



Cyber Security Research

Business Survey Findings



**Consumer
Protection**



This document was prepared by Colmar Brunton on behalf of CERT NZ, Consumer Protection, and The Ministry of Business, Innovation and Employment.

ISBN 978-1-99-100803-9

March 2021

Disclaimer

This document is a guide only. It should not be used as a substitute for legislation or legal advice. CERT NZ, Consumer Protection, and/or The Ministry of Business, Innovation and Employment is not responsible for the results of any actions taken on the basis of information in this document, or for any errors or omissions.

©Crown Copyright

The material contained in this report is subject to Crown copyright protection unless otherwise indicated. The Crown copyright protected material may be reproduced free of charge in any format or media without requiring specific permission. This is subject to the material being reproduced accurately and not being used in a derogatory manner or in a misleading context. Where the material is being published or issued to others, the source and copyright status should be acknowledged. The permission to reproduce Crown copyright protected material does not extend to any material in this report that is identified as being the copyright of a third party. Authorisation to reproduce such material should be obtained from the copyright holders.



CONTENTS



1	Background and objectives	4
2	Methodology	6
3	Executive summary	8
4	Digital presence of small businesses	10
5	Website capabilities	15
6	Cyber security awareness and knowledge	19
7	Perceptions of cyber security	24
8	Cyber security attitudes	27
9	Cyber security behaviour amongst online businesses	31
10	Impact of COVID-19 on e-commerce	35
11	Appendix	39

Background and objectives



BACKGROUND

This research is the result of a partnership between CERT NZ and the Consumer Protection team.

CERT NZ and the Consumer Protection team have partnered to work on a joint campaign initiative that focused on building cyber security confidence and capability among New Zealanders and those who shop online.

While CERT NZ has done some audience profiling to develop personas, it has not done any formal benchmarking or monitoring to better understand its audiences, including small businesses.

The purpose of this research is to help CERT NZ and Consumer Protection to better understand the landscape of where small businesses are at in terms of cyber security.

OBJECTIVES

Research objectives include:

- Awareness of cyber security
- Attitudes to cyber security
- Actions and intentions around cyber security
- The extent to which small businesses are trading online
- How COVID-19 has impacted online trading



Methodology



METHODOLOGY



An online survey was run across two waves. The first wave serves as a benchmark while the second wave enables a comparison with the benchmark results.

Comparisons are made between the pre and post survey waves, for those questions asked in both waves.

We also undertake analysis at the total level (i.e. combining the pre-wave and post-waves). This provides a larger sample size to determine how different groups of businesses feel and act around cyber security and online commerce.



PRE - WAVE

Sample size:
n=508

Fieldwork dates:
3 July to 12 July, 2020

POST - WAVE

Sample size:
n=501

Fieldwork dates:
30 November to 13 December, 2020



The sample population for the survey was small businesses with 0 to 19 employees. Weighting was applied to correct for the over-sampling of businesses with 0 to 19 employees. The results were also weighted by sector category.

Both changes between survey waves and subgroup differences are reported if they are statistically significant at the 95% confidence level.

The maximum margins of error associated with the results are shown below. These assume a survey result of 50%. The closer a result is to the absolutes of 0% or 100%, the lower the margin of error.

Total	±4.3%
--------------	--------------

PRE - WAVE / POST - WAVE	±3.1%
---------------------------------	--------------

Survey respondents were sourced from Colmar Brunton's online panel.

Executive summary



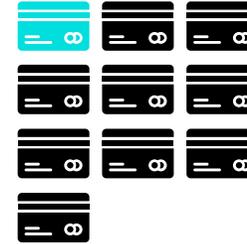
Executive summary

DIGITAL PRESENCE



6 in 10 small businesses have a digital presence.

Cyber security is not a deterrent for those who do not yet have a presence



1 in 10 small businesses surveyed have a website that enables e-commerce

This has the potential to almost double, with many online businesses considering this.

ACTION ON CYBER SECURITY

Cyber security is on the radar of small businesses, but a notable minority lack the motivation to act, and there is a recognition they should be doing more.

83%

83% think it's important for businesses to actively protect their website. But only...

54%

54% think their business is concerned about cyber security. And...

58%

58% think their business should do more to keep cyber secure.

PERCEPTIONS OF CYBER SECURITY

There is more to be done to build understanding on cyber security and to build capability.

31%

At least a good understanding of cyber security

54%

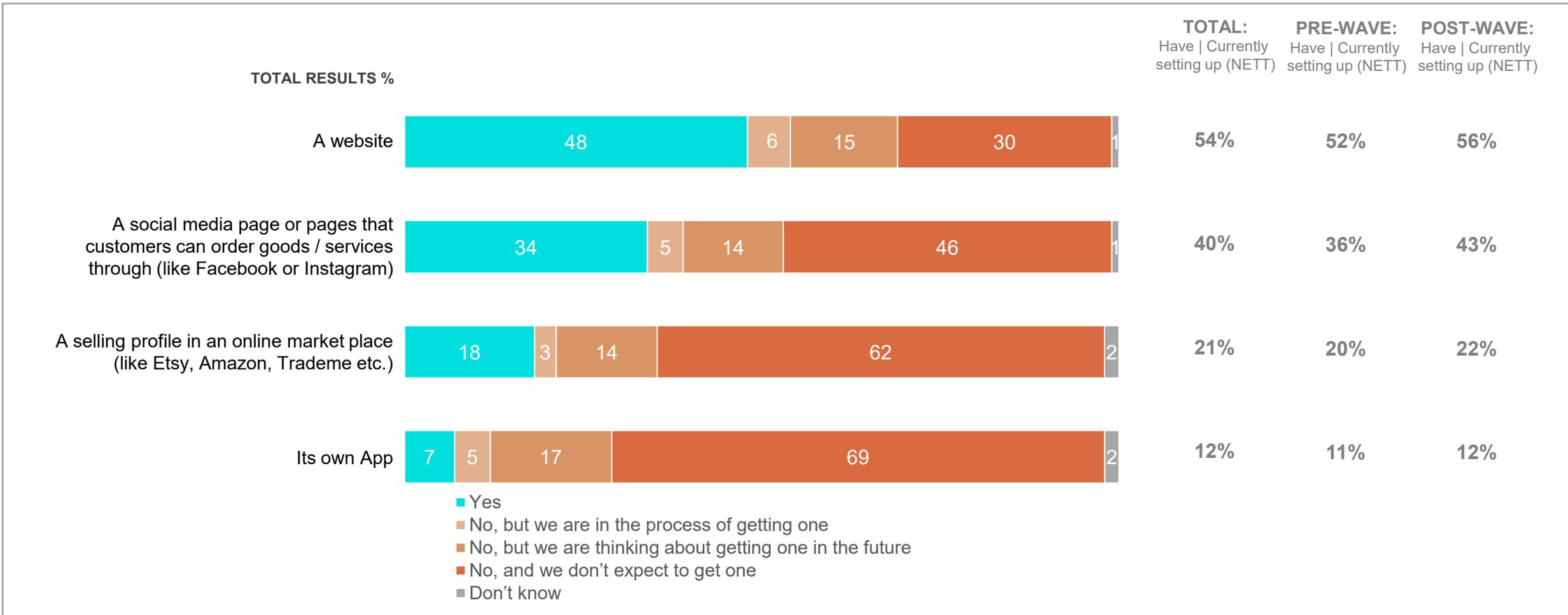
Think business is capable of keeping cyber safe

Digital presence of small businesses



Businesses' digital presence

Almost half of small businesses surveyed across the two waves have a website, while a further six percent are in the process of getting one. One in three small businesses are using social media pages as a way to sell to their goods. There is also notable investment in apps; seven percent currently have one, but a further five percent are in the process of getting one, while 17% are thinking about it.



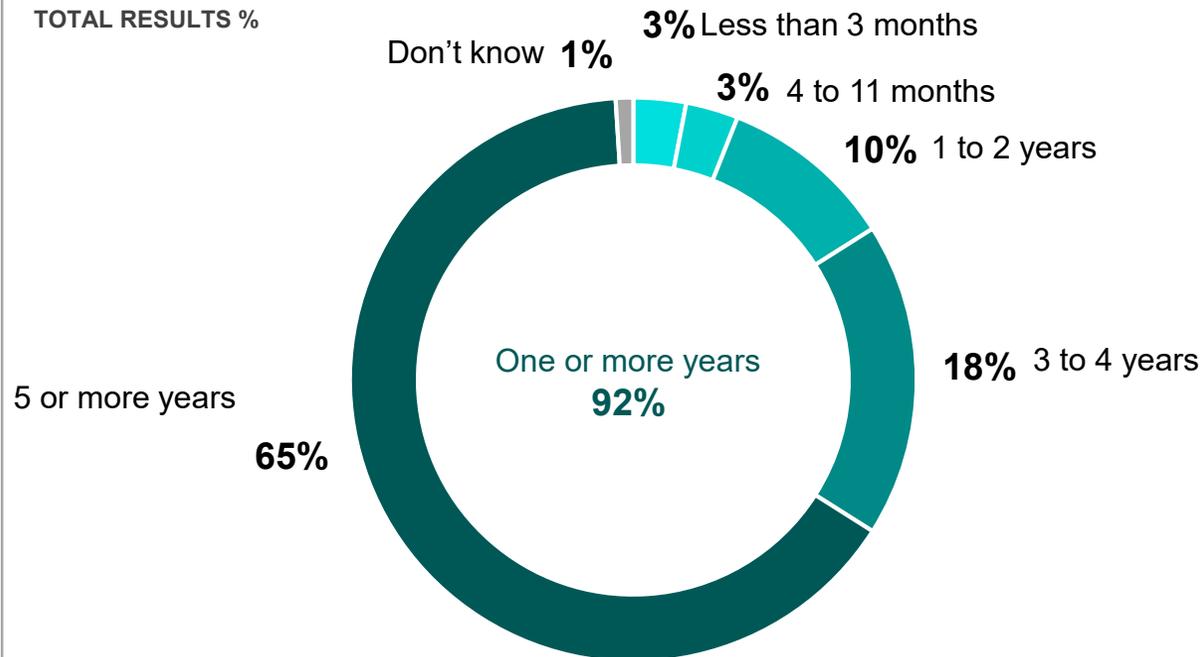
Base: All SMEs (Total SMEs n=1,009; Pre wave n=508; Post wave n=501)
 Source: A3. Does your business have...?

