.
- The avenues through which organisations’ actions might be further influenced differ significantly for organisations of different sizes.
- Smaller SMEs are more likely to do their own research and lean upon their bank for their cyber needs, while larger organisations are more likely to engage external IT suppliers, or even have internal teams.

The impact on New Zealand organisations



3

There has been a significant increase in the number of organisations experiencing cyber threats

The increase has occurred among organisations with 0-5 FTEs, where the proportion of those experiencing cyber threats and attacks has risen by 20 points.

Experienced at least one cyber threat

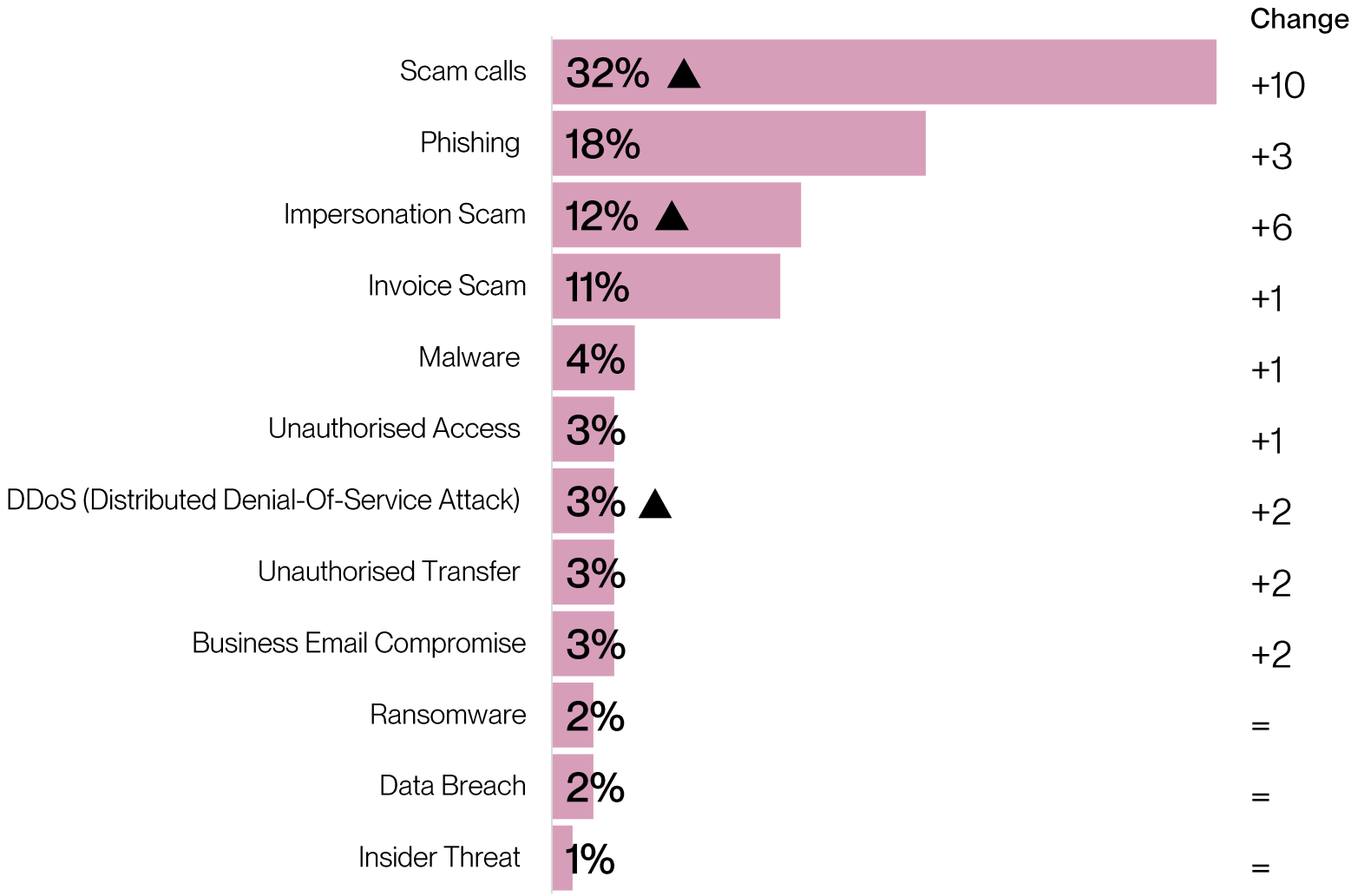
36% 2024

53% ▲ 2025

PERSONAL_EXPERIENCE: From this same list of cyber threats, online security attacks and crimes, can you please tell us which (if any) the organisation you own or work for has experienced in the past six months?
Base: 2024 n=349; 2025 n=374.

