VECTRA®

SECURITY THAT THINKS.®

VEC2101 Vectra IT Security Research Sweden

February 2022

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 1000 employees in Sweden.
- 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

91% have felt increased pressure to keep their organisation safe over the past year

51% have suffered a significant cybersecurity incident in the past year

82% have experienced a significant security event that required an incident response effort

82% have purchased a security solution that has failed on at least one occasion

63% feel they could use more security talent on their team

88% 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, 54% of companies invest more into prevention tools.

2

Poor integration poses dilemmas – Poor integration with other tools is the most frequent issue. 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

Swedish companies make use of the guidelines – The majority have read the cyber security guidelines, with most finding it at least somewhat useful. However only 15% felt they covered everything.

4

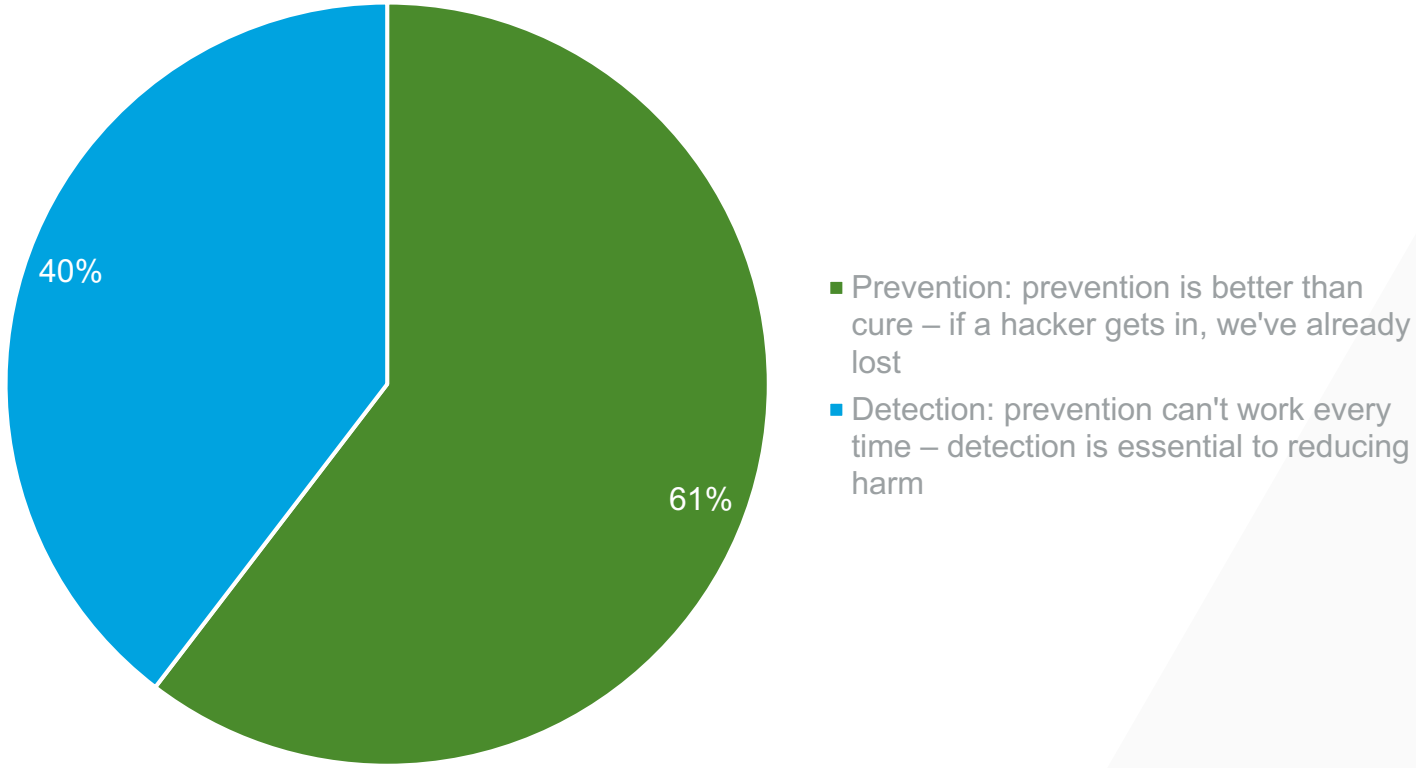
Regulators and legislators are generally up to speed – The general consensus is that regulators have adequate understanding of challenges while legislators are well-equipped for designing regulations. Those working in finance and owners are more supportive of regulators and legislators.

5

Room for improvement going forward – Many feel more security talent is needed on their team, particularly those who place greater importance on the detection of threats as opposed to prevention. Security tools are not always reliable and may miss threats.

Main Findings

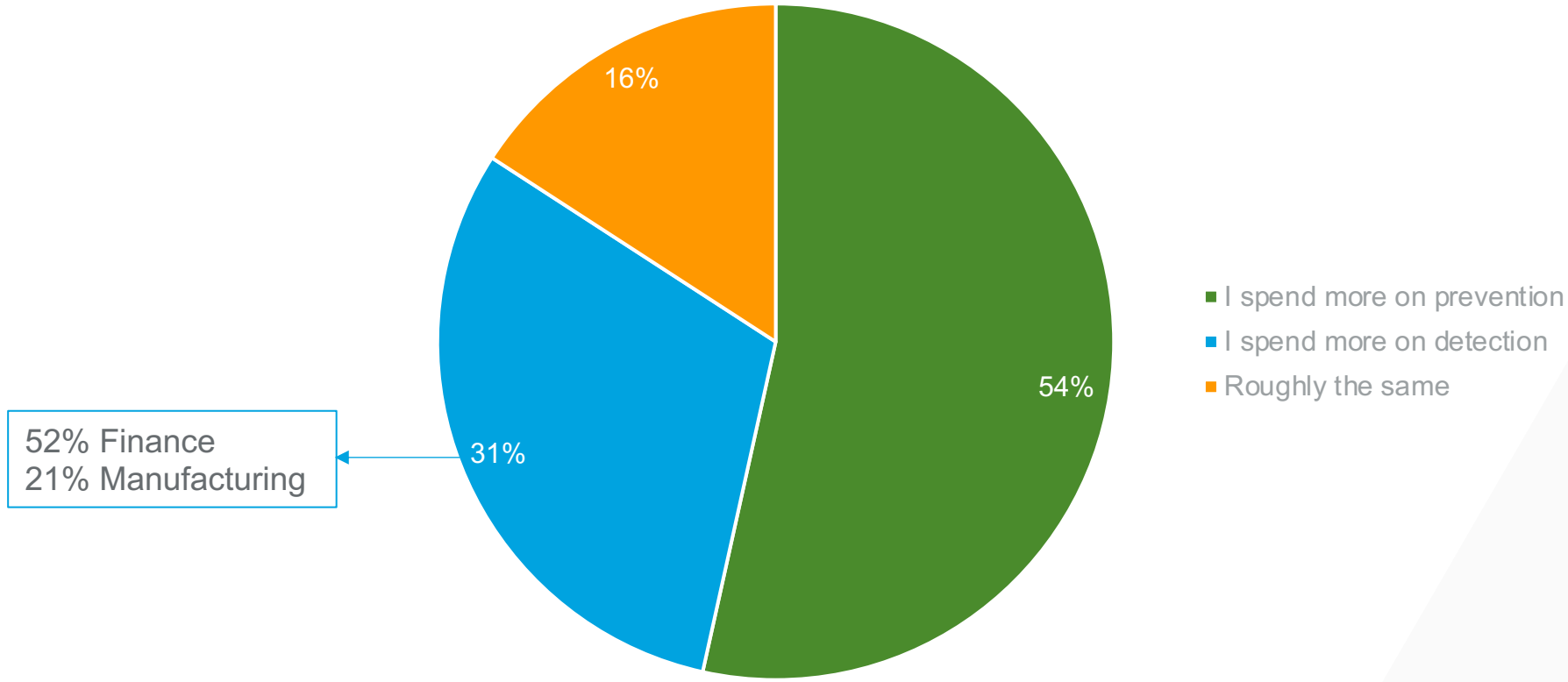
61% believe preventing hackers from breaching defences is more important than detection after a breach has already occurred



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

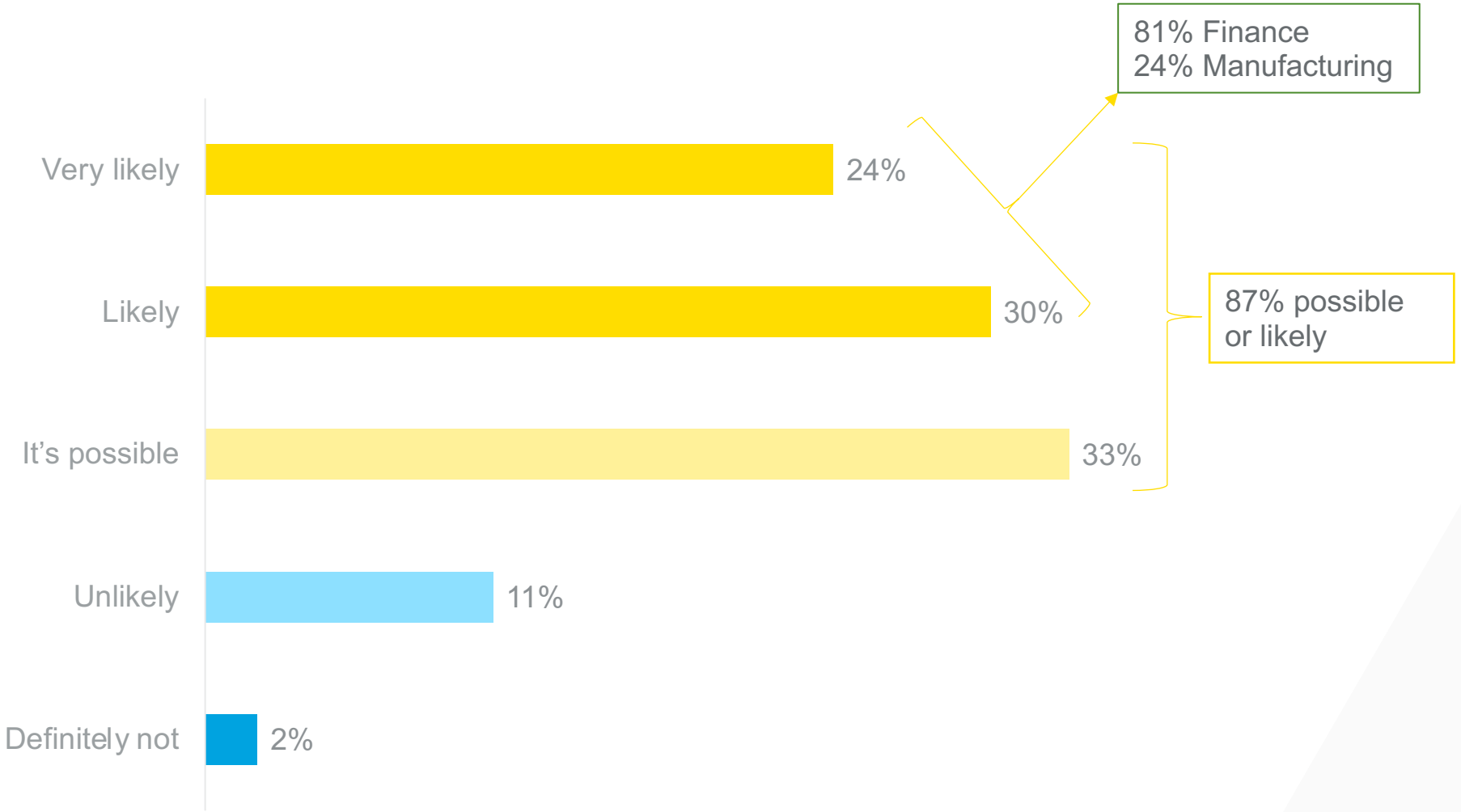
54% invest more into prevention tools
Just under a third spend more on detection (31%)



