SME Cyber Security Behaviour Tracker 2024

June 2024

TRA x NCSC

National Cyber Security Centre

TRA

Background

Small to medium enterprises (SMEs) make up 97% of all businesses in New Zealand - they are the backbone of commerce and are a linchpin of cyber resilience in Aotearoa. The cyber behaviours of SMEs are central to the progression of safe cyber behaviours in Aotearoa.

NCSC plays a key role in providing information and education to this market and, with initiatives like ‘Own Your Online’, aims to improve the cyber resilience of SMEs in New Zealand.

● This study

Overall Objective

Improve cyber understanding and behaviours in the SME market

● This study

Insight Objectives

Understand organisations' knowledge and capability when it comes to cyber security

Determine current threats, issues, and exposure

Measure cyber security attitudes and behaviours

The Approach

Survey

A 10-minute online survey sent out to the SME market (0-49 FTE)* in 2024.

The questionnaire was based on a 2022 study.

The definition of SMEs, survey content, and weighting differed between the two studies, meaning results are not directly comparable.

Content

The survey covered:

- SME demography
- Cyber security motivations and attitudes
- Knowledge
- Cyber security behaviours
- Current threats / issues
- Information sources and brand / agency perceptions

Key Sample

A total sample of n=349 SME IT / operational decision makers was achieved.

Fieldwork ran from the 29th April – 16th May 2024.

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 +/- 5.2%.

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

Summary

Findings

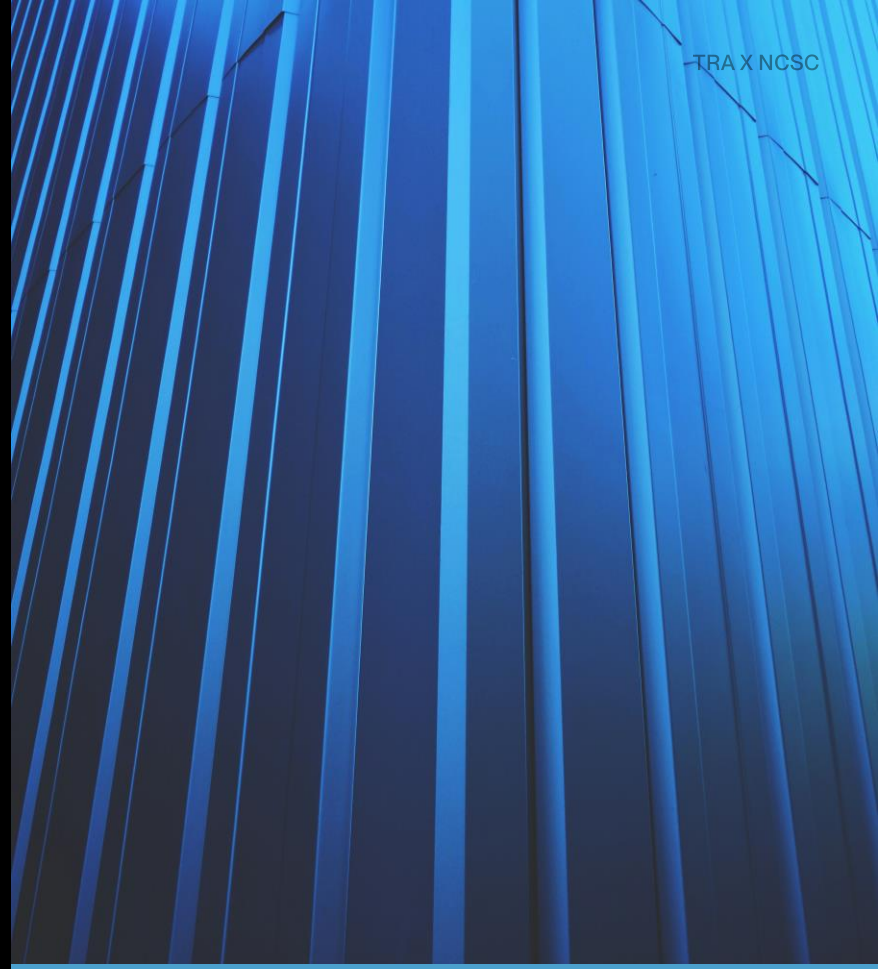
- Current news stories and media activity are helping heighten the importance of cyber security, but many organisations aren't making it a top priority, or don't know where to go or what to do to stop cyber-attacks
- Basic preventative actions have become normalised; however, more future-looking actions aren't as common – an ongoing mindset of vigilance is the next step for many
- There is a portion of cyber threats that, when experienced, are severe and take a significant toll
- SMEs would seek out a government agency first for cyber security issues, but don't know who that is, or how they're relevant

Jobs to be done

1. Drive relevance of the cyber security issue among SMEs
2. Making sure SMEs have access to trusted sources
3. Create a mentality of ongoing vigilance among SMEs
4. Promote 'being prepared' to encourage SMEs on their journeys

Agenda

The current landscape



1

SMEs are crucial to Aotearoa's overall cyber resilience

43%

of cybercrime is targeted at small businesses

$173k

The average cost of a data breach for a SME

Source: Both figures retrieved from One NZ media release 2023.

There's a need to identify current SME cyber security beliefs, motivations, and behaviours, in order to support SMEs

Let's take a look at the current environment they're operating in...

Cyber security has been in the spotlight for New Zealanders and organisations recently

There are many examples of recent cyber security breaches...

- MediaWorks hack seeing 2.5m New Zealanders' data stolen
- NZ Parliament was the target of a cyber hack in 2021
- Among smaller businesses, Mahony Horner Lawyers in Wellington seeing disgruntled clients due to a cyber incident

And the topic has generally taken on heightened relevance...

- ASB's recent One Step Ahead of Scammers campaign ranking as New Zealand's favourite ad

This is obviously touching on something that is highly relevant, topical, and emotionally involving for people.

Source: Radio New Zealand; Reuters; The Record from Recorded Future News: Cyber Security News; NZ Herald; TRA - New Zealand's Favourite Ads.

