Menlo Security Mobile Report 2021
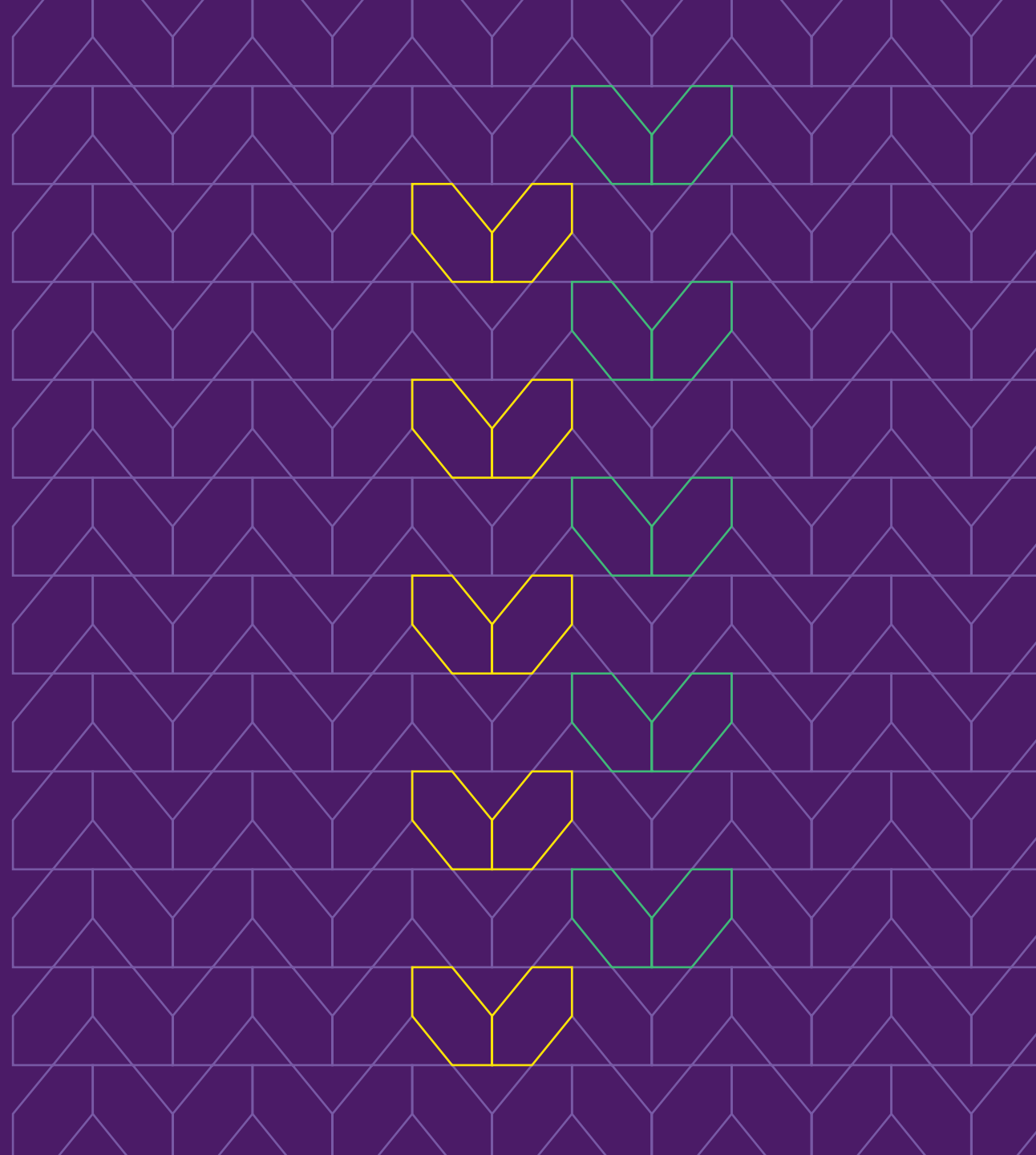
Menlo Security Mobile Report 2021

MENLO SECURITY

Project overview and methodology

- The survey was conducted among 617 IT decision makers from organisations with 1,000+ employees across the US, UK and Australia.

- At an overall level results are accurate to ± 3.9% at 95% confidence limits assuming a result of 50%.

- The interviews were conducted online by Sapio Research in April and May 2021 using an email invitation and an online survey.

MENLO
SECURITY

Respondent demographics summary

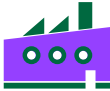| Demographics	Total respondents: 617
Country of residence	🇬🇧 204 🇺🇸 204 🇦🇺 209

Job Role
- 22% of respondents were CIOs
- 16% of respondents were CISOs
- 53% of respondents were IT Managers

Size of company

% of respondents	**30%**	**32%**	**21%**	**18%**

Business sector

Company sectors – top 3:	Software / Technology: 22%	Finance / Insurance / Accounting: 15%	Retail / Manufacturing : 12%

MENLO SECURITY

Key stats

93% said that mobile security was **high priority**: **59%** said it was **very high**

55% think that **organisations** should be responsible for the security of mobile devices used for work purposes

76% believe that end users are more open to attacks on mobile devices than they were a year ago

86% agree that attacks on mobiles are becoming **more frequent and sophisticated**, and that the number of different ways mobile devices are being attacked is increasing

Only **25%** think their employees report mobile browser vulnerabilities every time they occur

67% believe mobile browser vulnerabilities occur at least **several times a week**: **21%** think they occur **multiple times a day**

MENLO SECURITY

Summary and Overview

1 — **Mobile security an increasing concern** – The majority feel that attacks on mobile devices are increasingly frequent and sophisticated, and that end users are more vulnerable to attacks – and the vast majority consider mobile security to be high priority, including 99% of Australian respondents

2 — **Organisations should take responsibility** – Over half thought that organisations should be responsible for the security of mobile devices used for work purposes, particularly those in larger companies. Australian respondents, however, were more likely to think responsibility should lie with end users or mobile vendors

3 — **iOS and the Apple App Store perceived as more secure than Android and Google Play** – A third update their mobile device / operating system as soon as a new patch is issued, with those in larger companies and those who rate mobile security as very high priority being more likely to update immediately

4 — **Mobile browser vulnerabilities thought to be frequent, but employees not trusted to accurately report them** – Two thirds believe mobile browser vulnerabilities occur at least several times a week, while a fifth think they occur multiple times a day. Despite this, only a quarter think their employees report vulnerabilities every time they occur

5 — **Respondents remain confident in their organisations' abilities** – While agreeing that mobile attacks are an increasing issue, the majority of respondents also agree that they are confident in identifying malicious links and preventing attacks via them. Most have mobile security solutions in place - mobile device management was the most popular mobile security solution, followed by Isolation

MENLO
SECURITY

Main Findings
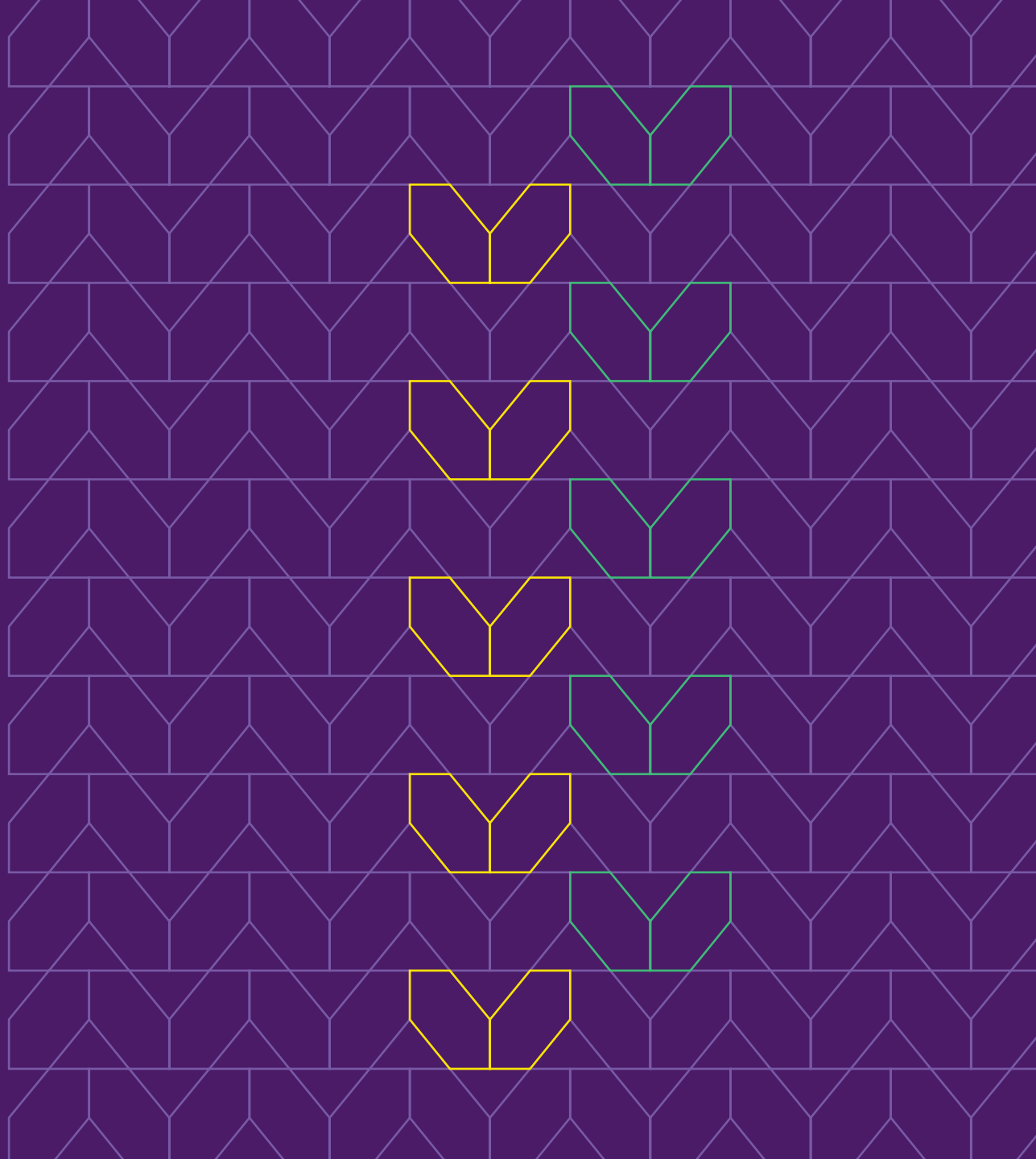
9 in 10 (93%) say that mobile security is a <u>high</u> priority, with 3 in 5 (59%) saying it is <u>very high</u>