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

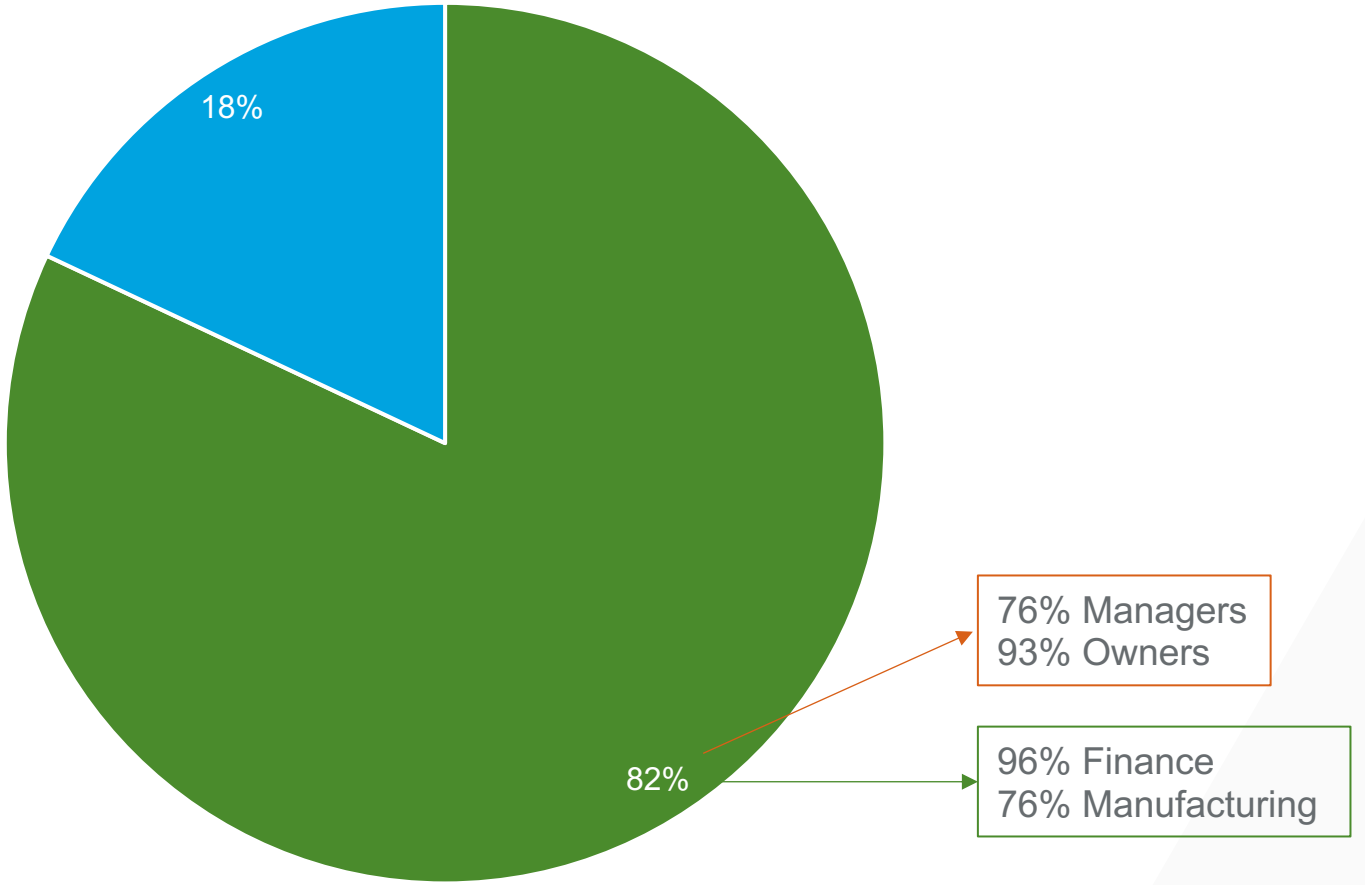
87% feel it is possible or likely they have been breached whilst being unaware of it happening



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

Base: 200

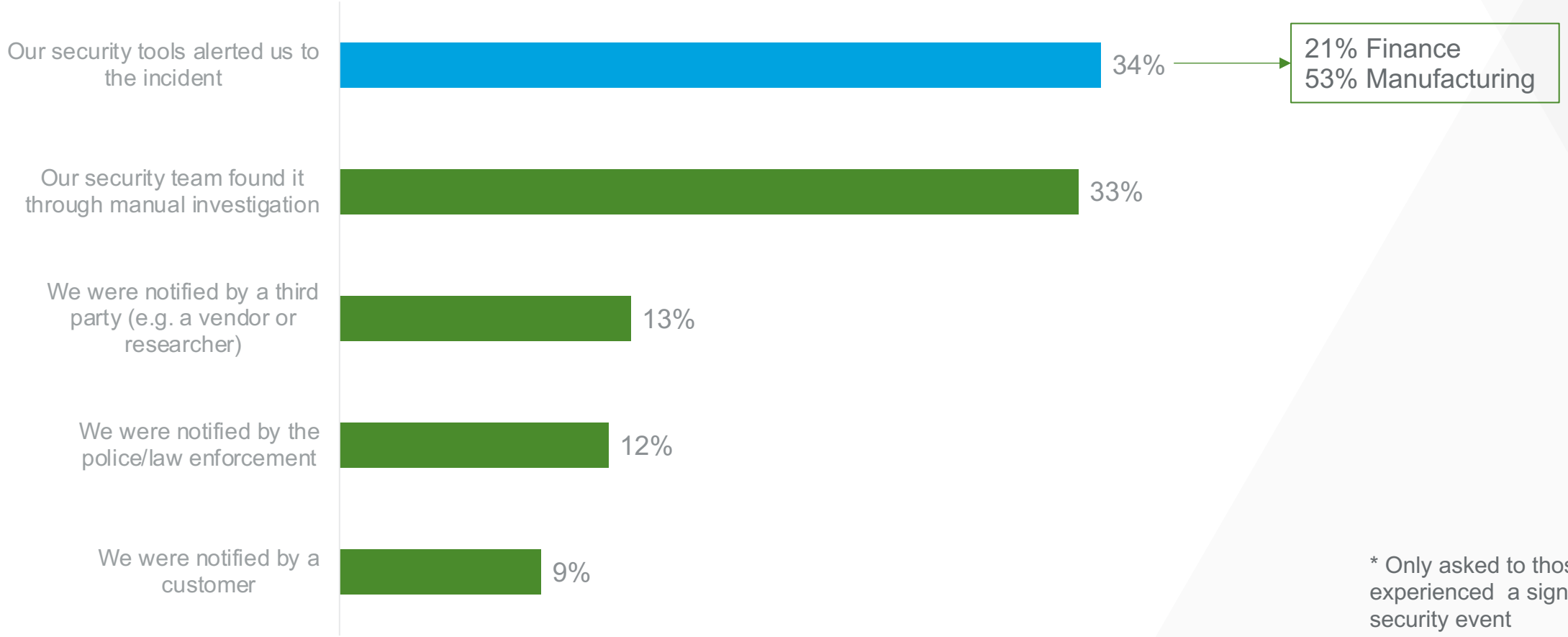
74% have experienced a significant security event that required an incident response effort



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 (34%)

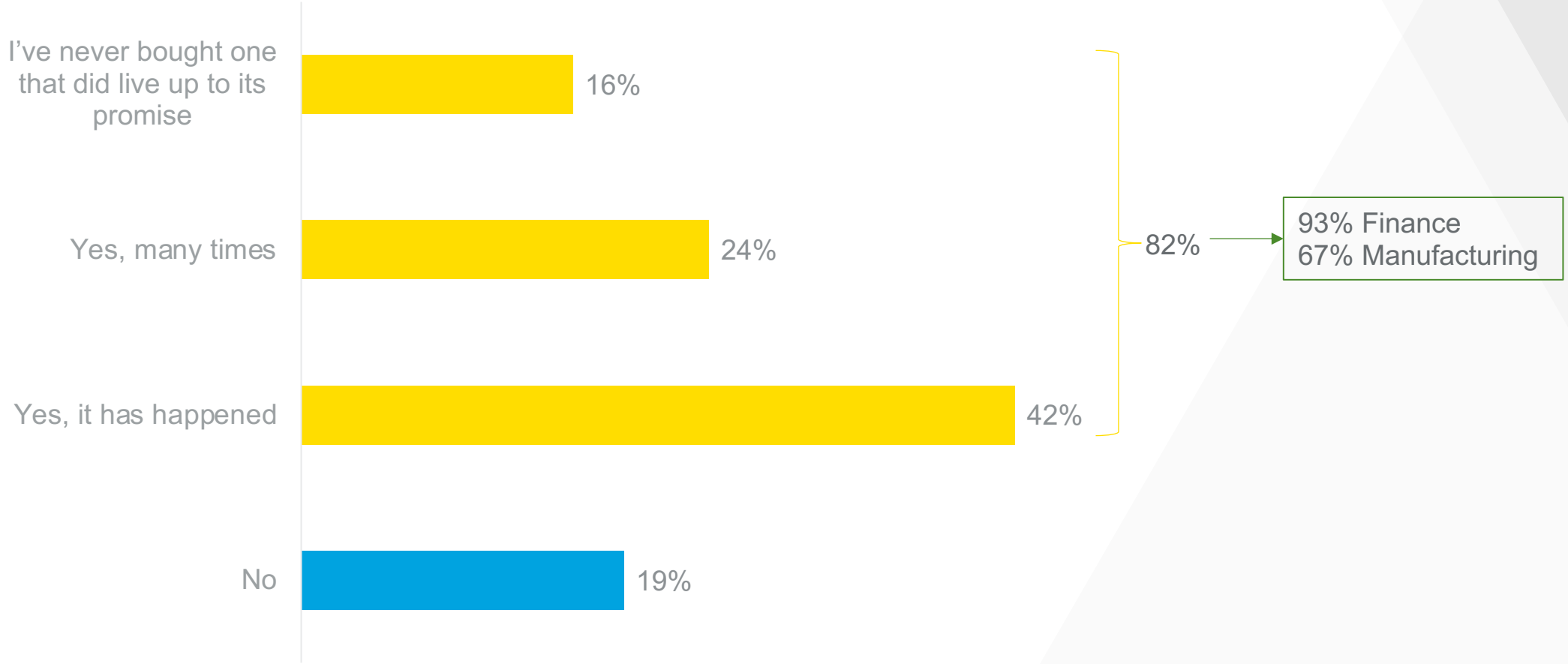


* Only asked to those who experienced a significant security event

* Base: 164

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

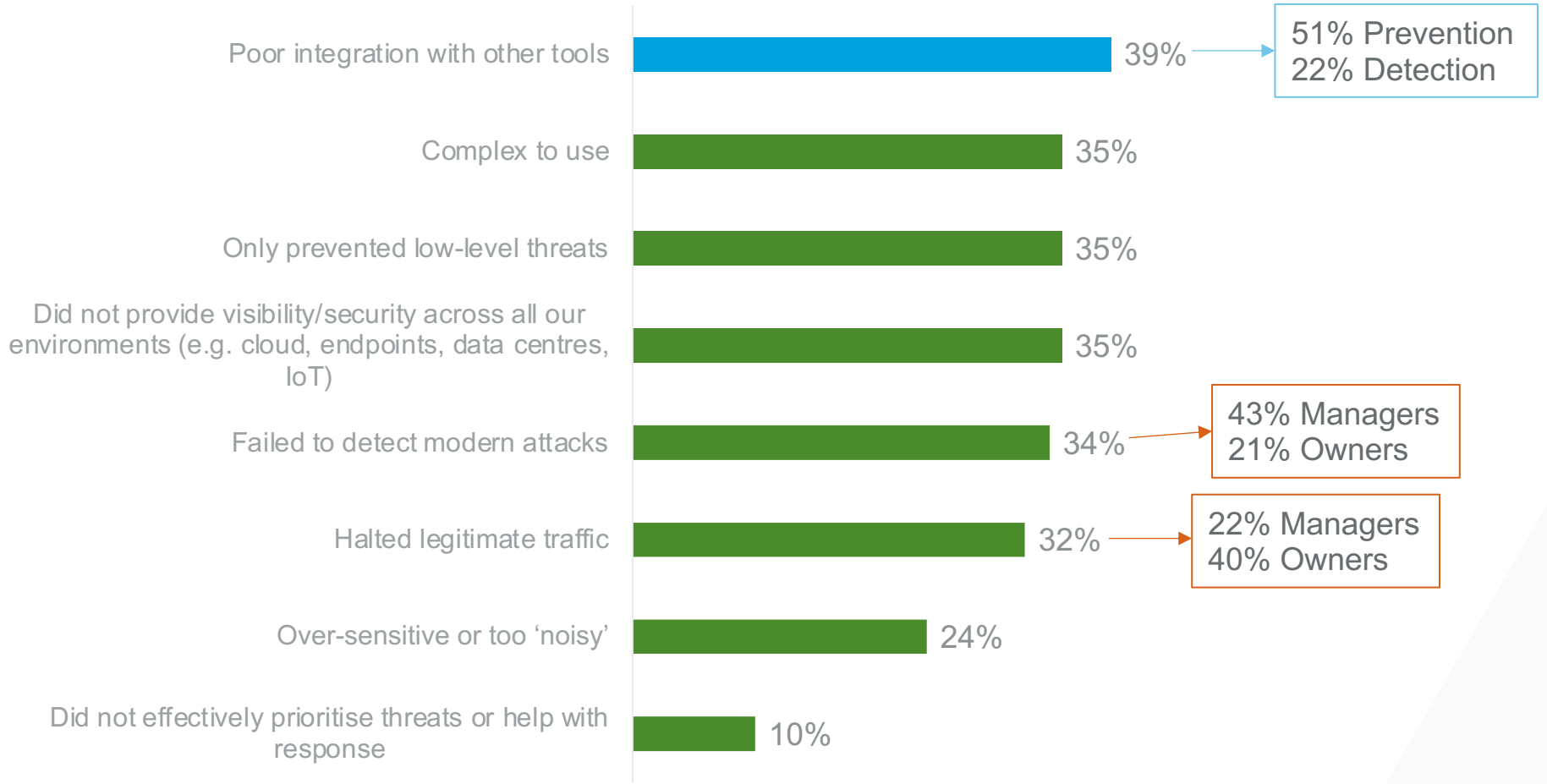
82% have purchased a security solution that has failed on at least one occasion



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

Base: 200

Poor integration with other tools is the most experienced issue (39%)