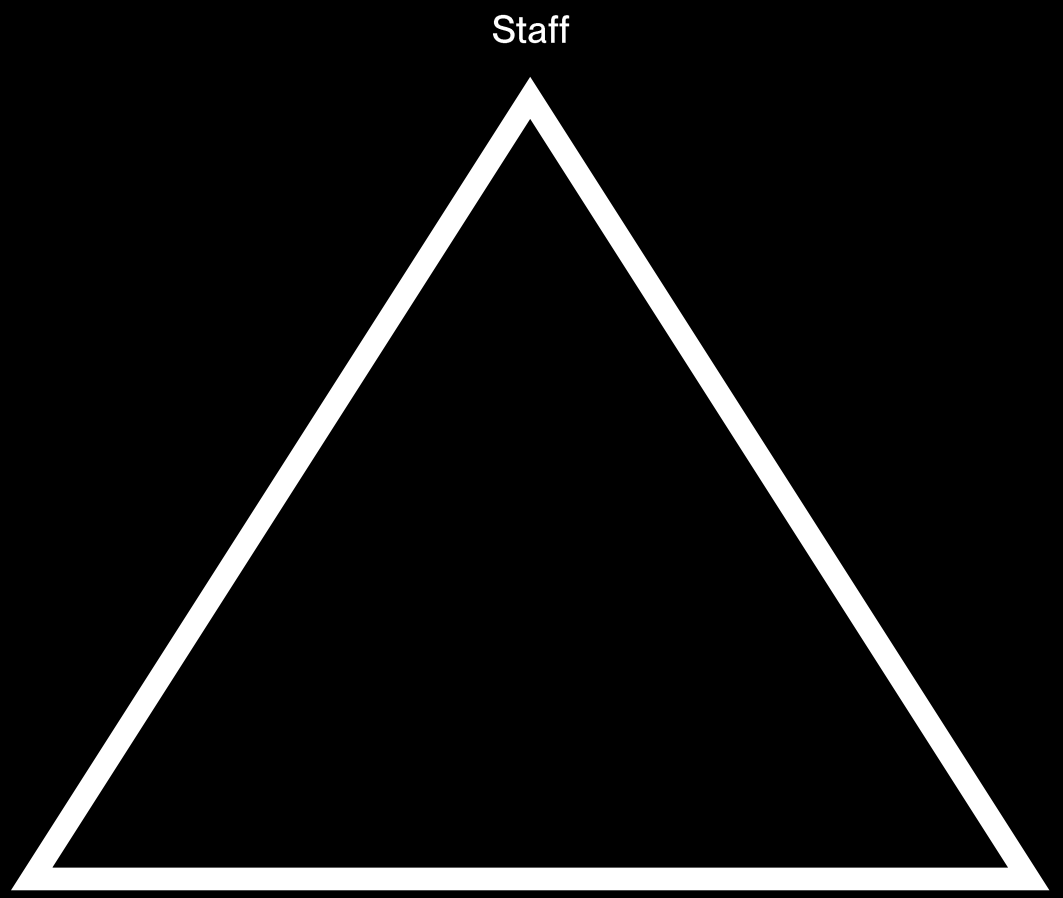
Implication

SME decision makers will have been exposed to cyber security conversations

These people do not turn off their ‘business brain’ when interacting with the world. Everything integrates together.

This will have dialled up the relevance of the issue to SMEs.

We know SMEs are wearing many different hats



“My staff mean everything to me. We primarily recruit based on cultural fit... As a result the team are amazing together, and I find myself acting in more of a leadership role - rather than micromanaging them.”

“**Treat every client** like they are your Mum and Dad – they are special and deserve respect at all times.”

Source: TRA Listening Project 2015.

Cyber security is the third biggest issue of concern for SME decision makers

It sits in the top three business concerns, in a longer list of issues that SMEs are always juggling.

SME concerns

3rd

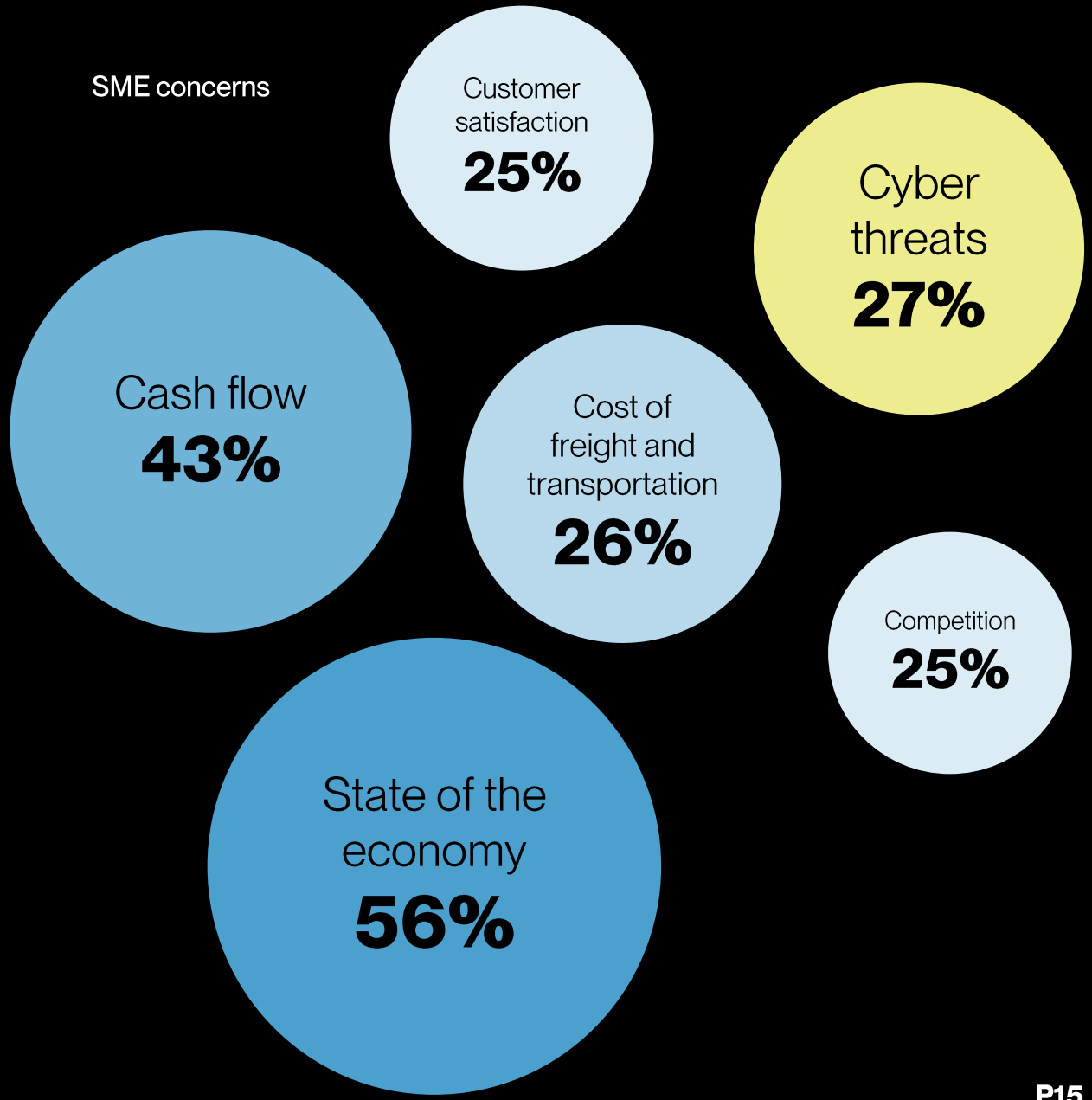
Highest ranking business concern

Cyber threats **27%**

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: Total n=349.

