VEC2101 Vectra IT Security Research Netherlands

May 2022

CONFIDENTIAL

Contents

- Project overview and methodology
- Respondent demographics summary
- Key stats
- Summary and Overview
- Main Findings
- Demographics

Project overview and methodology

- The survey was conducted among 200 IT security decision makers in companies with over 500 employees in the Netherlands.
- At an overall level results are accurate to ± 6.9% at 95% confidence limits assuming a result of 50%.
- The interviews were conducted online by Sapio Research in February 2022 using an email invitation and an online survey.
- Please note as a result of rounding, some %s do not add up to exactly 100%. This is normal when dealing with %s rounded to the nearest whole number.

Key stats

97% have felt increased pressure to keep their organisation safe over the past year

49% have suffered a significant cybersecurity incident in the past year

72% have experienced a significant security event that required an incident response effort

77% have purchased a security solution that has failed on at least one occasion

57% feel they could use more security talent on their team

87% feel their security tools are effective at keeping their organisation safe

Summary and Overview

1 **Prevention trumps detection** – Most believe prevention of hackers is more important than detecting the threats they pose. Unsurprisingly, 48% of companies invest more into prevention tools, whilst 20% invest more in detection.

2 **Poor integration of tools and handling of threats poses dilemmas** – Equally, most companies feel they may have been breached unbeknownst to them. For most, security solutions have failed to perform as expected on at least one occasion.

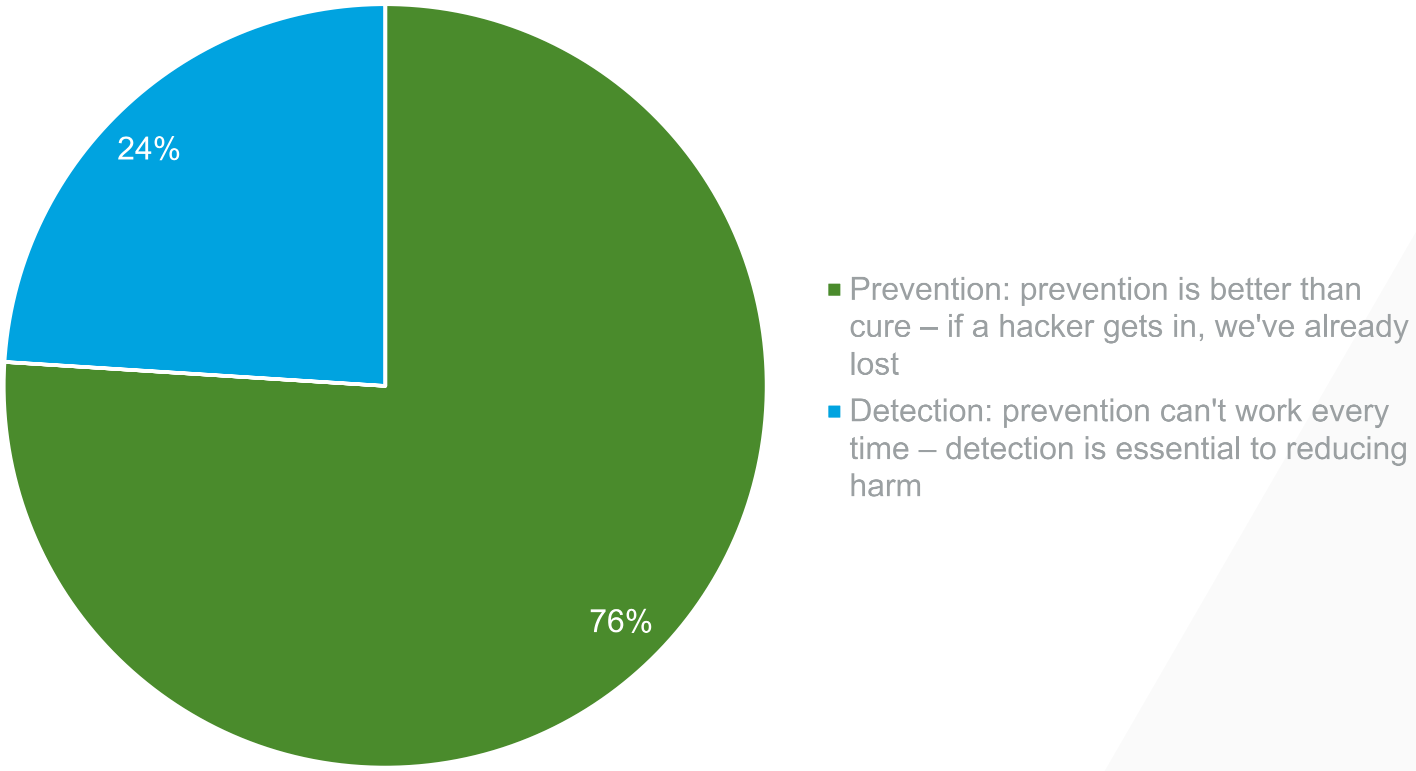
3 **Dutch companies make use of the guidelines** – Over half have read the cyber security guidelines, with most finding them at least somewhat useful. However there is room for improvement, with only 1 in 5 believing they covered everything.

4 **Regulators and legislators are generally up to speed** – The general consensus is that regulators have adequate understanding of challenges while legislators are considered well-equipped for designing regulations.

5 **Room for improvement going forward** – Over half feel more security talent is needed on their team. Equally, security tools are not always reliable and may miss threats.

Main Findings

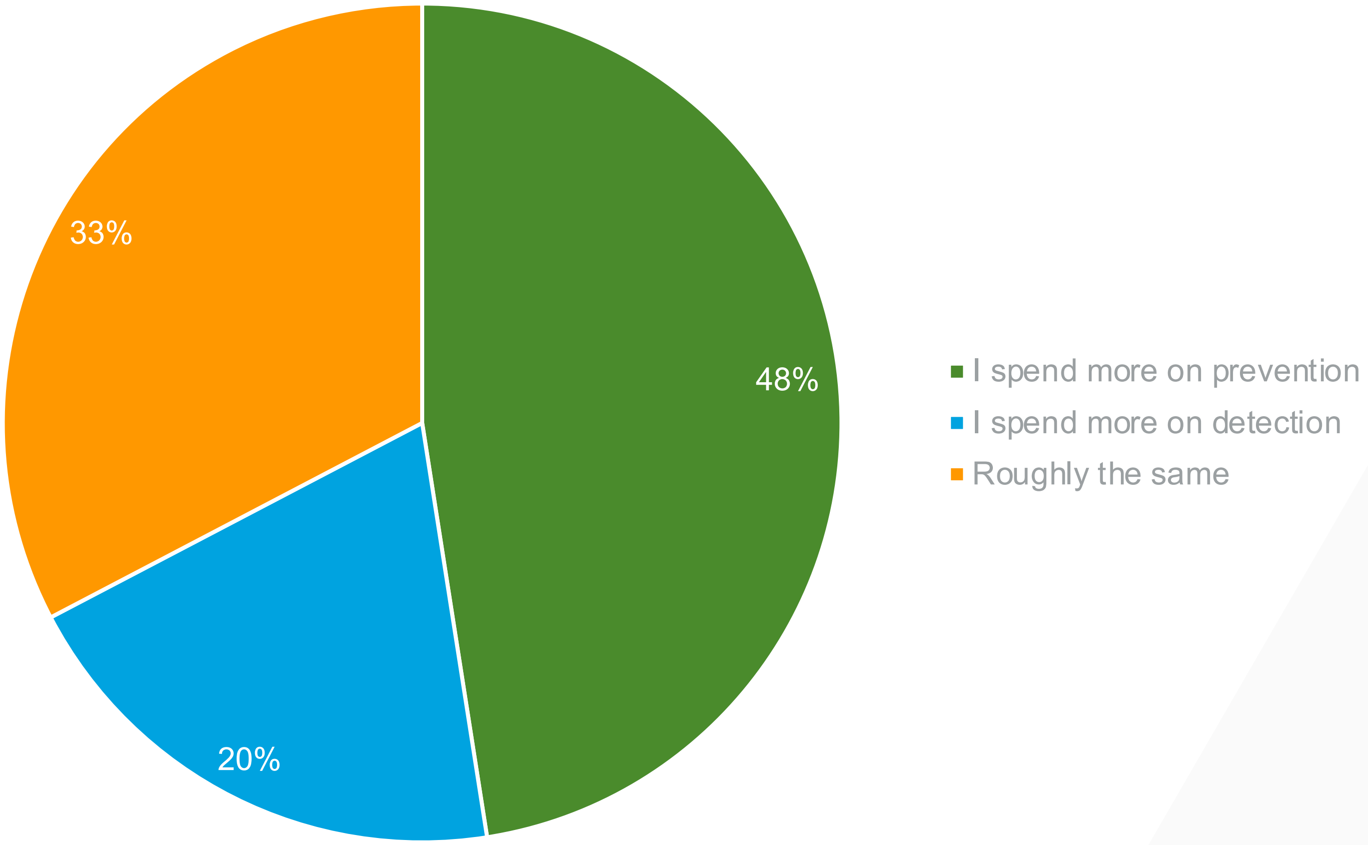
76% believe preventing hackers from breaching defences is more important than detection after a breach has already occurred



Q1. If you had to choose one, what do you think is more important – prevention (i.e. stopping hackers from breaching your defences) or detection (i.e. finding hackers that have already infiltrated your environment)? Select one

Base: 200

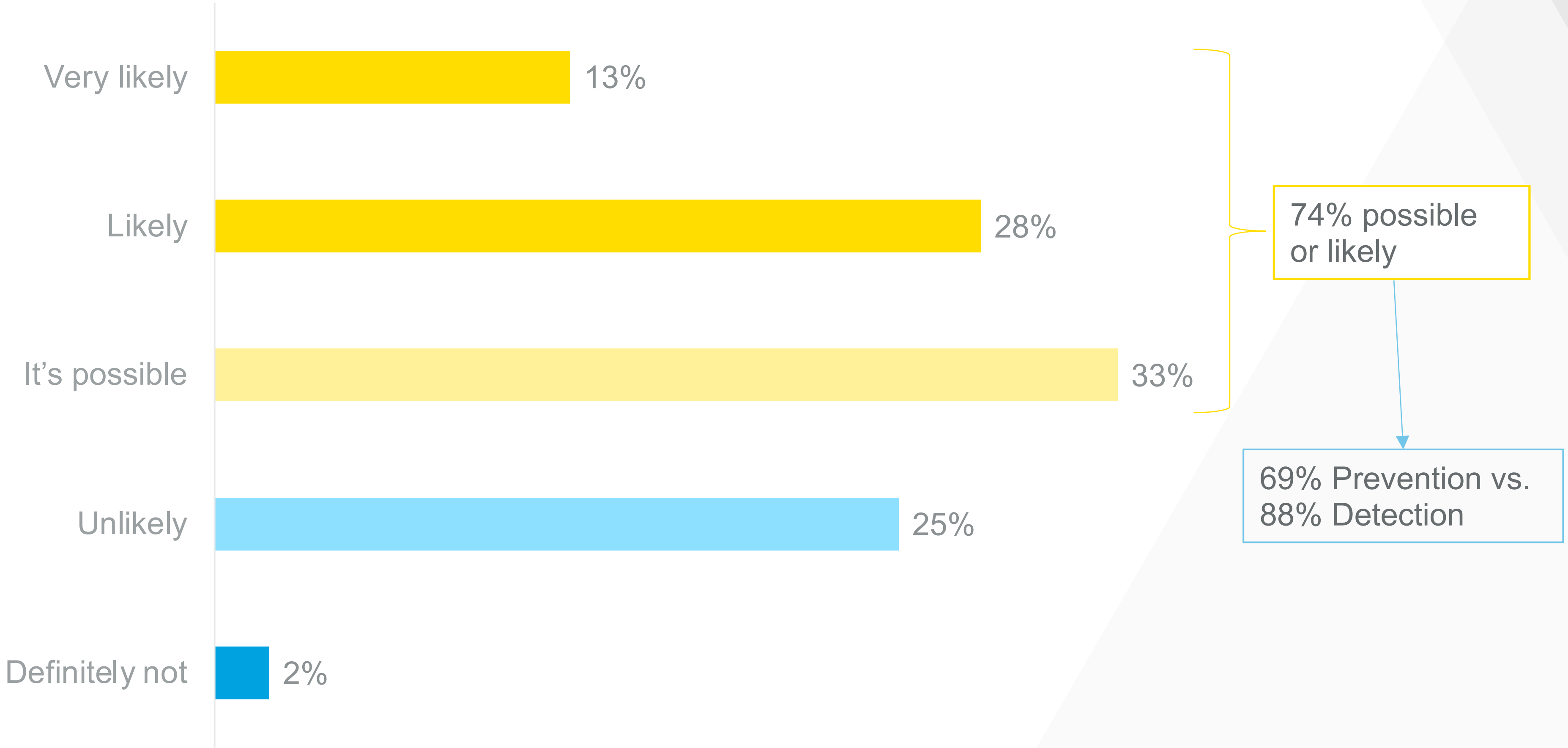
48% invest more into prevention tools
20% invest more into detection



Q2. How does this belief impact your buying behaviour – do you invest more in prevention tools (e.g. Multi-factor authentication, firewalls, etc.) or detection tools (e.g. Threat Detection & Response)? Select one

Base: 200

74% feel it is possible or likely they have been breached whilst being unaware of it happening



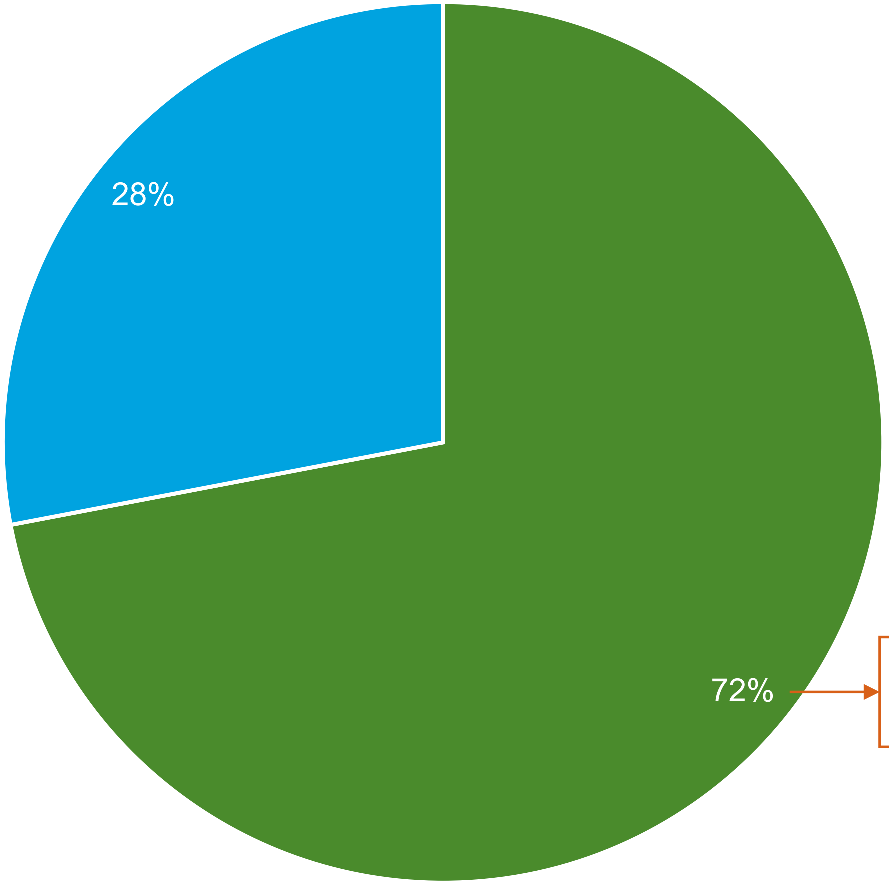
74% possible or likely

69% Prevention vs. 88% Detection

Q3. How likely is it you have been breached and you don't know about it yet? Select one