When and how the website was built

Most small businesses with a website, have had it place for at least one year, with six percent having put a website in place in the 12 months prior to completing the survey. Around half of all small businesses with a website had it custom built, while 44% say it was mainly or completely an 'off the shelf' product.

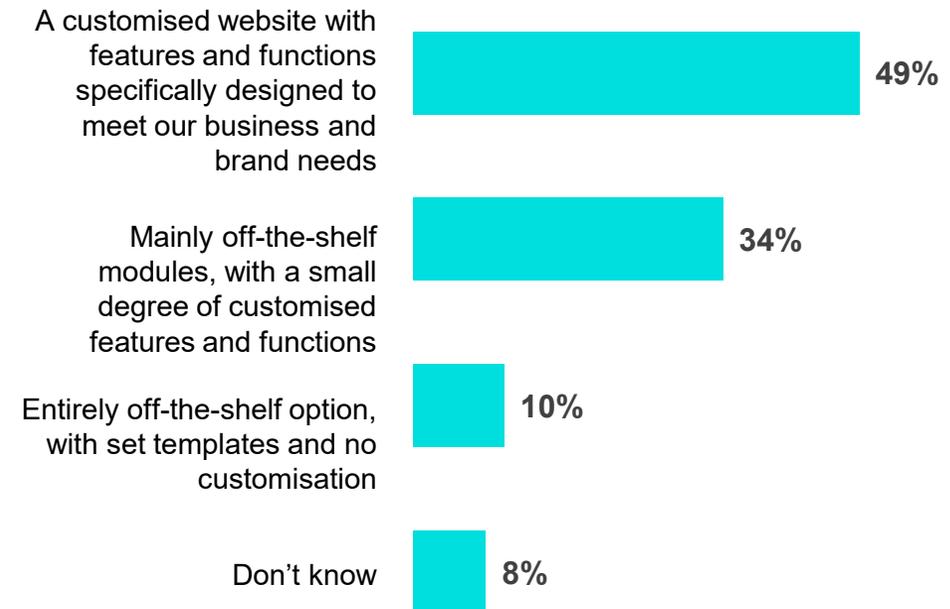
WHEN THE WEBSITE WAS BUILT

TOTAL RESULTS %



HOW THE WEBSITE WAS BUILT

TOTAL RESULTS %



Businesses without a digital presence

Nearly two in five businesses (38%) do not have, or are planning to have, a digital presence.

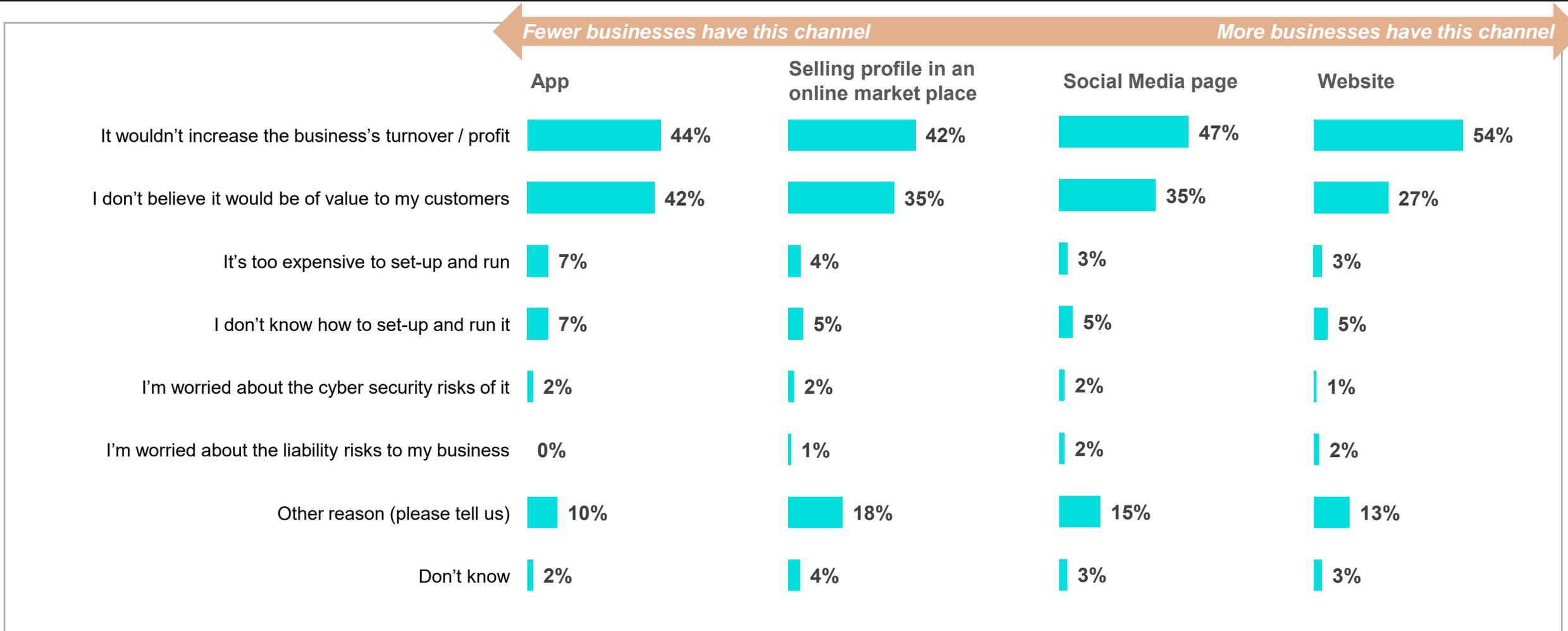
38%

of businesses
do not have
a digital
presence



Barriers to having a digital presence

The main reasons why some small businesses do not want to go online is that they don't think it will help their bottom line, and that it will not be of value to their customers. Very few (one to two percent) say that concerns over cyber security deters them from having a digital presence.

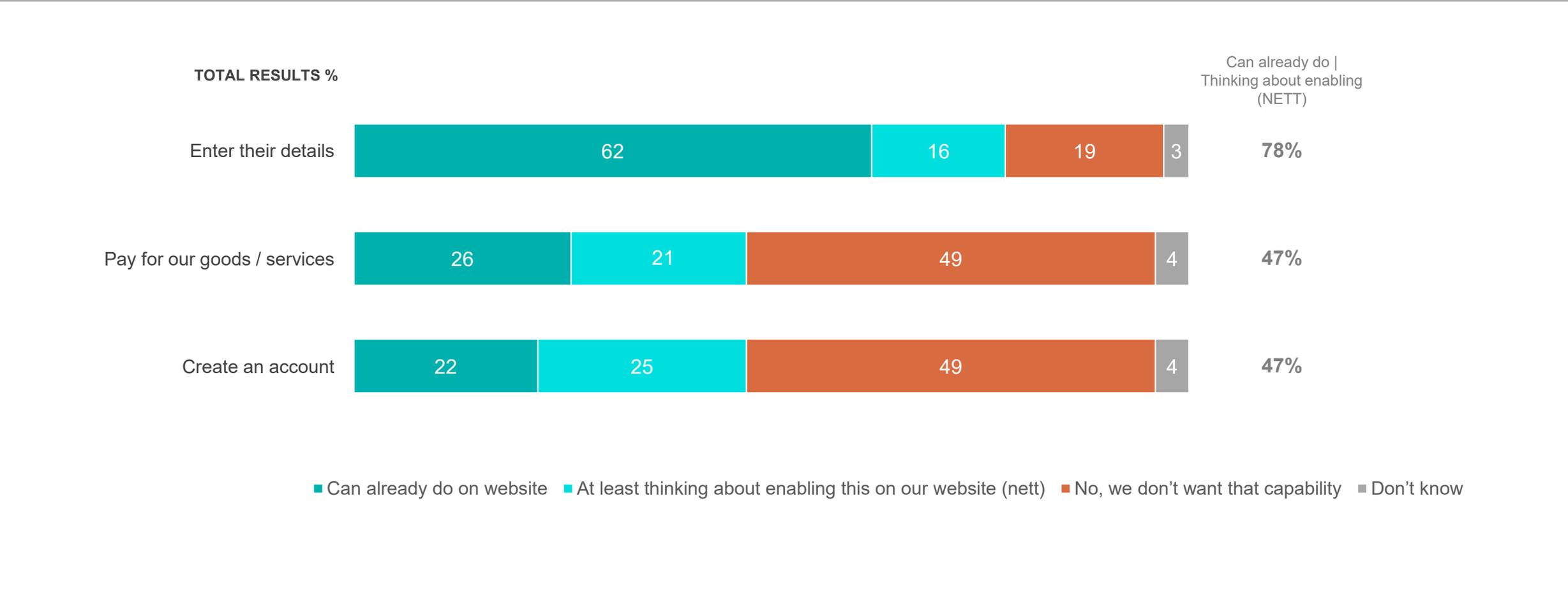


Website capabilities



Website capabilities for online businesses

The majority of small online businesses allow customers to enter their details using the website (62%), while a further 16% are thinking about enabling this function. One in four small business websites (26%) allow customers to pay for goods or services, which equates to 12% of all small businesses surveyed. There is the potential for expansion, with 21% of online businesses thinking of enabling this function.