Scam calls and impersonation scams are the main contributors to the rise in incidents amongst SMEs

Cyber threats SMEs experience 2025



PERSONAL_EXPERIENCE: From this same list of cyber threats, online security attacks and crimes, can you please tell us which (if any) the organisation you own or work for has experienced in the past six months?
Base: 2025 n=374.

▼▲ Significantly lower/higher than 2024

Not only are cyber attacks on SMEs more prevalent today, they are also having a greater impact

Larger SMEs that experience cyber attacks are more likely to have been severely impacted (21%) compared to smaller SMEs (7%).

Cyber attack severity

	2024	2025
No impact	44%	47%
Minor	42%	▼ 27%
Moderate	17%	23%
Significant	13%	9%
Severe	2%	▲8%

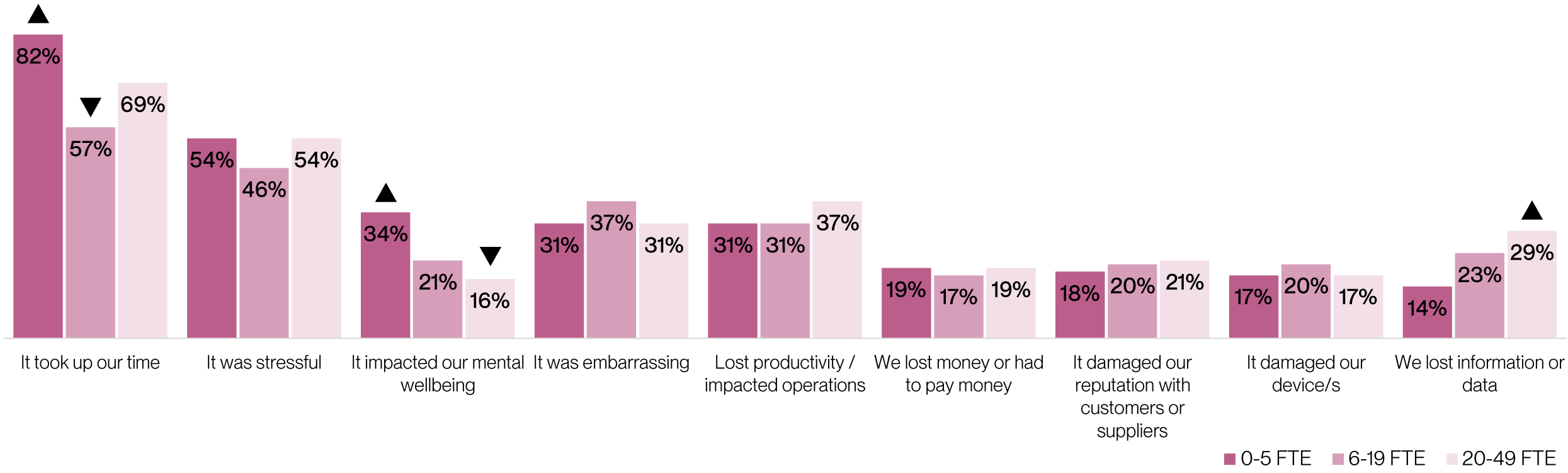
CYBER_SEVERITY: Below are the online security issues the organisation you own or work for has experienced in the past six months. For each, can you please rank how much of an impact the cyber threat, attack or crime had on the organisation?
Base: Experienced cyber attack 2024 n=169; 2025 n=194.

▼▲ Significantly lower/higher than 2024

Personal impacts like time loss and stress are common, and serious threats have bigger organisational consequences

Smaller SMEs are more likely to have their mental wellbeing impacted or to have their time taken up, while larger SMEs are more prone to losing information or data.