Base: 200

72% have experienced a significant security event that required an incident response effort

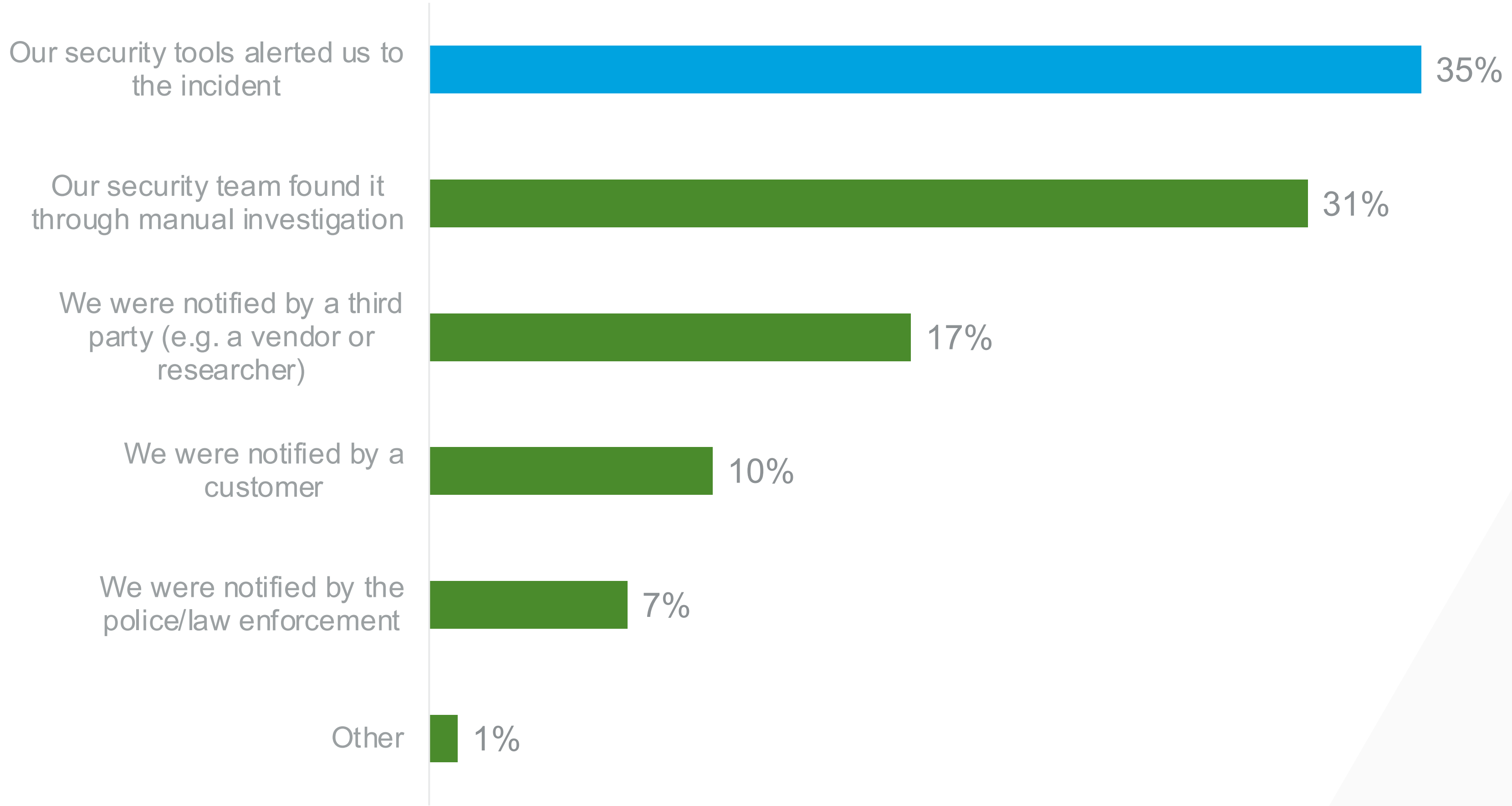


67% Managers vs.
84% C-level Executives

Q4. In your career, have you ever experienced a significant security event that required a significant incident response effort? Select one

Base: 200

Security incidents are most often discovered through alerts from security tools (35%)

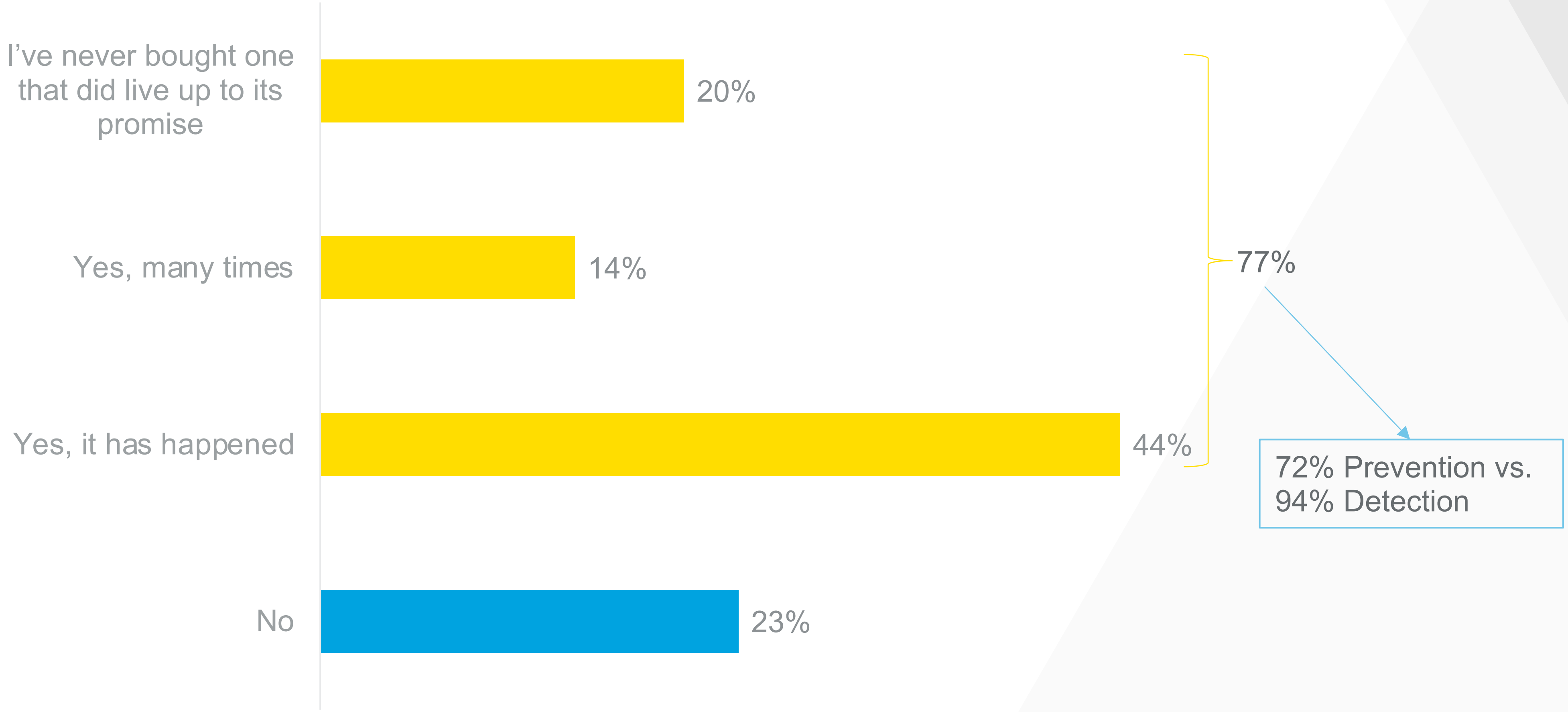


* Only asked to those who experienced a significant security event

* Base: 144

Q5. When this security event happened, how did the incident come to your attention? Select one

77% have purchased a security solution that has failed on at least one occasion

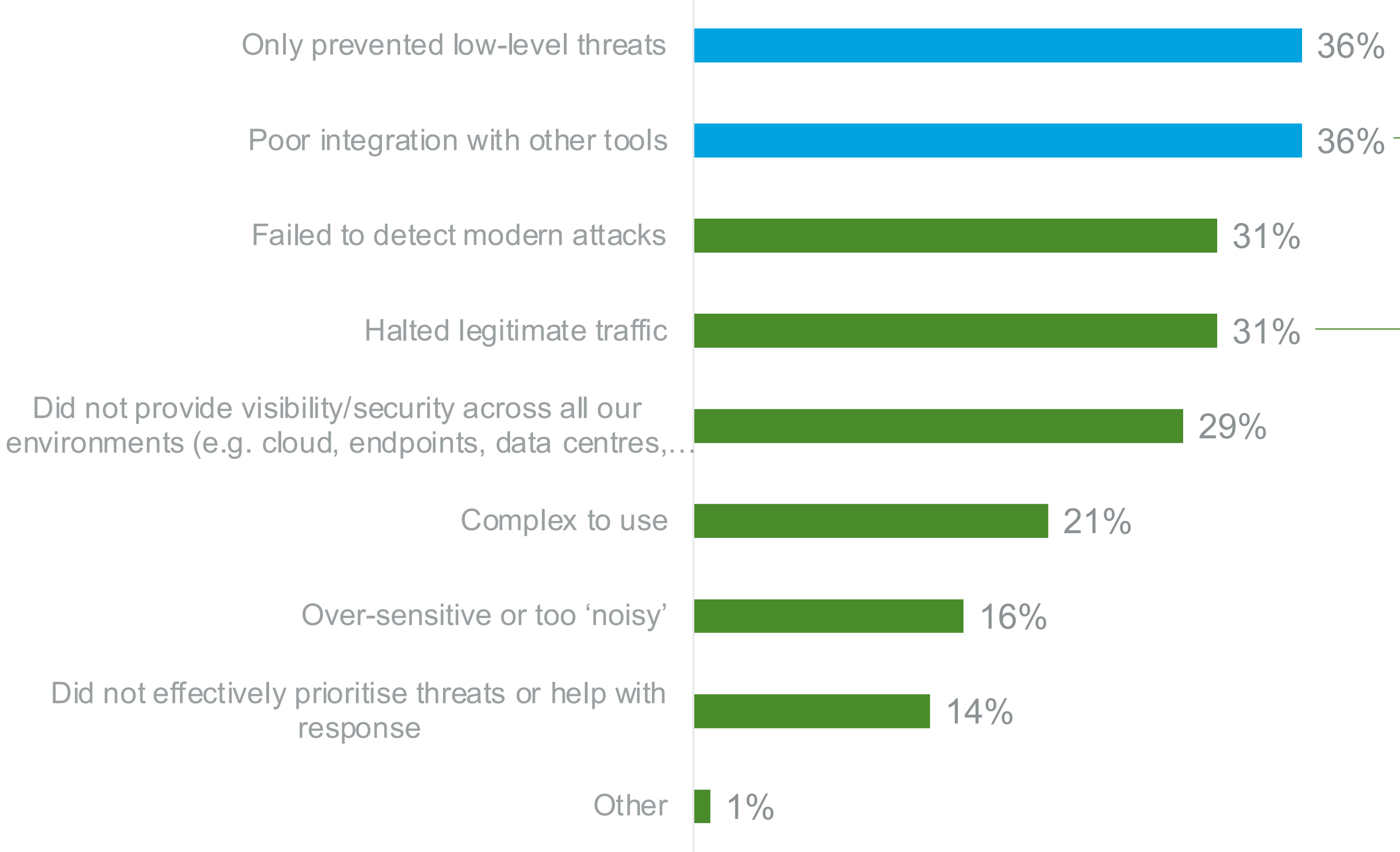


72% Prevention vs. 94% Detection

Q6. Have you ever purchased a security solution that failed to deliver on its promise? Select one

Base: 200

Merely preventing low level threats and poor integration with other tools are the most experienced issues (36%)



Top response for Managers (39%)

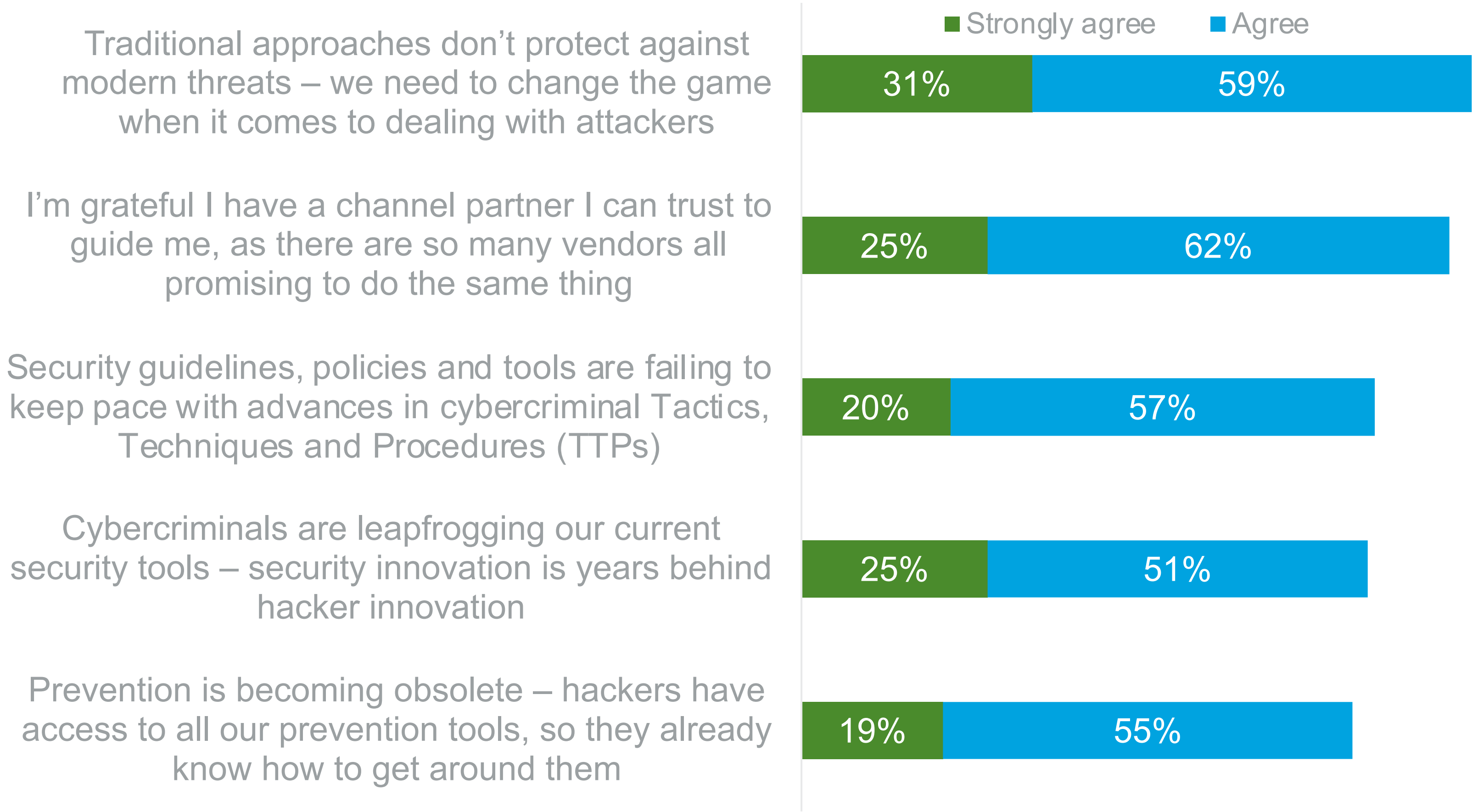
501 – 1000 employees (**50%**)
1001 – 5000 employees (**22%**)