93%

99% CIO vs **73%** Other IT role

97% companies with 3,000-4,999 employees vs **86%** companies with 10,000+ employees

Country	% High
UK	90%
US	90%
Australia	**99%**

59%

34%

6%

1%

0%

Very high | High | Medium | Low | Not a priority
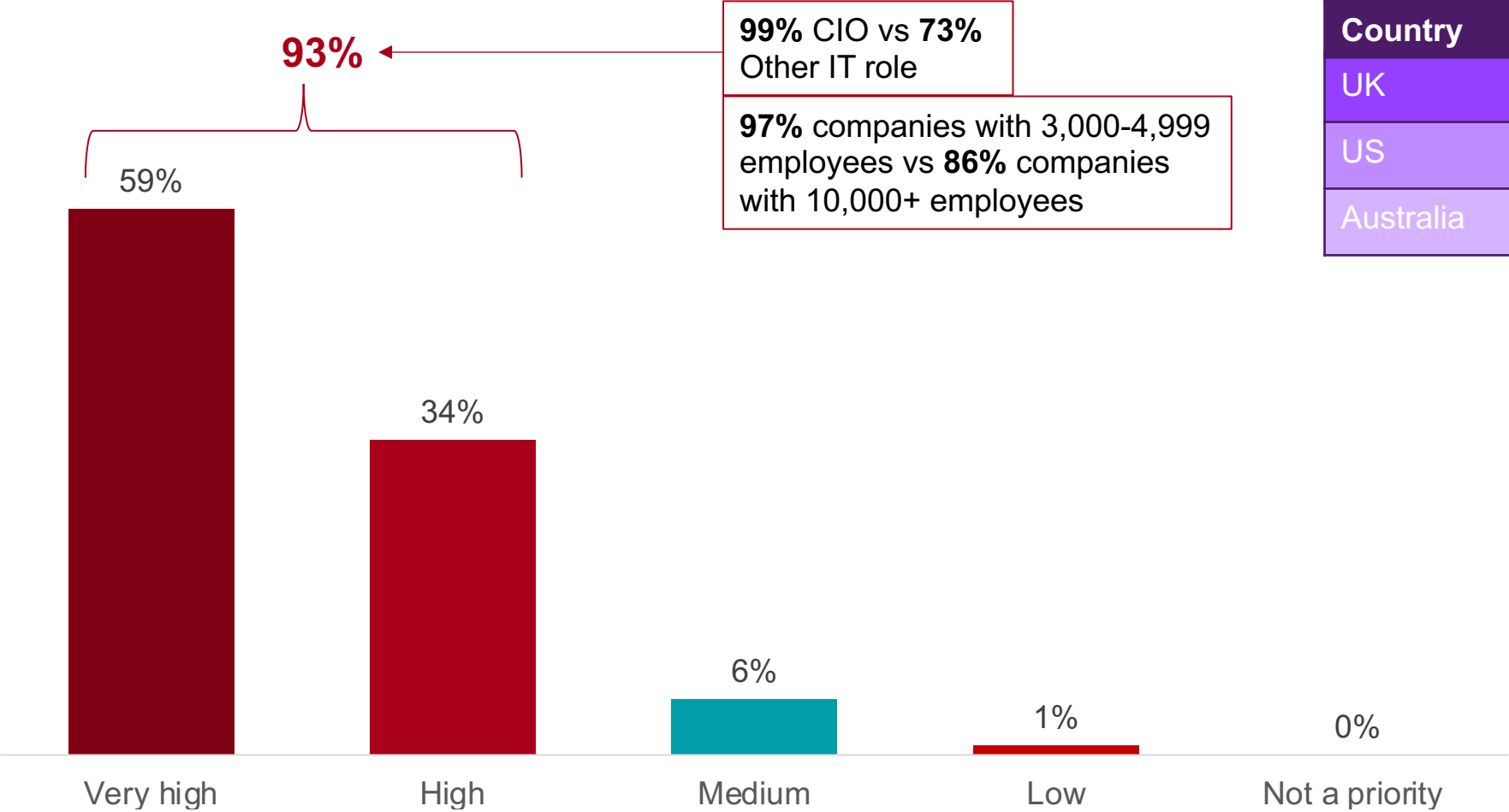
Three quarters believe that end users are more open to attacks on mobile devices than they were a year ago (76%)

Legend: ■ Significantly more ■ Slightly more ■ About the same ■ Slightly less ■ Significantly less

...a year ago?
- Significantly more: 39%
- Slightly more: 37%
- About the same: 14%
- Slightly less: 7%
- Significantly less: 3%

76% More

83% companies with 5,000-9,999 employees vs **70%** companies with 10,000+ employees

...five years ago?
- Significantly more: 45%
- Slightly more: 28%
- About the same: 14%
- Slightly less: 8%
- Significantly less: 5%

73% More

Country	% More
UK	67%
US	72%
Australia	**80%**

Q2. Do you believe that end users are more open to attacks on mobile devices than they were... Please select one answer per row

Base: 617

Phishing was the most common mobile security attack or attempt in the last 12 months (71%)
Only 1 in 10 did not experienced any mobile attacks or attempts in the last 12 months (11%)

Phishing — 71%

Malware — 66%

Top for US
58% UK vs **71%** Australia

Advanced Persistent Threats (APTs) — 42%

31% UK vs **51%** Australia

Something else — 2%

We have not experienced any mobile security attacks or attempts in the last 12 months — 11%

8% companies with 5,000-9,999 employees vs **18%** companies with 10,000+ employees

Q3. Has your organization experienced any of the following mobile security attacks or attempts in the last 12 months? Please select all that apply

Base: 617

While over half thought that organisations should be responsible for the security of mobile devices used for work purposes (55%), this remains a fairly split decision

UK	US	Australia
22%	22%	**30%**

UK	US	Australia
15%	18%	**28%**

End-users
25%

Mobile
vendors
20%

Organizations
55%

48% companies with 3,000-4,999 employees vs **61%** companies with 10,000+ employees