Harm caused by cyber attacks in 2024 and 2025



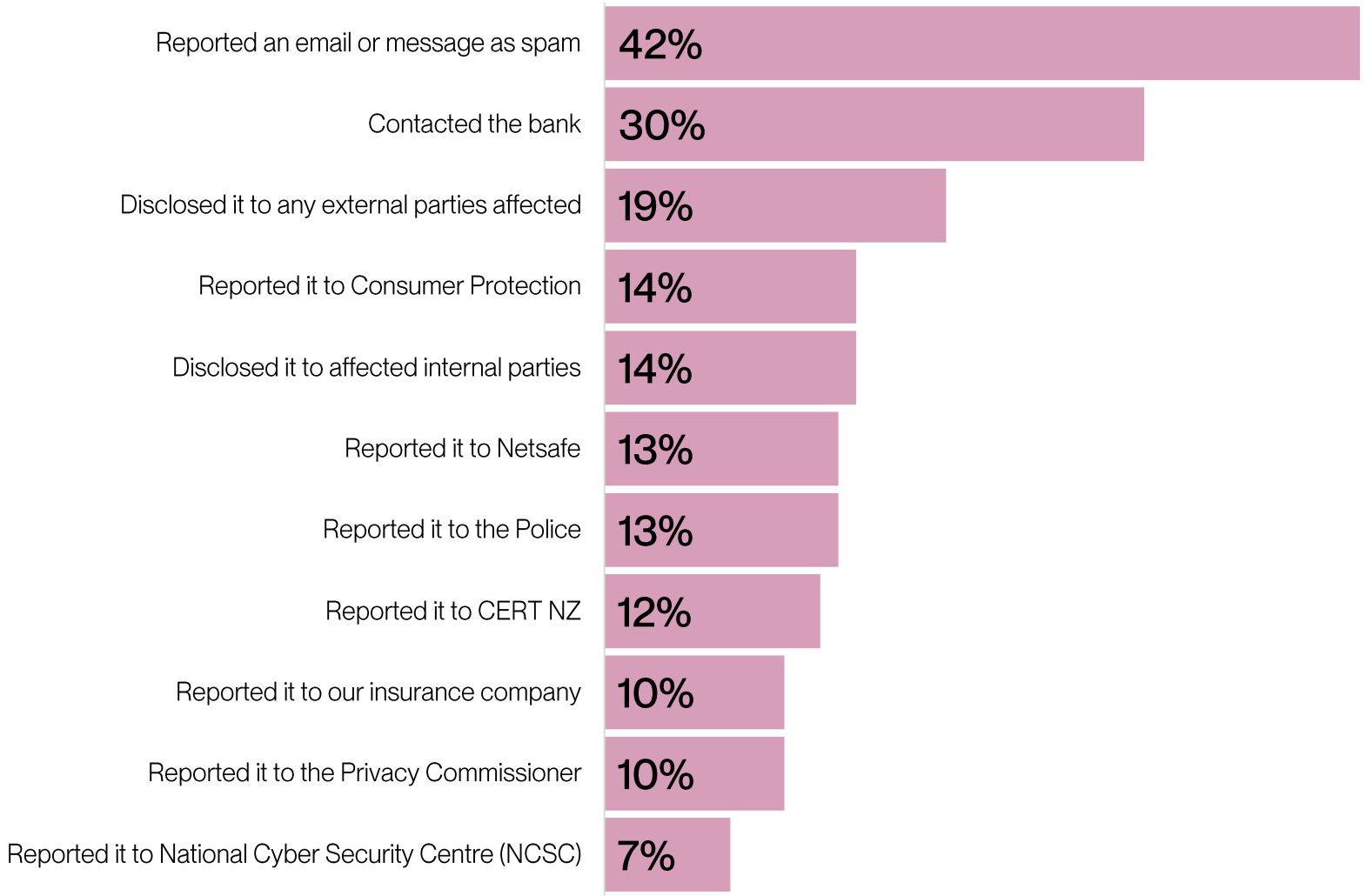
CYBER_HARM: Regarding the cyber threats, online security attacks and crimes your organisation experienced, in what way was your organisation affected?
Base: Experienced cyber attack of minor to severe severity in 2024 or 2025 0-5 FTE n=85; 6-19 FTE n=99; 20-49 FTE n=78.

▼▲ Significantly lower/higher than other groups

Organisations are more likely to contact their bank over government agencies

This is more the case with smaller organisations. 30% of 20-49 FTE organisations reported it to the NCSC, compared to only 5% for 0-5 FTEs.