* Only asked to those who purchased a security solution that failed to deliver on its promise

* Base: 154

Q7. What issues have you experienced? Select all that apply

There is wide consensus over the inability of traditional approaches to protect against modern threats (90%)



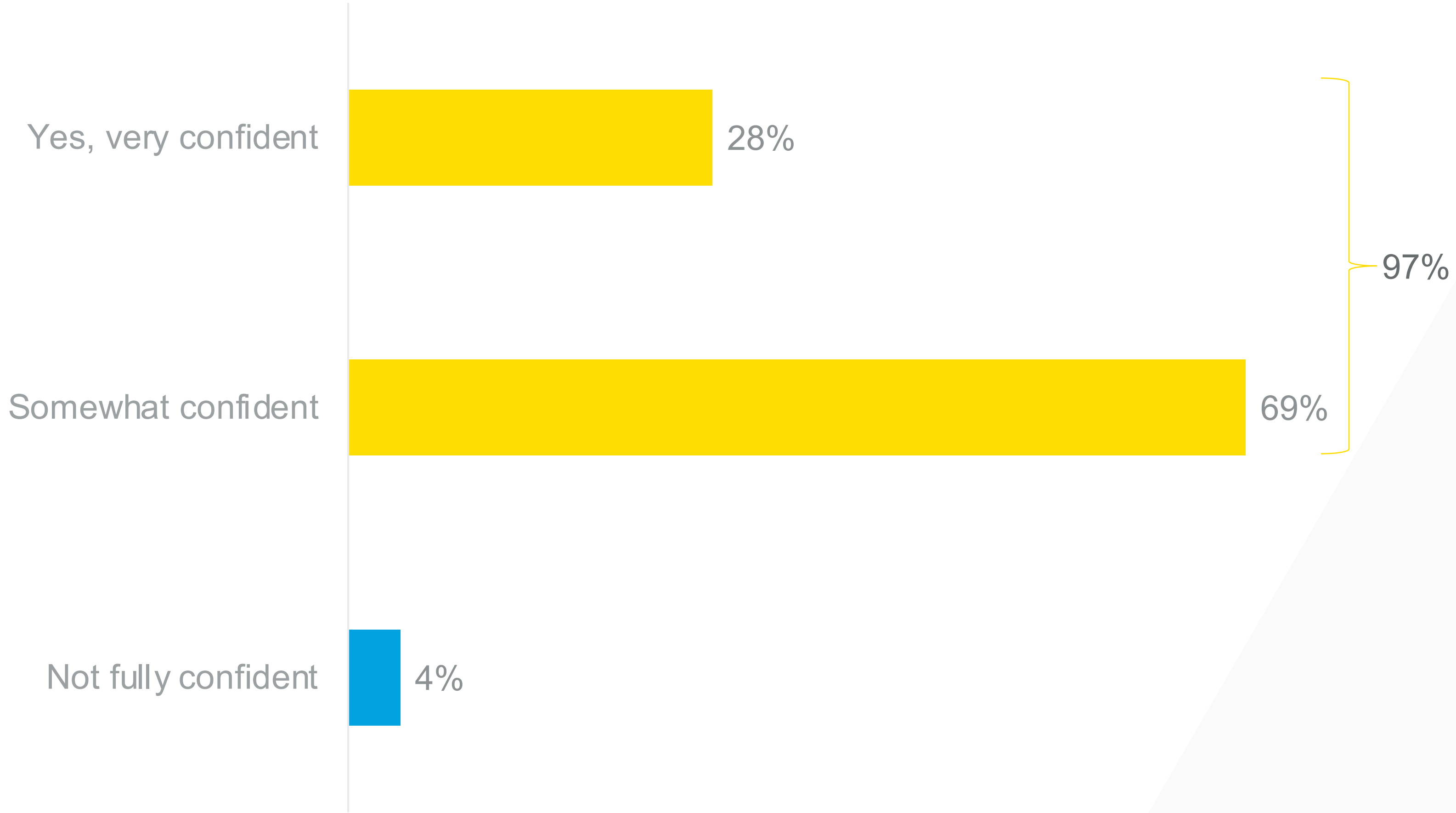
% Agree
90%
87%
76%
76%
74%

Base: 200

Q8. To what extent do you agree with the following statements: Select one per row

4% are not fully confident their security tools would protect against sophisticated attacks

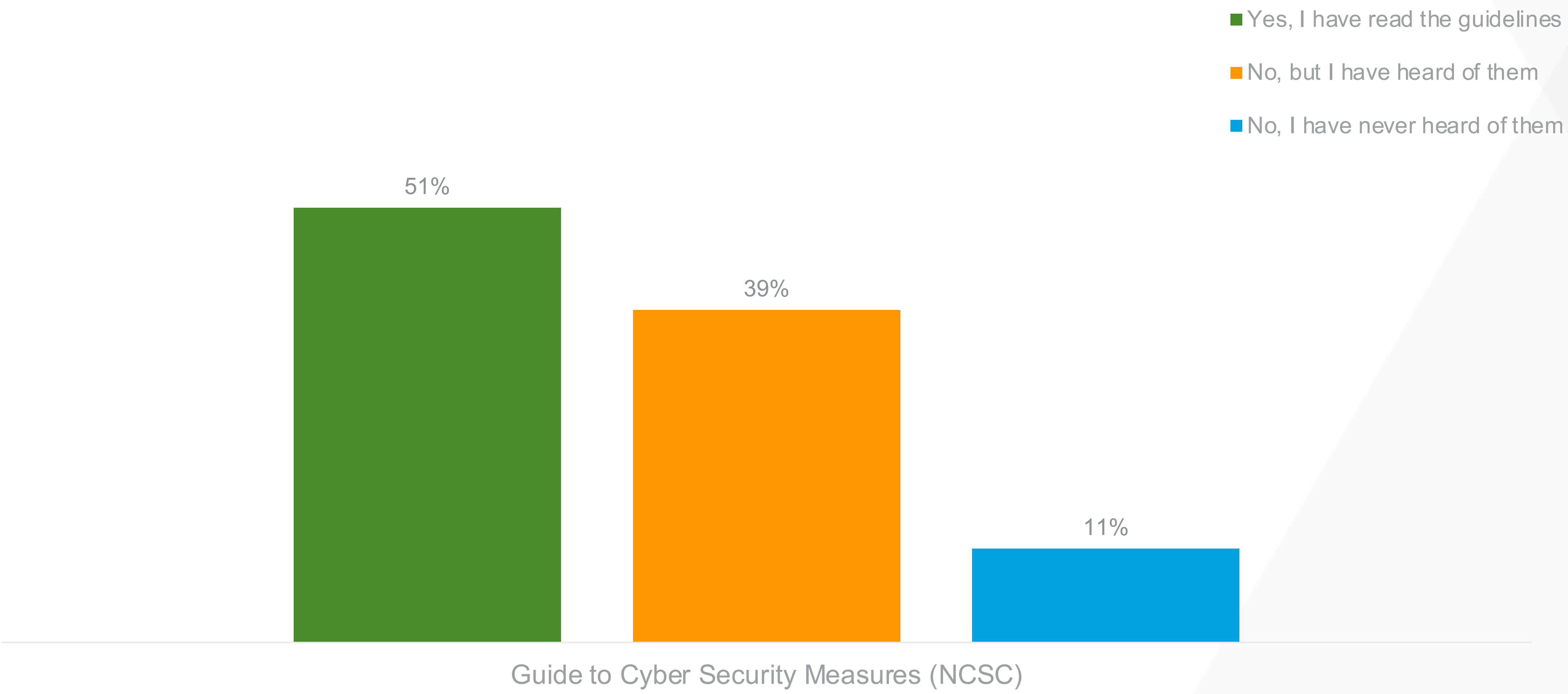
Only 28% are fully confident



Q9. Are you fully confident that your security tools would enable you to detect and protect against the type of sophisticated tactics involved in recent attacks? Select one

Base: 200

51% of Dutch respondents have read the “Guide to Cyber Security Measures” guidelines from the NCSC

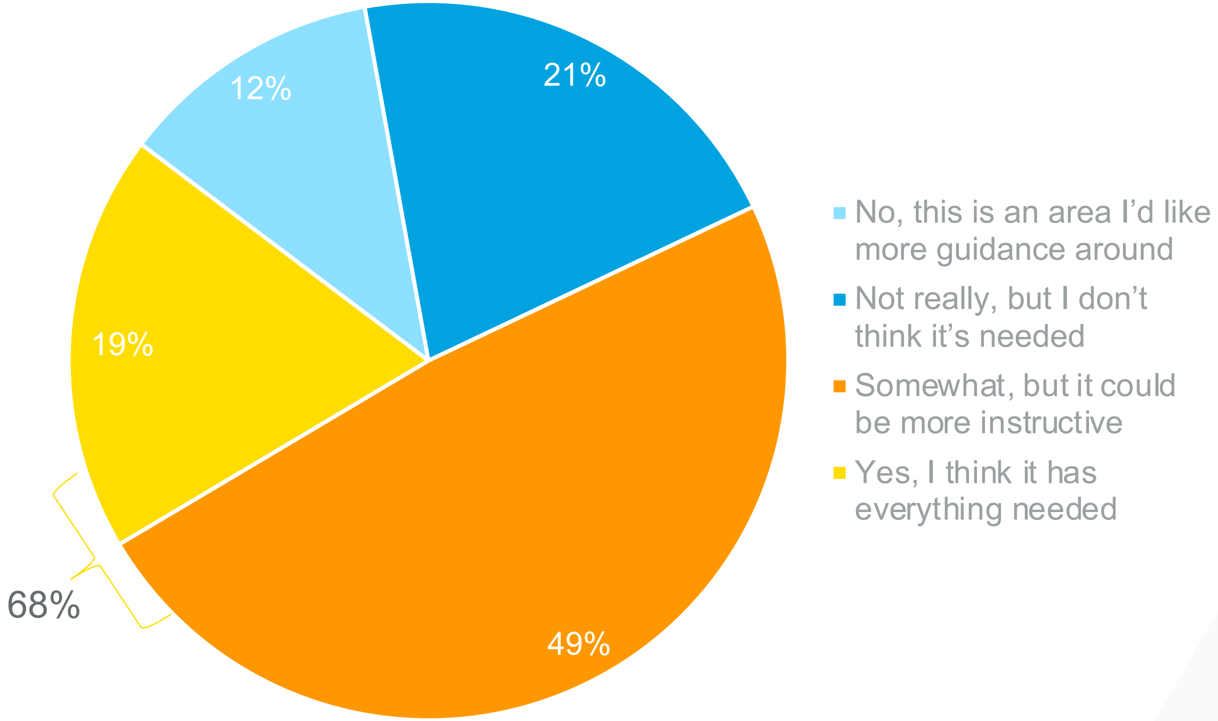


Base: 200

Q10. Have you read the cyber security guidance…? Select one

Of those that have read the guidance, 68% found it at least somewhat useful

Only 19% felt it had everything needed

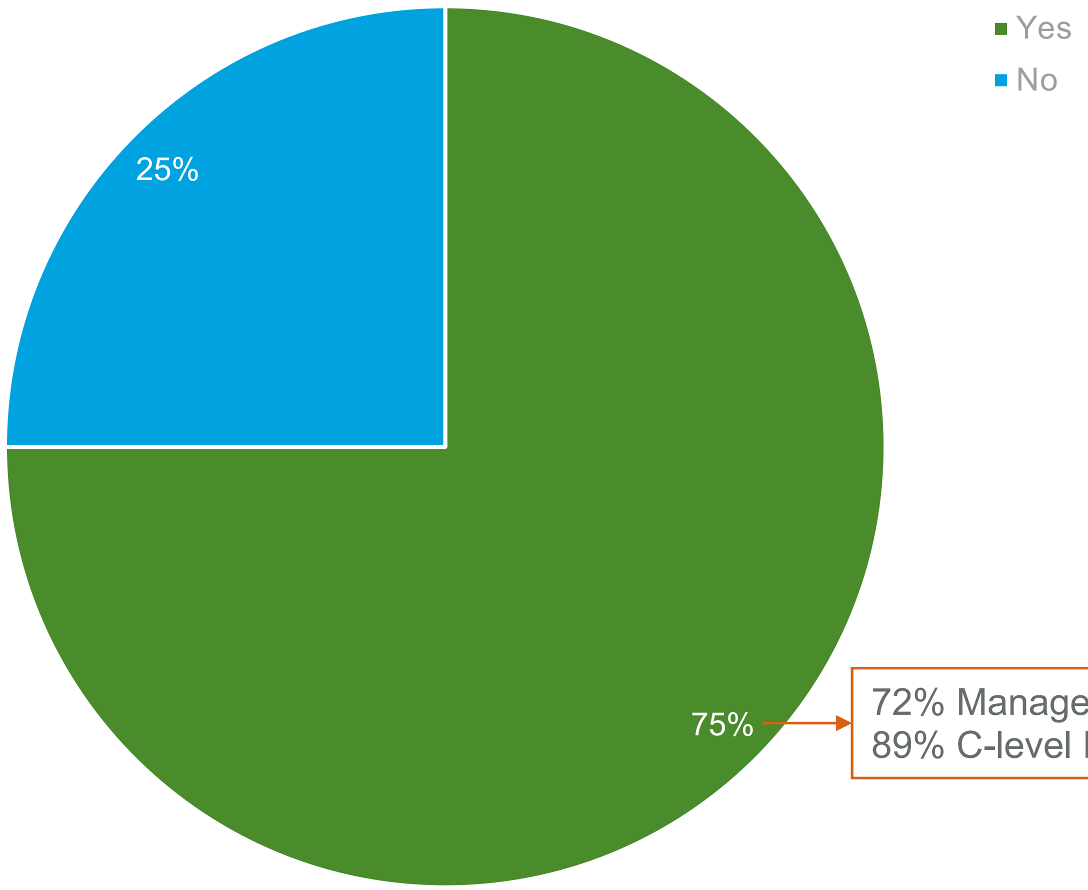


* Only asked to those who have read the guidelines

* Base: 102

Q11. Have you found the guidance useful when trying to enhance your threat detection and response capabilities? Select one

75% feel regulators have a strong enough understanding of the harsh realities that security teams face