39% CISO vs
73% Other IT role

UK	US	Australia
63%	60%	42%
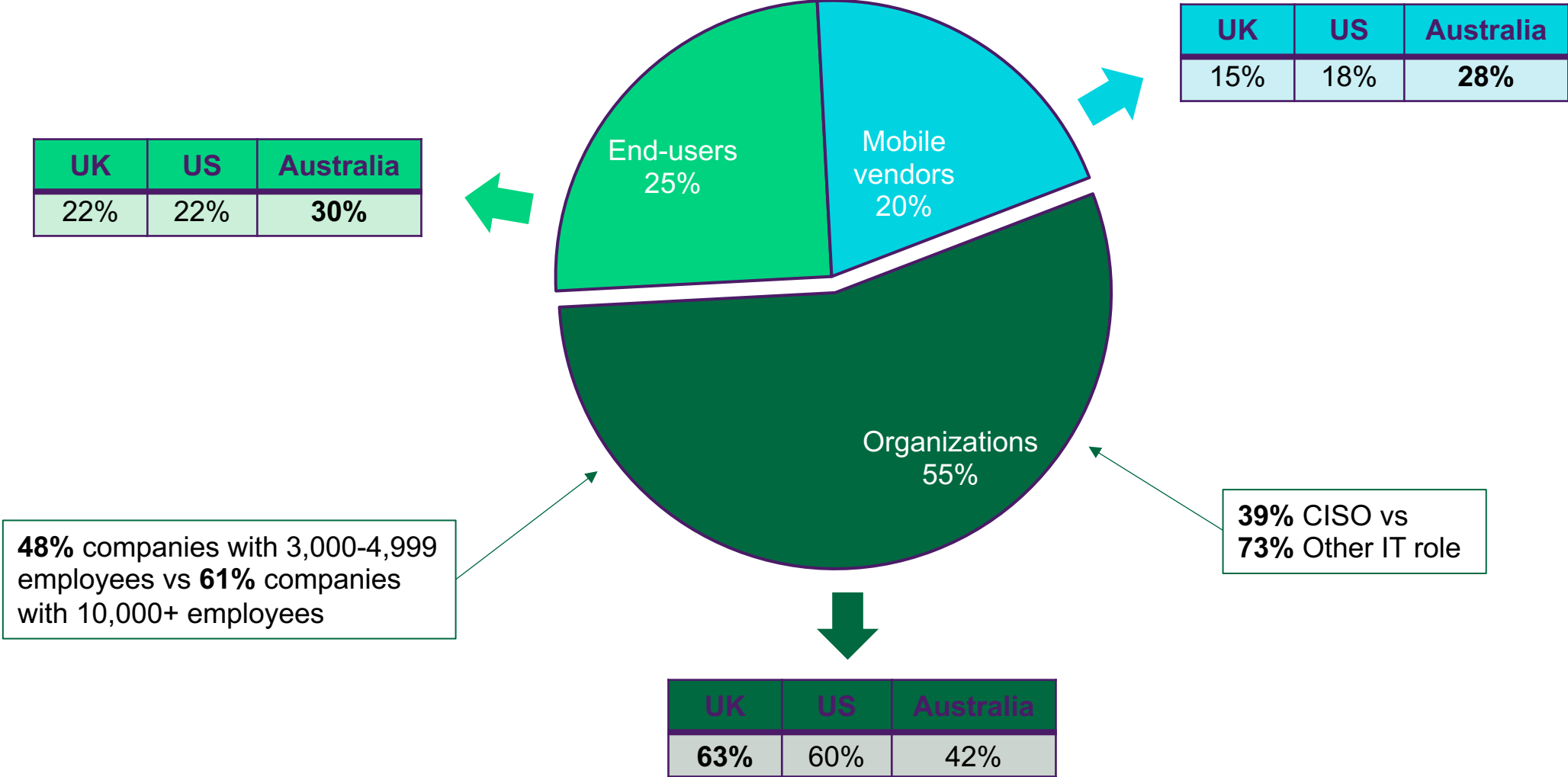
Only a third update their mobile device / operating system as soon as a new patch is issued (34%)
Over 1 in 10 (14%) will leave it 3 days or longer to update their mobile device / operating system

Category	Percentage
As soon as it is issued	34%
The same day	25%
Within 1-2 days	27%
Within 3-5 days	8%
Within a week	5%
When I remember	1%

45% CIO

27% companies with 5,000-9,999 employees vs **43%** companies with 10,000+ employees

43% Mobile security is very high priority vs **23%** Mobile security is high priority
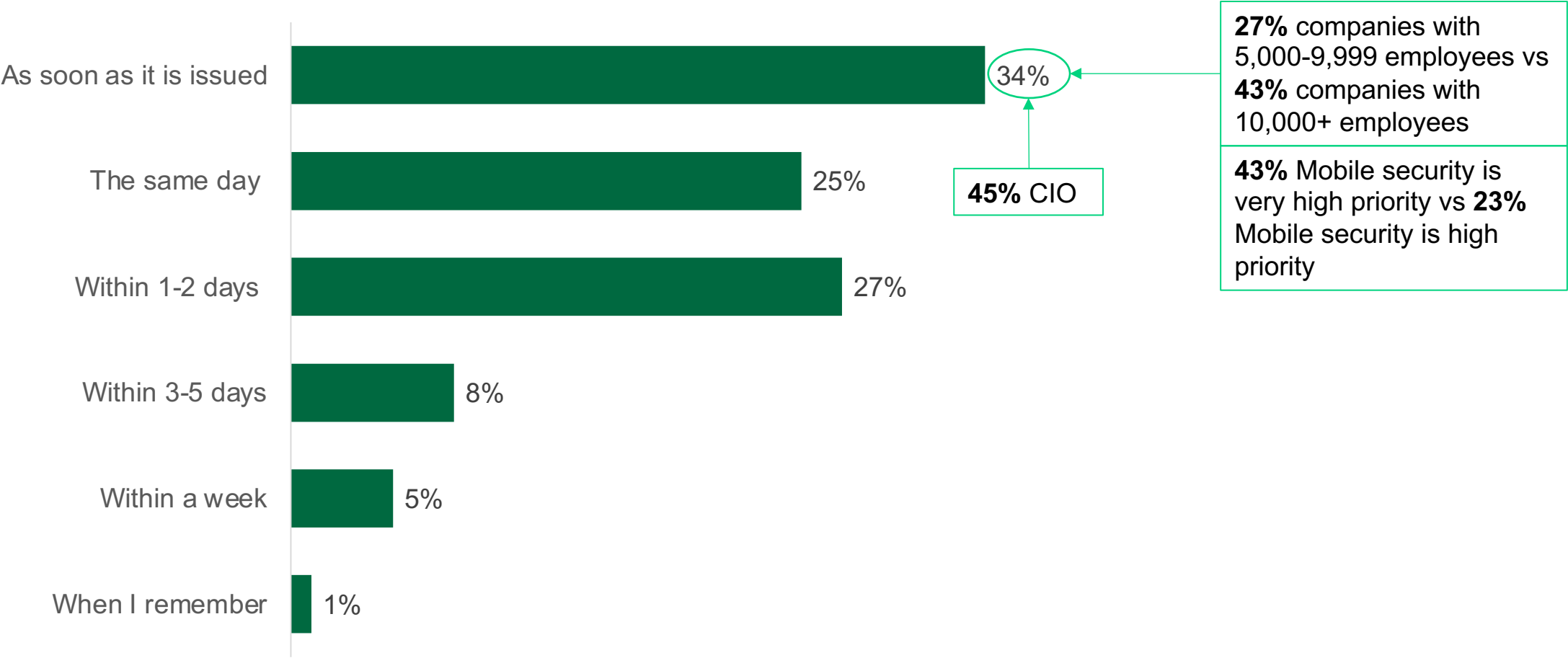
The majority think that iOS (62%) and the Apple App Store (58%) are more secure than Android and Google Play

Operating Systems

iOS
62%

Android
38%
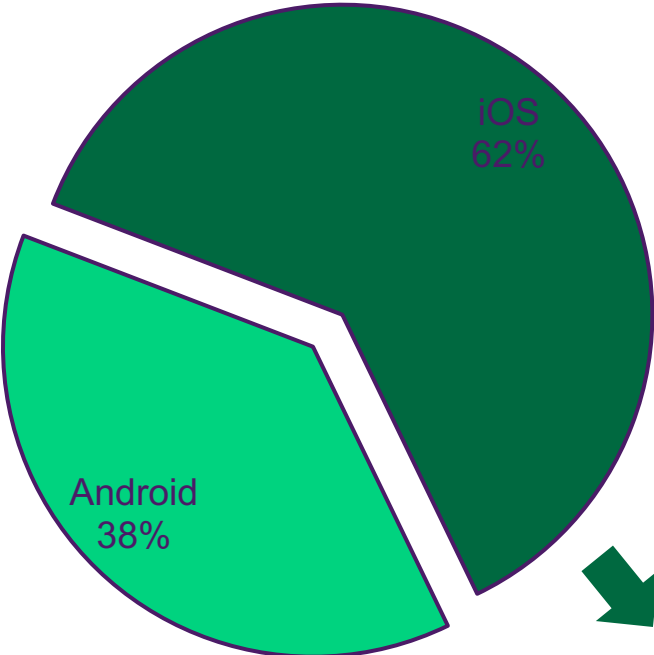
52% companies with 3,000-4,999 employees