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

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

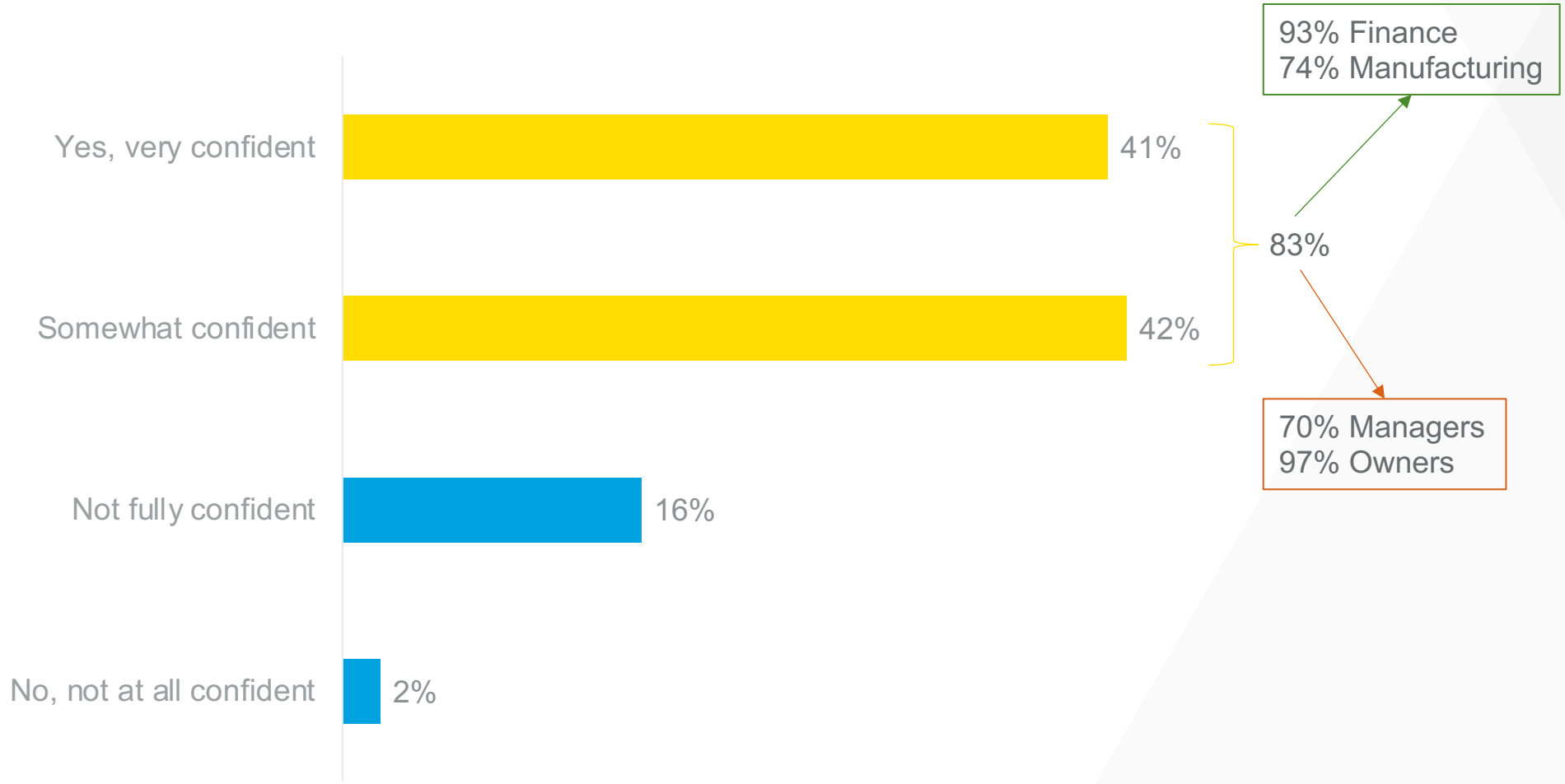
* Base: 163

There is wide consensus over the importance of a trusted channel partner as a guide (90%)

Base: 200

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

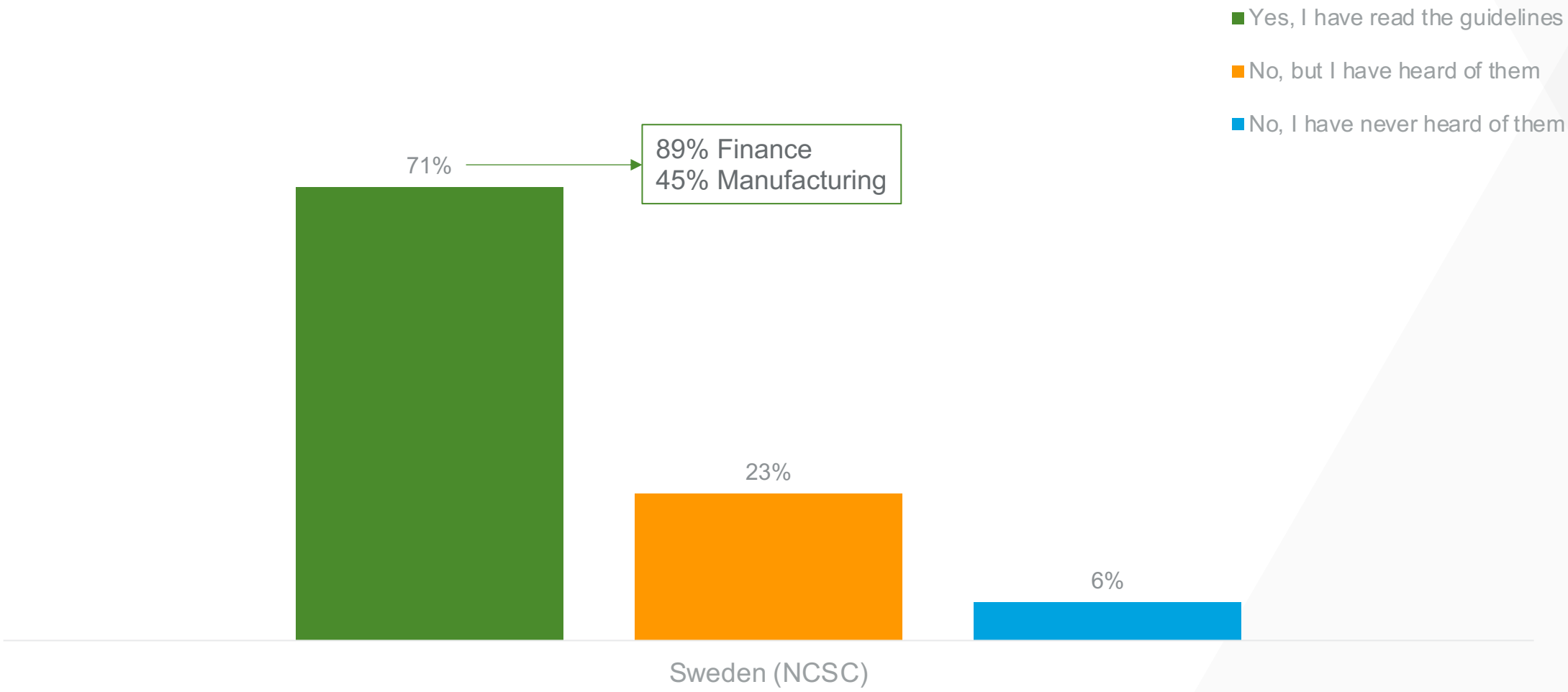
83% are confident their security tools would protect against sophisticated attacks



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

71% of Swedish respondents have read the “Cybersäkerhet i Sverige – Rekommenderade säkerhetsåtgärder” guidelines from the Swedish NCSC