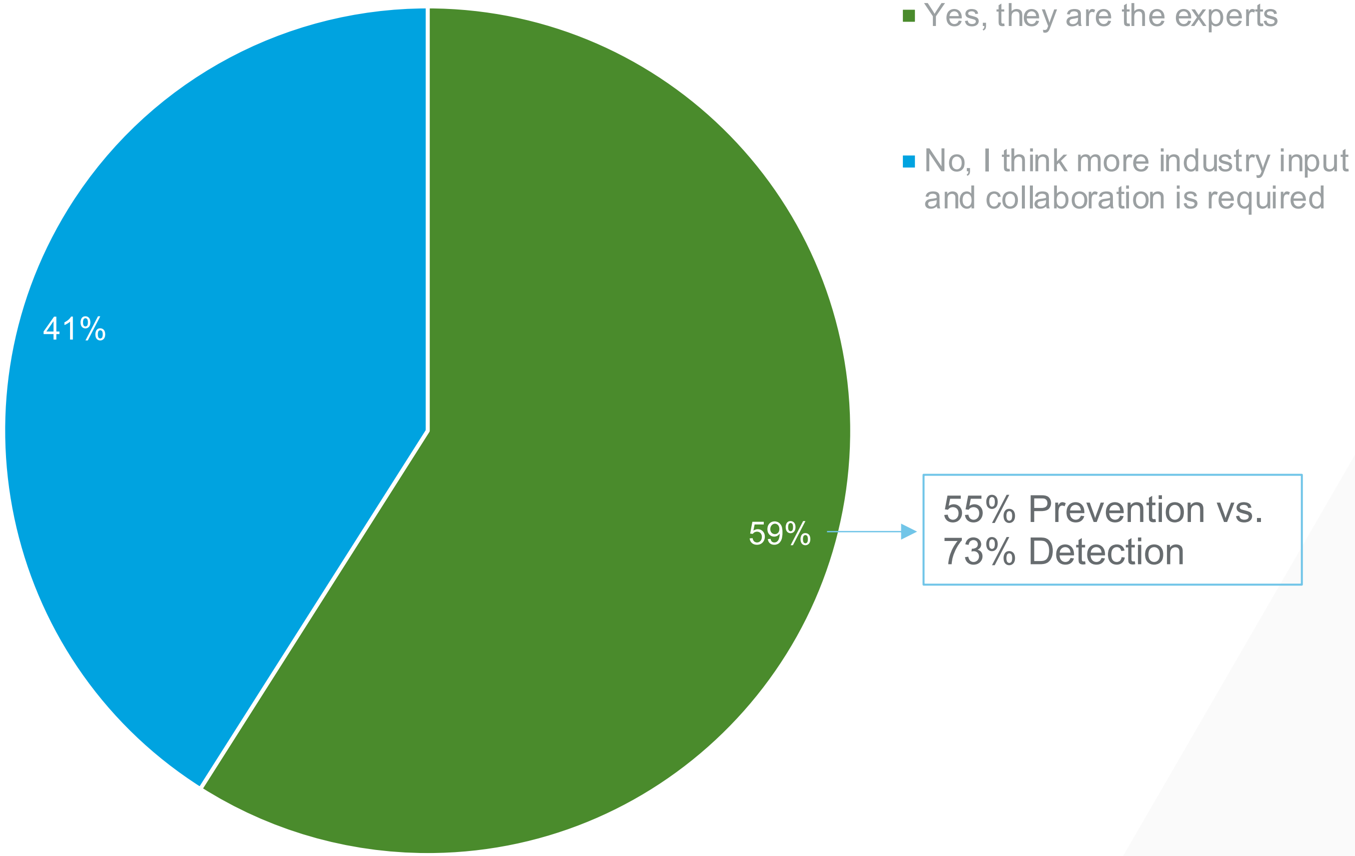


72% Managers vs.
89% C-level Executives

Q12. Do you think regulators have a strong enough understanding of the harsh realities that security teams are experiencing? Select one

Base: 200

59% feel legislators are well-equipped to be making decisions around cybersecurity related regulations

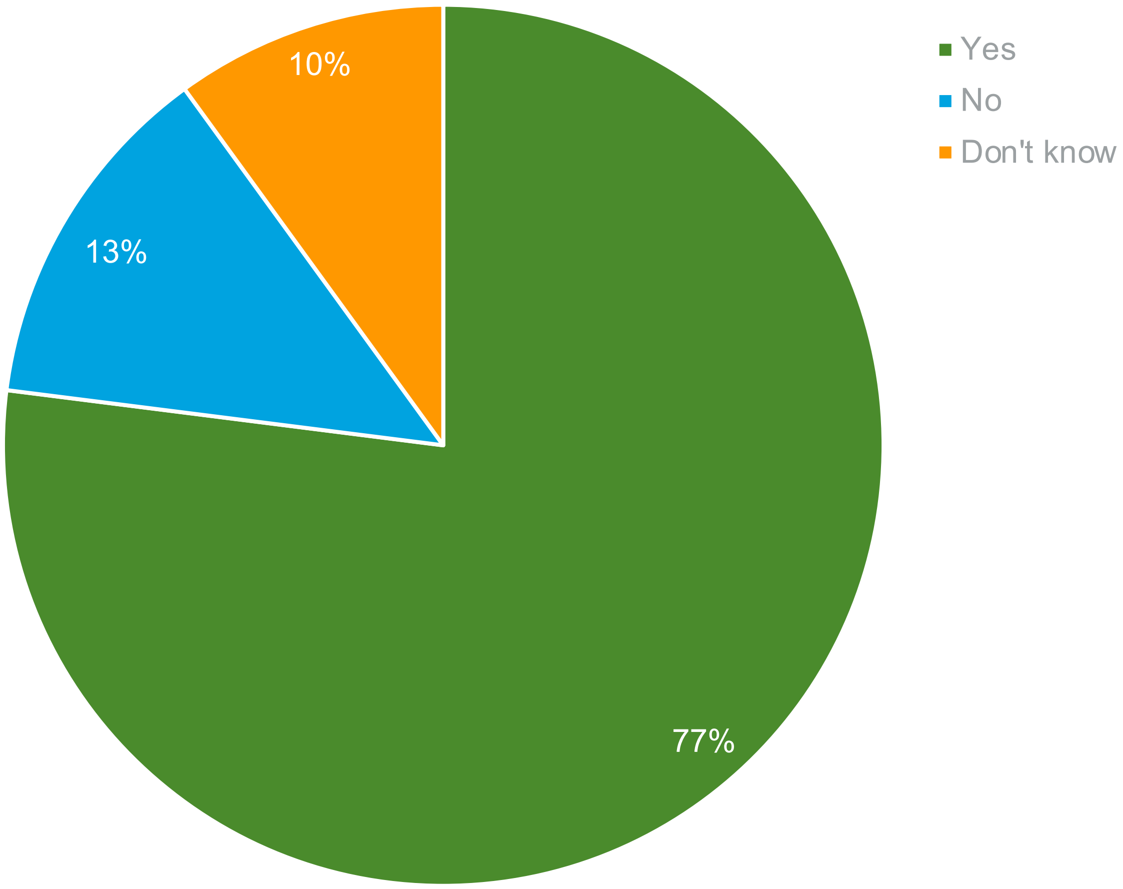


55% Prevention vs.
73% Detection

Base: 200

Q13. Do you think legislators are well-equipped to be making decisions around cybersecurity related regulations? Select one

Of those who have read or heard of the guidelines, 77% feel the guidelines are effective in helping defend against modern cyber-attacks



Q14a. Do you feel the previously mentioned guidelines are effective in helping organisations defend against modern cyber-attacks? Select one

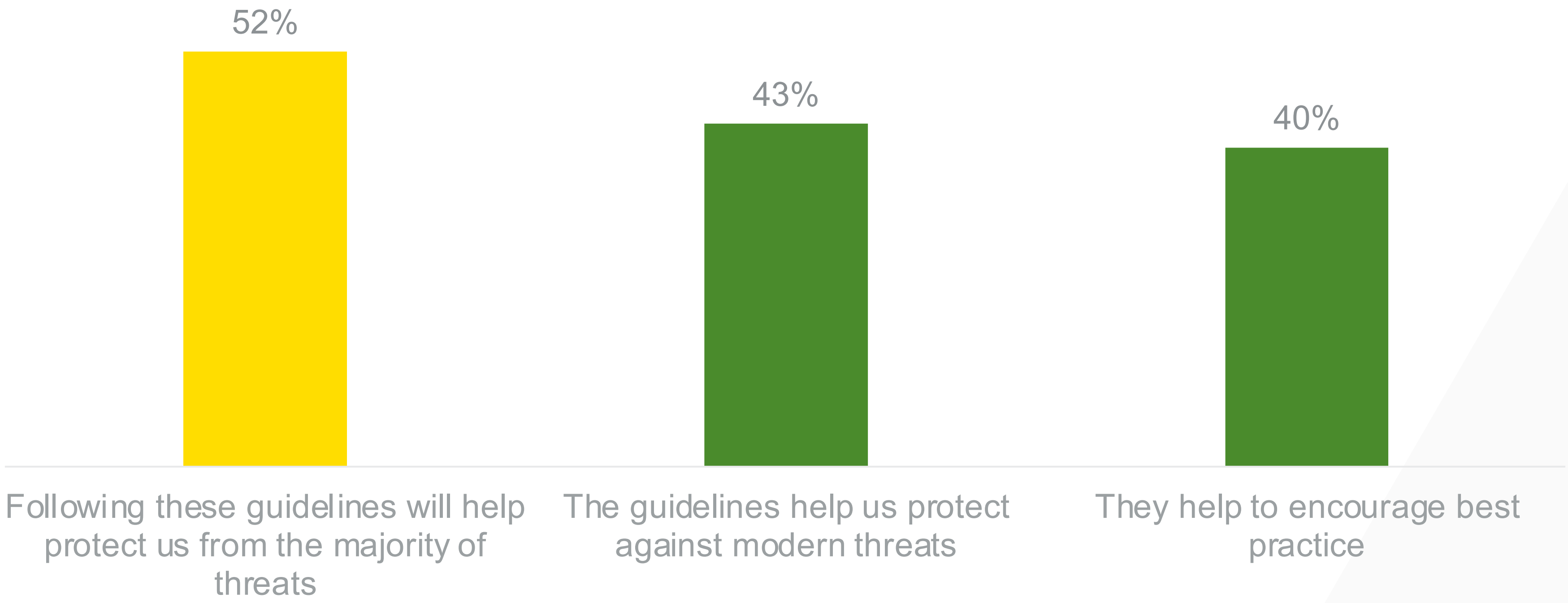
* Only asked to those who have read or heard of the the guidelines

* Only asked to those who have read or heard of the the guidelines

*Base: 1736

* Base: 179

Of those who consider the guidelines effective, 52% feel the guidelines will help mitigate most threats



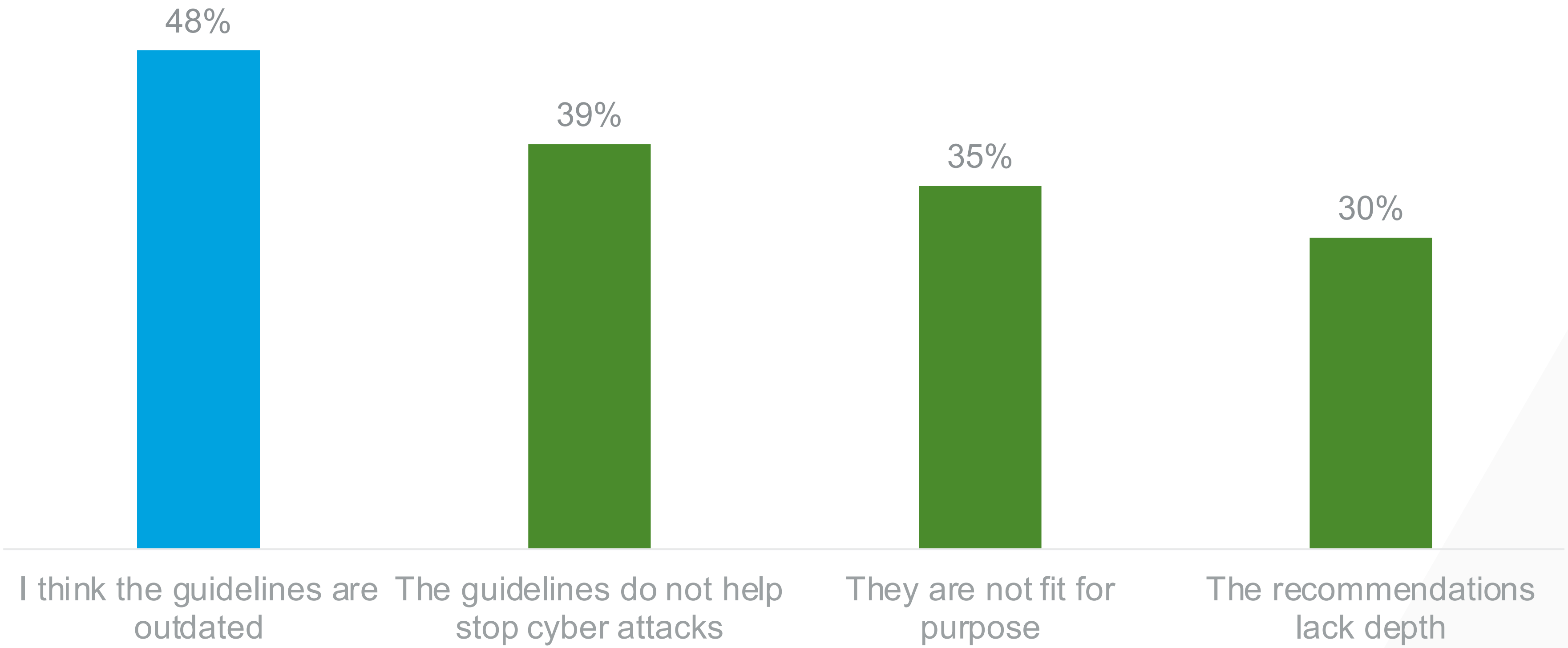
* Only asked to those who think the guidelines are effective

* Base: 138

Q14b. Why? Select all that apply

Of those who consider the guidelines ineffective, 48% feel the guidelines are outdated

NOTE: Low base size, recommend caution if using this data



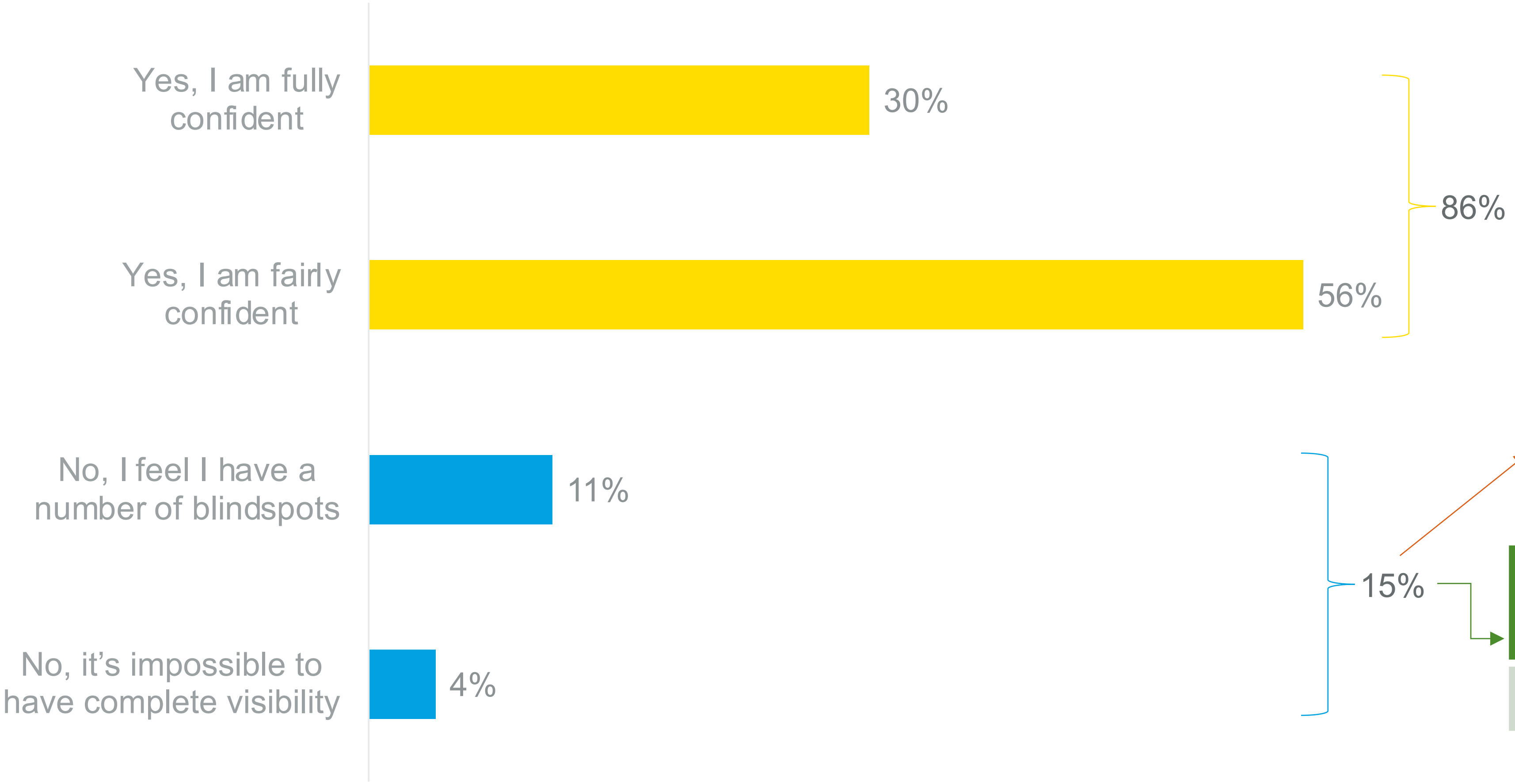
* Only asked to those who think the guidelines are ineffective