But it's overshadowed by financial concerns, and sits alongside other key concerns

This is reflective of the fact that SMEs have many hats to wear at once.

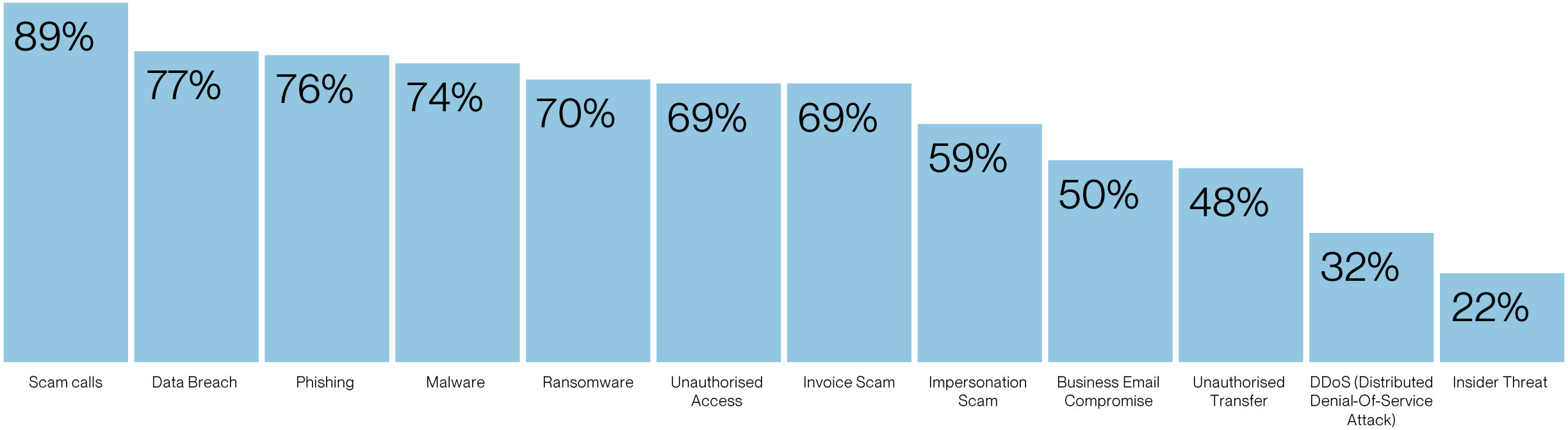


LIFE_CONCERNS: From this list of topics below, can you please tell us which (if any) are currently a concern for the organisation you work for?
Base: Total n=349.

In terms of the threats that could impact them, most SMEs have an understanding of basic cyber threats

There's at least a surface level understanding of the threats their organisations could be exposed to.

Awareness of cyber/online threats, attacks and crime

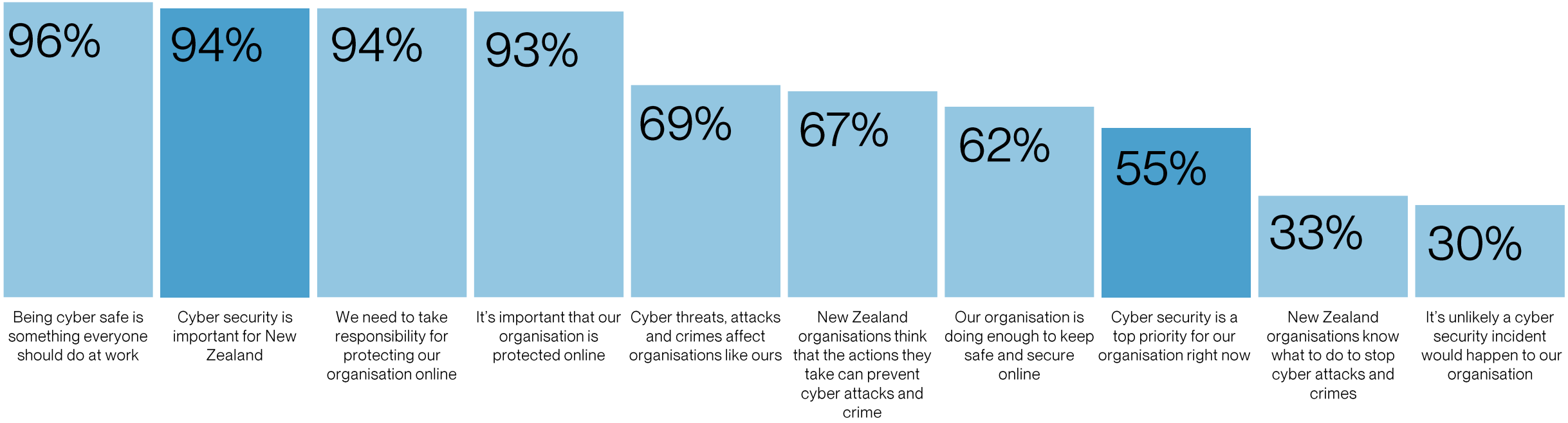


CYBER_AWARE: From this list of cyber threats, online security attacks and crimes, can you please tell us which (if any) you are aware of?
Base: Total n=349.

SMEs acknowledge the importance of being secure online, but fewer describe it as a top organisational priority

Nearly all say cyber security is important for New Zealand, but only 55% describe it as a top priority for their organisation specifically.