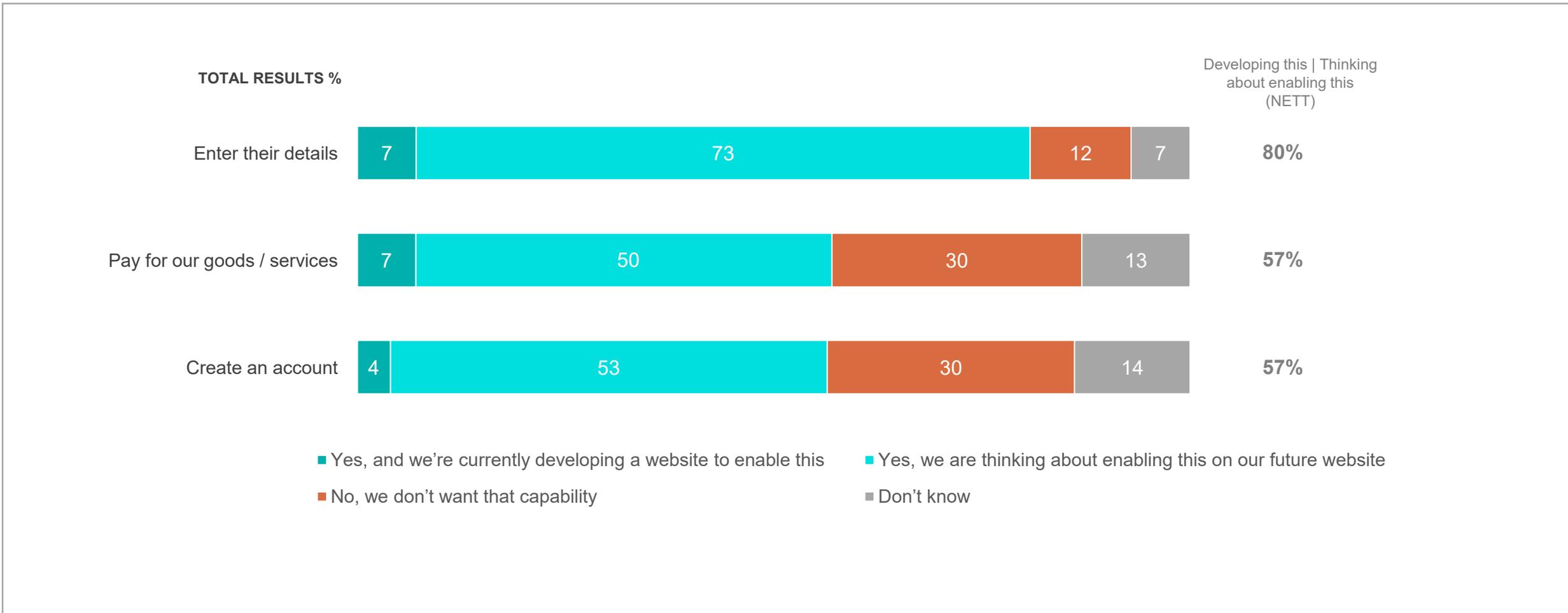


Base: All online businesses (Total SMEs n=622)

Source: A6. What can your customers do on your website? | A7a. Would you like people to be able to do the following things on your website?

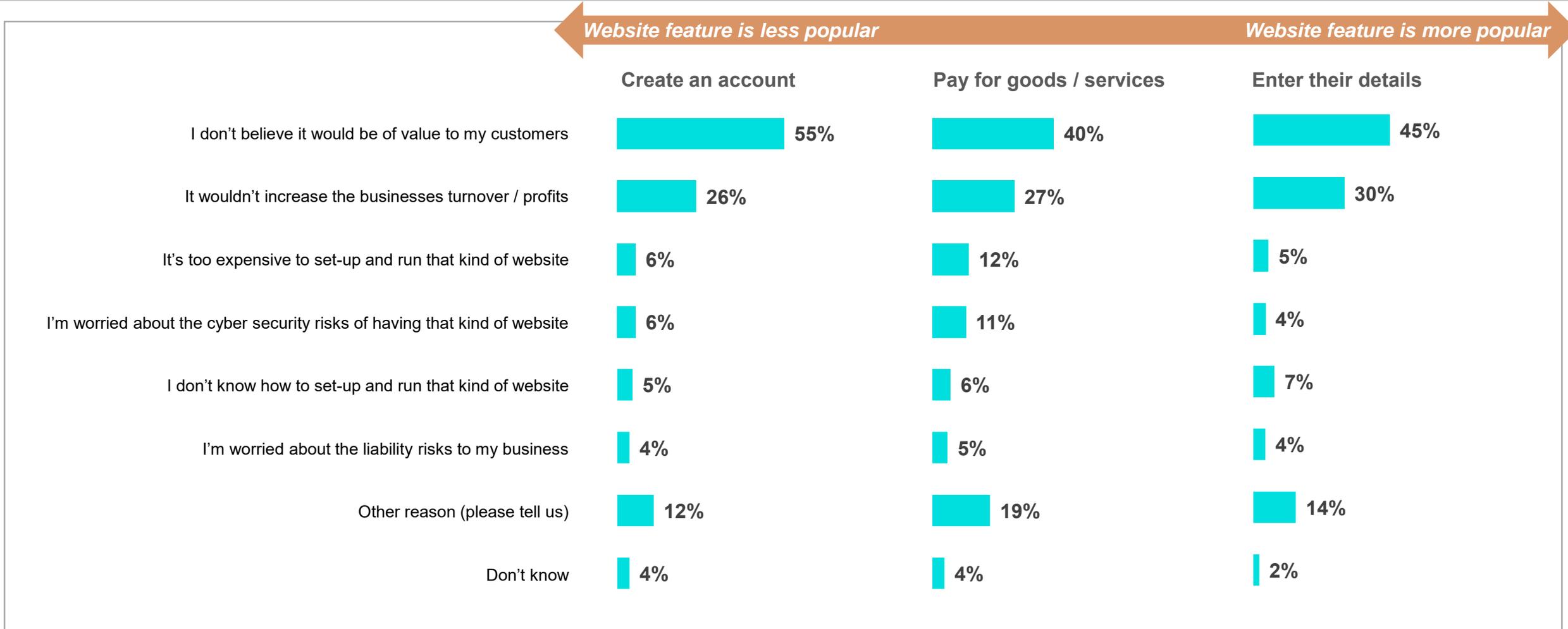
Website capabilities for business planning a website

The majority of small businesses who are in the process of getting a website, or thinking of doing so in future, would like to be able to offer a payment function to their customers. Of those who are in the process of building a website, 22% say they their website will allow online payments.



Barriers to the inclusion of different website capabilities

The main reason why some small businesses (either with a website or may get one in future) shy away from certain features included in the survey is that they don't believe they will be of value to their customers. In general cyber security is not seen as a key barrier to including these features. Cyber security is more of a deterrent to enabling a payment feature, than the other two features.