* Base: 23

Q14c. Why not? Select all that apply

15% do not feel confident that they have visibility of all threats facing their organisation

This is higher for Managers than C-Level Execs



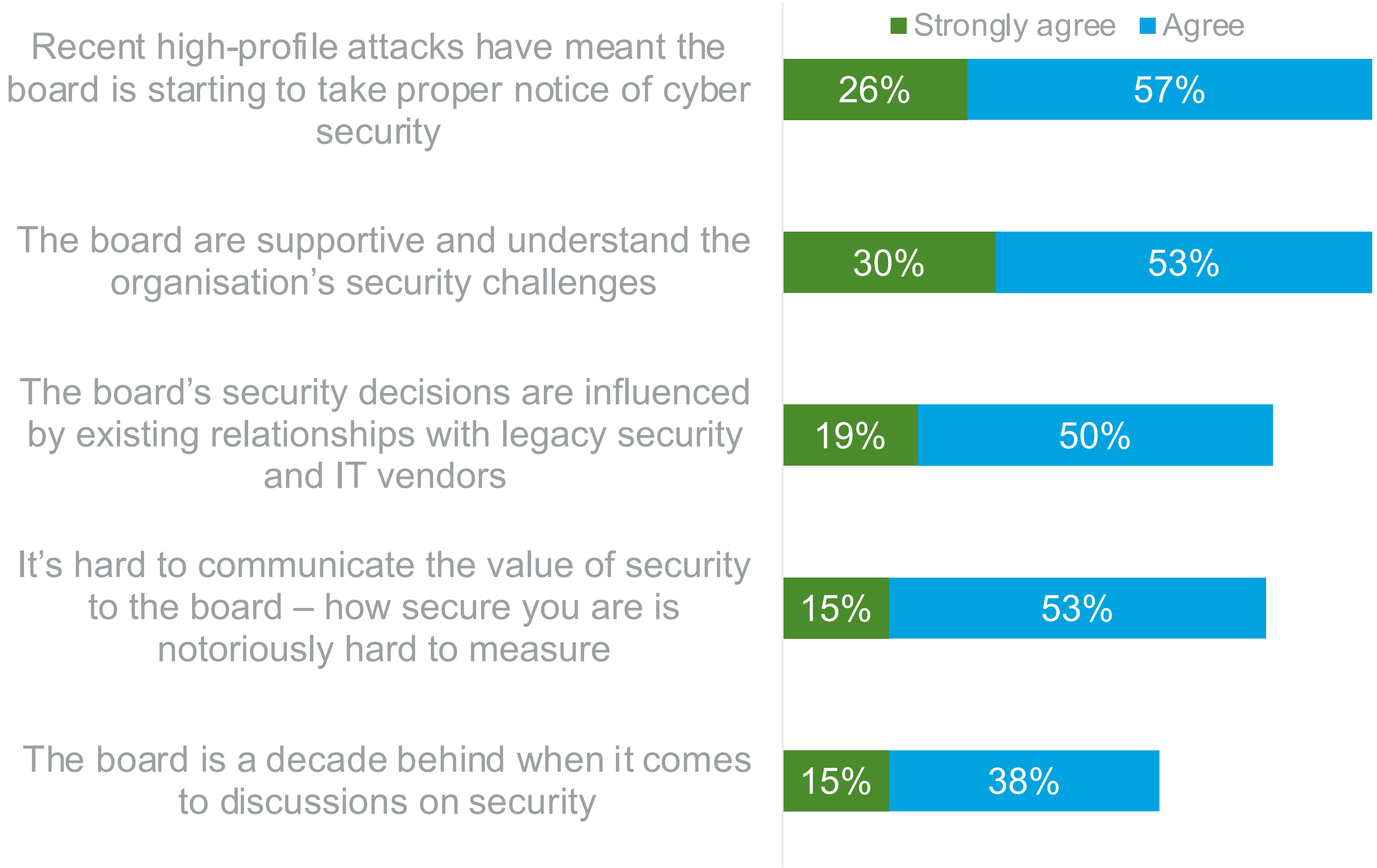
19% Managers vs.
5% C-Level Executives

501 - 1,000 employees	1,001 - 5,000 employees	5,001 - 10,000 employees	10,001+ employees
10%	10%	15%	32%

Q15. Do you feel confident that you have visibility of all the threats facing your organisation? Select one

Base: 200

There is wide consensus over the board beginning to take proper notice of cyber security (83%)



% Agree

83% → 501 – 1000 employees (**90%**)
10001+ employees (**58%**)

82% → 76% Managers vs.
95% C-Level Executives

69% → 5001 – 10000 employees (**80%**)
10001+ employees (**58%**)

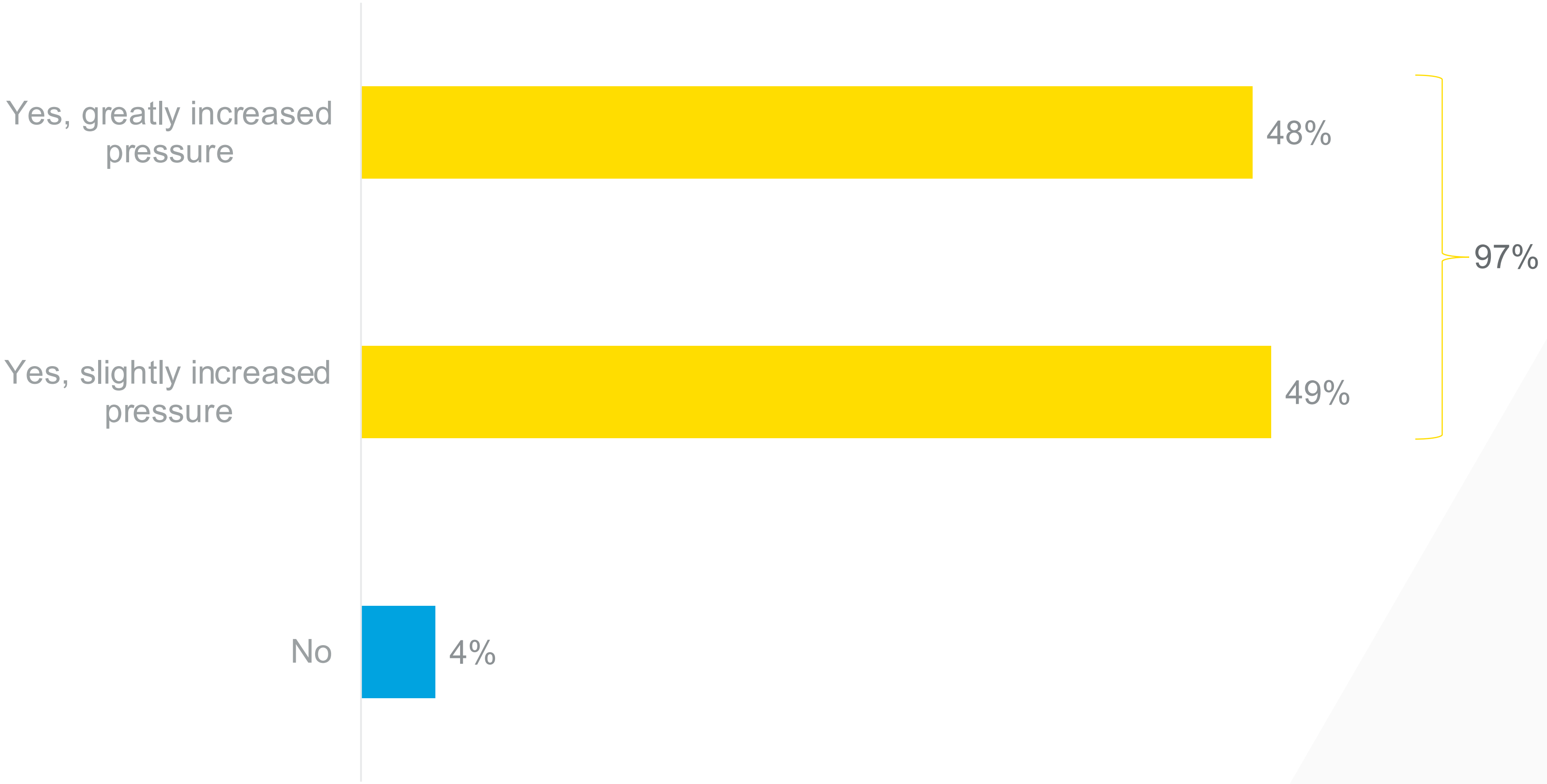
68% → 63% Prevention vs.
81% Detection

53% → 50% IT/Telecoms vs.
79% Professional Services

Q16. To what extent do you agree with the following statements? Select one per row

Base: 200

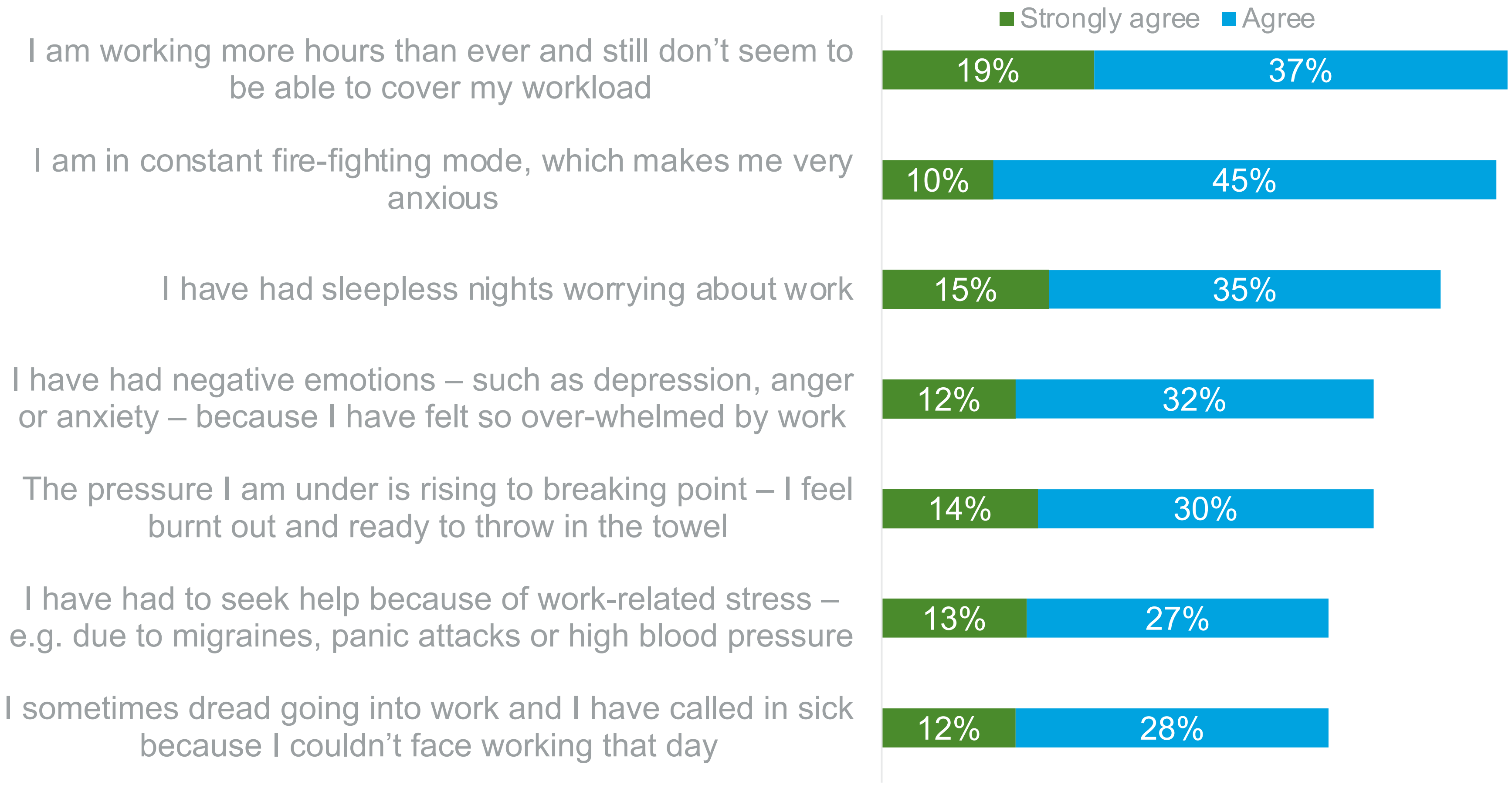
97% have felt increased pressure to keep their organisation safe over the past year



Q17. Have you felt increased pressure to keep your organisation safe over the past year? Select one

Base: 200

There is wide consensus over the common experience of not covering workloads despite working more hours (56%)