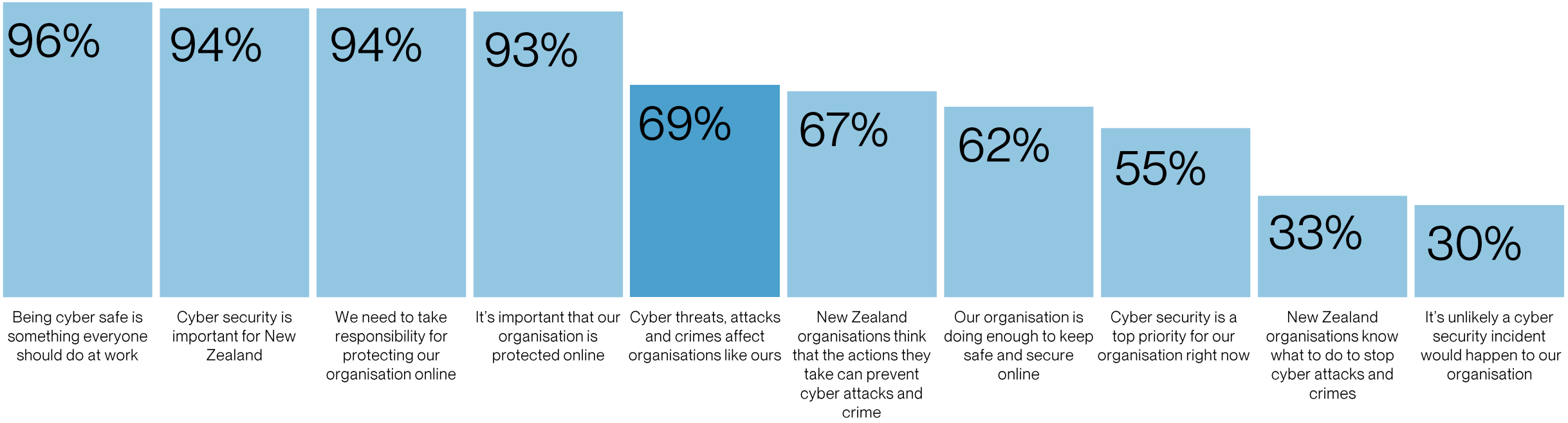
Cyber security beliefs
(Strongly agree / agree)



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=349.

And many SMEs don't expect a cyber attack to affect them

Cyber security beliefs
(Strongly agree / agree)



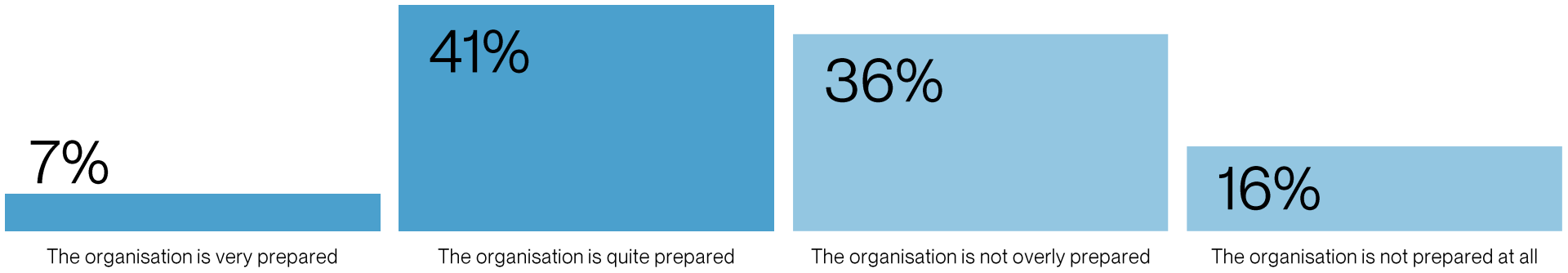
TRA // National Cyber Security Centre

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=349.

Less than half of SMEs would describe their organisation as prepared (48%)

And only 7% would say they are very prepared.

Cyber security preparedness



PREPARED: How prepared is the organisation when it comes to preventing a cyber security breach?
Base: Total n=349.

Implication

SMEs don’t know how to respond to the importance of cyber security, meaning they feel less prepared than they should

SMEs are aware of the importance of the issue.

However, they wear many ‘hats’ and have other pressures to consider.

Cyber security behaviours

2

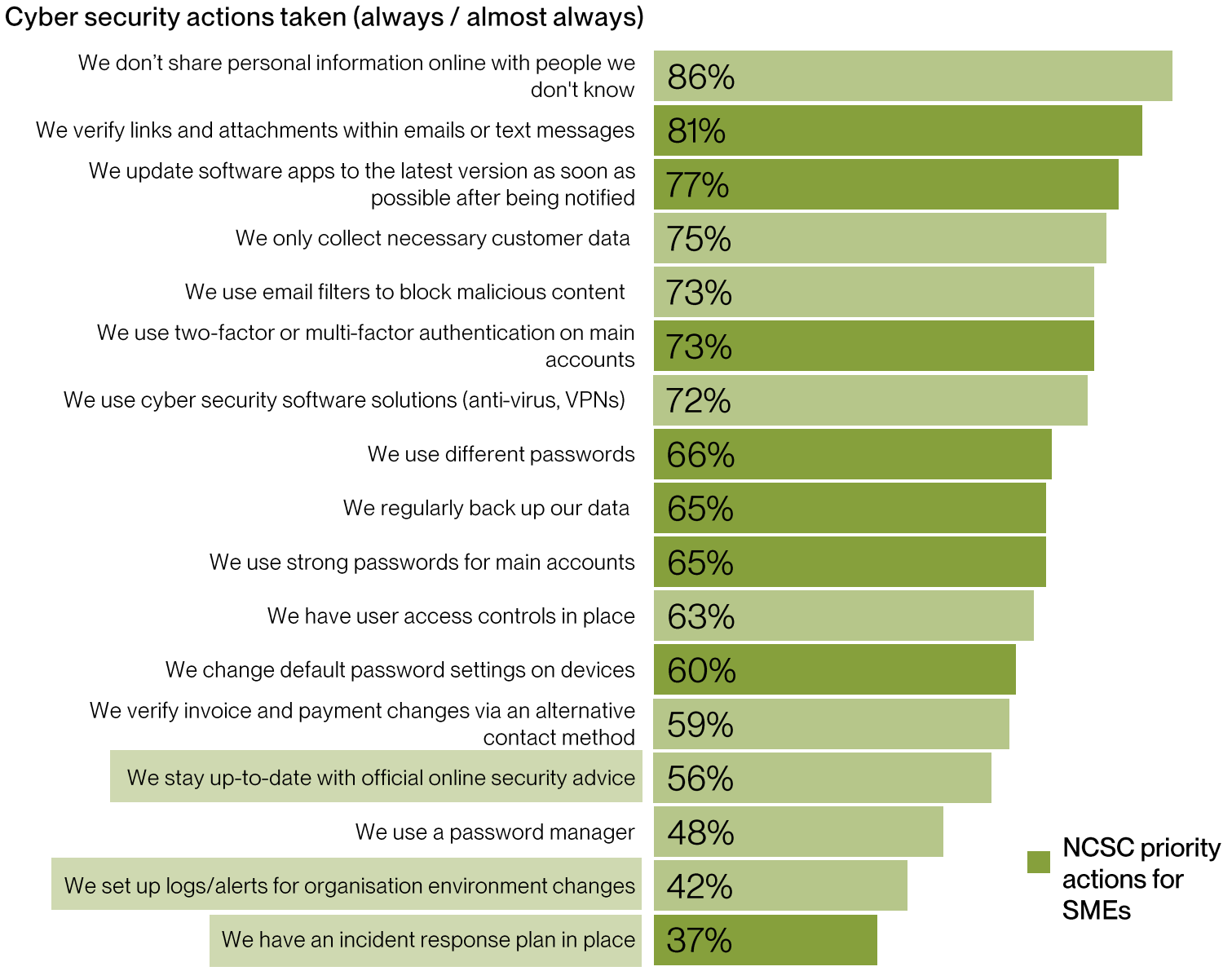
Many preventative actions have become normalised

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: Total n=349.