44% CISO

UK	US	Australia
72%	60%	56%

Third Party App Stores
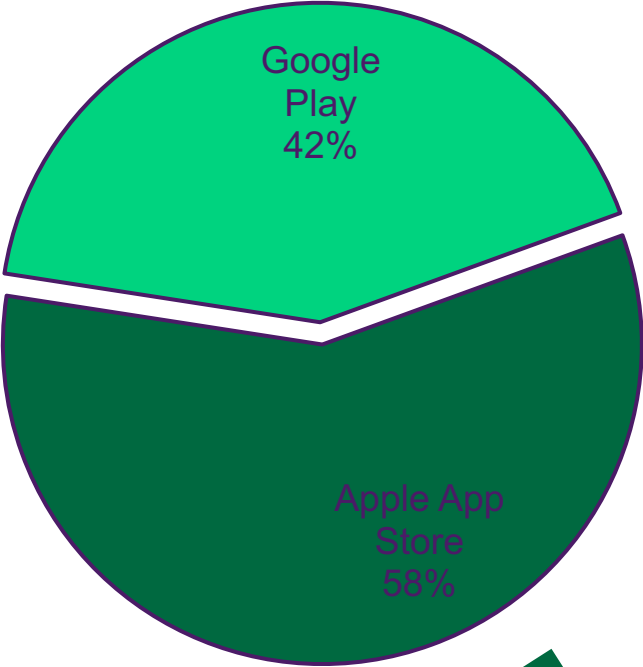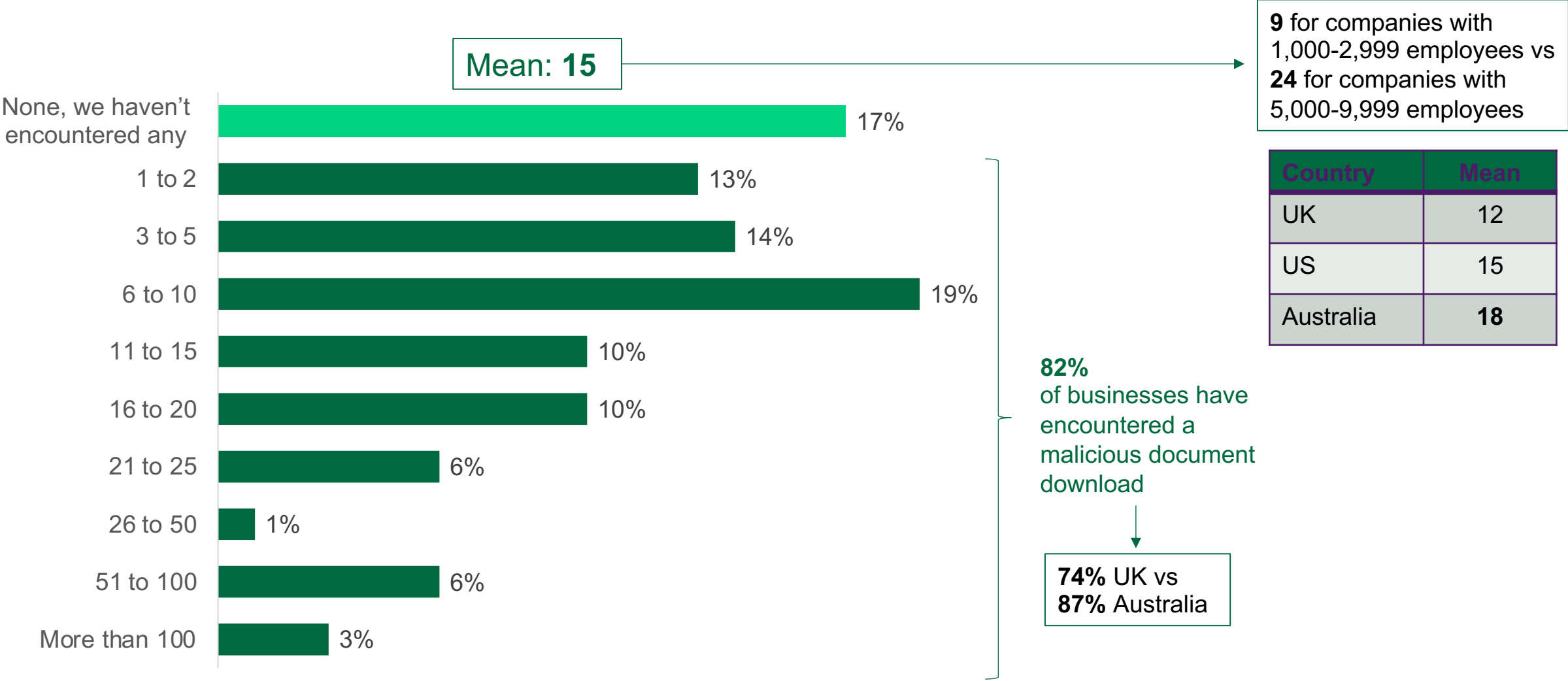

Google Play
42%

Apple App Store
58%

UK	US	Australia
68%	55%	50%

82% of IT decision makers have encountered malicious document downloads on corporate owned devices over the past 12 months
Those who have, encountered an average of 15 malicious downloads

9 for companies with 1,000-2,999 employees vs **24** for companies with 5,000-9,999 employees

Mean: **15**

Country	Mean
UK	12
US	15
Australia	**18**

Category	Percentage
None, we haven't encountered any	17%
1 to 2	13%
3 to 5	14%
6 to 10	19%
11 to 15	10%
16 to 20	10%
21 to 25	6%
26 to 50	1%
51 to 100	6%
More than 100	3%

82% of businesses have encountered a malicious document download

74% UK vs **87%** Australia

The majority have specific mobile security solutions in place either on the end users' device or within your organization (96%)
Over 4 in 5 use mobile device management as a mobile security solution **(84%)**

84%

41%

35%

4%

| Mobile Device Management | Isolation | DLP | No, we do not have any solutions in place yet |

91% Finance / Insurance / Accounting

78% UK vs **90%** Australia

36% UK vs **48%** Australia

25% UK vs **43%** Australia

49% Retail
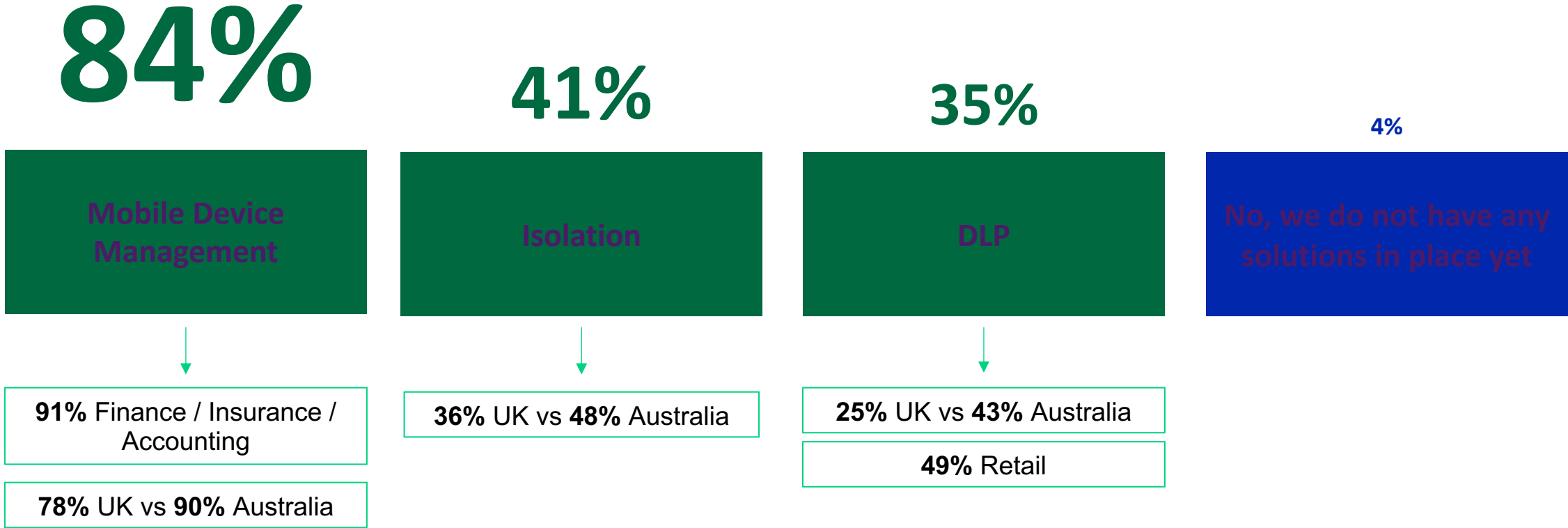
N.B. Other = 1%

Two thirds believe mobile browser vulnerabilities occur at least several times a week (67%)
A fifth think they occur multiple times a day (21%)

29% US vs
13% Australia

14% companies with
3,000-4,999 employees vs
32% companies with
10,000+ employees

67%

Category	Value
Multiple times a day	21%
At least once a day	19%
Several times a week	27%
Several times a month	16%
A few times a month	7%
Less than a few times a month	6%
I don't know	3%