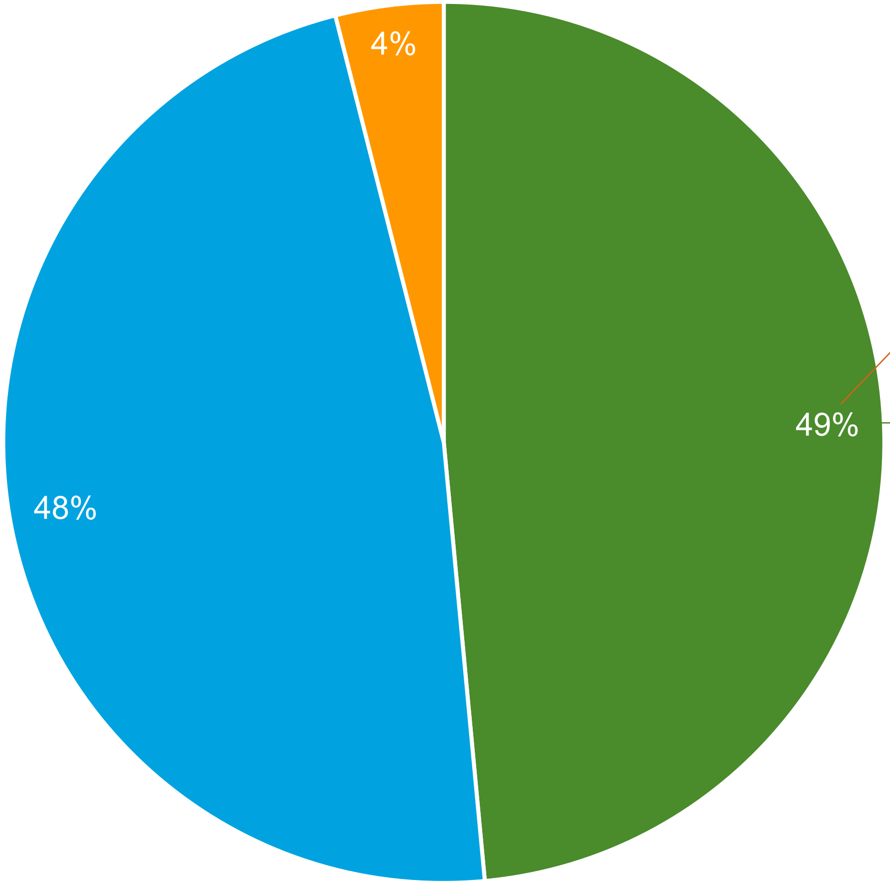


% Agree	
56%	1001 – 5000 employees (**66%**) 5001 - 10000 employees (**45%**)
55%	46% Managers vs. 78% C-Level Executives
49%	40% Managers vs. 70% C-Level Executives
44%	38% Prevention vs. 63% Detection
43%	
40%	
40%	

Q18. To what extent do you agree with the following statements? Select one per row

Base: 200

49% have suffered a significant cybersecurity incident in the past year



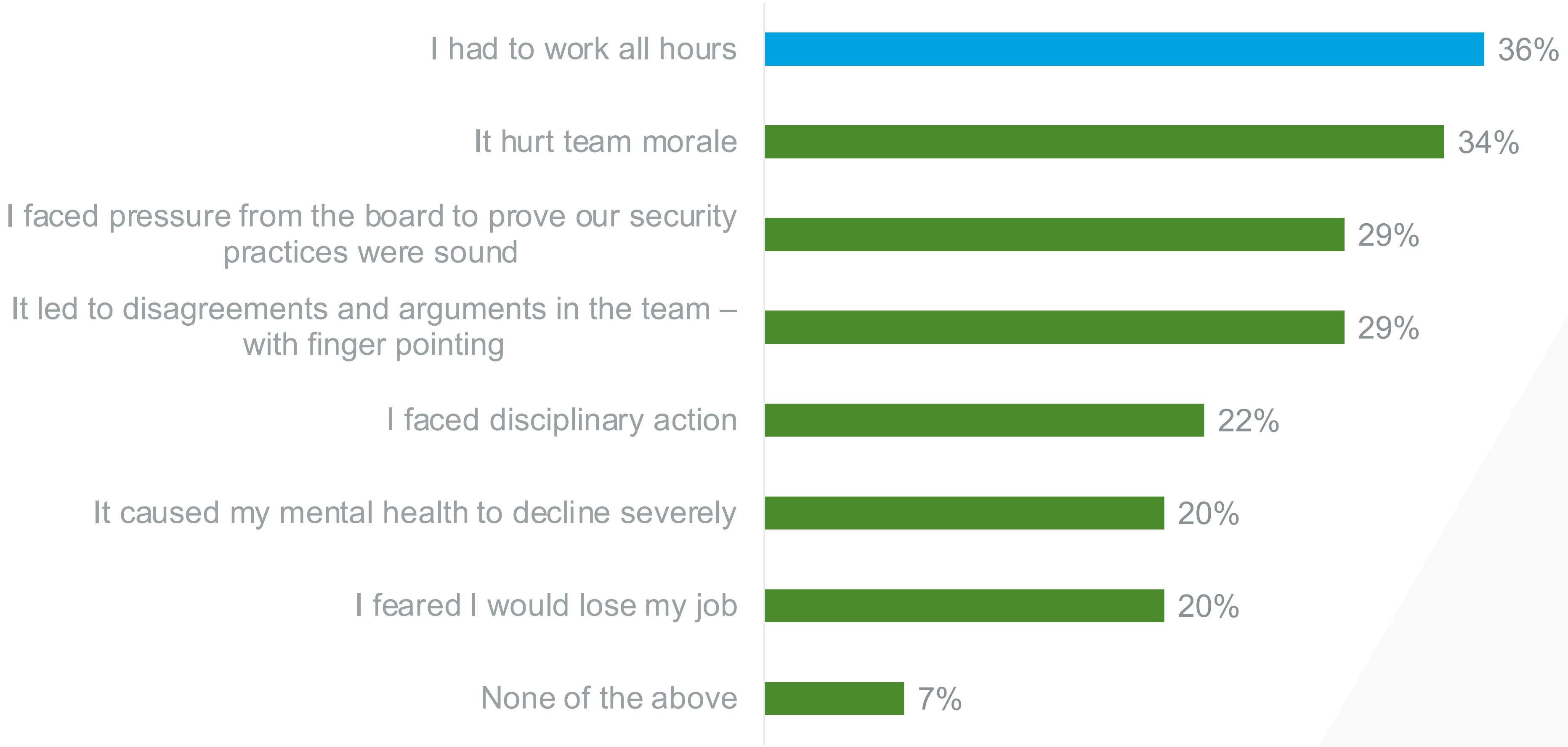
41% Managers vs.
62% C-Level Executives

41% IT/Telecoms vs.
66% Professional Services

Q19. Has your organisation suffered a significant cybersecurity incident in the past year? Select one

Base: 200

Of those who suffered a major cybersecurity attack in the past year, the most common experience was having to work all hours (36%)

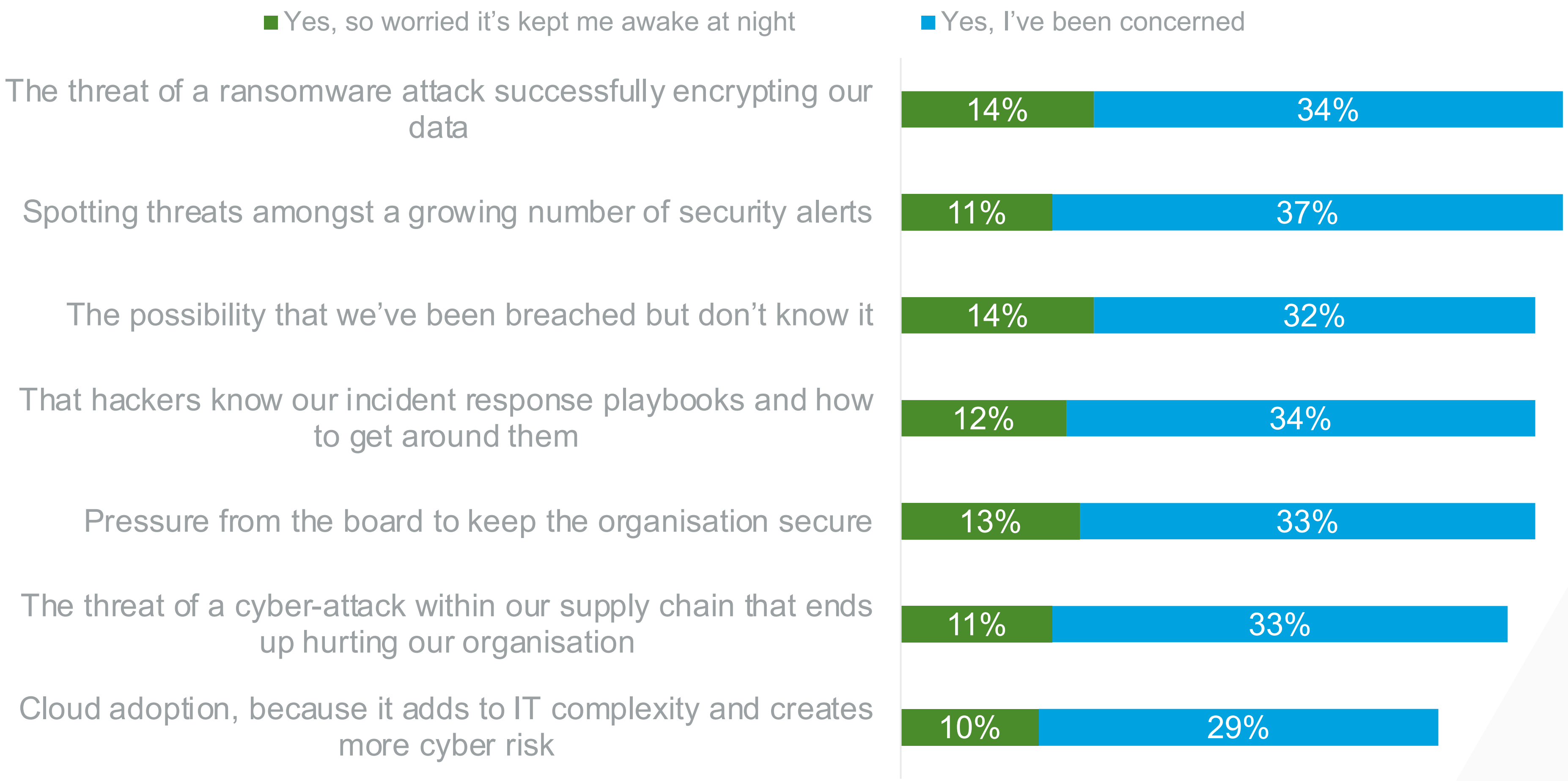


* Only asked to those who have suffered a significant cyber security incident in the past year

* Base: 97

Q20. What was the effect of this incident on you and your team? Select all that apply

Respondents are most concerned with ransomware attacks or spotting threats amongst a growing number of alerts (48%)

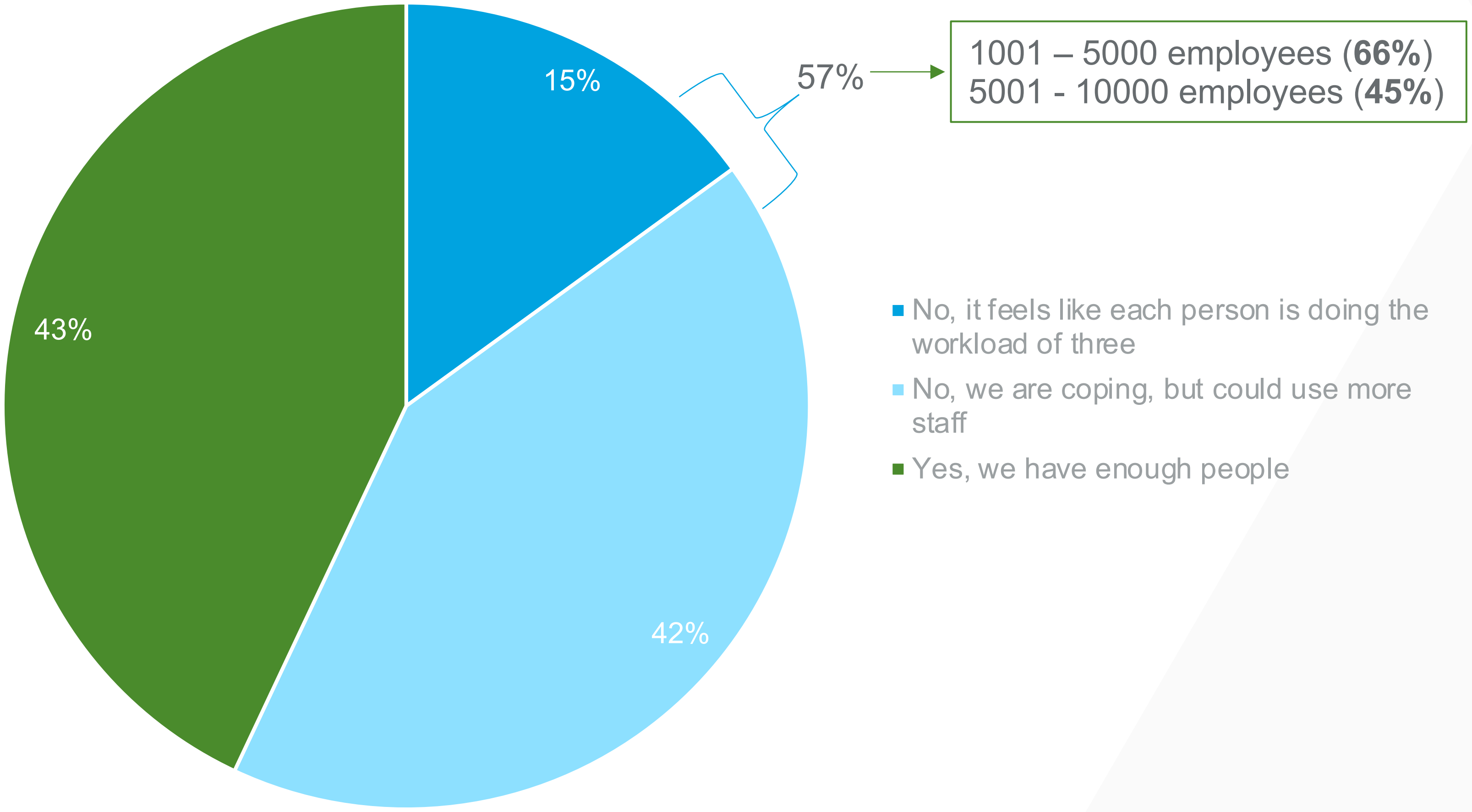


% Concerned
48%
48%
46%
46%
45%
44%
39%

Base: 200

Q21. Have you worried about the following over the past year? Select one per row

57% feel they could use more security talent on their team

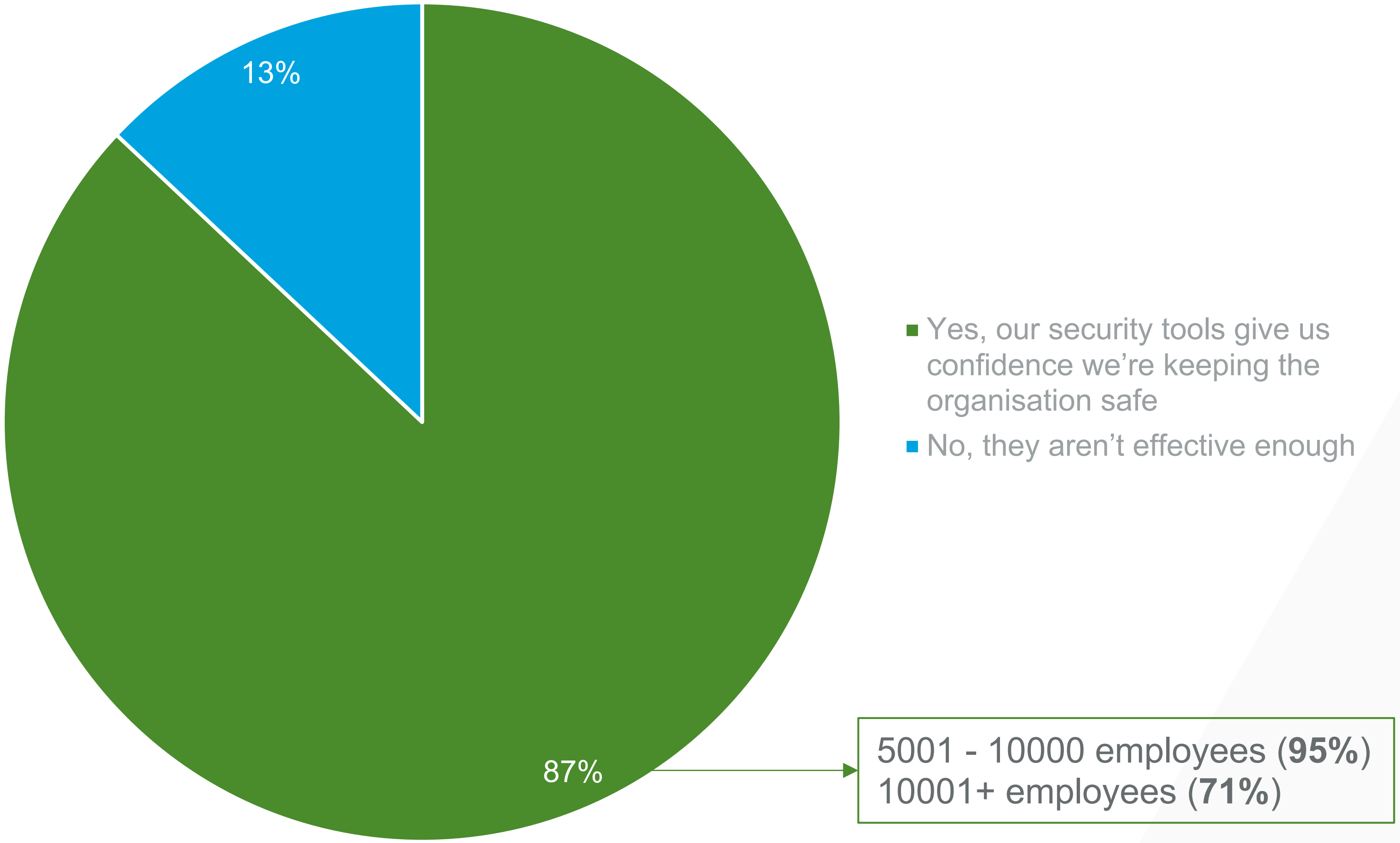


1001 – 5000 employees (**66%**)
5001 - 10000 employees (**45%**)