TRA // National Cyber Security Centre

But some of the more future-oriented actions aren't as common

Just over half are staying up to date with the latest online security advice and only a third have an incident response plan in place.



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: Total n=349.

TRA // National Cyber Security Centre

SMEs who take cyber security actions are more likely to have recognised the personal relevance to them

Top five motivators for those taking the following cyber security actions (always / almost always)

1. We update software apps to the latest version as soon as possible after being notified
2. We use two-factor or multi-factor authentication on main accounts
3. We regularly back up our data

The safety and security of our information online is important to us	**61%**
We understand that cyber security is our responsibility	**52%**
We know how to do the right thing to keep secure online	**42%**
We're worried about cyber security breaches happening to us	**39%**
It does not take long to implement cyber security measures to be secure online	**38%**

WHY_MOTIVATORS: For behaviours where you answered always or almost always, please tell us what motivates your organisation into doing those.
Scores shown are the average motivation scores across those taking the NCSC listed actions actions always / almost always.
Base: NCSC priority actions always / almost always n=308.

But for some, even basic actions don't happen, due to complacency and time constraints

% Not taking cyber security actions

35%
Don't regularly back up their data

27%
Don't regularly use two-factor or multi-factor authentication

23%
Don't regularly update software apps to the latest version

Top five barriers for those not regularly taking NCSC priority cyber security actions

We keep forgetting to	25%
We feel we are already doing enough to protect ourselves against cyber threats	24%
We don't have time	17%
We don't know how to do it / it's too complicated	16%
We don't know what to do	14%

TRA // National Cyber Security Centre

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 sometimes / rarely / never.
WHY_BARRIERS: For behaviours where you answered sometimes, rarely, or never, please tell us what is stopping your organisation from doing that action.

Scores shown are the average barrier scores across those taking the NCSC priority actions sometimes / rarely / never.
Base: Total n=349; NCSC listed actions taken sometimes / rarely / never n=162.

SMEs are in three distinct groups on their cyber security journeys

1. The Cyber Complacent

Low level of care about cyber security

Preventative actions taken always / almost always:

Less than 10 out of 17

40% of SMEs

- Missing some basic actions
- Less likely to believe cyber threats affect organisations like theirs
- One third of this group would say the organisation is not prepared at all for a cyber security breach

2. The Cyber Compliant

Moderate level of care about cyber security

Preventative actions taken always / almost always:

10-14 out of 17

28% of SMEs

- Taking most basic actions, but not the more proactive actions
- Believe cyber security is important, but still not confident NZ organisations know what to do

3. The Cyber Compelled

High level of care about cyber security

Preventative actions taken always / almost always:

15+ out of 17

32% of SMEs

- Taking nearly all actions, including the more proactive actions (e.g. staying up to date with the latest cyber security info)
- Believe cyber security is important, and more confident in what to do

*See appendix for breakdown of specific beliefs and actions of each group.

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: Total n=349.

Implication

When basic actions have become normalised, the next step is an ongoing mindset of vigilance

For the Cyber Complacent group, motivation is the key issue even for basic actions. They don't see how an organisation like theirs could be impacted.

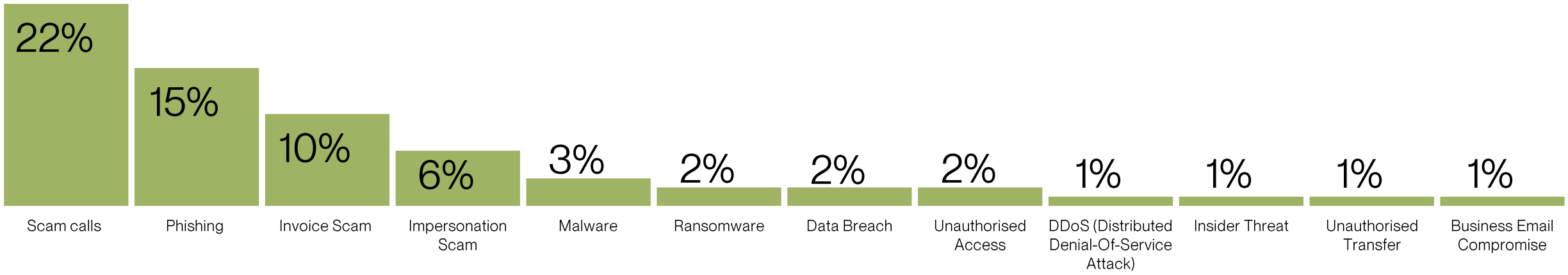
For the Cyber Compliant, there's a lack of knowledge and confidence in the next actions they can take to provide additional layers of protection.

The Cyber Compelled by contrast, are motivated, and know what they need to do in order to keep their organisation safe.

36% of SMEs experienced at least one cyber attack in the last six months

Scam calls, phishing, and invoice scams are the main threats experienced.

Cyber threats SMEs experience



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: Total n=349.

For a quarter of SMEs experiencing cyber attacks, there's been a moderate impact, or worse

We also see a link between threat exposure and taking new safety actions.

Cyber attack severity

14%

Severe / significant

11%

Moderate

- 9 in 10 of those impacted severely / significantly found this situation stressful, and for two-thirds it impacted their wellbeing.
- 57% of this group have taken new actions to keep themselves more secure online in the last six months, compared to 27% for those that haven't experienced a severe / significant cyber attack.

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?
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 n=169; Not experienced severe / significant cyber attack n=311; cyber harm was severe / significant n=38.

Implication

Cyber security incidents have at least a moderate impact on a quarter of SMEs who experience them

This illustrates the importance of there being an ongoing mindset of vigilance among SMEs.

And for all to understand the specific relevance to their organisation, and have the confidence to know how to futureproof themselves.