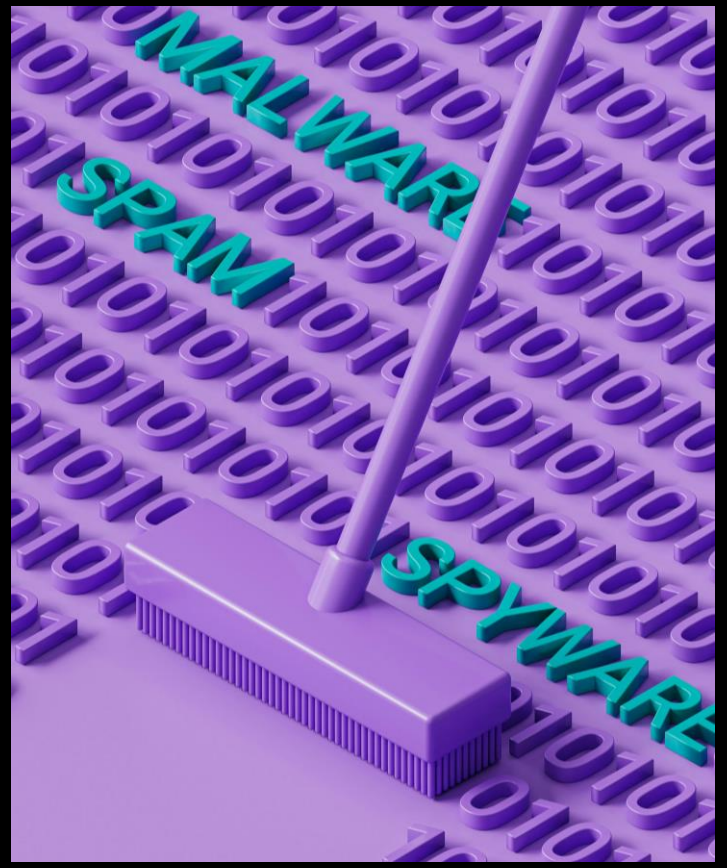
Actions taken after cyber attack 2025



CYBER_ACTIONS: Can you please tell us which actions were taken as a direct result?
Base: Experienced cyber attack n=194.

TRA NCSC

The growing prevalence of attacks highlights the pressing need for varied interventions.

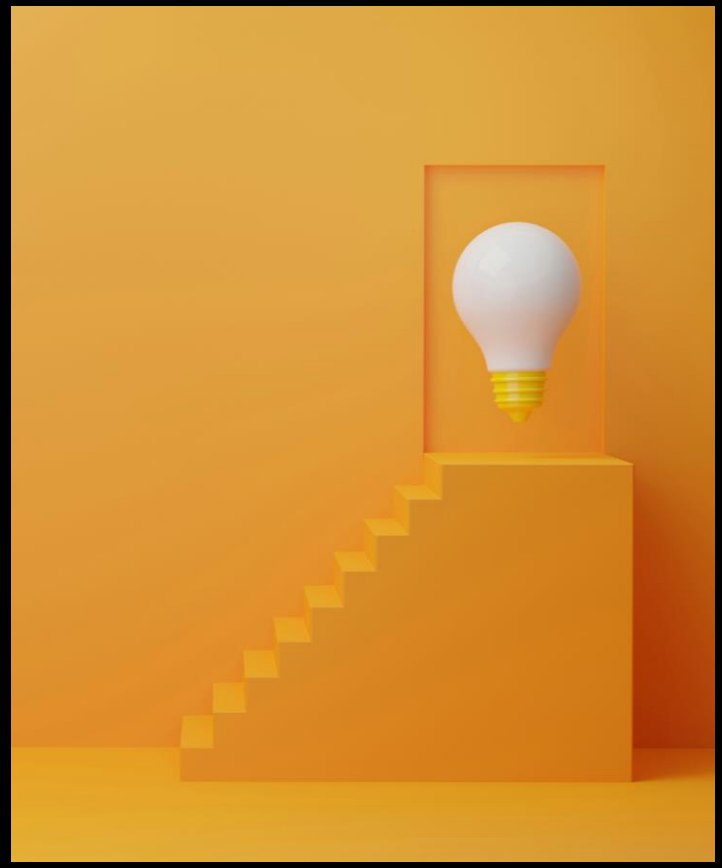


Bringing it all together

4

What have we learned?

- Cyber security looks very different across the SME landscape.
- Implementation of preventative actions has significantly grown, but so has the experience of cyber threats.
- Larger SMEs are more likely to have dedicated systems and IT teams, while smaller ones often operate without formal structures or support, and rely on other sources of advice.
- In order to effectively support the needs of all SMEs, we need to...
    1. Show up in the right channels
    2. Lean into meaningful partnerships
    3. Deliver messages and content that drive the relevance of cyber security



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