Q22. Do you have enough security talent on your team? Select one

Base: 200

87% feel their security tools are effective at keeping their organisation safe



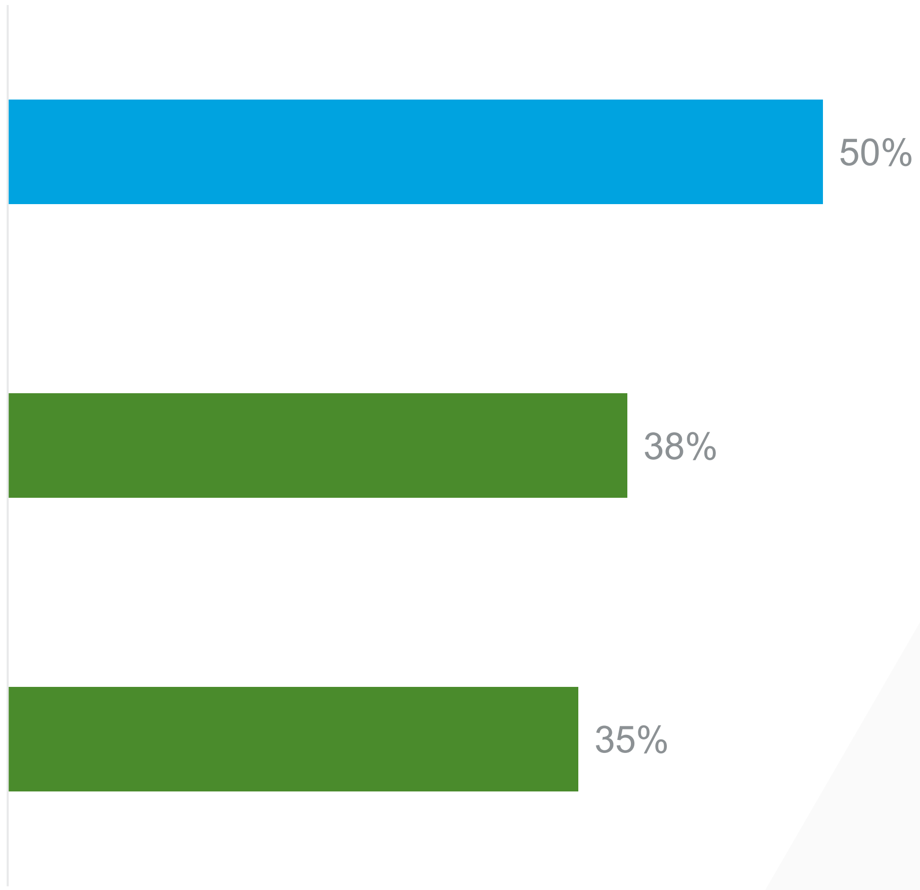
5001 - 10000 employees (**95%**)
10001+ employees (**71%**)

Q23a. Are your security tools effective enough at reducing the pressures your team faces? Select one

Base: 200

Of those who feel their security tools are ineffective, most are worried the tools have missed something (50%)

NOTE: Low base size, recommend caution if using this data



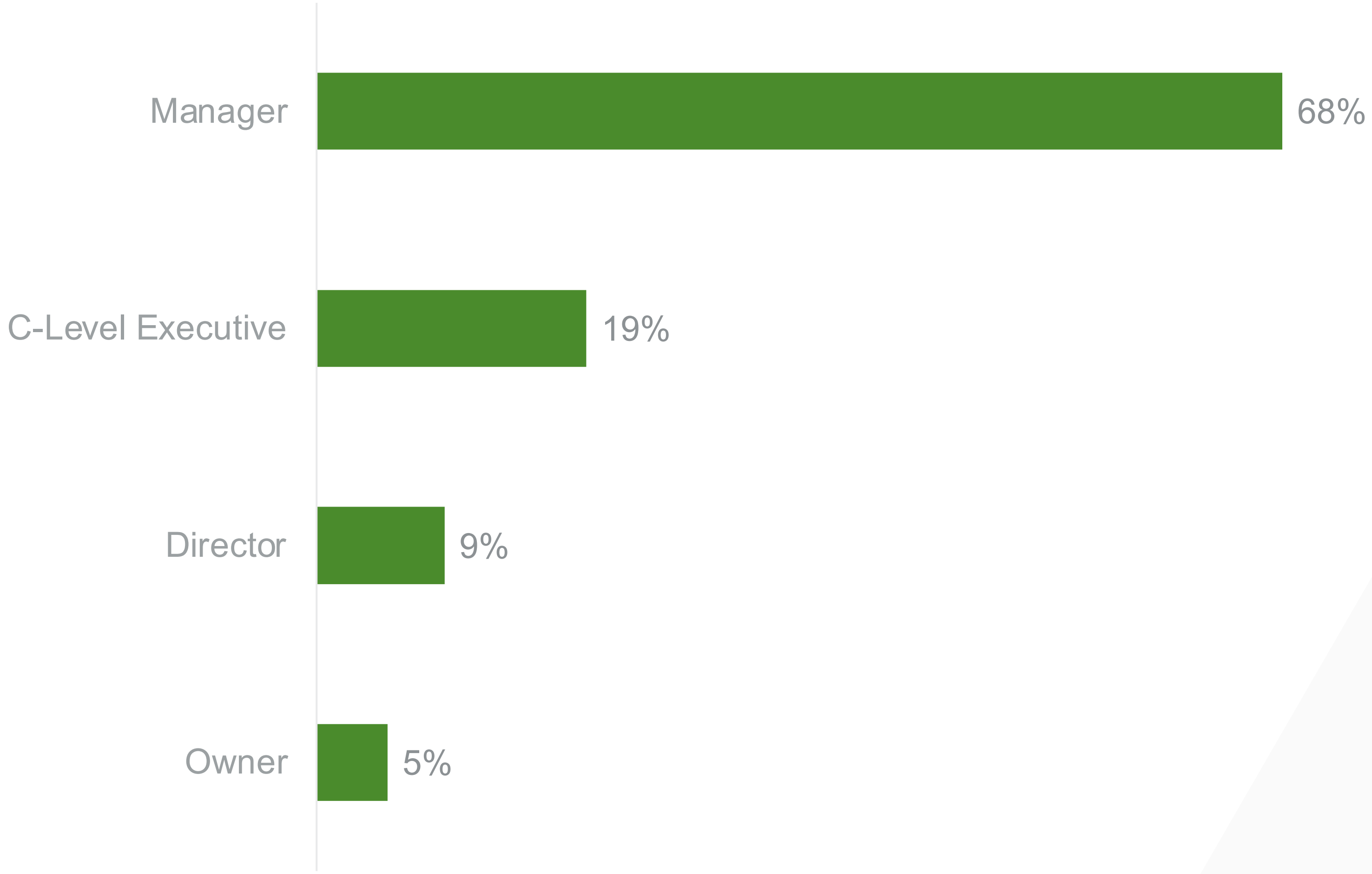
* Only asked to those who think their security tools are not effective enough