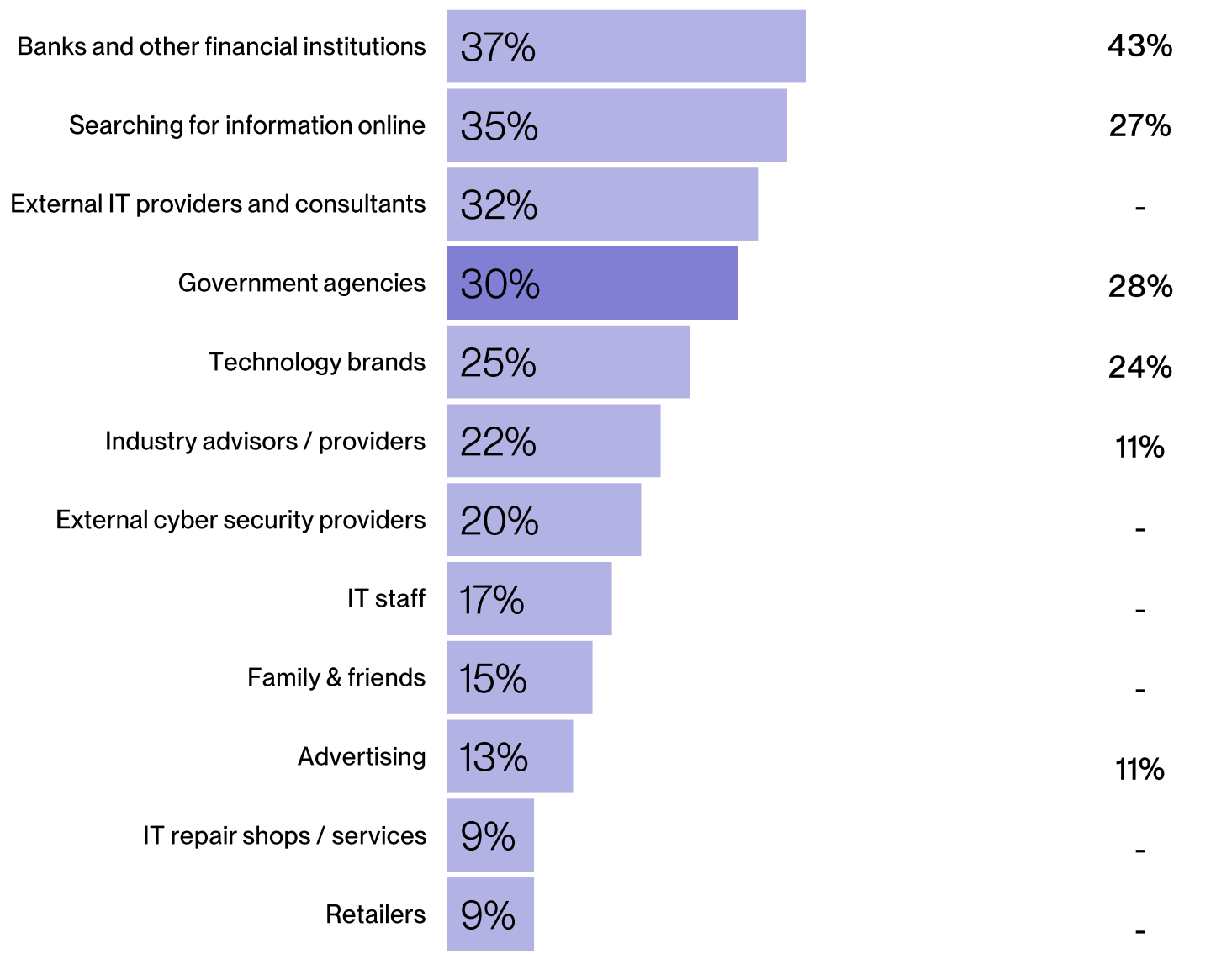
Trusted sources of information

3

In terms of where SMEs go for cyber security information, banks are number one

Government agencies sit in fourth place, still in the top tier of sources.

SMEs are searching online for specific cyber information more so than consumers, indicating there is a specific need when it comes to information and advice.

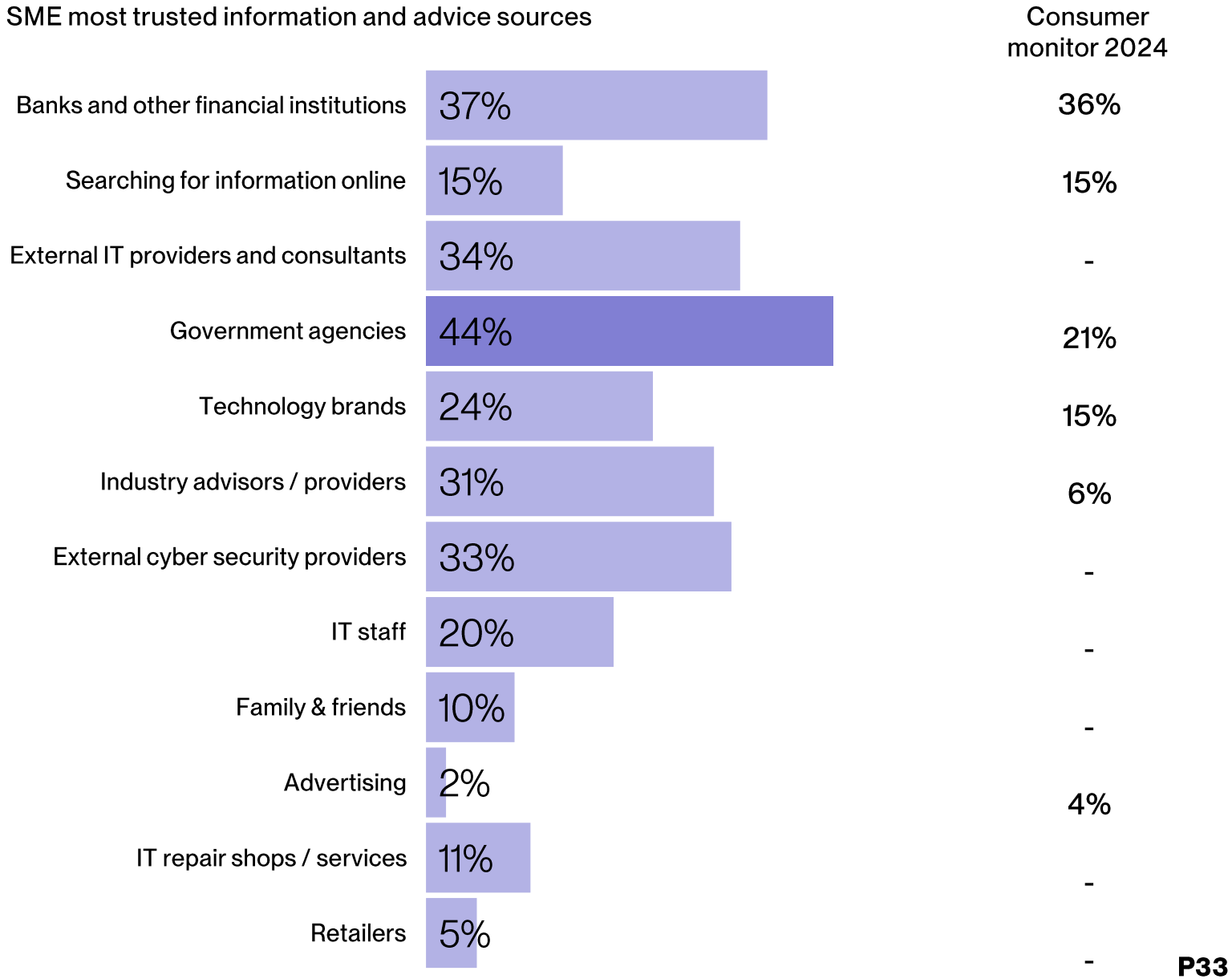


INFO_SOURCE: Where does your organisation currently get cyber security information and / or advice from?
Base: Total n=349.