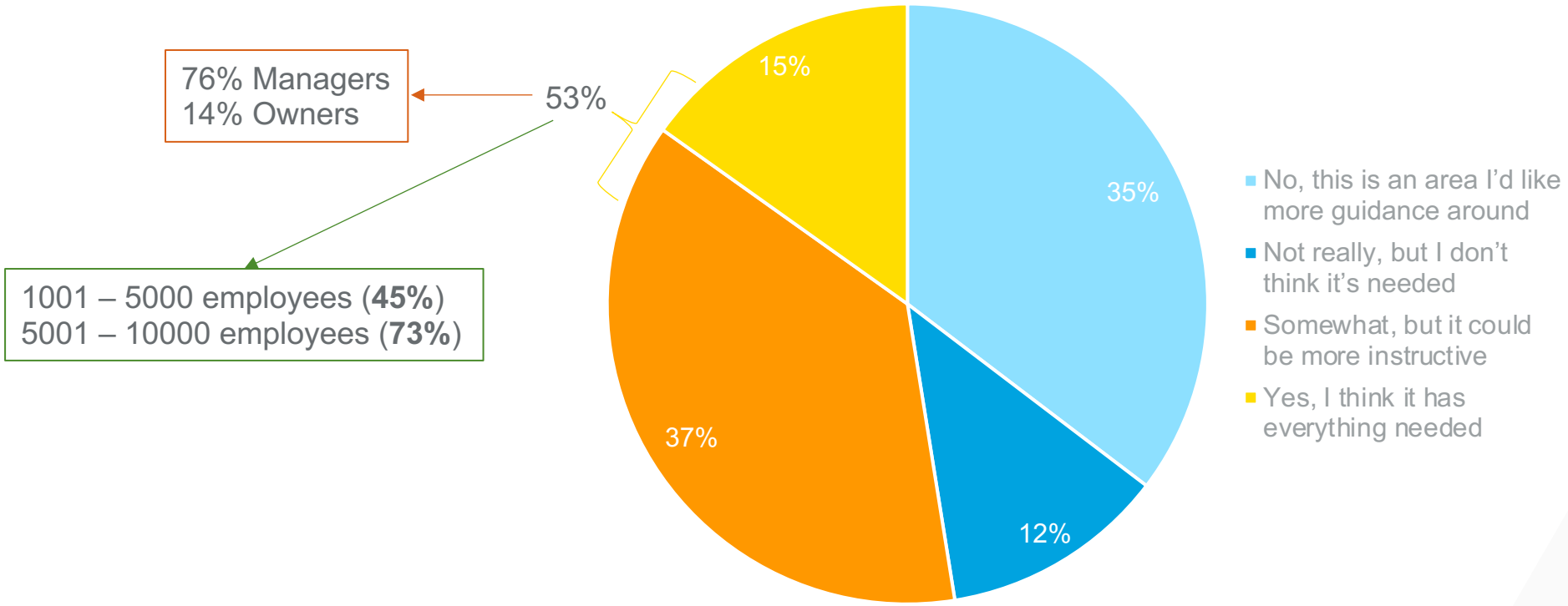


Base: 200

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

Of those that have read the guidance, 53% found it at least somewhat useful

Only 15% felt they covered everything – which drops to 6% for owners

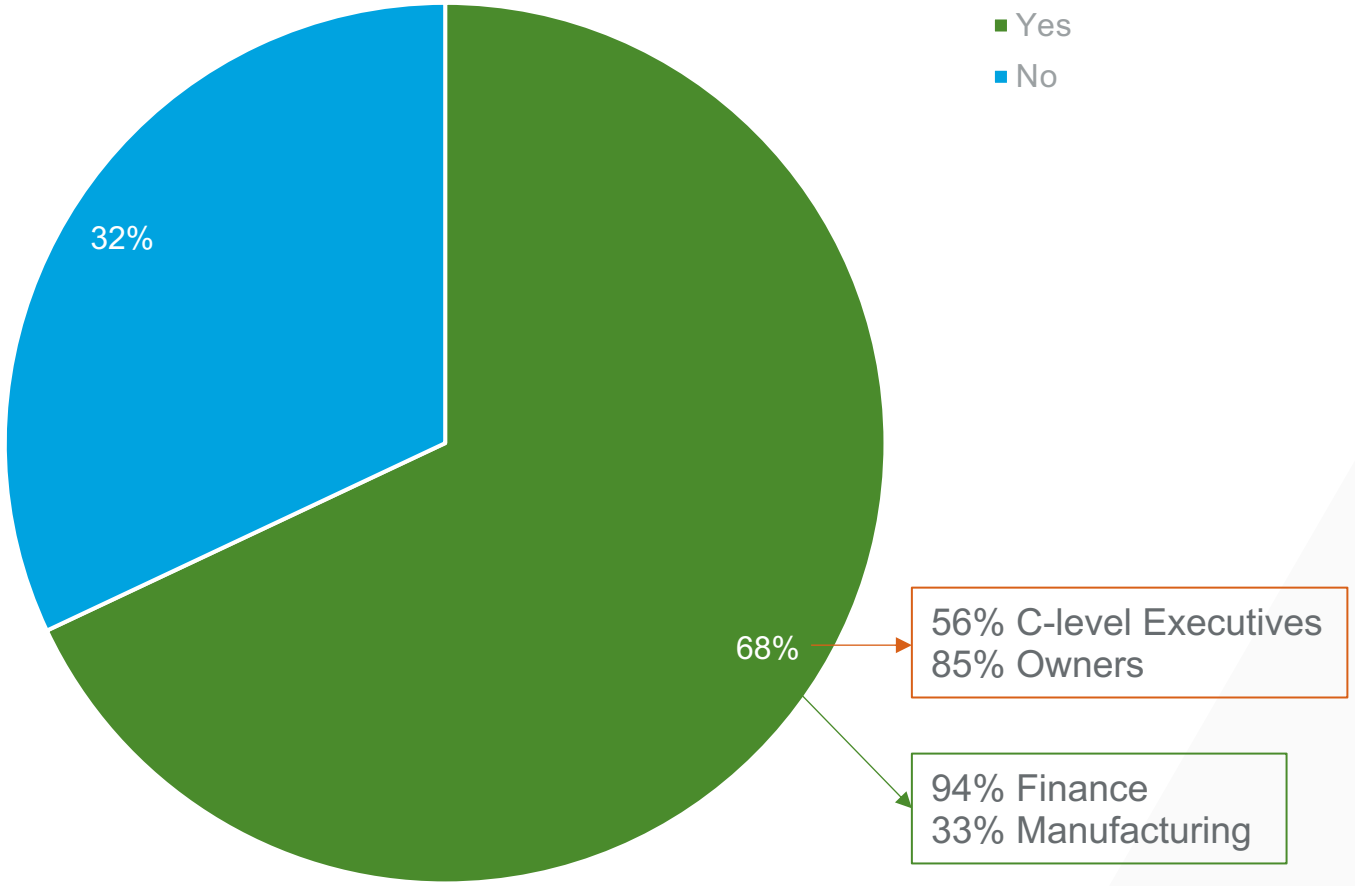


* Only asked to those who have read the guidelines

* Base: 142

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

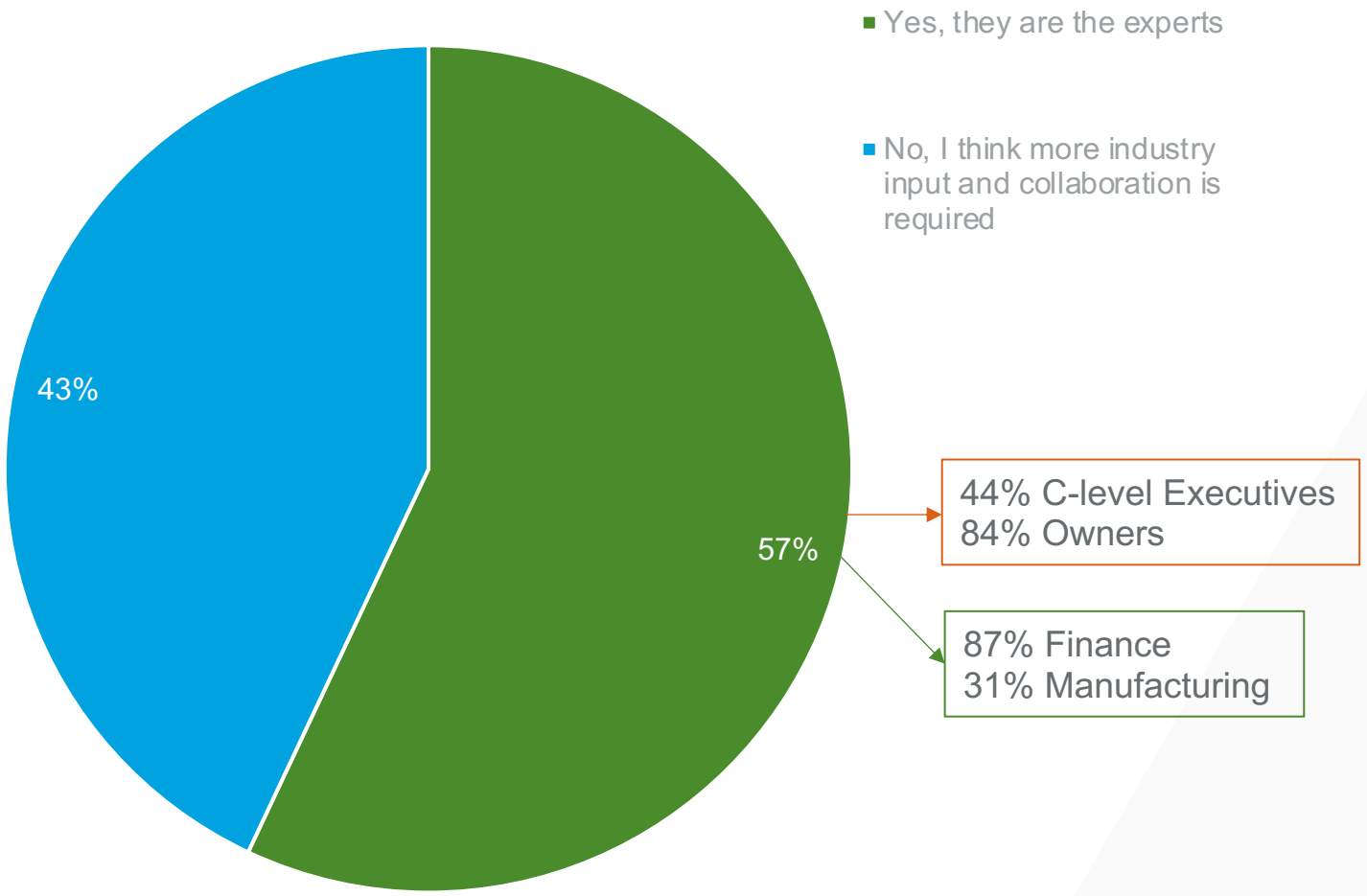
68% feel regulators have a strong enough understanding of the harsh realities that security teams face



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

Base: 200

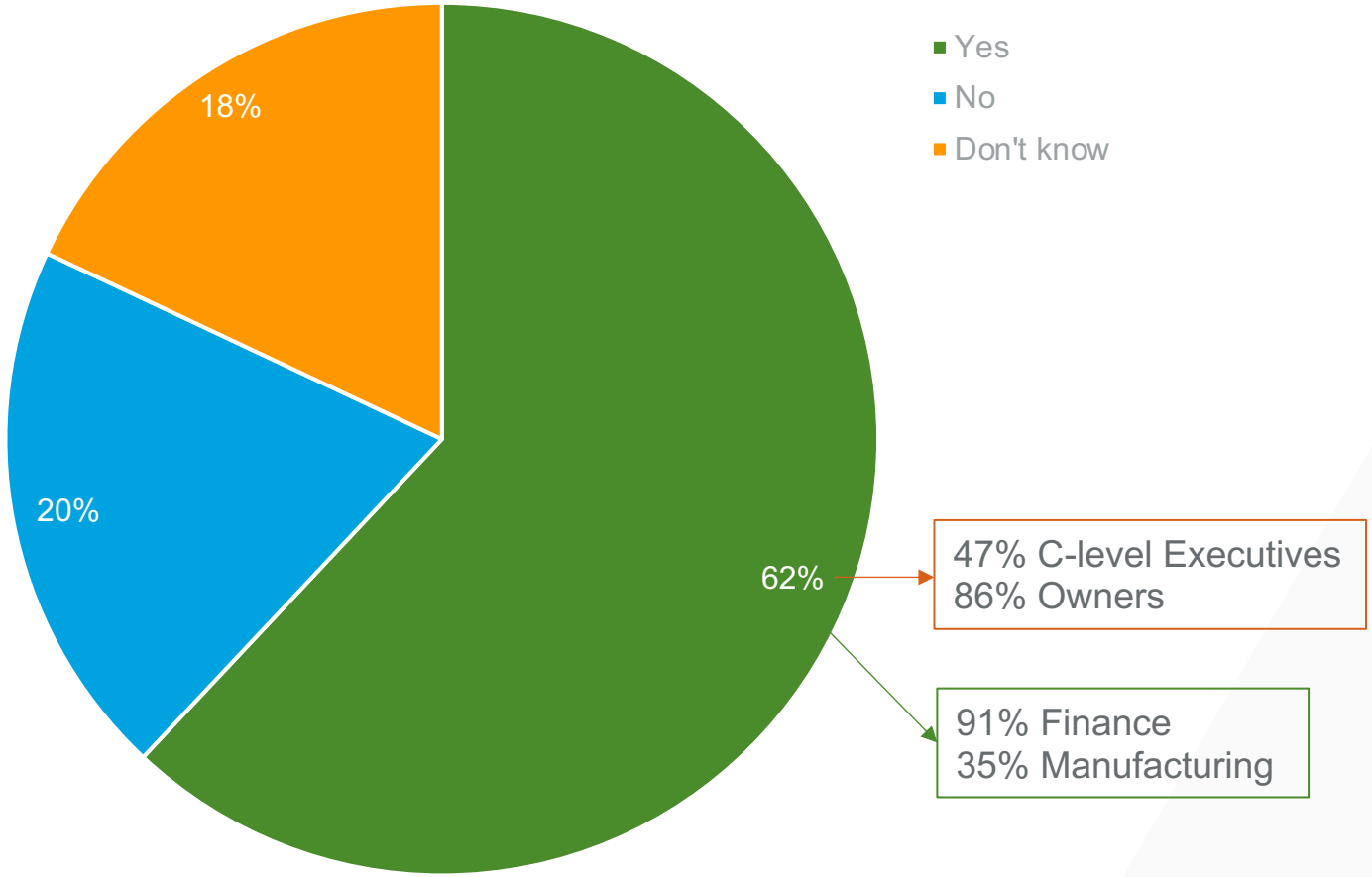
57% feel legislators are well-equipped to be making decisions around cybersecurity related regulations



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, 62% feel the guidelines are effective in helping defend against modern cyber-attacks



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

* Base: 188

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

Of those who consider the guidelines effective, 46% feel the guidelines will help mitigate most threats

* Only asked to those who think the guidelines are effective

* Base: 117

Q14b. Why? Select all that apply

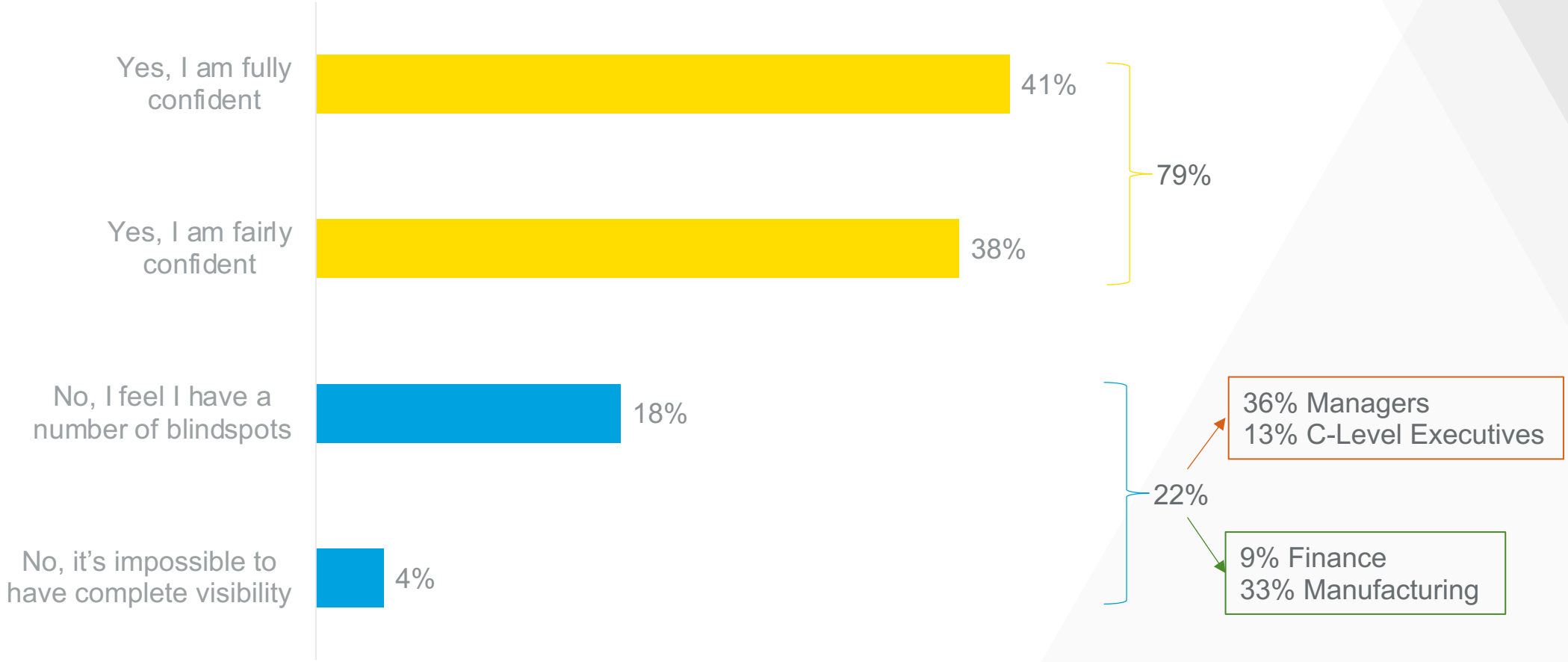
Of those who consider the guidelines ineffective, 48% feel the guidelines are outdated