* Base: 26

Q23b. Why not? Select all that apply

Demographics

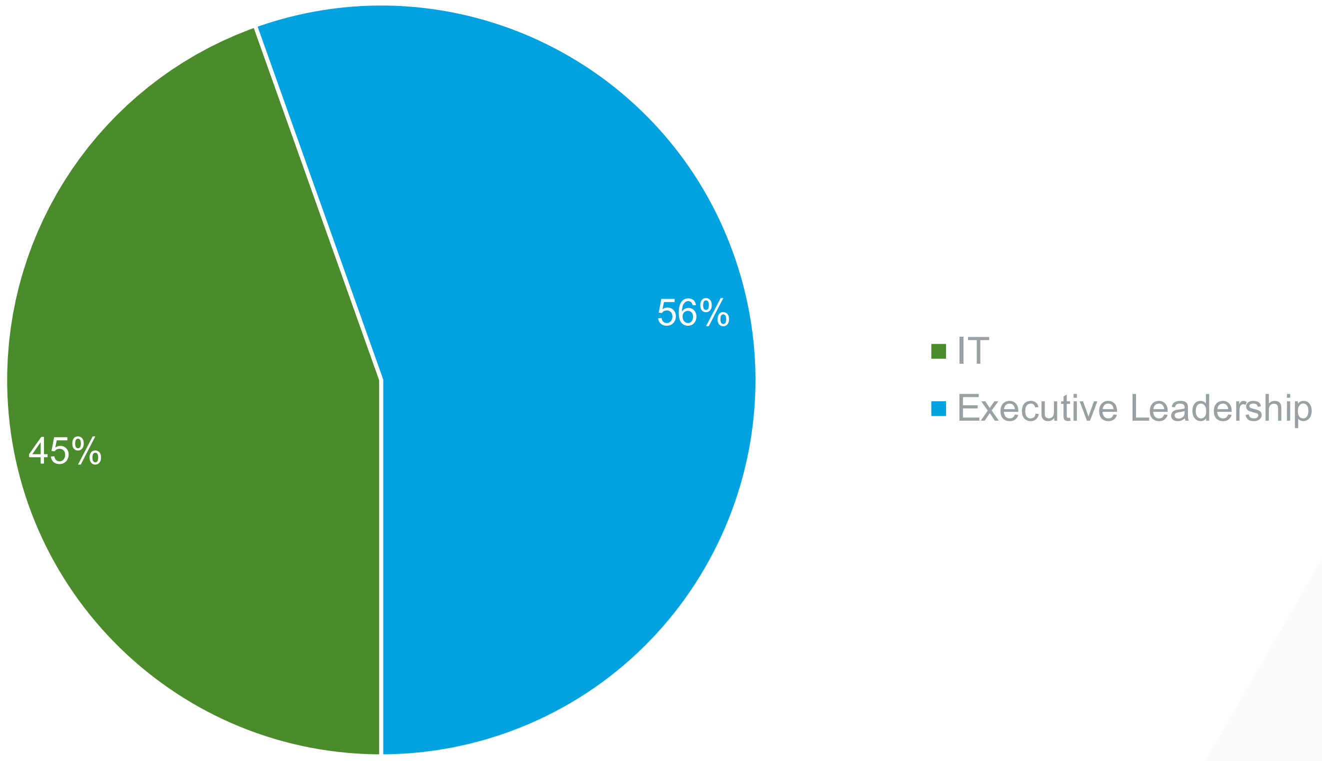
Role



S1. Which of these best describes your role? Select one

Base: 200

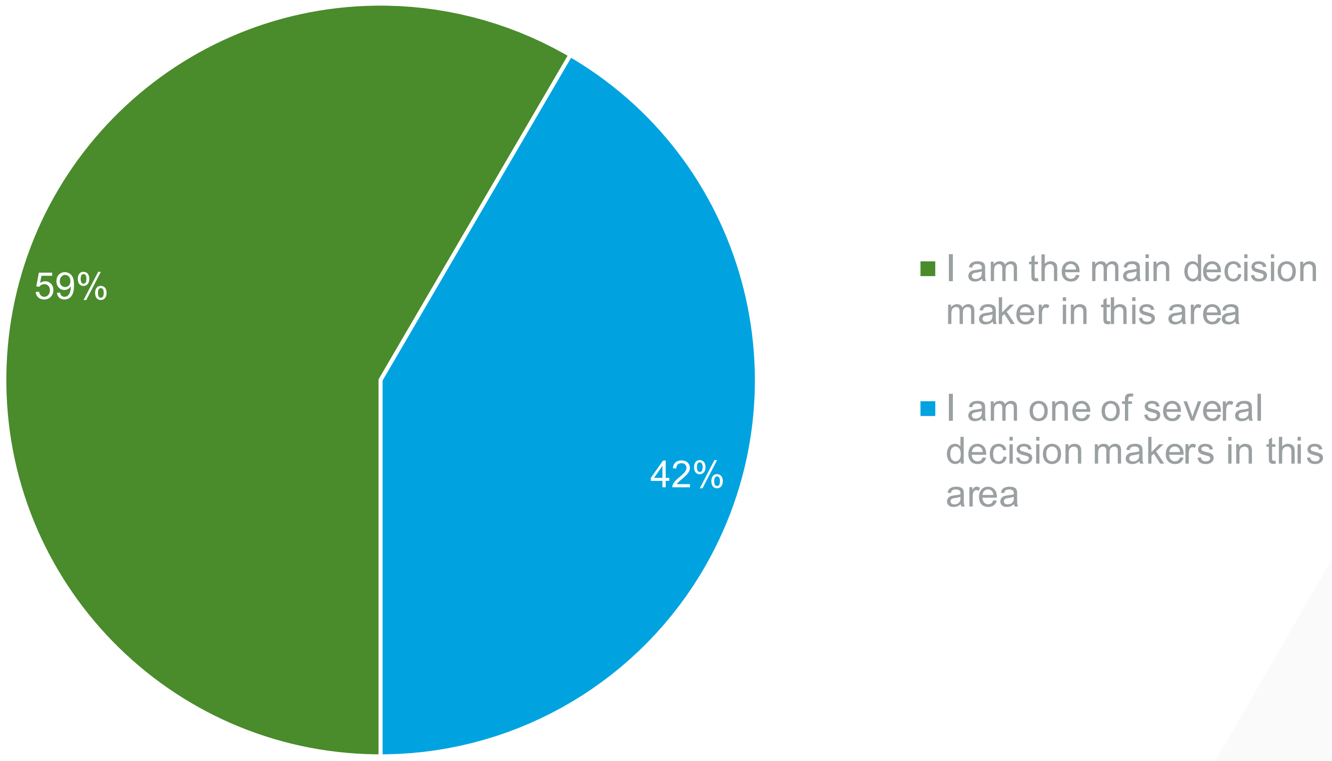
Area of Work



S1a. What best describes the area you work in? Select one

Base: 200

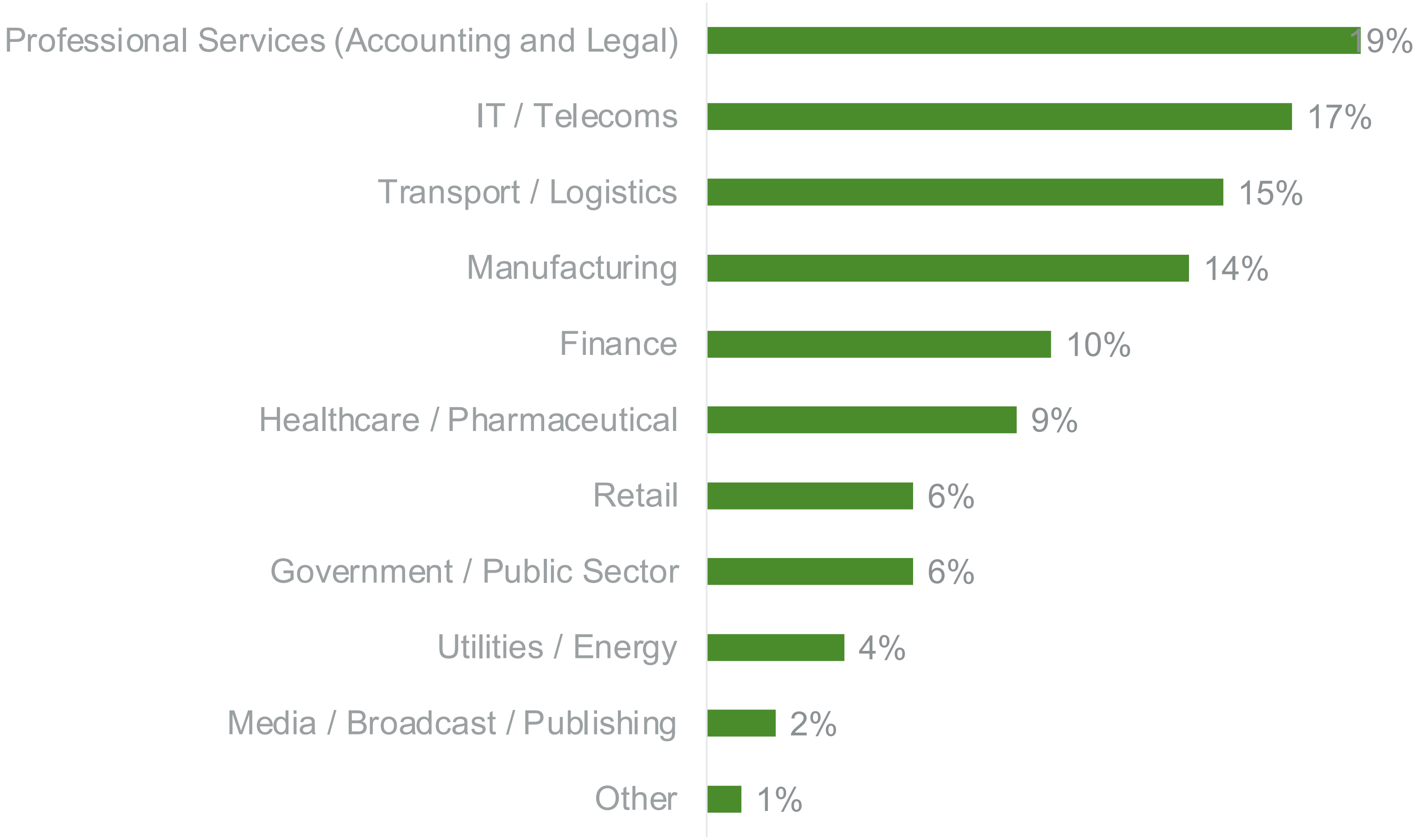
Decision-making Influence



S2. How much influence do you have over IT security decisions at your company? Select one

Base: 200

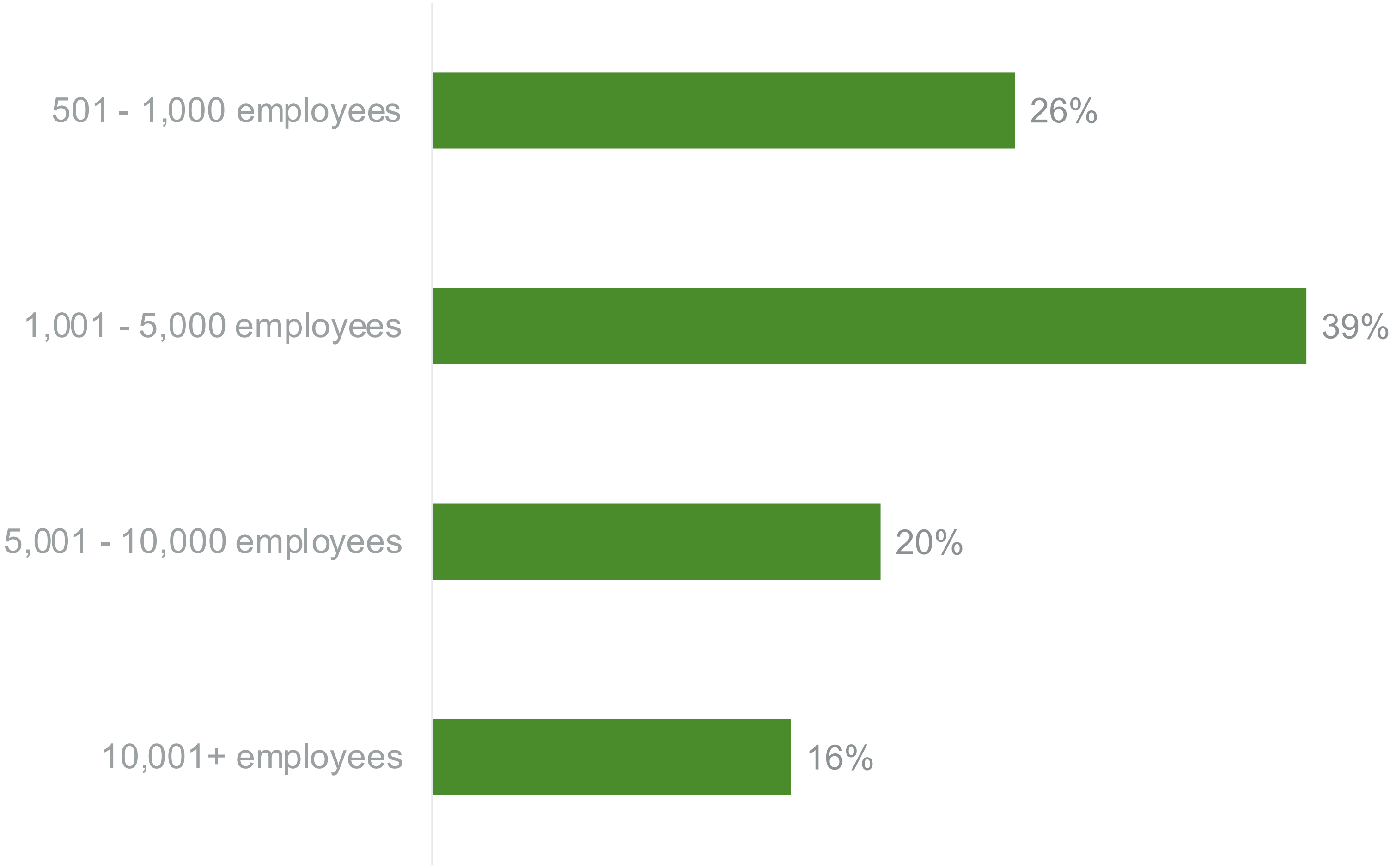
Industry



S3. Which of the following most closely describes your industry? Select one

Base: 200

No. of Employees

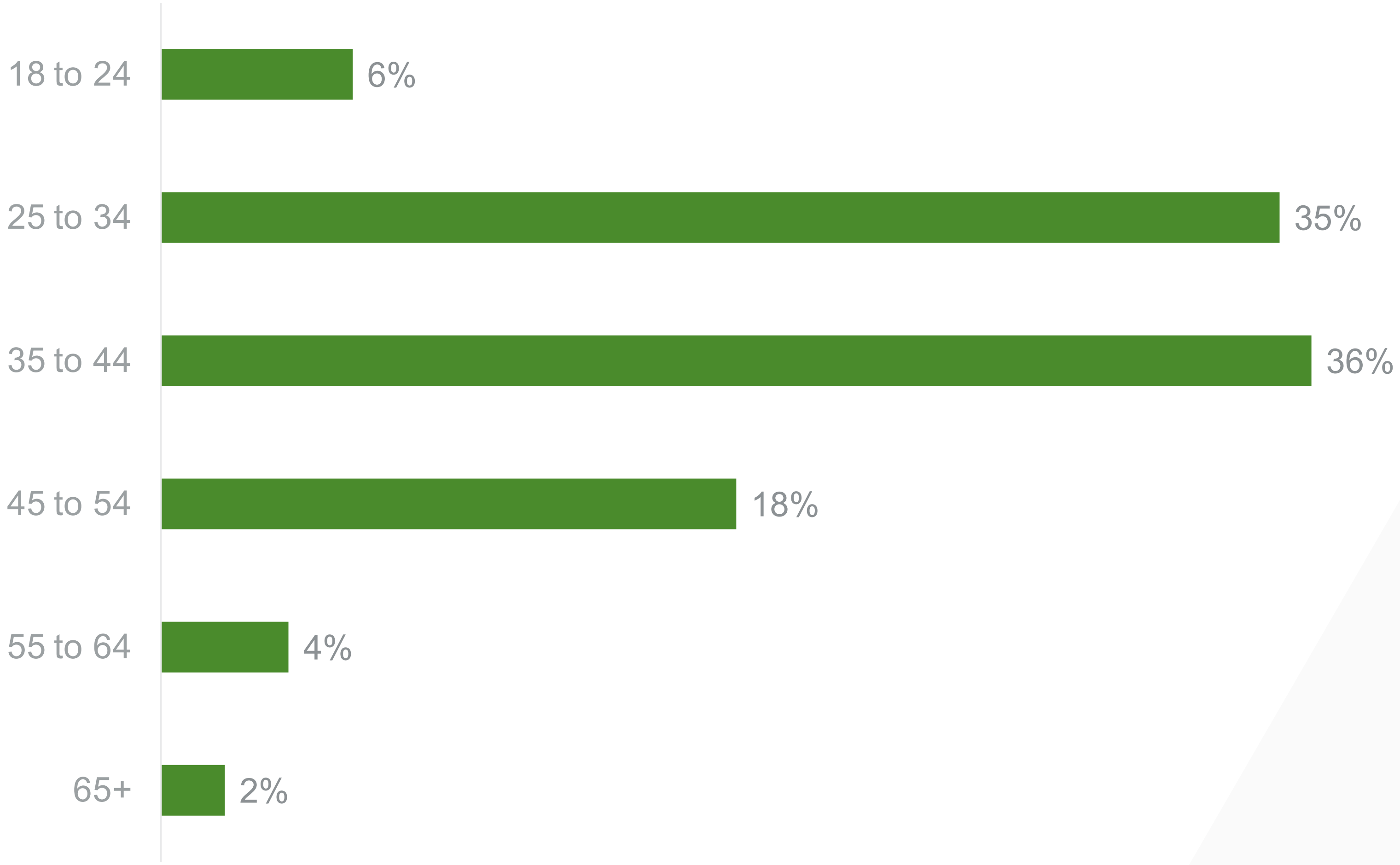


S4. How many people does your organisation employ? Select one

Base: 200

VECTRA
SECURITY THAT THINKS.

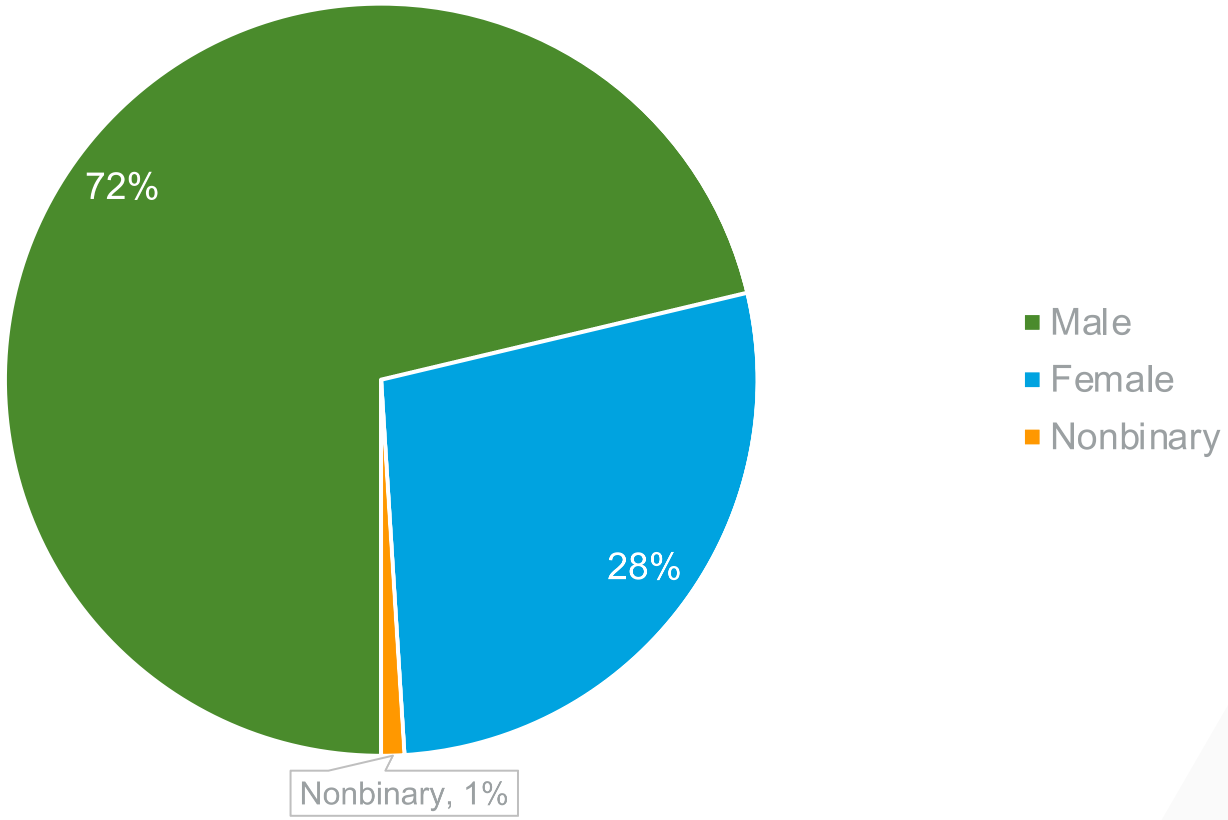
Age



D1. How old are you? Select one

Base: 200

Gender



D2. Are you… Select one

Base: 200

Sapio Research

We are an enthusiastic **team of market researchers** based in London. Our agency is passionate about providing **high quality, precise, cost-effective and efficient solutions** for your research needs.

We help our clients in all areas of **quantitative and qualitative research**, and welcome complex, challenging briefs. We can help to formulate the approach, to create the scope and design the process.

We will **propose whatever approach works best**, and you-can rely on us to tell you what we really believe, rather than what we think you might want to hear.

Whether agency, brand, charity, consultancy, you will find us **friendly, forthright, flexible and fast.**

SAPIO RESEARCH

Audience | Brand | Content Research

www.sapioresearch.com

VECTRA®

SECURITY THAT THINKS.®