TRA // National Cyber Security Centre

However, government agencies are the most trusted source for information

Sitting well ahead of banks, online searches and external IT providers.



INFO_RANKING: And from that same list of information sources, please rank the top three most trusted sources for the organisation.
Base: Total n=349.

TRA // National Cyber Security Centre

Implication

Many SMEs would go to a government agency for cyber security information

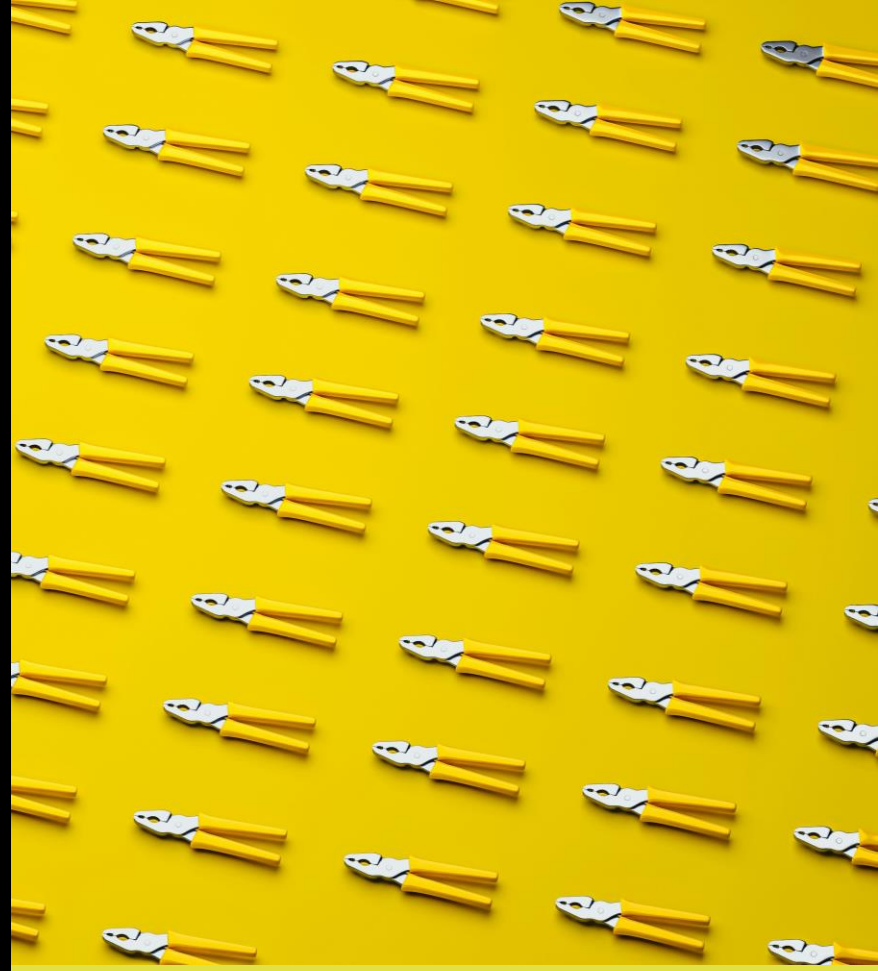
There is trust in government agencies when it comes to cyber security. However, banks and online search behaviour is the predominant behaviour for organisations in New Zealand.

Own Your Online could play a more prominent role for information and education for SMEs.

Implication

There’s trust in government around cyber security, but there is significant opportunity to grow awareness and relevance

The jobs to be done



4

Lessons learned

- Current news stories and media activity is helping heighten the importance of cyber security, but many organisations aren't making it a top priority, and don't know where to go or what to do to stop cyber attacks
- Basic preventative actions have become normalised; however, more future-looking actions aren't as common – an ongoing mindset of vigilance is the next step for many
- There is a portion of cyber threats that, when experienced, are severe and take a significant toll
- SMEs would seek out a government agency first for cyber security issues, but don't know who that is, or how they're relevant

The jobs to be done

1. Drive relevance of the issue among SMEs

Many understand the importance of the issue, but the ‘Cyber Complacent’ group can’t see it impacting a business like theirs directly.

The jobs to be done

2. Making sure SMEs have access to trusted sources, like Own Your Online

A lot of SMEs have good intentions and are ‘compliant’ with the basic actions they know to take. They lack the confidence to do more though.

The jobs to be done

3. Create a mentality of ongoing vigilance

The gold standard is where SMEs are ‘compelled’ to take proactive action in cyber security.

This vigilance is the long-term mindset that we want to drive among all SMEs. Where they are keeping up to date with information, processes and potential threats, even as they evolve.

Appendix

Cyber security beliefs by SME group

	The Cyber Complacent	The Cyber Compliant	The Cyber Compelled
It's important that our organisation is protected online	86% ▼	95%	99% ▲
Cyber threats, attacks and crimes affect organisations like ours	52% ▼	71%	87% ▲
Cyber security is important for New Zealand	91%	99% ▲	94%
It's unlikely a cyber security incident would happen to our organisation	40%	25%	23%
We need to take responsibility for protecting our organisation online	90%	99% ▲	96%
Our organisation is doing enough to keep safe and secure online	45% ▼	63%	82% ▲
Being cyber safe is something everyone should do at work	94%	98%	97%
Cyber security is a top priority for our organisation right now	27% ▼	64%	83% ▲
New Zealand organisations know what to do to stop cyber attacks and crimes	20% ▼	24%	58% ▲
New Zealand organisations think that the actions they take can prevent cyber attacks and crime	59%	75%	69%

▼▲ Significantly lower/higher compared to other groups

BELIEFS: Please look at the following statements and indicate how strongly you agree or disagree with each of these... (agree / strongly agree).
Base: The Cyber Complacent (less than 10 preventative actions taken) n=111; The Cyber Compliant (10-15 preventative actions taken) n=107;
The Cyber Compelled (15+ preventative actions taken) n=131.