* Only asked to those who think the guidelines are ineffective

* Base: 38

Q14c. Why not? Select all that apply

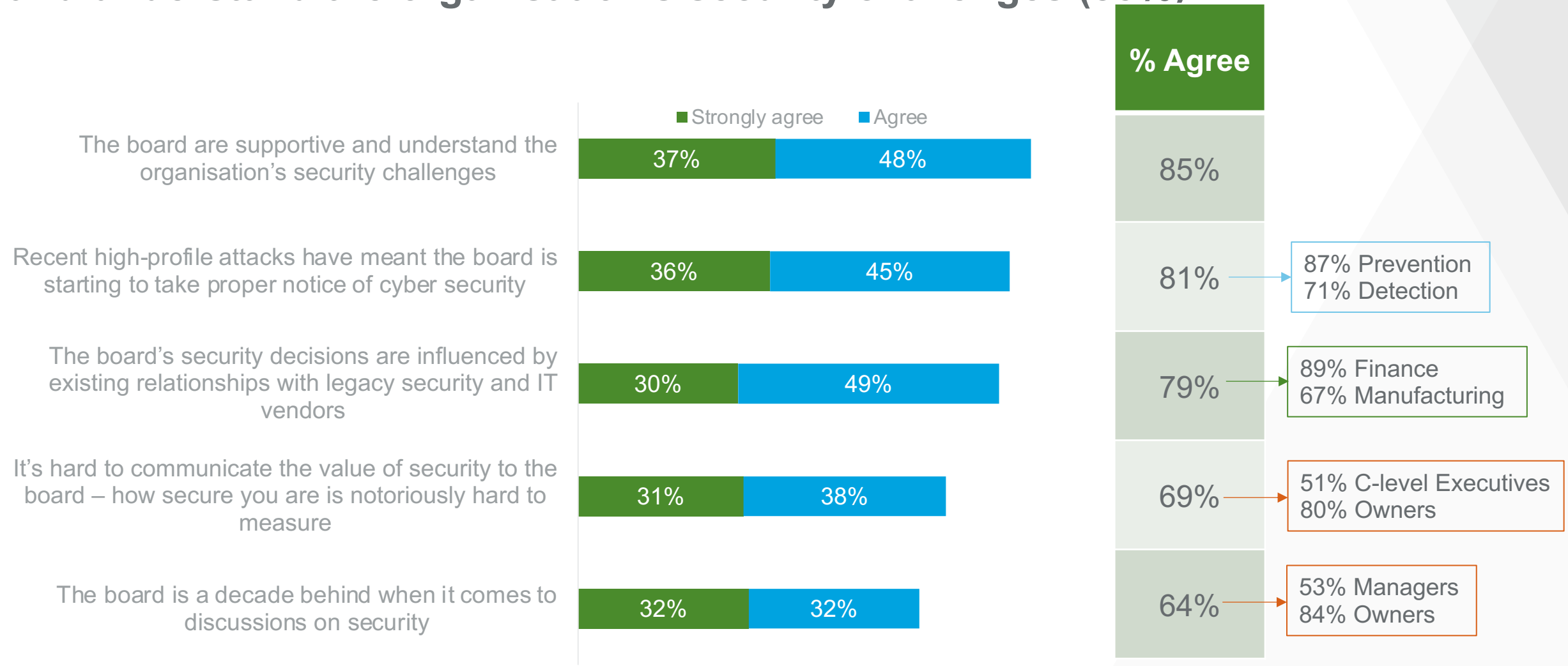
22% do not feel confident that they have visibility of all threats facing their organisation



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's ability to be supportive and understand the organisation's security challenges (85%)

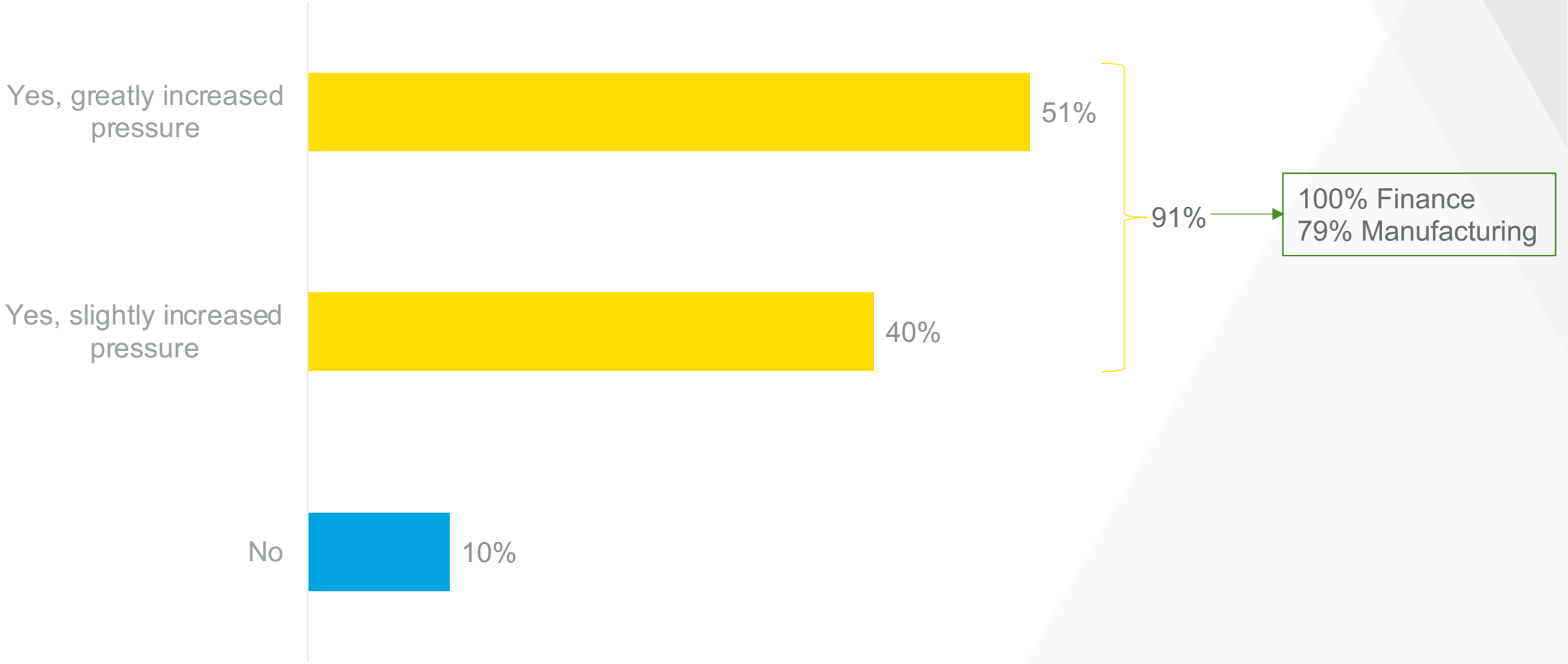


Q16. To what extent do you agree with the following statements? Select one per row

Base: 200

91% have felt increased pressure to keep their organisation safe over the past year

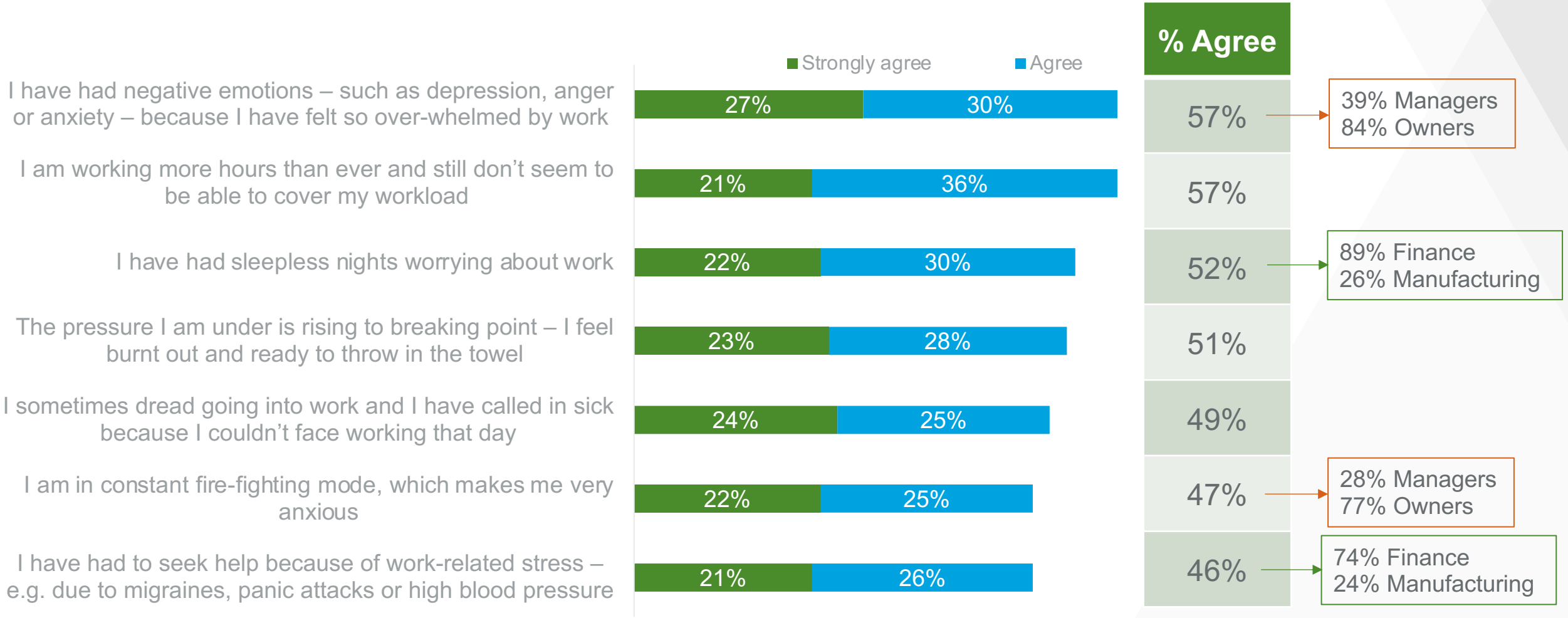
This increased to 100% for this in finance



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

Base: 200

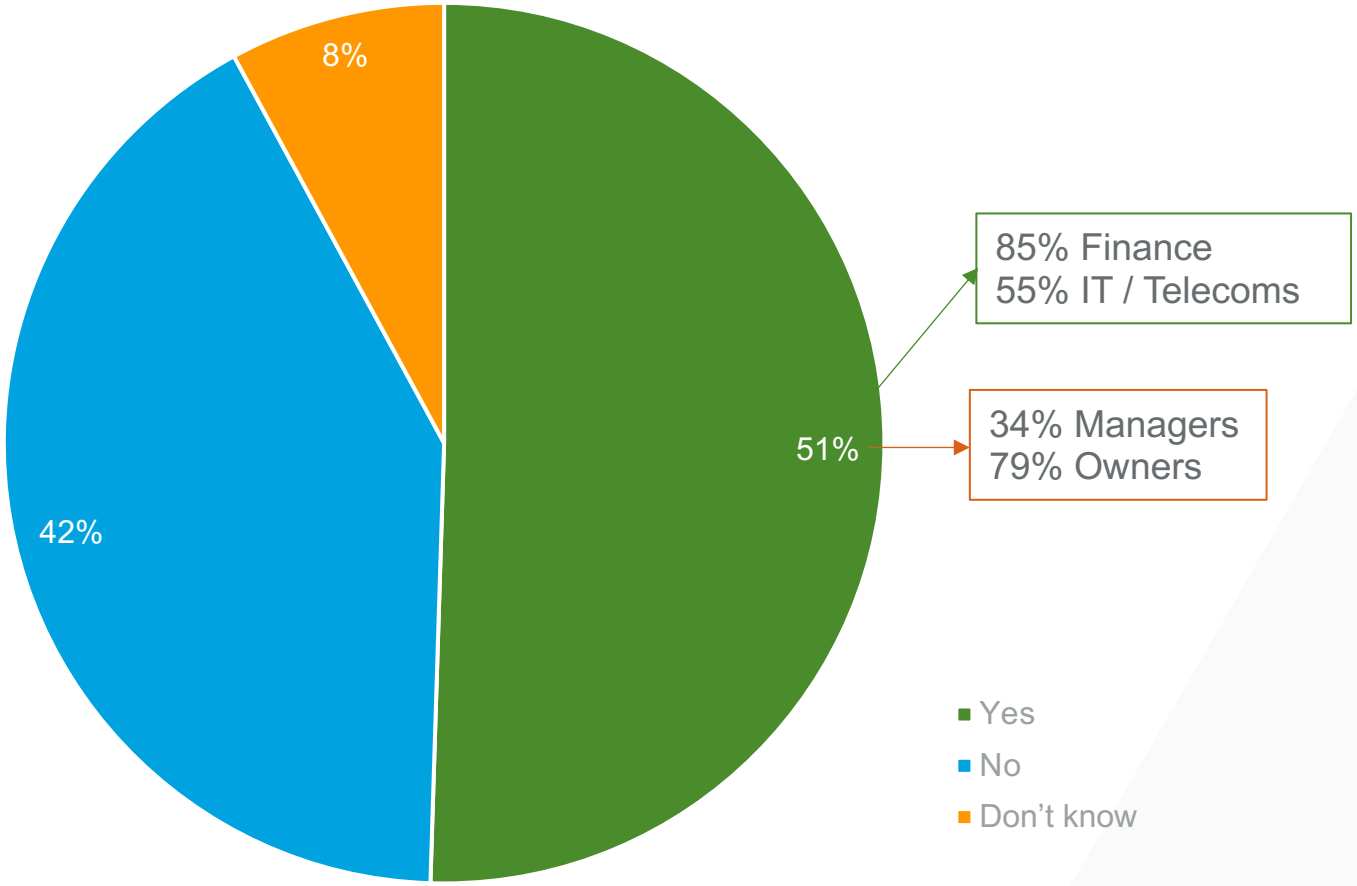
There is wide consensus over the common experience of negative emotions or working longer hours (57%)