73% Mobile security is very high priority vs **58%** Mobile security is high priority
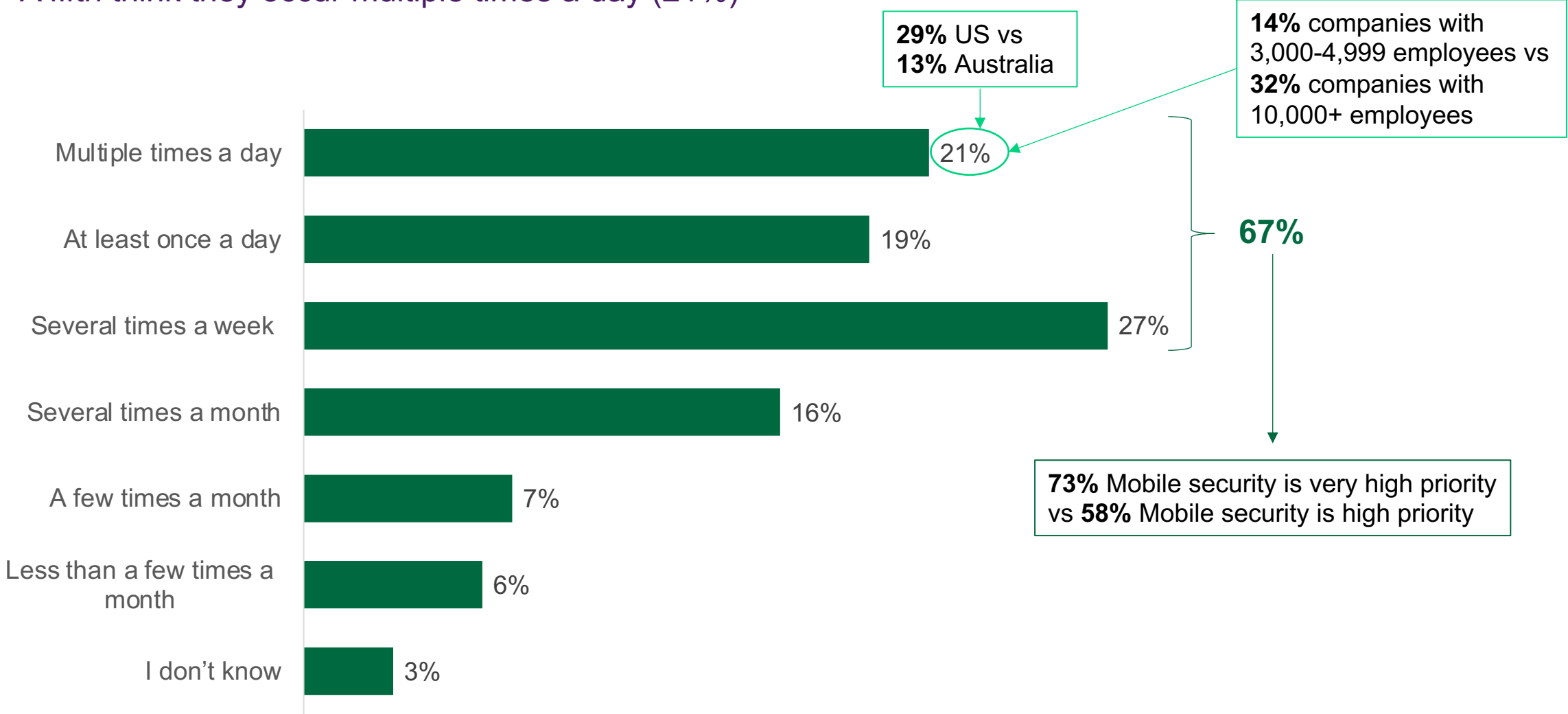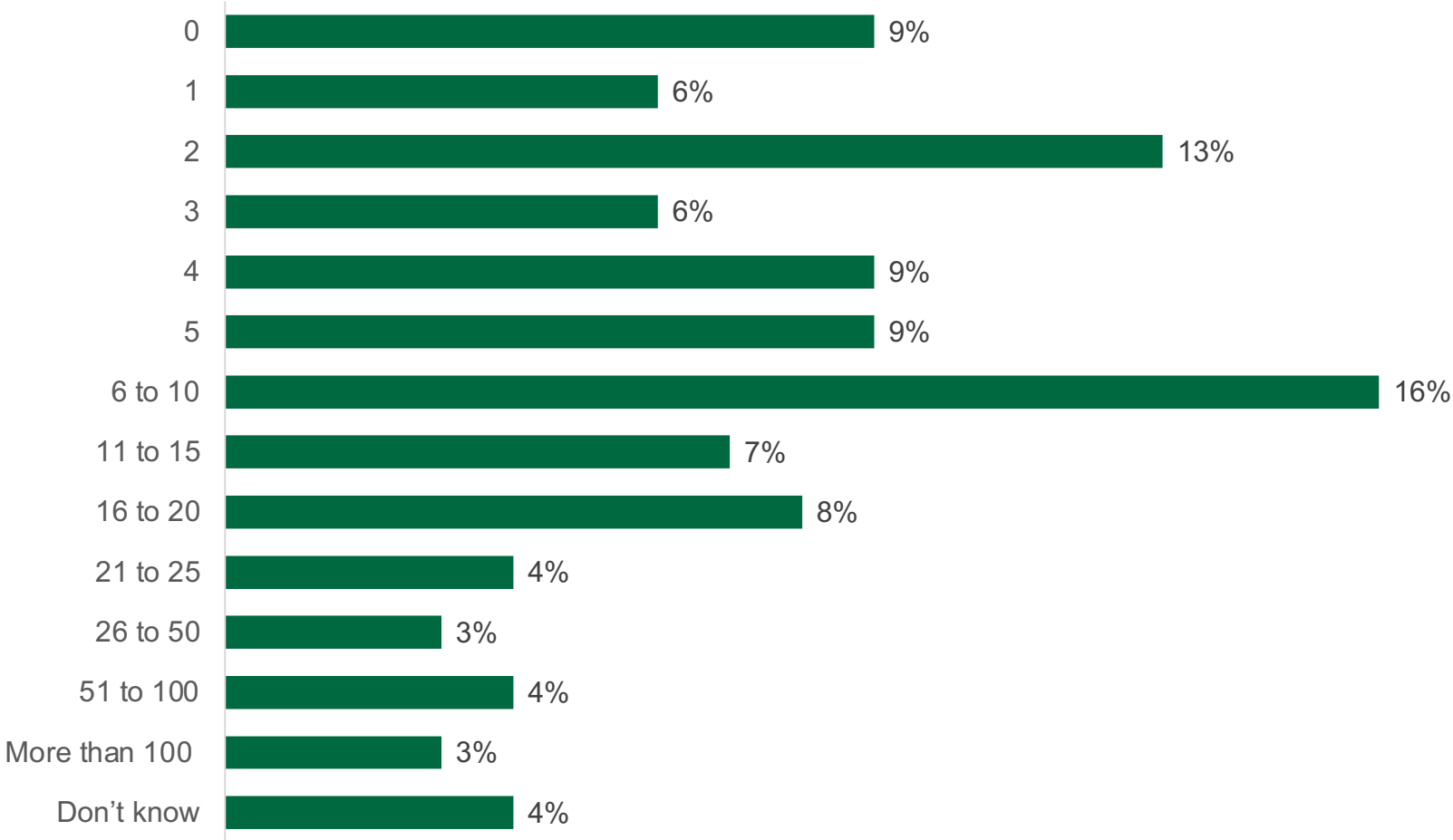
Respondents detected an average of 14 mobile security threats in the last month
Australian respondents detected the most (16) and UK respondents the least (12)

Mean: 14

9 for companies with 1,000-2,999 employees vs **24** for companies with 5,000-9,999 employees

Country	Mean
UK	12
US	14
Australia	**16**

Number of mobile security threats you have detected in the last month

Number	%
0	9%
1	6%
2	13%
3	6%
4	9%
5	9%
6 to 10	16%
11 to 15	7%
16 to 20	8%
21 to 25	4%
26 to 50	3%
51 to 100	4%
More than 100	3%
Don't know	4%