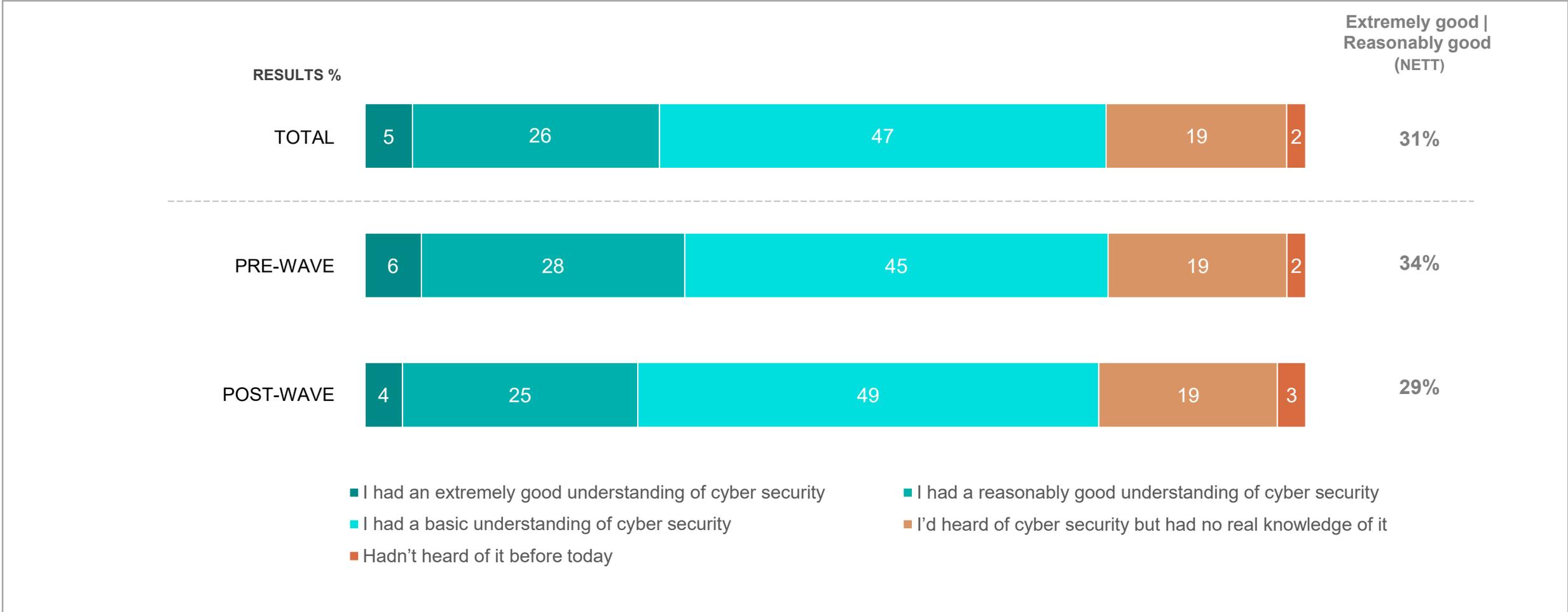


Cyber security awareness and knowledge



Perceived understanding of cyber security

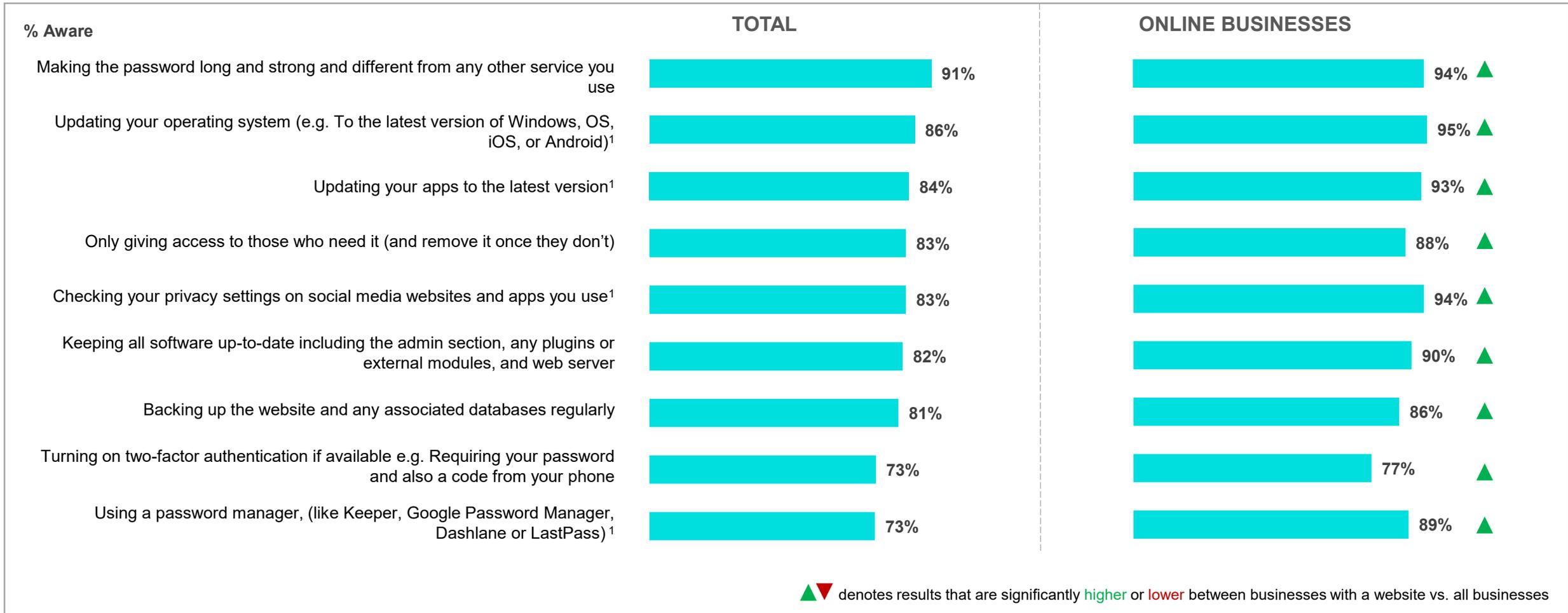
There is a broad lack of understanding of cyber security amongst small business decision makers. Around one in three businesses across the two waves say they have at least a good understanding of cyber security. A further 47% say they have a basic understanding.



Base: All SMEs (Total SMEs n=1,009; Pre wave n=508; Post wave n=501)
 Source: D1. Before today, what level of understanding did you have about cyber security?

Businesses' awareness of the different cyber security actions (1 of 2)

While small businesses are somewhat hesitant about their perceived understanding of cyber security, they are aware of many of the actions they (or others) should be taking in order to keep their website secure. This slide shows those actions where awareness is highest, while the following shows where it is relatively lower. The most well known actions are to make passwords long and strong, and update operating systems. Online businesses consistently have higher levels of awareness than all businesses.

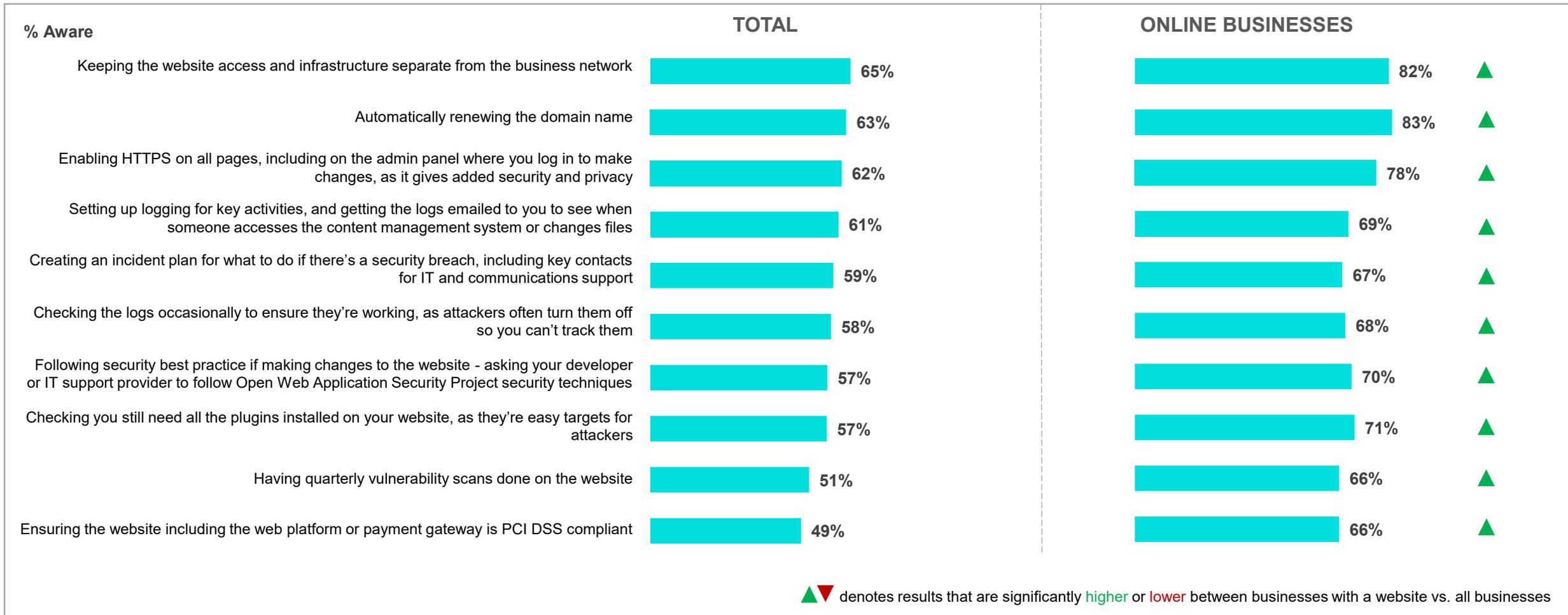


Base: All SMEs (Total SMEs n=1,009; Online businesses n=622). ¹ All SMEs in Post Wave only (Total SMEs n=501; Online businesses n=309).

Source: C2. Before today, were you aware of each of the following actions to help keep a business website secure? | C1. Which, if any, of the following actions does your business take to keep its website secure?

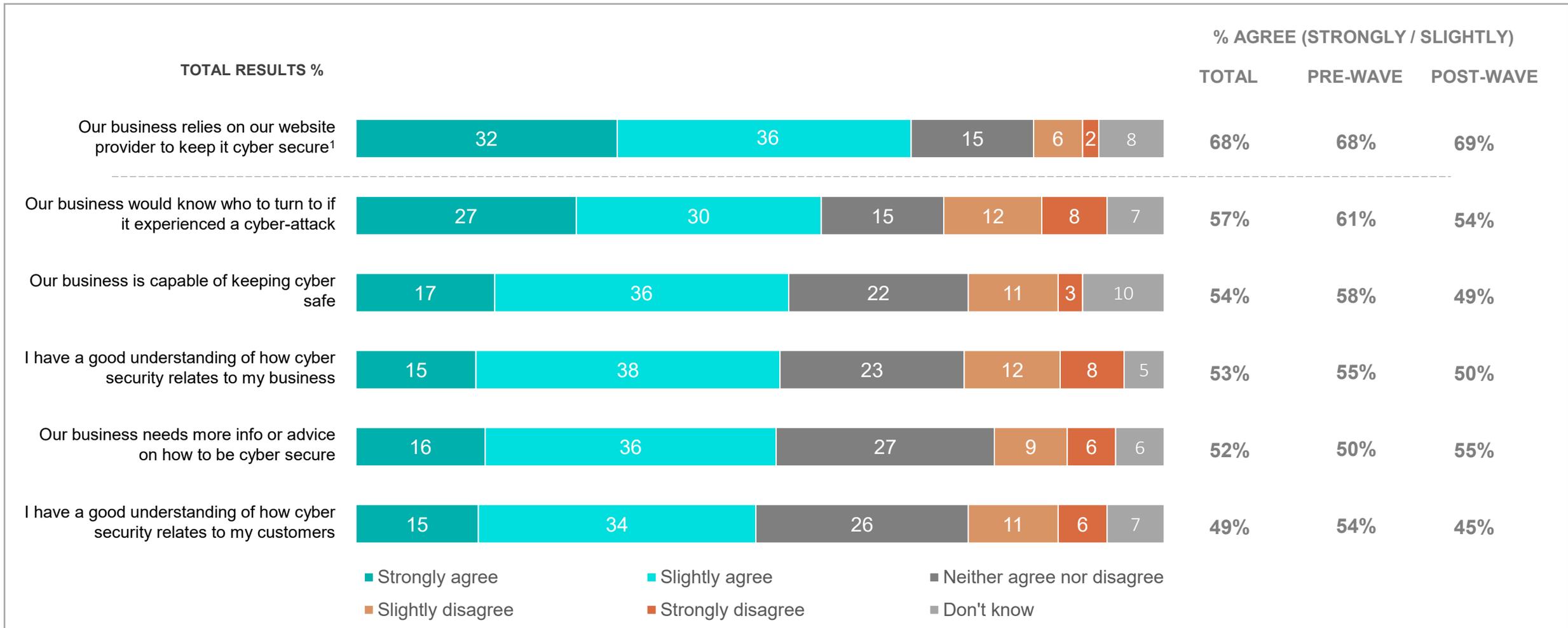
Businesses' awareness of the different cyber security actions (2 of 2)

This slides shows those actions where awareness is relatively lower. Only around half of small businesses say they had heard of having vulnerability scans performed on a website or ensuring the website or payment gateway is PCI DSS compliant. Once again online businesses are more likely to be aware of each of these actions. Awareness is often highest amongst those with an e-commerce site; this includes ensuring the payment gateway is PCI DSS compliant (82% are aware).