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

Base: 200

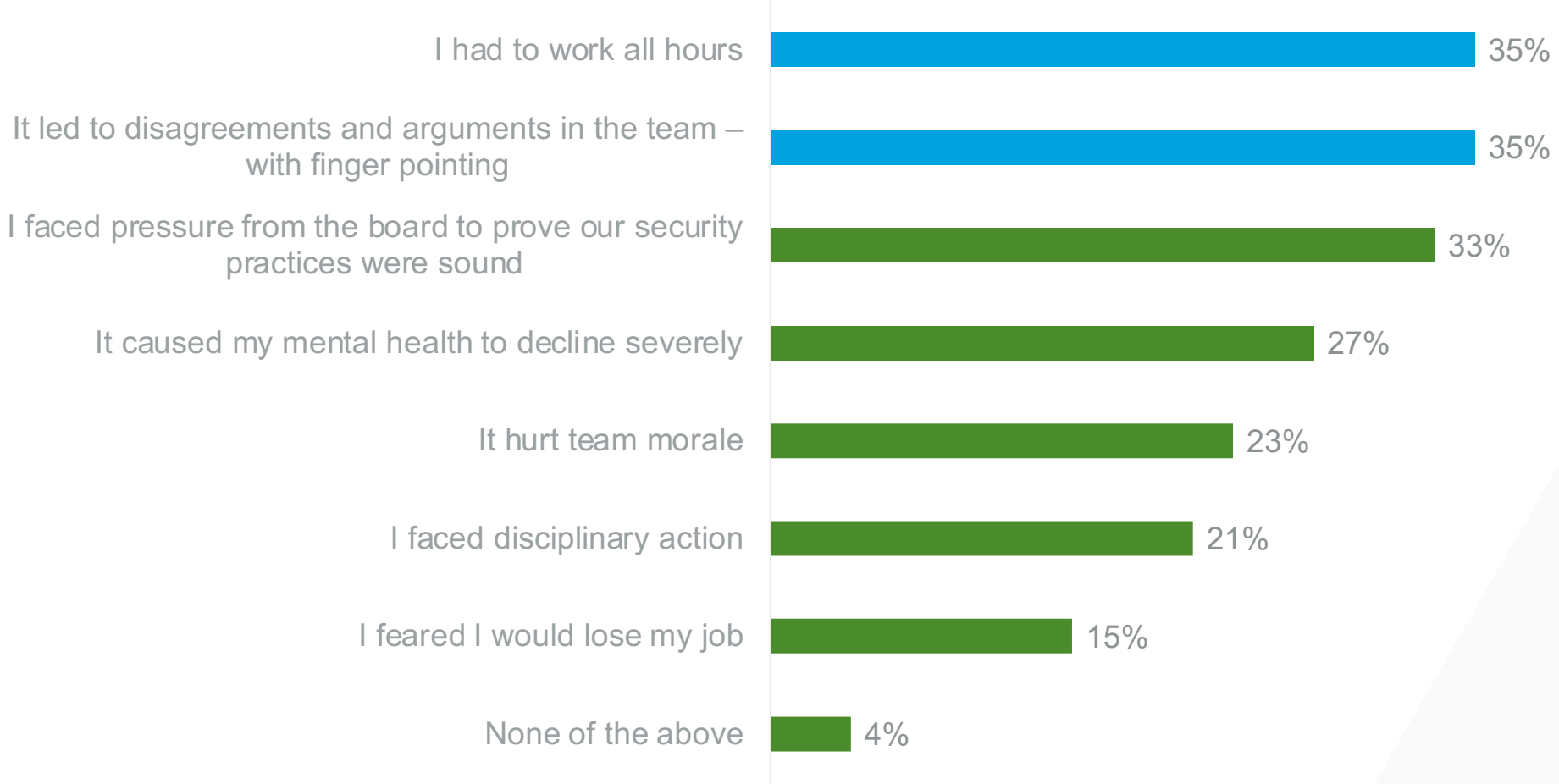
51% have suffered a significant cybersecurity incident in the past year



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 or having disagreements in the team (35%)



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

* Base: 101

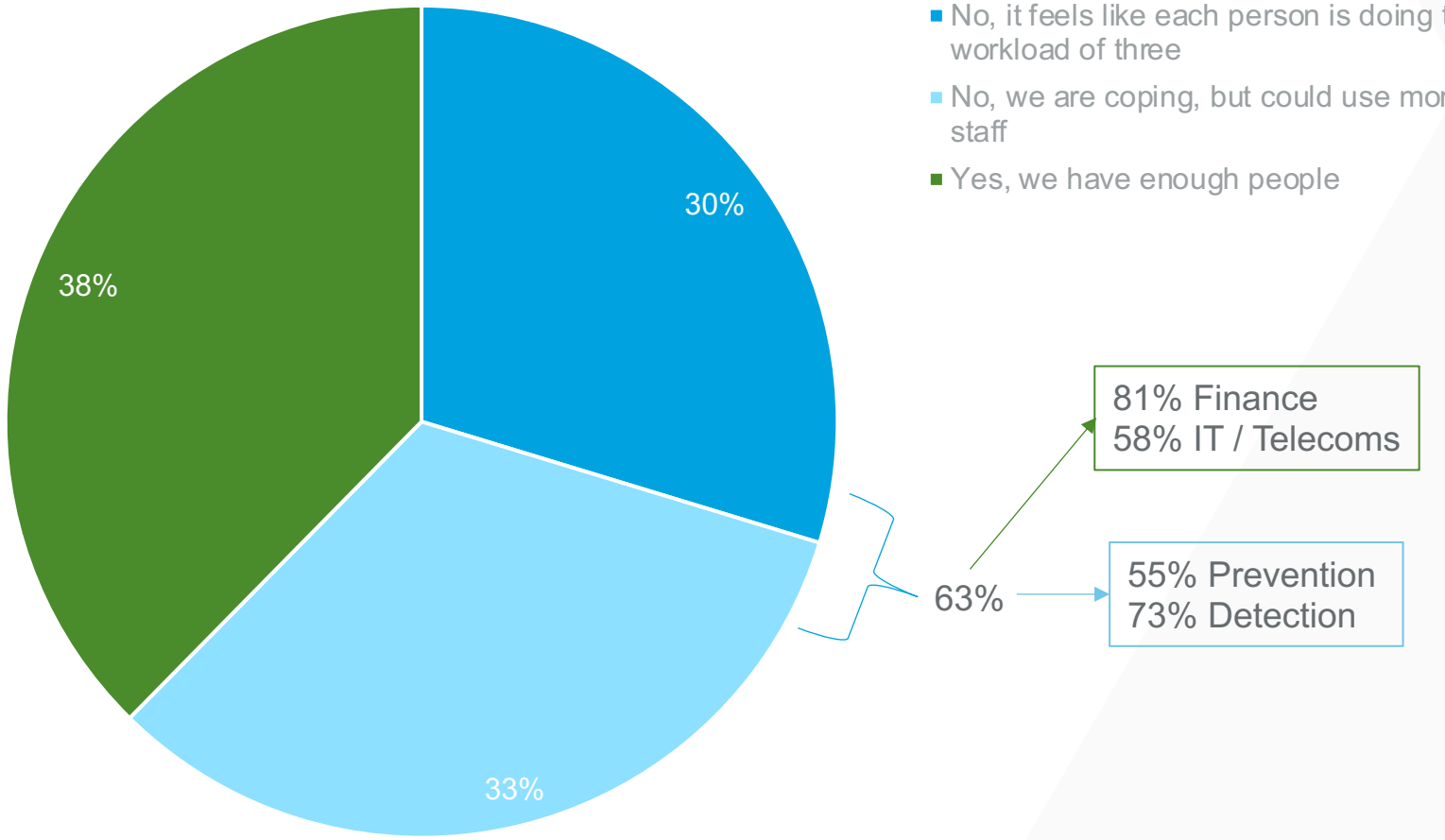
Q20. What was the effect of this incident on you and your team? Select all that apply

Respondents are most concerned with cyber-attacks within their supply chain (57%)

Base: 200

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

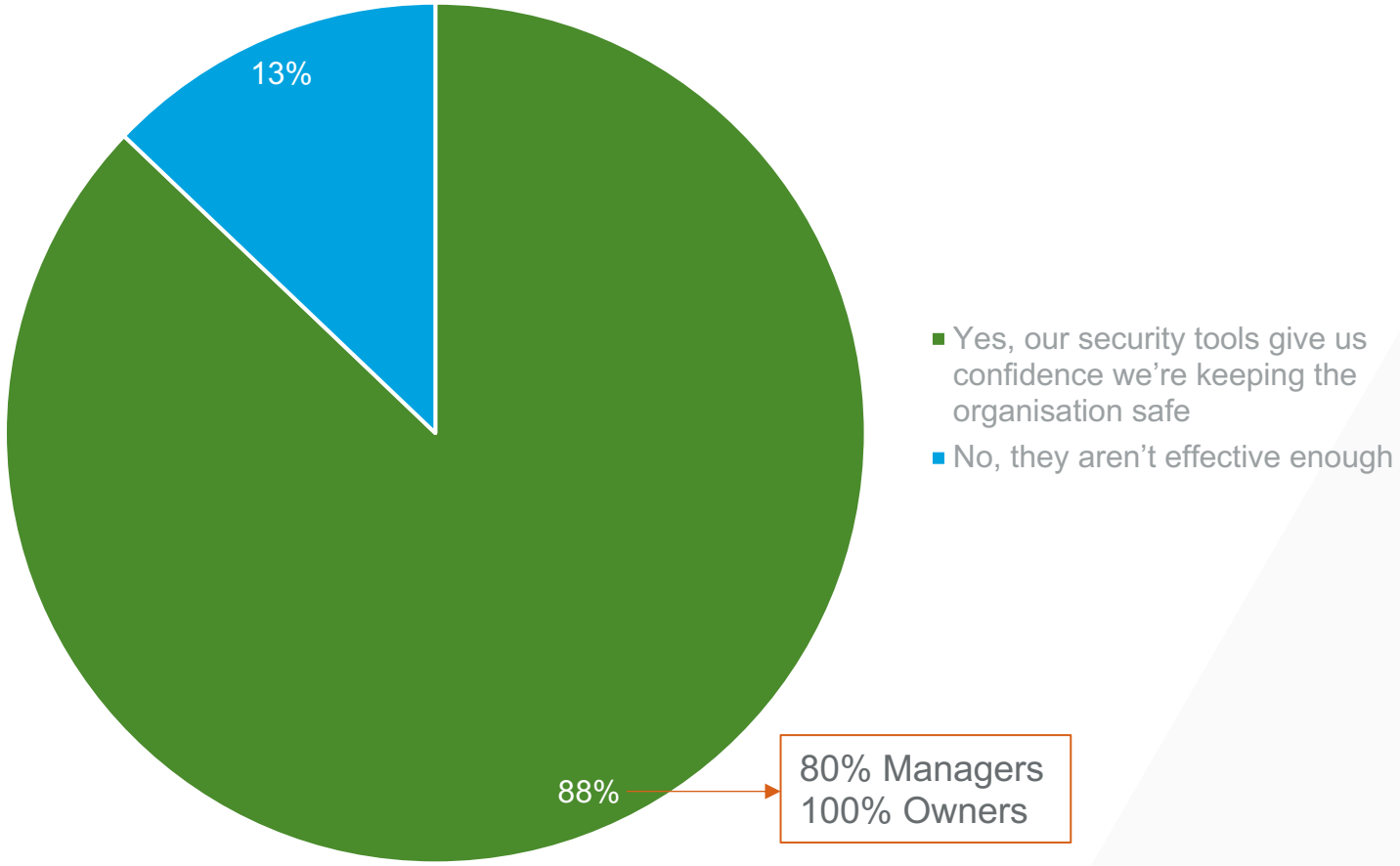
63% feel they could use more security talent on their team



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

Base: 1800

88% feel their security tools are effective at keeping their organisation safe

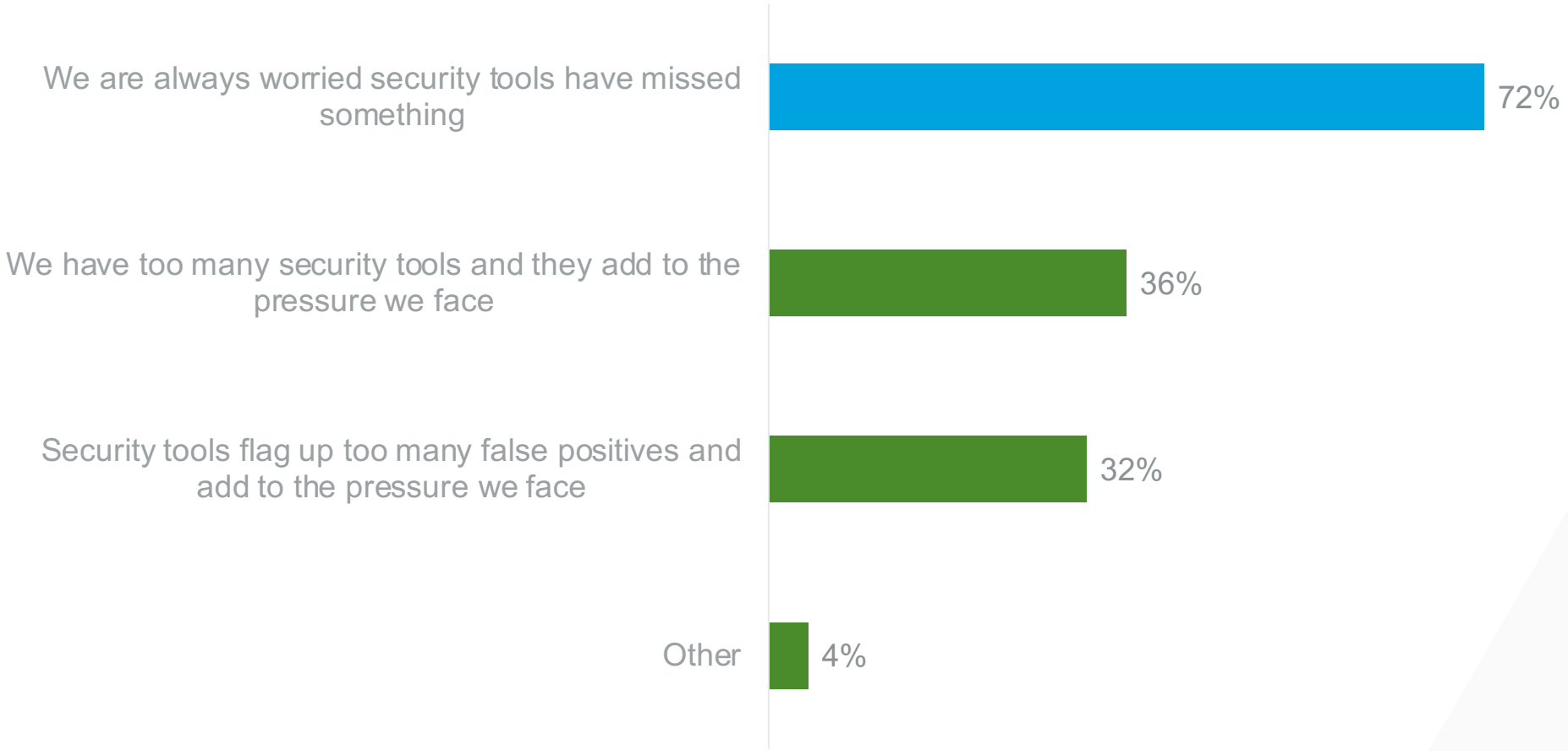


Q23a. Are your security tools effective enough at reducing the pressures your team faces? Select one