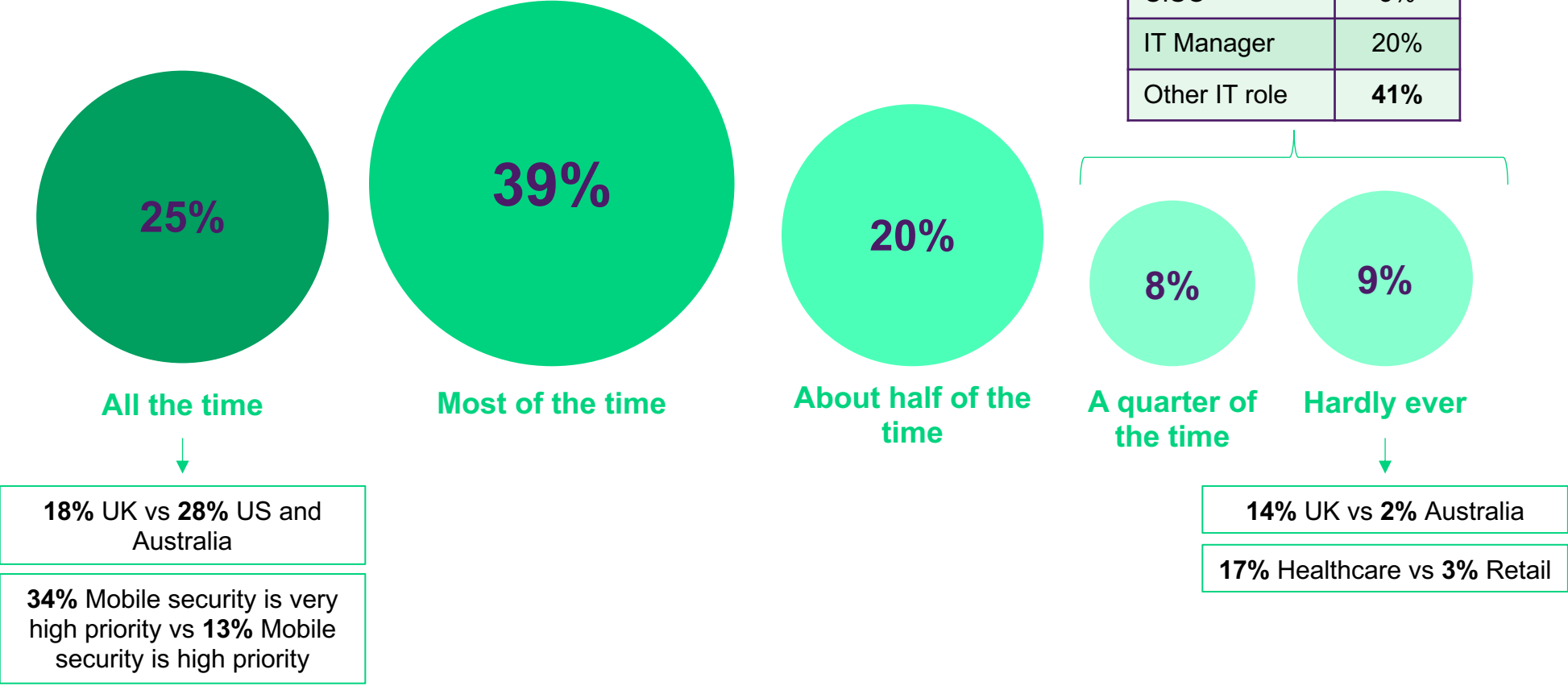Q9a. And how many mobile security threats have you detected in the last month? Please select one answer only
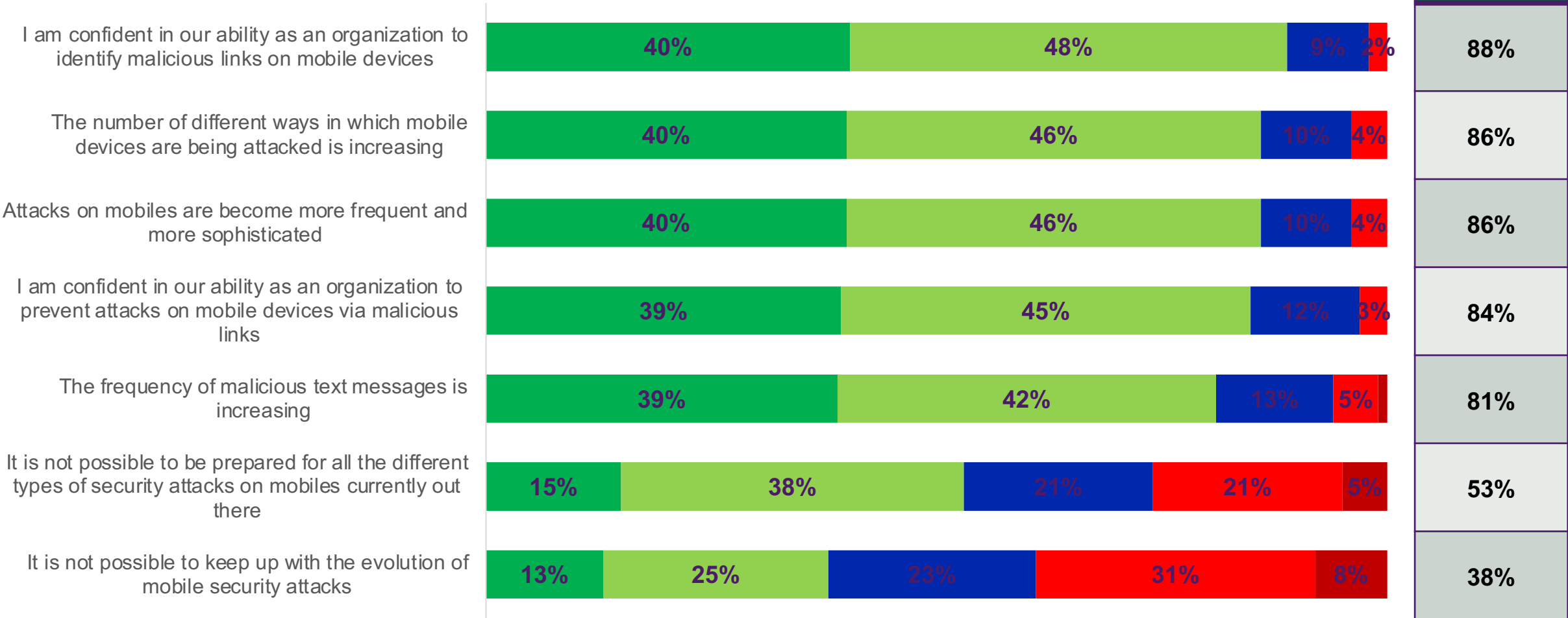
Base: 617

Only a quarter think their employees report mobile vulnerabilities every time they occur (25%)
The UK have the least trust in their employees, less than a fifth **(18%)** think mobile vulnerabilities are reported every time

Role	%
CIO	9%
CISO	3%
IT Manager	20%
Other IT role	**41%**

25%

39%

20%

8%

9%

All the time

Most of the time

About half of the time

A quarter of the time

Hardly ever

18% UK vs **28%** US and Australia

34% Mobile security is very high priority vs **13%** Mobile security is high priority

14% UK vs **2%** Australia

17% Healthcare vs **3%** Retail

Q9b. And when they occur, how often do you think mobile vulnerabilities are reported by your employees? Please select one answer only