Knowledge and understanding of cyber security

There is evidence that many small businesses lack the capability to keep their businesses cyber secure. Online businesses are likely to rely on their website provider to keep the site safe. The remaining attitudes are based on all small businesses. Around half of all respondents agree with each of the statements, indicating they (or their business) has reasonable knowledge and understanding of these aspects of cyber security. However, this means a high proportion are unsure or actively disagree with each statement, suggesting room for improvement.



Base: All SMEs (Total SMEs n=1,009; Pre wave n=508; Post wave n=501). ¹All online businesses (Total SMEs n=622, Pre wave n=313; Post wave n=309)
 Source: D6. How much do you agree or disagree with the following statements?

Perceptions of cyber security



Perceived likelihood of future cyber attacks, and concern around cyber attacks: all businesses

This slide is based on all small businesses surveyed. Most businesses do not feel concerned about a cyber attack and do not feel it will happen to them. Less than half of small businesses (44%) are concerned about the impact of a cyber attack, and 31% feel their business is likely to come under attack.

TOTAL RESULTS %

Concern over cyber attack



■ Not at all concerned: 0 ■ 1 or 2 ■ 3 or 4 ■ 5 ■ 6 or 7 ■ 8 or 9 ■ Extremely concerned: 10

% CONCERNED (6-10 OUT OF 10)

TOTAL	PRE-WAVE	POST-WAVE
44%	43%	45%

TOTAL RESULTS %

Likelihood of cyber attack



■ It definitely won't happen: 0 ■ 1 or 2 ■ 3 or 4 ■ 5 ■ 6 or 7 ■ 8 or 9 ■ It definitely will happen: 10

% LIKELY TO HAPPEN (6-10 OUT OF 10)

TOTAL	PRE-WAVE	POST-WAVE
31%	28%	35%

Perceived likelihood of future cyber attacks, and concern around cyber attacks: businesses with a digital presence

This slide is based on businesses with a digital presence and shows they feel very similarly: they are not overly concerned about a cyber attack or feel like it will happen to them. Forty-seven percent of small businesses (with a digital presence) are concerned about the impact of a cyber attack. In addition, only around one in three feel they're likely to come under attack. This lack of perceived risk may be driving the lack of concern.

RESULTS AMONG THOSE WITH A DIGITAL PRESENCE%

Concern over cyber attack



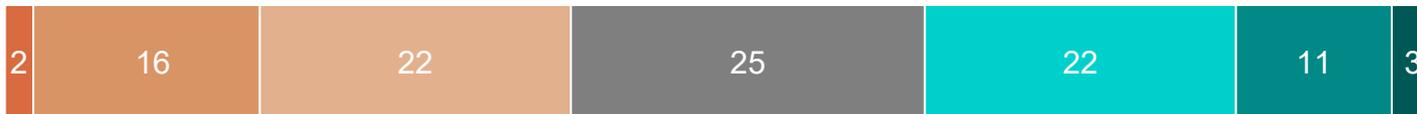
■ Not at all concerned: 0 ■ 1 or 2 ■ 3 or 4 ■ 5 ■ 6 or 7 ■ 8 or 9 ■ Extremely concerned: 10

% CONCERNED (6-10 OUT OF 10)

TOTAL	PRE-WAVE	POST-WAVE
47%	47%	48%

TOTAL RESULTS %

Likelihood of cyber attack



■ It definitely won't happen: 0 ■ 1 or 2 ■ 3 or 4 ■ 5 ■ 6 or 7 ■ 8 or 9 ■ It definitely will happen: 10

% LIKELY TO HAPPEN (6-10 OUT OF 10)

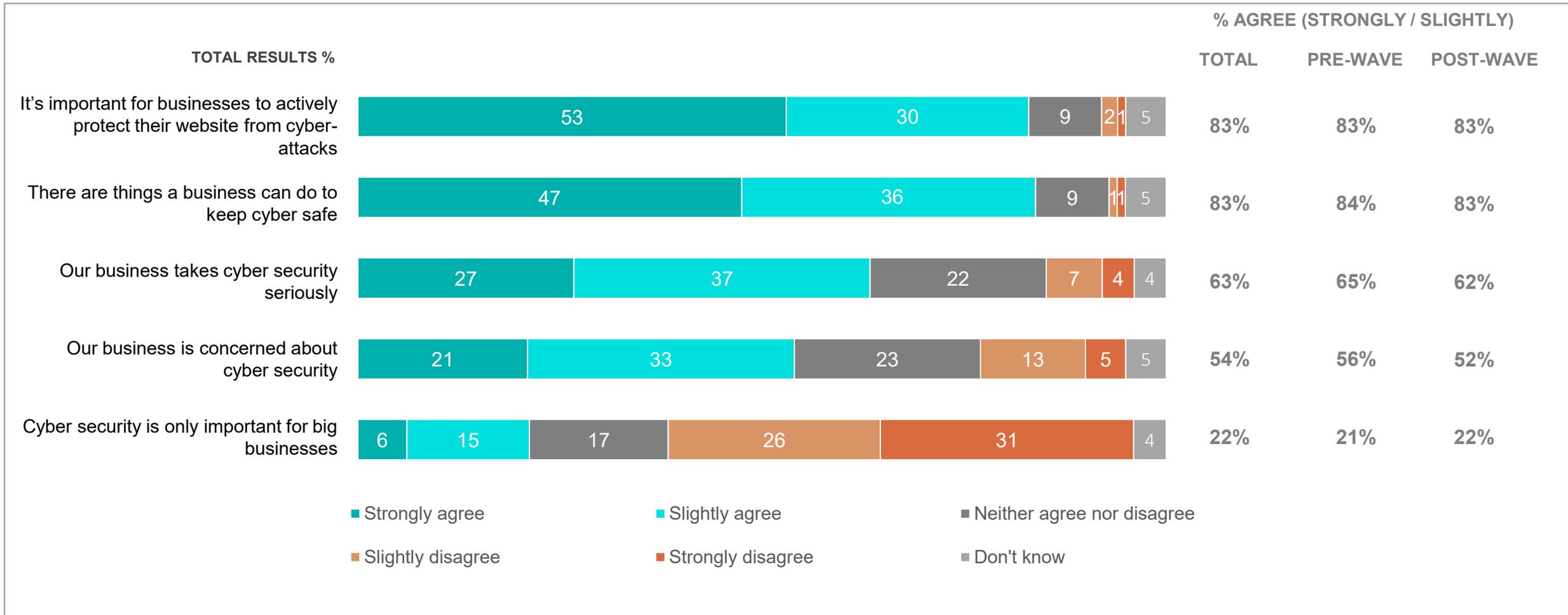
TOTAL	PRE-WAVE	POST-WAVE
35%	34%	36%

Cyber security attitudes



Motivation to act on cyber security

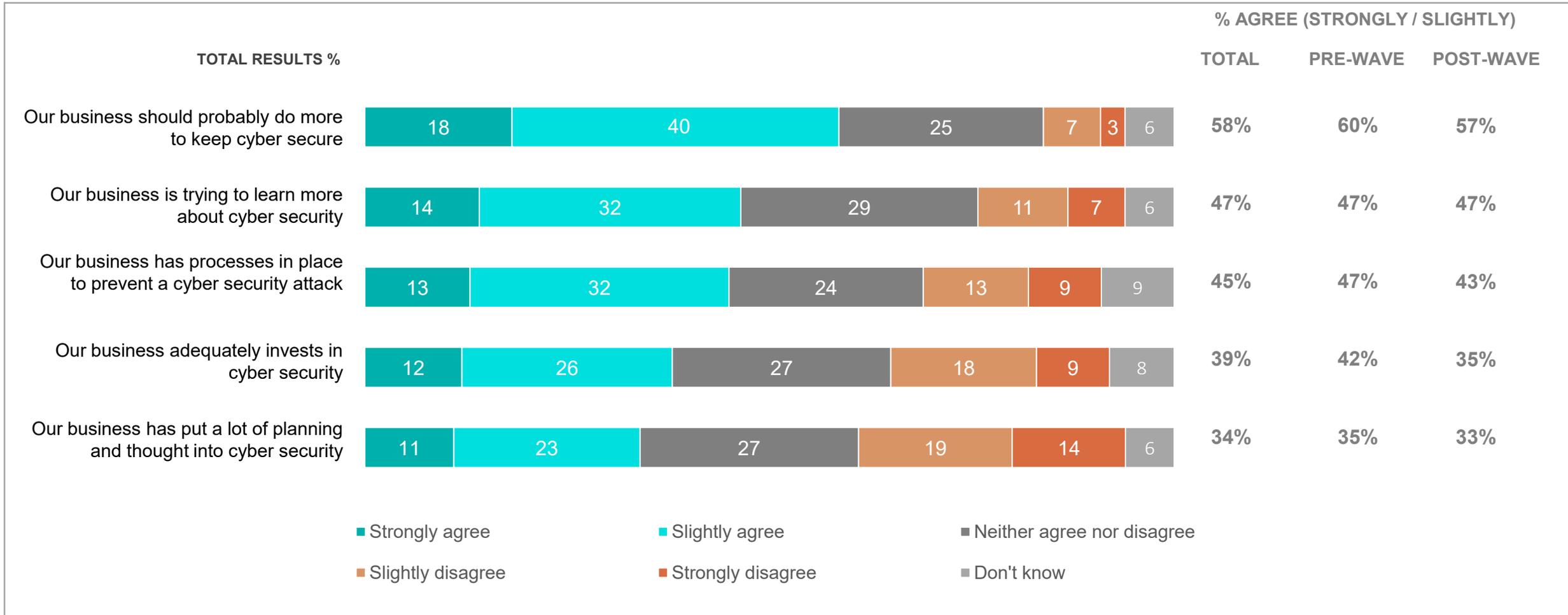
Cyber security is on the radar of small businesses, but a notable minority lack the motivation to act. Small businesses are broadly of the view they need to be proactive to protect their website, and there are indeed things they can do to keep cyber safe. However there is evidence that some small businesses lack the motivation to take action (54% of respondents feel their business is concerned about cyber security). Views on cyber security differ depending on where businesses are at in terms of web development. Those with plans for a website are most concerned (70%), while those with no plans are least concerned (53%). Those with a website are in line with the average (66% are concerned).