Base: 200

Of those who feel their security tools are ineffective, most are worried the tools have missed something (72%)

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



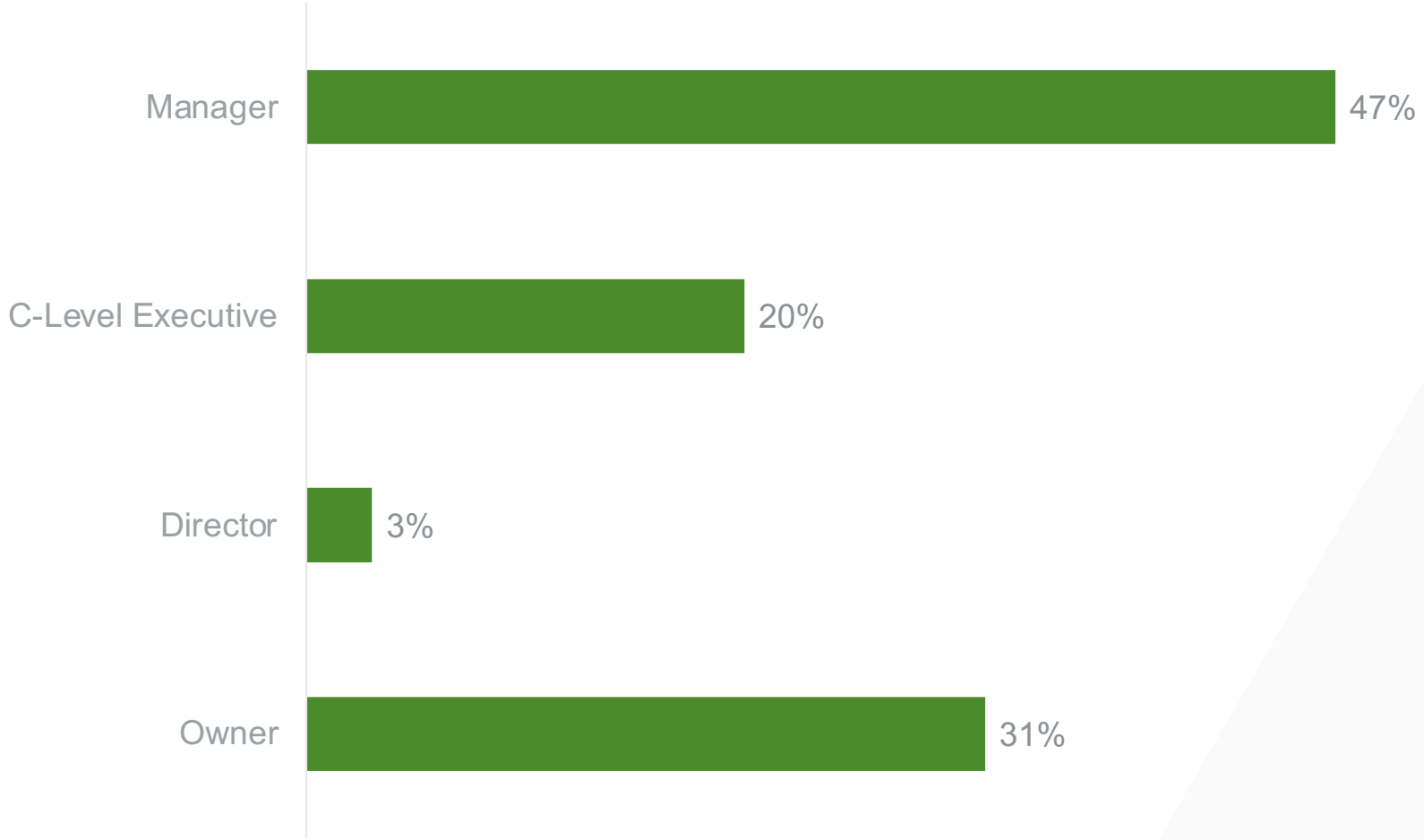
* Only asked to those who think their security tools are not effective enough