Cyber security actions taken by SME group

	The Cyber Complacent	The Cyber Compliant	The Cyber Compelled
We don't share personal information online	71% ▼	93%	100% ▲
We verify links and attachments within emails	58% ▼	92% ▲	100% ▲
We update software apps to the latest version	54% ▼	86%	97% ▲
We only collect necessary customer data	47% ▼	88% ▲	100% ▲
We use email filters to block malicious content	42% ▼	87% ▲	100% ▲
We use two-factor or multi-factor authentication	47% ▼	81%	99% ▲
We use cyber security software solutions (anti-virus, VPNs)	40% ▼	88% ▲	98% ▲
We use different passwords	36% ▼	76%	95% ▲
We regularly back up our data	29% ▼	76%	100% ▲
We use strong passwords	40% ▼	66%	96% ▲
We have user access controls in place	21% ▼	81% ▲	100% ▲
We change default password settings on devices	28% ▼	61%	99% ▲
We verify payment changes via an alternative contact method	22% ▼	66%	99% ▲
We stay up-to-date with official online security advice	20% ▼	63%	94% ▲
We use a password manager	20% ▼	48%	84% ▲
We set up logs/alerts for organisation environment changes	10% ▼	30%	91% ▲
We have an incident response plan in place	6% ▼	15% ▼	94% ▲

▼▲ Significantly lower/higher compared to other groups

TRA // National Cyber Security Centre

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: The Cyber Complacent (less than 10 preventative actions taken) n=111; The Cyber Compliant (10-15 preventative actions taken) n=107; The Cyber Compelled (15+ preventative actions taken) n=131.

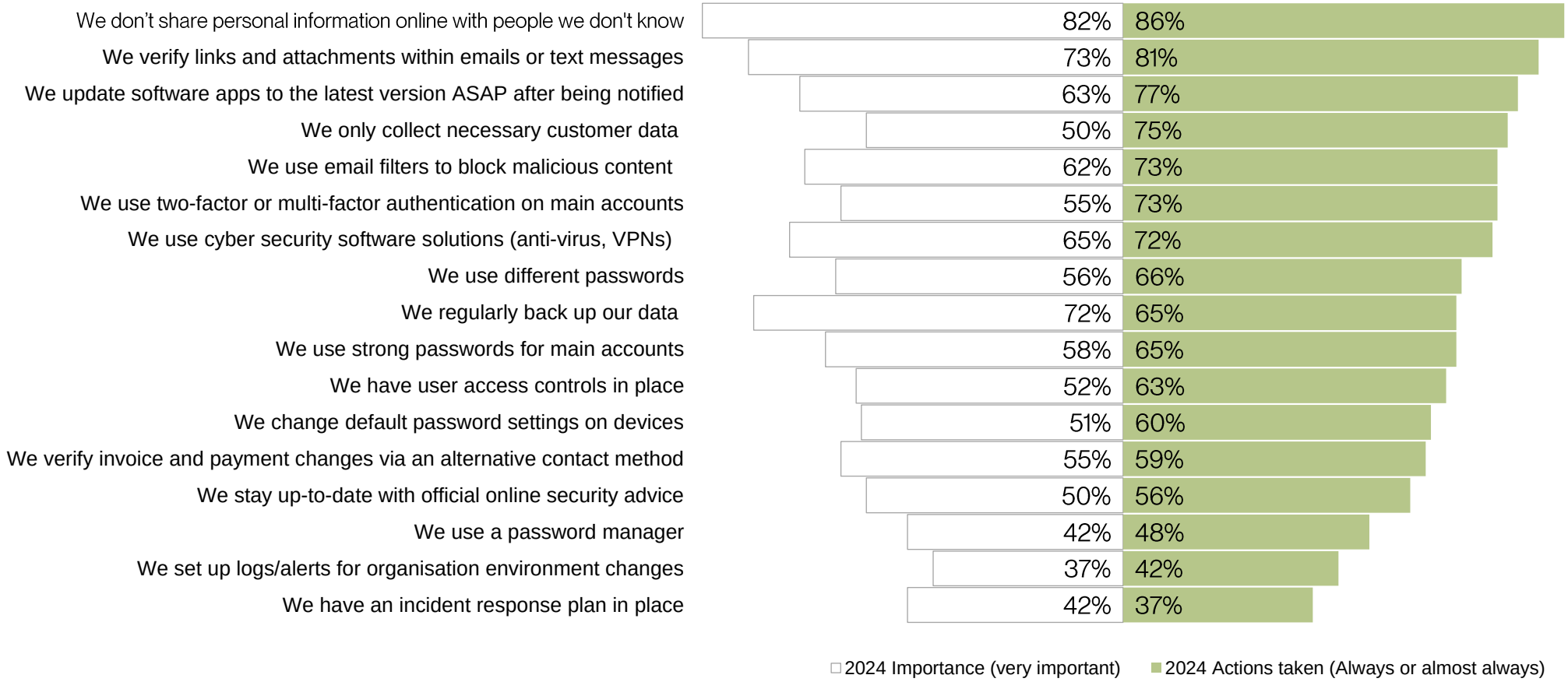
Cyber security attitudes and behaviours by SME size

	0-5 employees	6-19 employees	20-49 employees
Cyber security behaviours and preparedness			
New behaviours undertaken in the last 6 months	28%	36%	44%
Preparedness: the organisation is very / quite prepared	46% ▼	65%	83% ▲
Cyber security actions taken always / almost always (only significant differences shown)			
We verify invoice and payment changes via an alternative contact method	58%	60%	86% ▲
We have an incident response plan in place	34% ▼	59% ▲	67% ▲
We set up logs/alerts for organisation environment changes	40% ▼	58%	71% ▲
Beliefs (only significant differences shown)			
Cyber security is important for New Zealand (agree strongly / agree)	95%	83% ▼	96%
Being cyber safe is something everyone should do at work (agree strongly / agree)	97% ▲	86% ▼	95%
New Zealand organisations know what to do to stop cyber attacks and crimes (agree strongly / agree)	30% ▼	58% ▲	62% ▲

▼▲ Significantly lower/higher compared to other groups

NEW_BEHAV: In the past six months, has your organisation taken any new actions to keep yourself more secure online?
PREPARED: How prepared is the organisation when it comes to preventing a cyber security breach?
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.
BELIEFS: Please look at the following statements and indicate how strongly you agree or disagree with each of these... (strongly agree / agree).
Base: 0-5 employees n=165; 6-19 employees n=109; 20-49 employees n=74.

Cyber security actions taken always / almost always and the importance of the action



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.
CYBER_IMPORTANCE: From this list can you please tell us how important you believe these are for your organisation? (very important)
Base: Total n=349.