Base: 617

While 9 in 10 are confident in their ability as an organisation to identify malicious links on mobile devices (88%), 86% agree that attacks on mobiles are becoming more frequent and sophisticated, and that the number of different ways mobile devices are being attacked is increasing
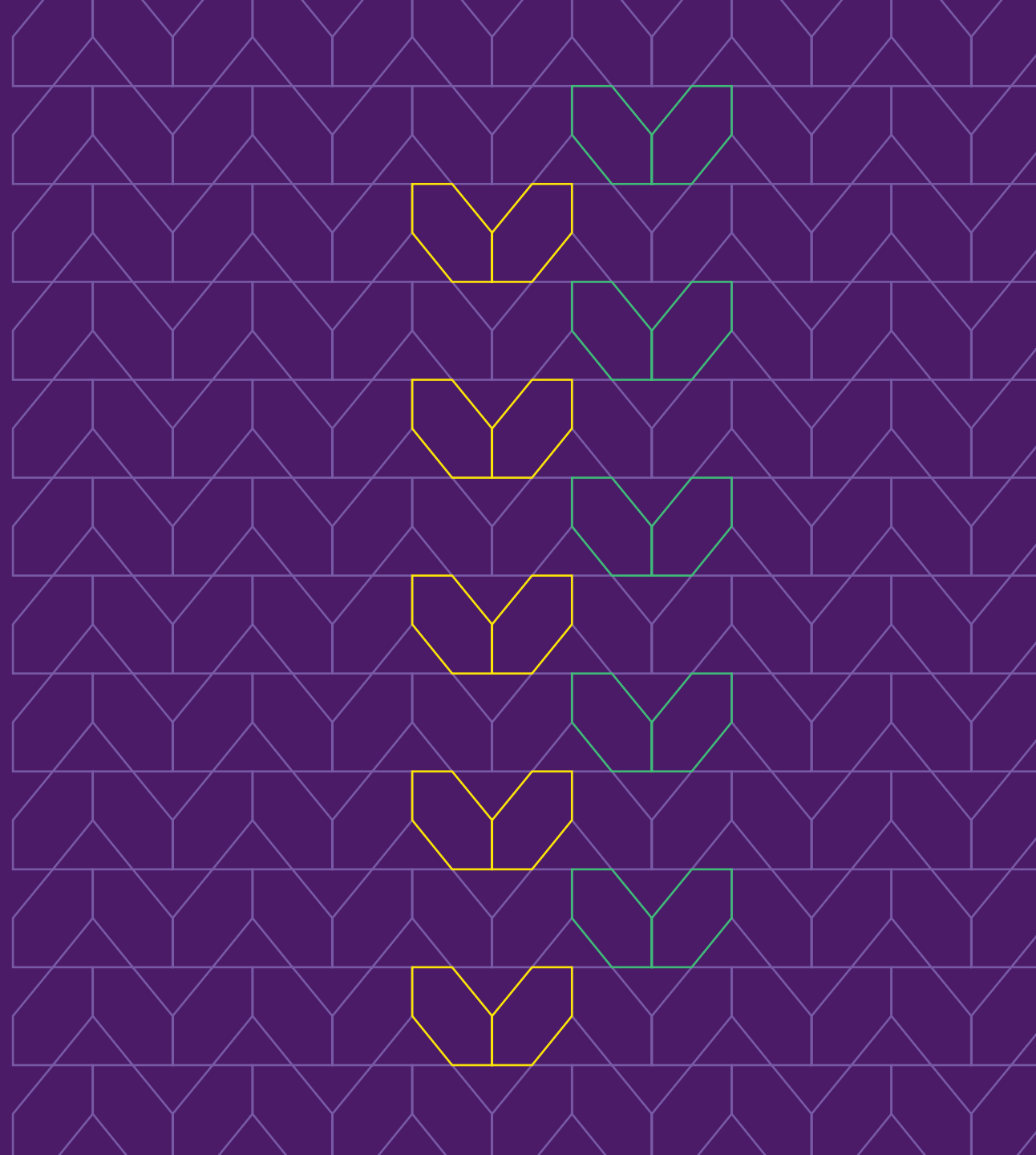
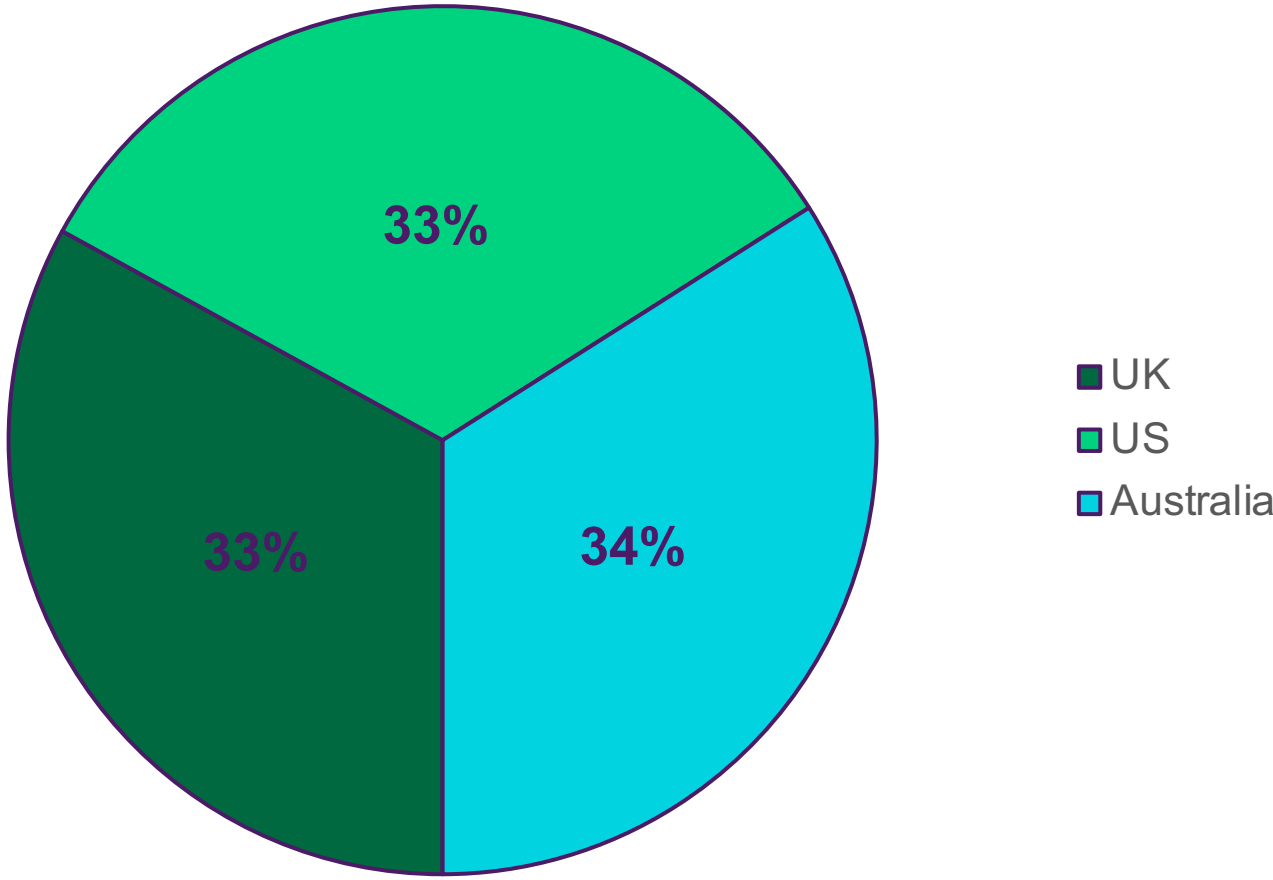Legend: ■ Strongly agree ■ Agree ■ Neither agree nor disagree ■ Disagree ■ Strongly disagree

Statement	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	% Agree
I am confident in our ability as an organization to identify malicious links on mobile devices	40%	48%	9%	2%		88%
The number of different ways in which mobile devices are being attacked is increasing	40%	46%	10%	4%		86%
Attacks on mobiles are become more frequent and more sophisticated	40%	46%	10%	4%		86%
I am confident in our ability as an organization to prevent attacks on mobile devices via malicious links	39%	45%	12%	3%		84%
The frequency of malicious text messages is increasing	39%	42%	13%	5%		81%
It is not possible to be prepared for all the different types of security attacks on mobiles currently out there	15%	38%	21%	21%	5%	53%
It is not possible to keep up with the evolution of mobile security attacks	13%	25%	23%	31%	8%	38%

Q10. How much do you agree or disagree with the following statements: Please select one answer per row