* Base: 25

Q23b. Why not? Select all that apply

Demographics

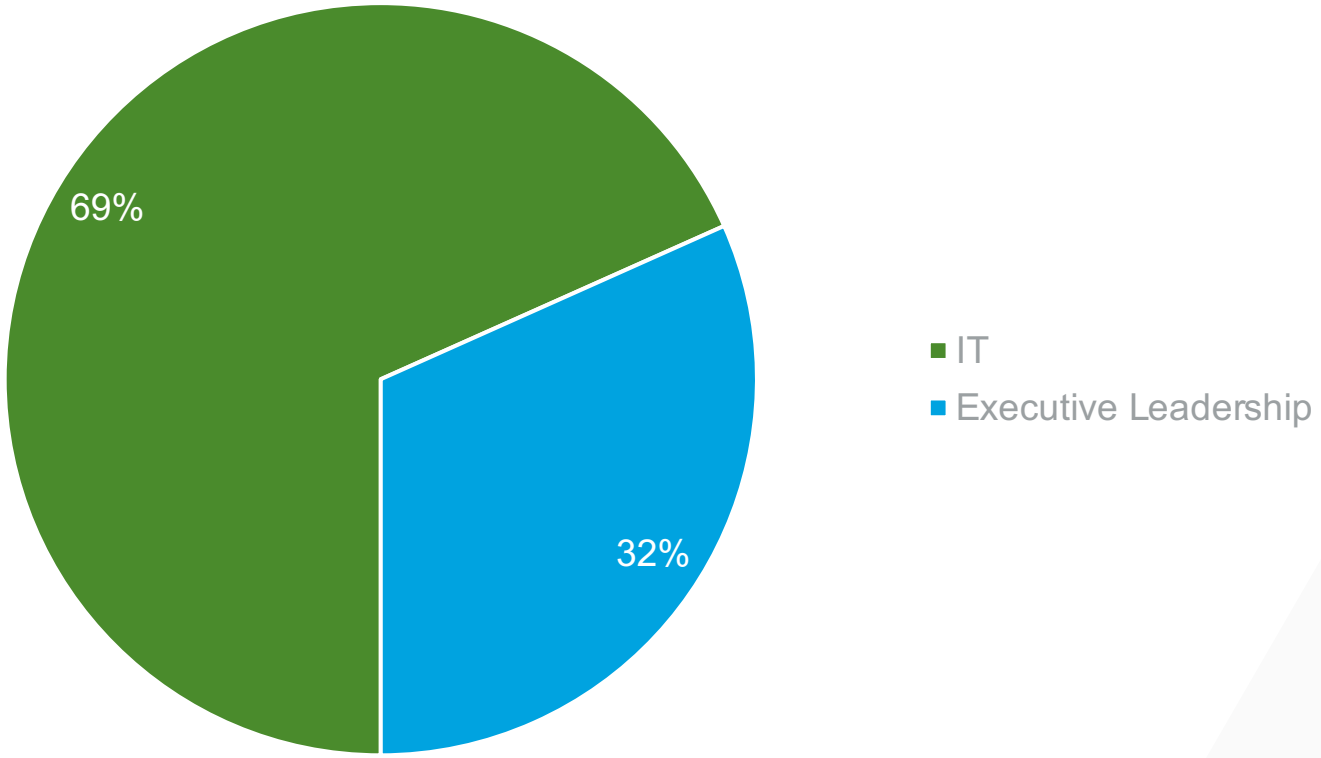
Role



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

Base: 200

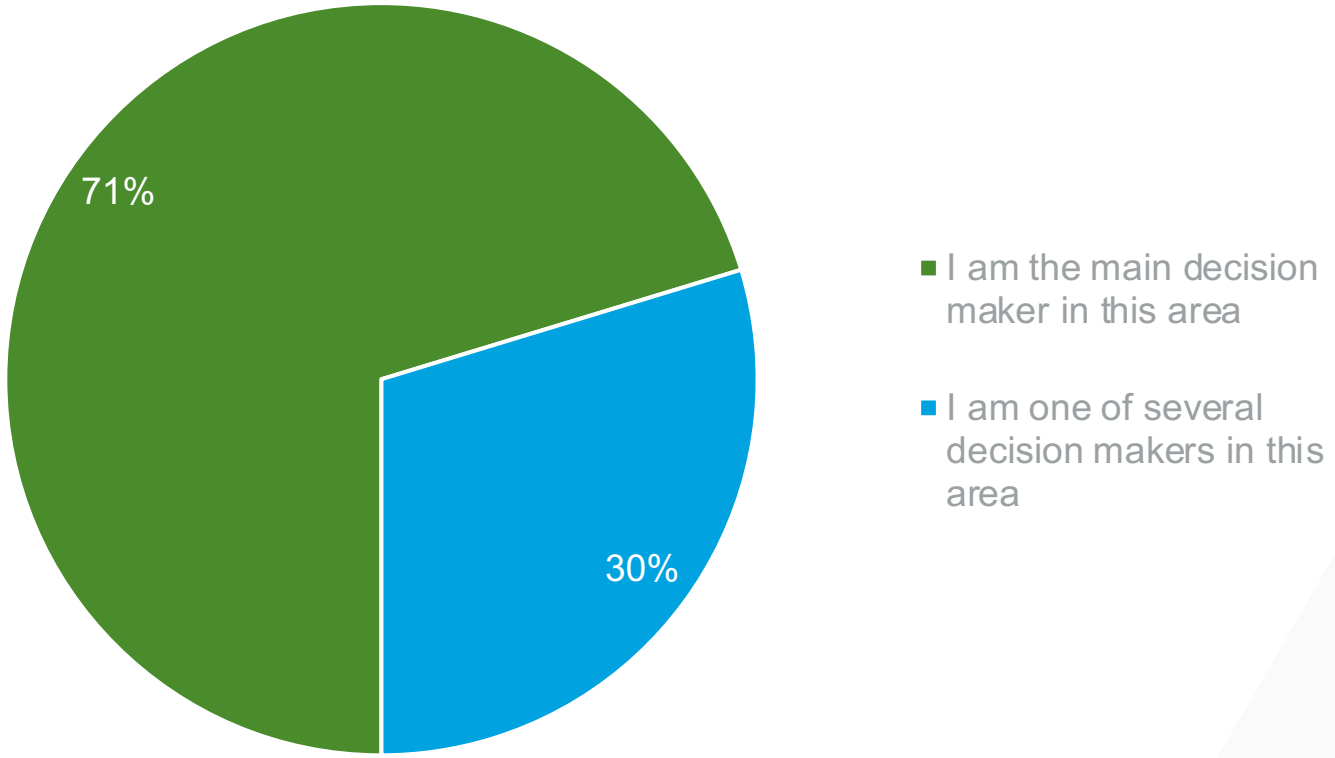
Area of Work



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

Base: 200

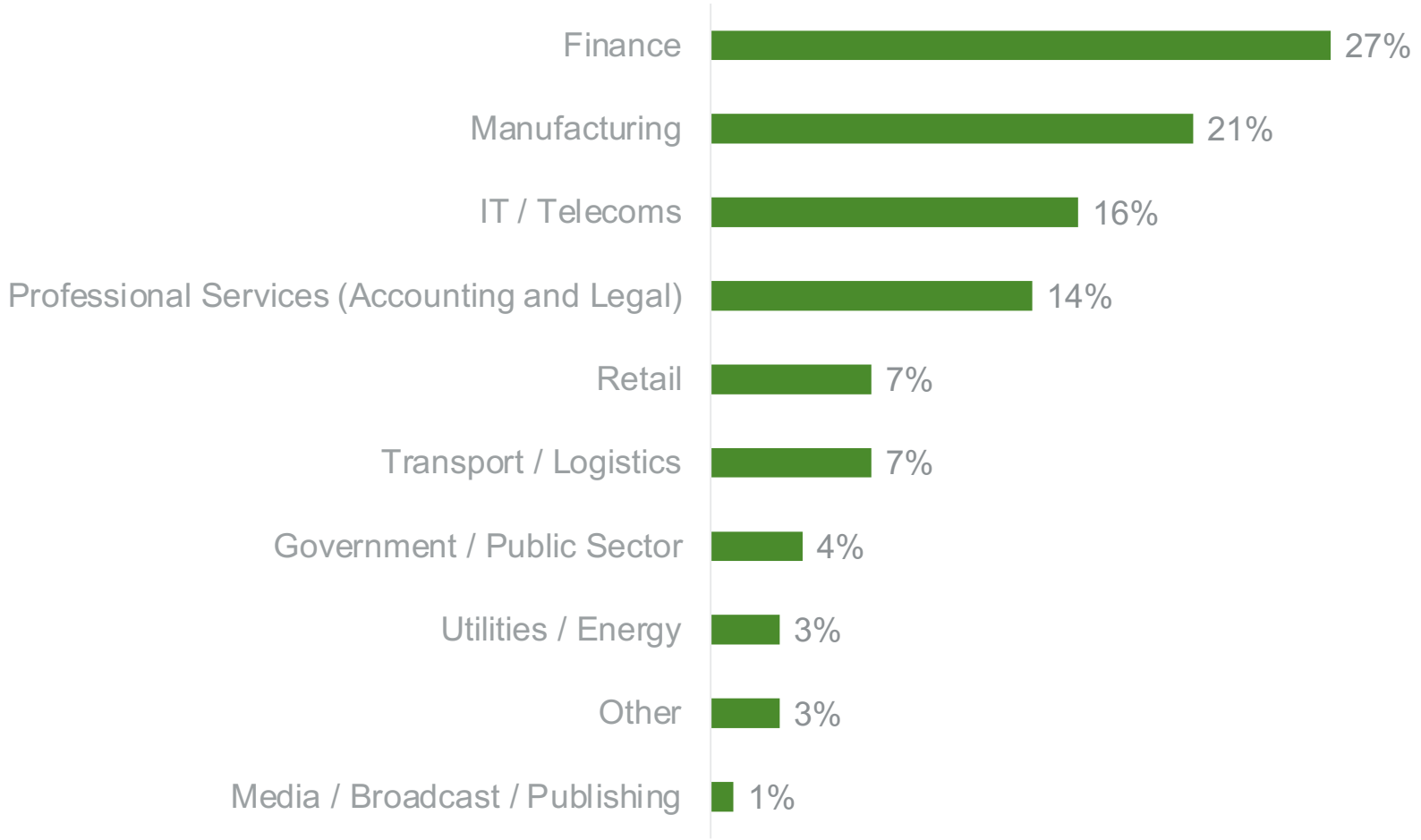
Decision-making Influence



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

Base: 200

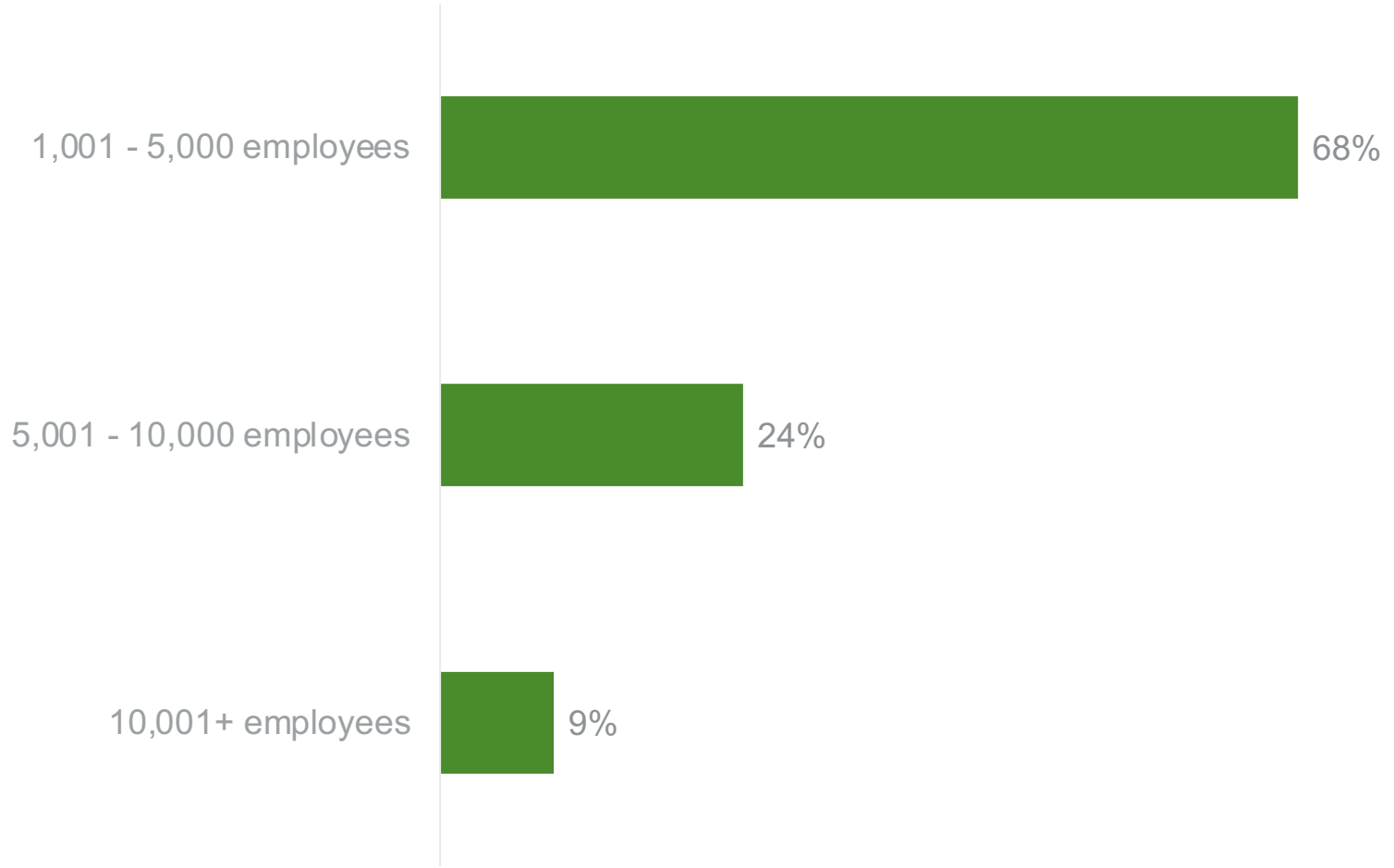
Industry



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

Base: 200

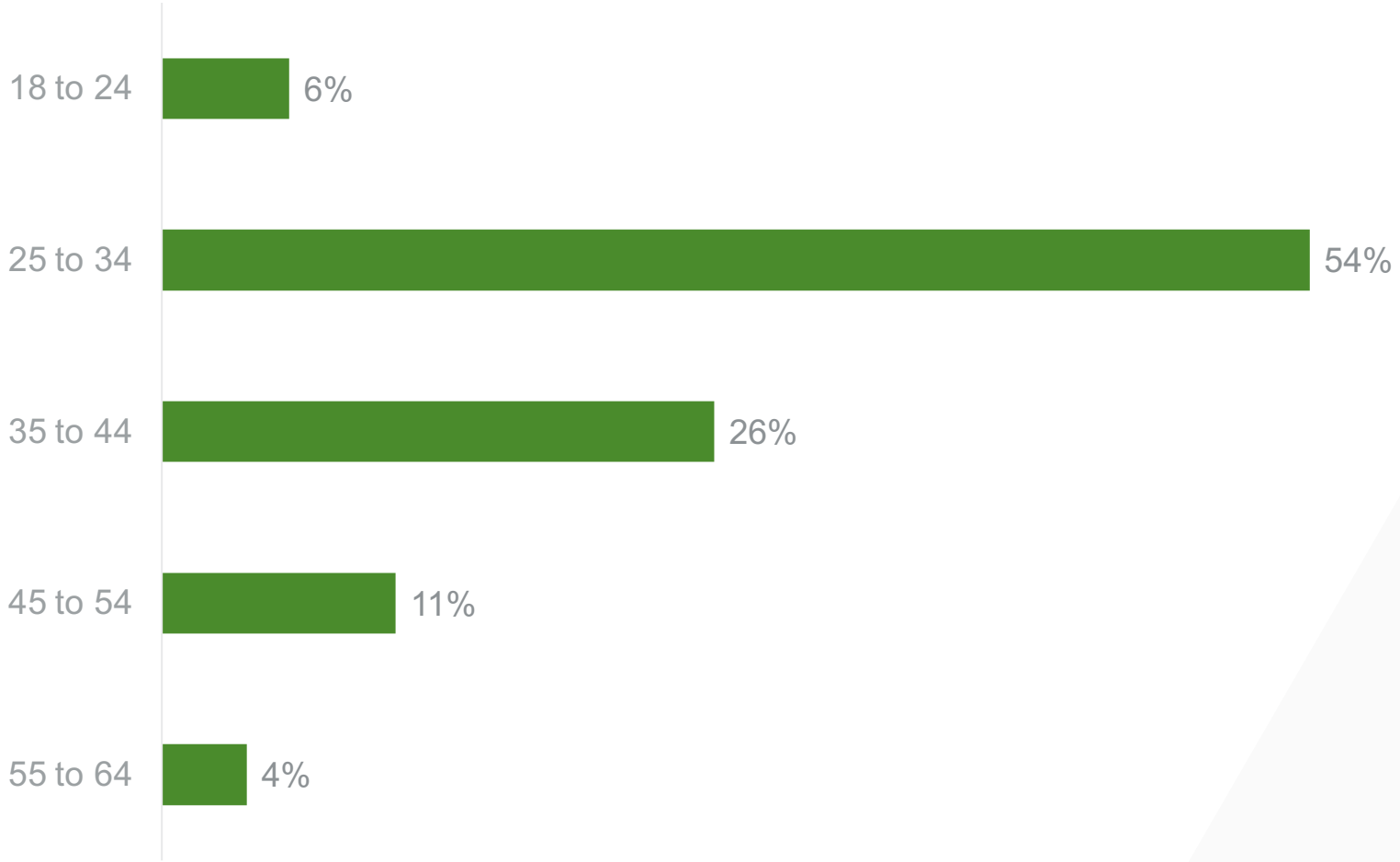
No. of Employees



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

Base: 200

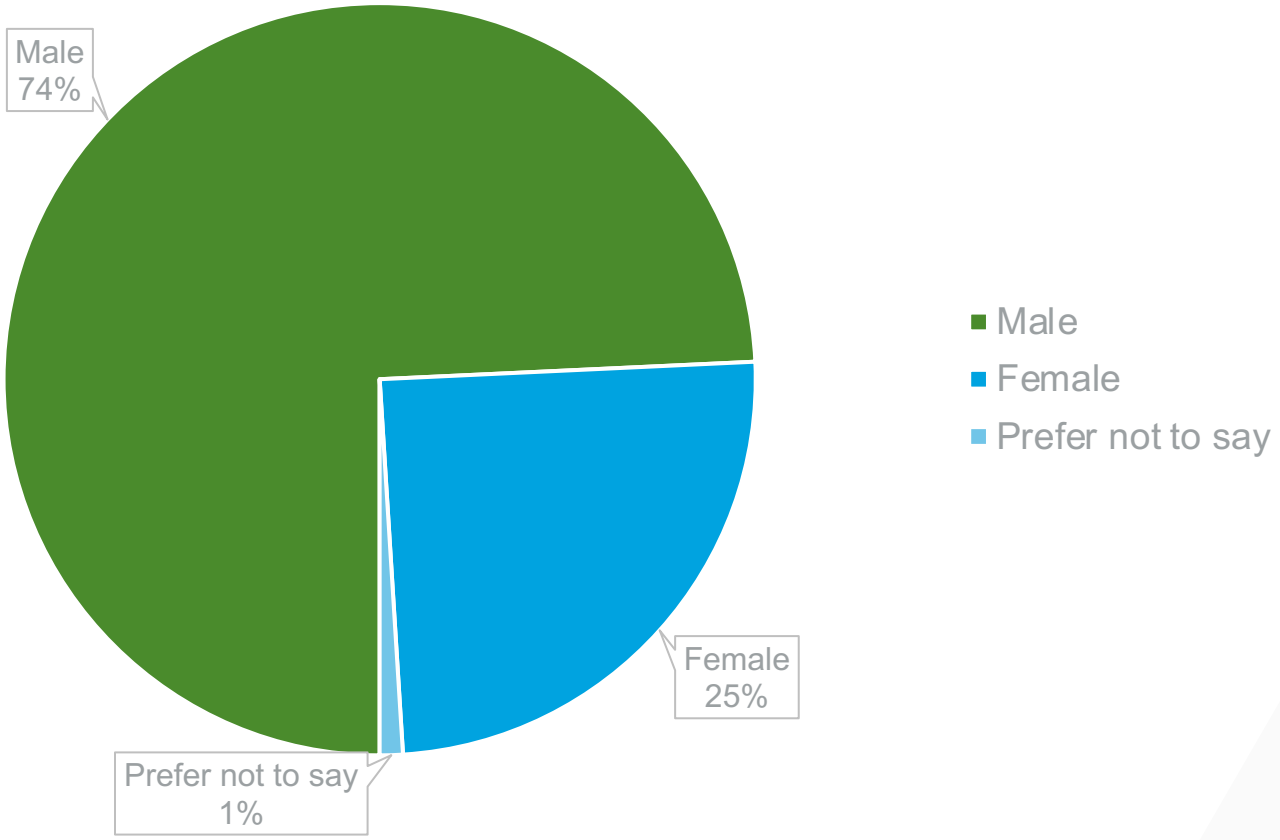
Age



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.**