Base: All SMEs (Total SMEs n=1,009; Pre wave n=508; Post wave n=501)
 Source: D6. How much do you agree or disagree with the following statements?

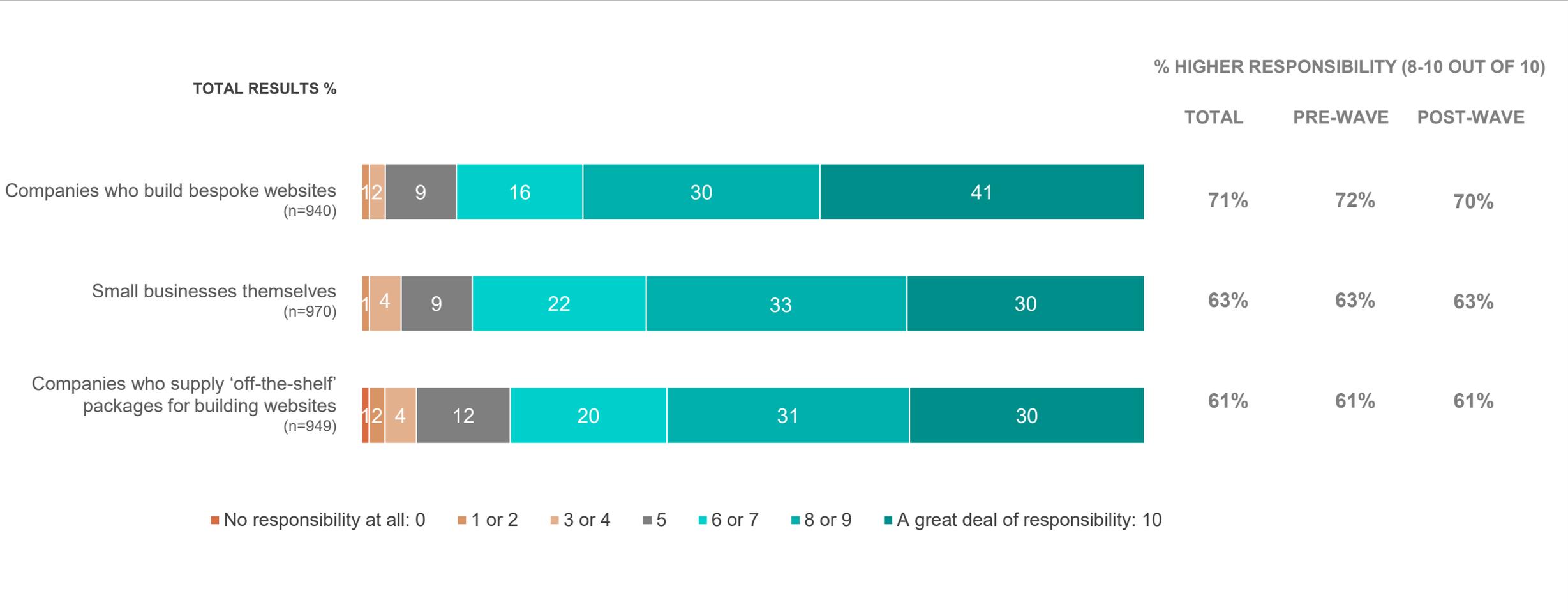
Cyber security attitudes: evidence of action

There is evidence of action on cyber security from some small businesses but the prevailing view is that they should probably be doing more. Only one in three respondents say their business has put a lot of planning and thought into cyber security, while 39% feel their business adequately invests in cyber security. Just under half actually have processes in place to prevent an attack. A similar proportion is trying to learn more.



Responsibility for keeping small business websites secure

Small businesses feel there is a shared responsibility for keeping websites secure. While 63% believe they hold a high level of responsibility themselves, they also believe that web designers (71%) and companies who supply off the shelf packages (61%) hold a high level of responsibility.



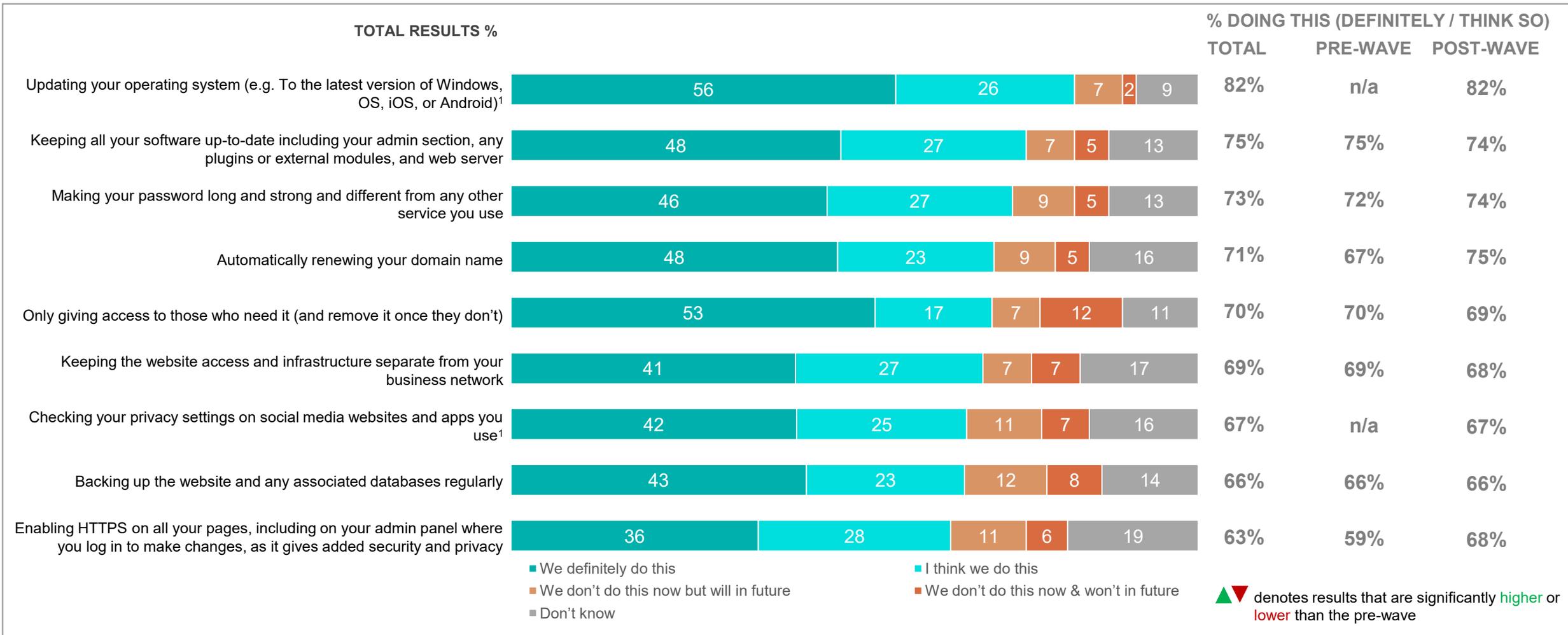
Base: All SMEs excluding Don't knows. Bases for total shown in brackets. Pre-wave bases (n=477, n=487, n=481). Post wave bases (n=463, n=483, n=468). Excludes Don't Knows
 Source: D6a. How much responsibility do you think each of the following has to ensure that small business websites are secure?