Base: 617

Demographics

MENLO
SECURITY
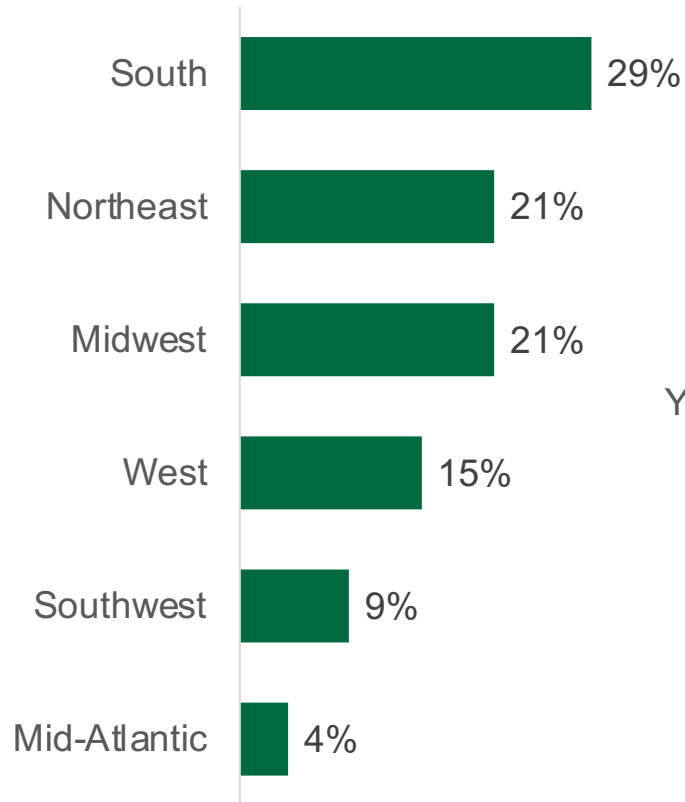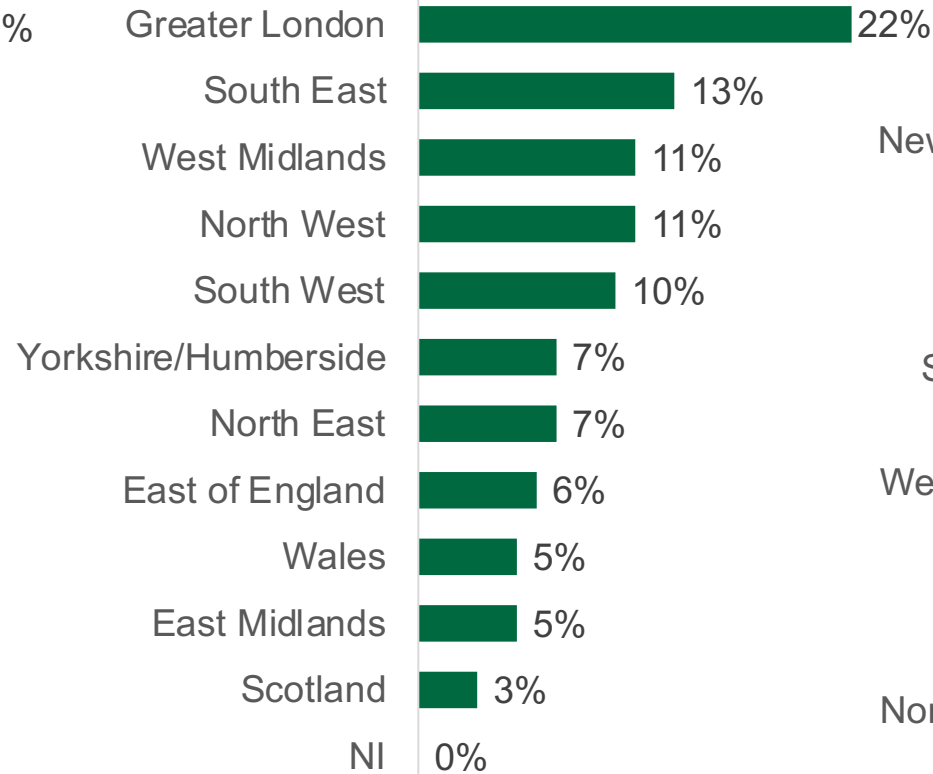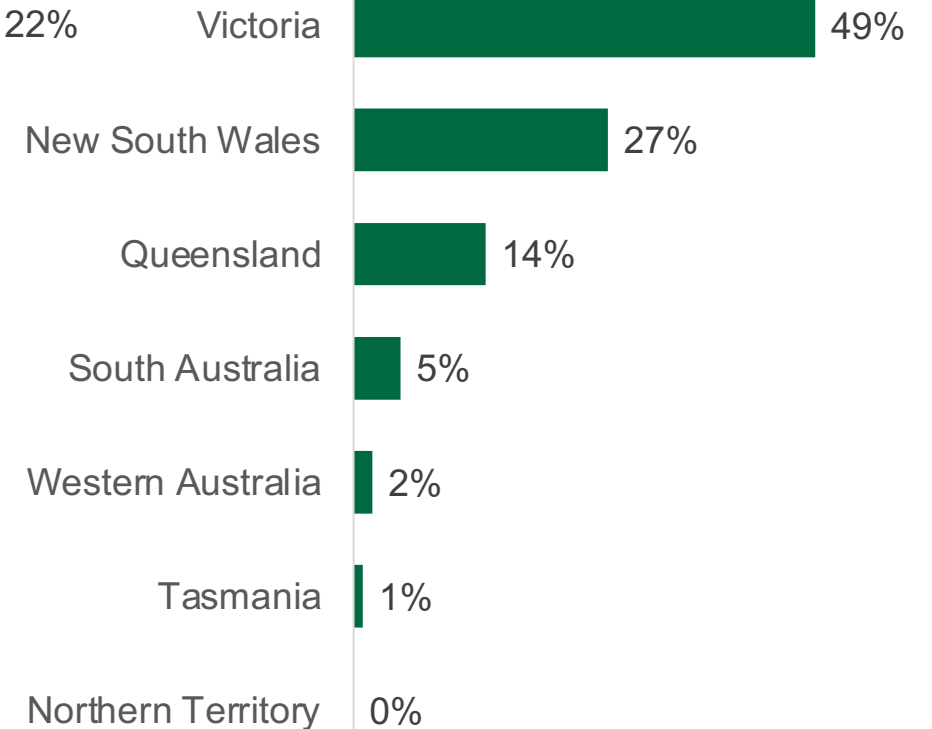
Country

Legend:
- UK
- US
- Australia

Pie chart values: 33% (US), 34% (Australia), 33% (UK)

Region

US

Region	Percentage
South	29%
Northeast	21%
Midwest	21%
West	15%
Southwest	9%
Mid-Atlantic	4%

UK

Region	Percentage
Greater London	22%
South East	13%
West Midlands	11%
North West	11%
South West	10%
Yorkshire/Humberside	7%
North East	7%
East of England	6%
Wales	5%
East Midlands	5%
Scotland	3%
NI	0%

Australia

Region	Percentage
Victoria	49%
New South Wales	27%
Queensland	14%
South Australia	5%
Western Australia	2%
Tasmania	1%
Northern Territory	0%

Industry

Industry	Percentage
Software/Technology	22%
Finance/Insurance/Accounting	15%
Retail	12%
Manufacturing	12%
Telecommunication	10%
Healthcare	7%
Government	6%
Education	4%
Construction	4%
Other	3%
Transportation/Utilities	3%
Wholesale trade	1%
Real Estate	1%
Hospitality	0%
Communication/Marketing/Advertising	0%
Agriculture	0%

Company Size

30%	32%	21%	18%
1,000 - 2,999 employees	3,000 - 4,999 employees	5,000 - 9,999 employees	10,000+ employees

Role

93%

7%

- IT
- Executive

Job Title

IT Manager	CIO	CISO	Other IT role
53%	22%	16%	9%

Management of IT Security

76%

24%

■ Yes, I am fully responsible
■ Yes, I am involved

S9. Are you responsible for or actively involved in the management and control of your organisation's IT security? Please select one answer only

Base: 617
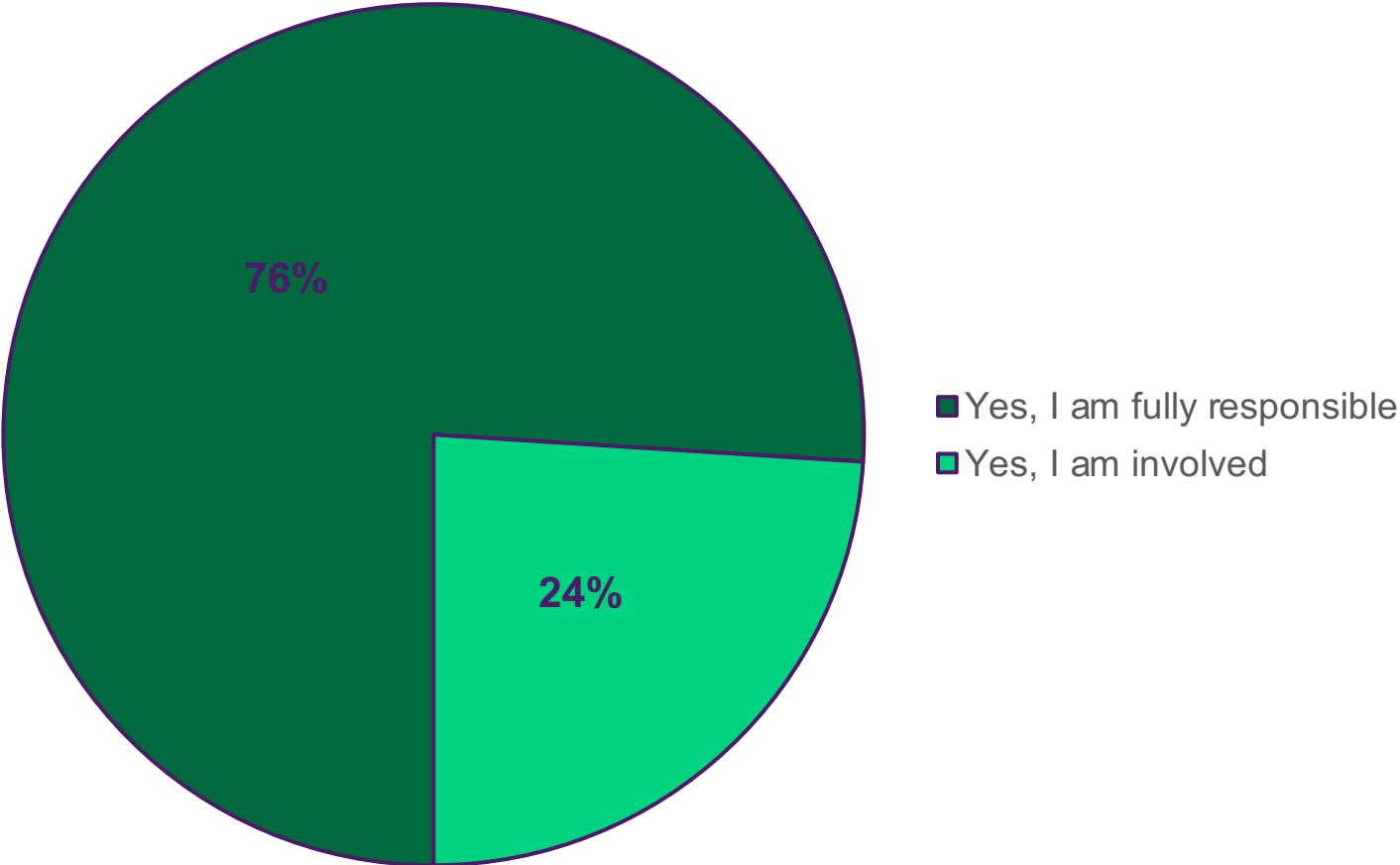
MENLO

SECURITY

menlosecurity.com