**Cyber security
behaviour
amongst online
businesses**



Actions online businesses use to keep their website secure (1 of 2)

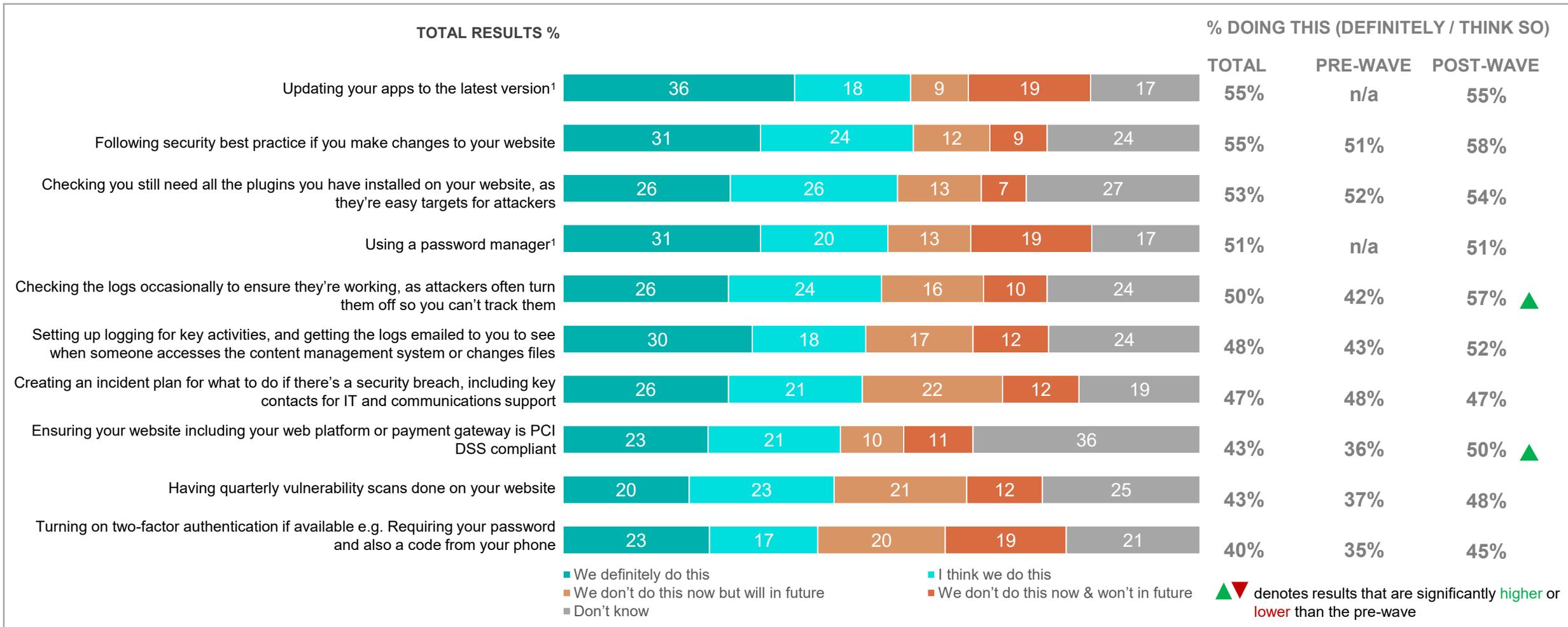
Small online businesses generally take some actions to keep their site cyber secure, but as indicated earlier they could be doing more. This slide shows the most common actions businesses take to protect their website. At least two in three say they definitely do, or think they do, each one of these actions.



Base: All online businesses (Total SMEs n=622; Pre wave n=313; Post wave n=309). ¹All online businesses in post-wave only (n=309)
 Source: C1. Which, if any, of the following actions does your business take to keep its website secure?

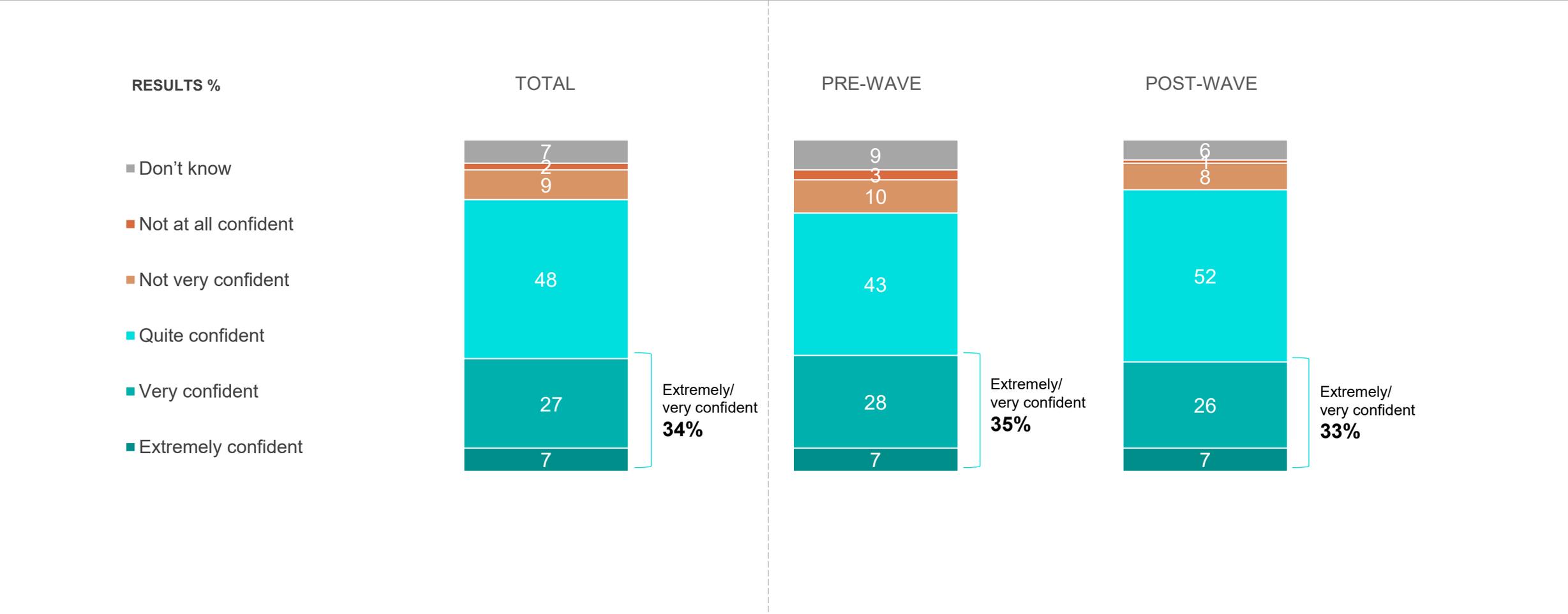
Actions online businesses use to keep their website secure (2 of 2)

This slide shows those actions that small businesses are less likely to be doing to keep their website secure. The proportion who are undertaking these less popular actions has generally increased between the two waves, and some of these increases are statistically significant. They include checking the logs occasionally to ensure they're working, and ensuring your website or payment gateway is PCI compliant.



Level of confidence that business website is secure

Online businesses are somewhat hesitant about the security of their website. One in three are very or extremely confident that it is secure while a further 48% are quite confident. This reinforces the notion that they feel they could do more.



Base: All online businesses (Total SMEs n=622; Pre wave n=313; Post wave n=309)
 Source: D4. How confident or not are you that your website is secure?

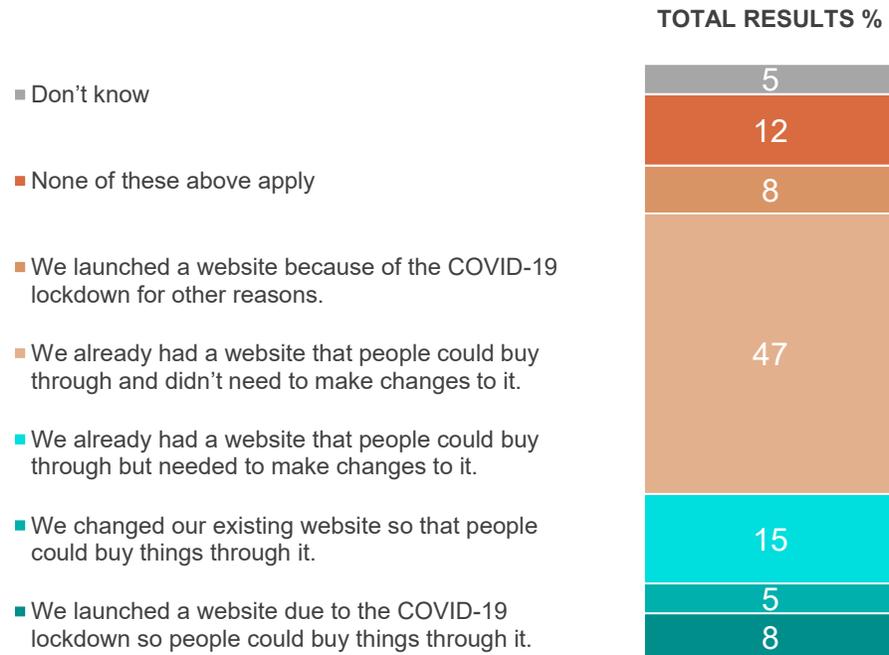
Impact of COVID-19 on e-commerce



How, if at all, COVID-19 affected businesses with an e-commerce website

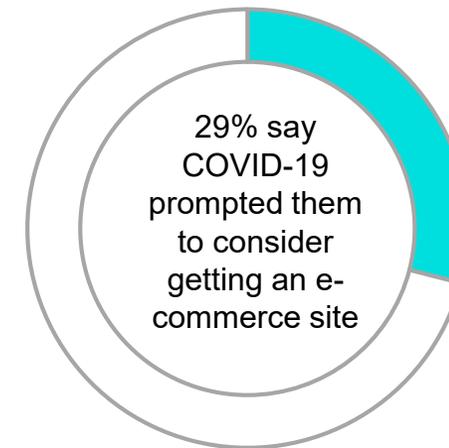
As previously noted 12% of all small businesses surveyed have an e-commerce website. COVID-19 (and the subsequent lockdowns) was a catalyst for change for some of these businesses. 28% of e-commerce businesses launched or changed their offering in some way in response to COVID-19: 8% actually launched an e-commerce website, 5% added a payment facility to an existing website, and 15% made changes to their e-commerce site as a result of COVID-19. Of the 3% of businesses currently implementing an e-commerce website, 29% said this decision was prompted by COVID-19.

IMPACT OF COVID-19 ON BUSINESSES WITH AN E-COMMERCE WEBSITE



IMPACT OF COVID-19 ON BUSINESSES IMPLEMENTING E-COMMERCE

TOTAL RESULTS %



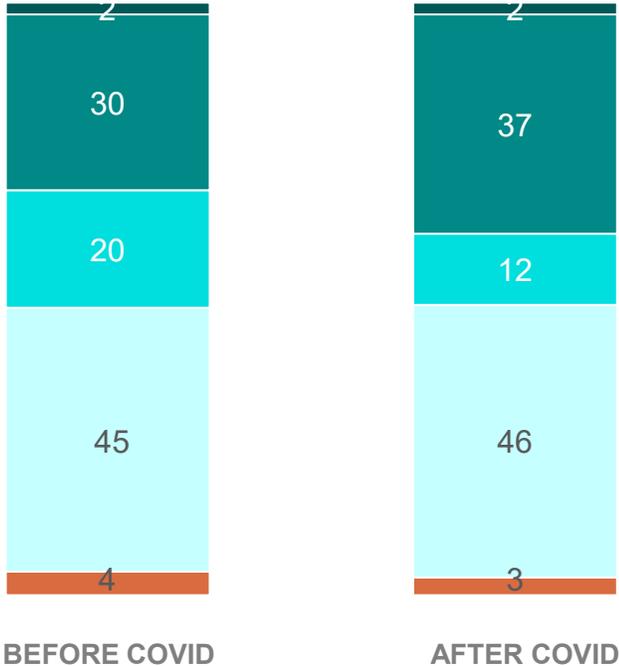
Proportion of turnover generated via website: before and after COVID-19 lockdowns

Following the COVID-19 lockdowns, the proportion of e-commerce businesses who get more than half their turnover via their website is 39%. This compares to an estimate of 32% before COVID-19. The difference is not statistically significant but is indicative that COVID-19 has resulted in a shift in consumer behaviour. In addition, half of all e-commerce businesses expect that online sales will be a bigger part of their business in future with only 16% expecting it to be a smaller part.

PROPORTION OF TURNOVER GENERATED BY WEBSITE

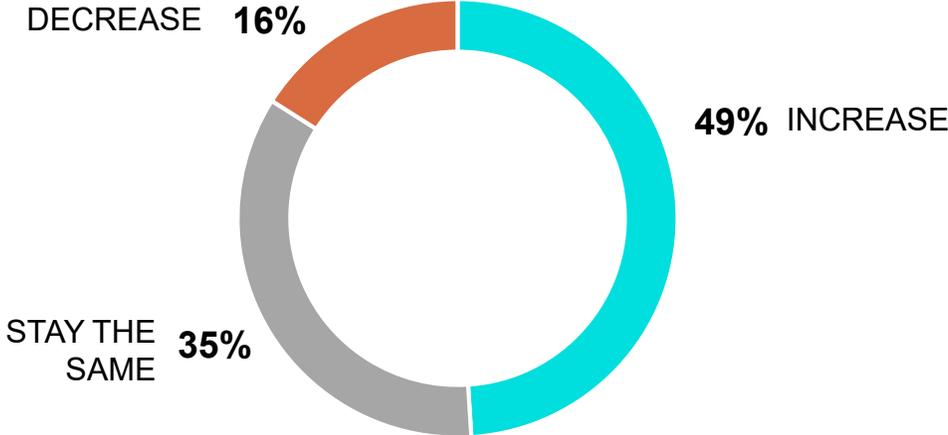
TOTAL RESULTS %

- 100%
- 51% to 99%
- 50%
- 1% to 49%
- None



FUTURE EXPECTATIONS OF THE PROPORTION OF TURNOVER GENERATED BY WEBSITE

TOTAL RESULTS %

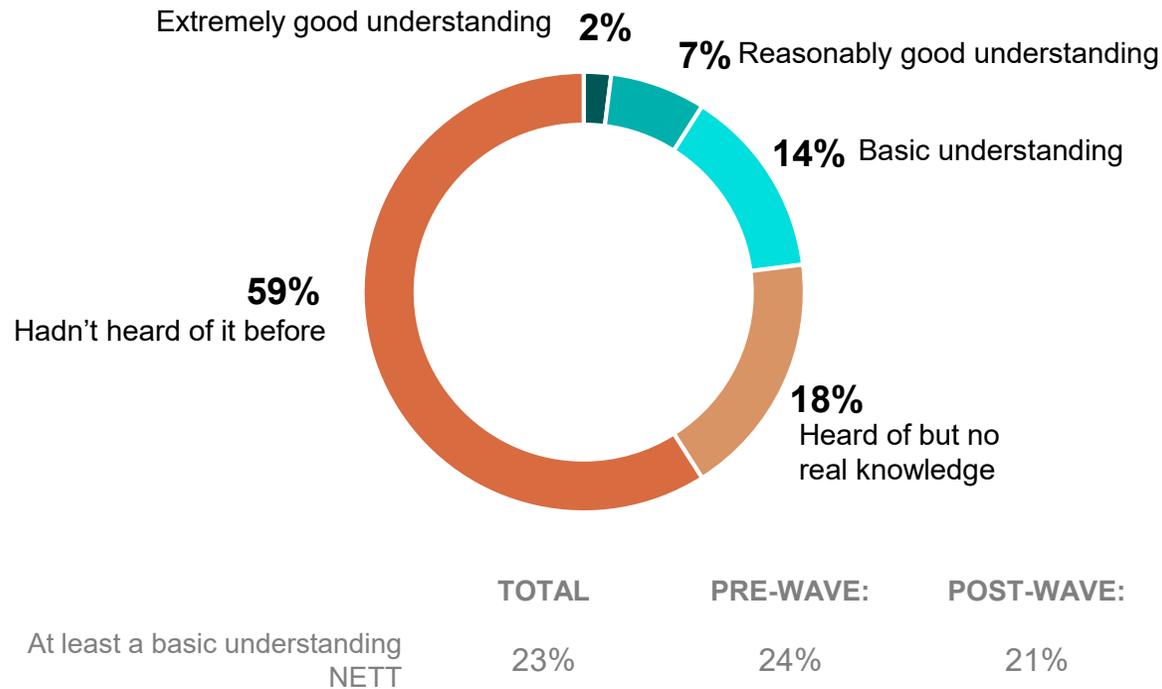


Source: E3. Approximately what proportion of your turnover was generated via your website...? | Base: All SMEs who have an e-commerce website excluding Don't Know (Before COVID n=181, After COVID n=180).
 Source: E4. In future, do you expect the proportion of your turnover generated via your website to ...? | Base: All SMEs who have an e-commerce website excluding Don't Know (n=186).

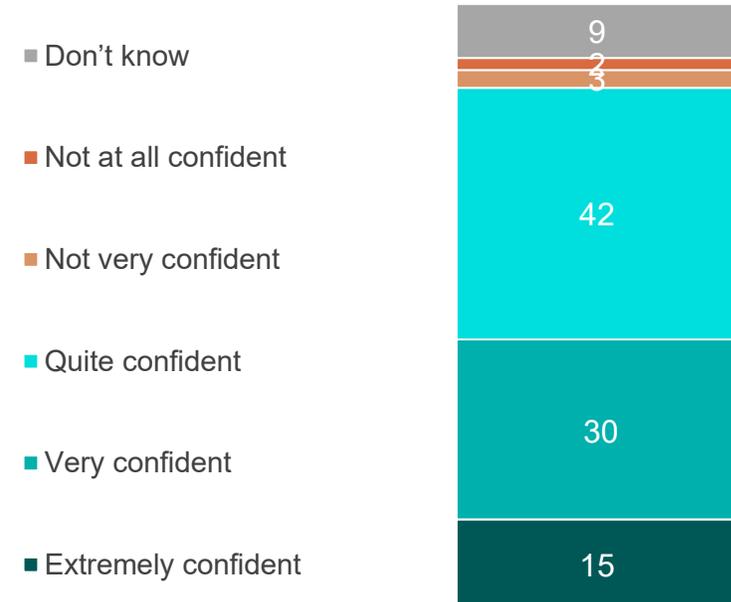
Understanding of and compliance with PCI DSS standards

There is relatively low awareness and understanding of PCI DSS (Payment Card Industry Data Security Standard). 41% of small businesses are aware of it, but only 23% say they have a basic understanding of it. Awareness and understanding amongst those with an e-commerce website increases to 65% and 50% respectively. Of those e-commerce sites who have heard of PCI DSS, 44% are very or extremely confident they are compliant, while a further 42% are quite confident.

Aware of PCI DSS



Compliant with PCI DSS



Appendix



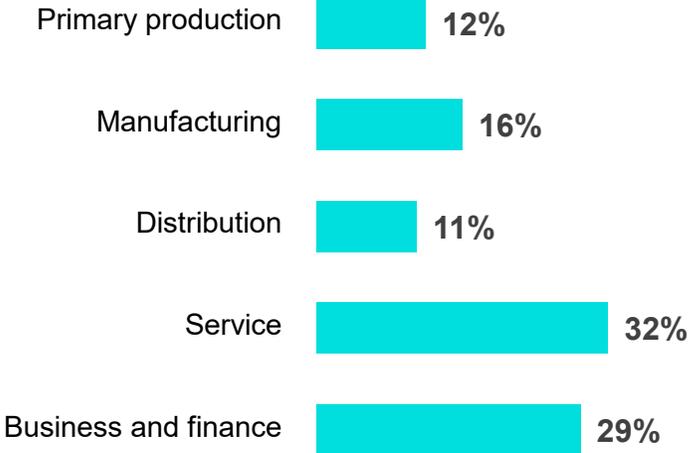
Sample profile

The sample profile for size of business and industry is provided below.

Number of employees



Industry



Base: All respondents (Total SMEs n=1,009)
Source: A1. Not including the owner or owners, how many employees are there in your business? (By employees we mean the number of full-time equivalent employees working at least 30 hours per week. Several part-time employees may convert to one full time employee.) | A2. Which of the following industries is your business in?

