Menlo Security Mobile Report 2021

Menlo Security Mobile Report 2021
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.
Respondent demographics summary

<table>
<thead>
<tr>
<th>Demographics</th>
<th>Total respondents: 617</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country of residence</td>
<td><img src="flag_uk.png" alt="Flags" /> 204 <img src="flag_us.png" alt="Flags" /> 204 <img src="flag_au.png" alt="Flags" /> 209</td>
</tr>
</tbody>
</table>
| 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% |
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.
Summary and Overview

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.

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.

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.

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.

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

Q1. Where does mobile security rank in terms of your priorities? Please select one answer only.

- Very high: 93%
- High: 59%
- Medium: 6%
- Low: 1%
- Not a priority: 0%

Base: 617

Country | % High
--|--
UK | 90%
US | 90%
Australia | 99%

99% CIO vs 73% Other IT role
97% companies with 3,000-4,999 employees vs 86% companies with 10,000+ employees
Three quarters believe that end users are more open to attacks on mobile devices than they were a year ago (76%)
Phishing was the most common mobile security attack or attempt in the last 12 months (71%). Only 1 in 10 did not experience any mobile attacks or attempts in the last 12 months (11%).

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

- Phishing: 71%
- Malware: 66%
- Advanced Persistent Threats (APTs): 42%
- Something else: 2%
- We have not experienced any mobile security attacks or attempts in the last 12 months: 11%

Top for US: 58% UK vs 71% Australia

31% UK vs 51% Australia

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

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.

Q4. Who should be responsible for the security of the mobile devices used for work purposes? Please select one answer only.

<table>
<thead>
<tr>
<th>UK</th>
<th>US</th>
<th>Australia</th>
</tr>
</thead>
<tbody>
<tr>
<td>22%</td>
<td>22%</td>
<td>30%</td>
</tr>
</tbody>
</table>

End-users 25%

Mobile vendors 20%

Organizations 55%

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

UK | US | Australia
---|----|-----------|
15%| 18%| 28%       

39% CISO vs 73% Other IT role

<table>
<thead>
<tr>
<th>UK</th>
<th>US</th>
<th>Australia</th>
</tr>
</thead>
<tbody>
<tr>
<td>63%</td>
<td>60%</td>
<td>42%</td>
</tr>
</tbody>
</table>

Base: 617
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.

Q5. How quickly do you update your mobile device/operating system when a new patch is issued? Please select one answer only.

- 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%)

Base: 617

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.
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.

Q7. Over the past 12 months, have you encountered instances of malicious document downloads on corporate owned devices?

- 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%

Mean: 15

82% of businesses have encountered a malicious document download.

<table>
<thead>
<tr>
<th>Country</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK</td>
<td>12</td>
</tr>
<tr>
<td>US</td>
<td>15</td>
</tr>
<tr>
<td>Australia</td>
<td>18</td>
</tr>
</tbody>
</table>

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

74% UK vs 87% Australia.

Base: 617
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%).

Q8. Do you have specific mobile security solutions deployed on your end users’ device or within your organization, if so, what are they? Please select all that apply.

- Mobile Device Management: 84%
  - 91% Finance / Insurance / Accounting (78% UK vs 90% Australia)
  - 36% UK vs 48% Australia
- Isolation: 41%
- DLP: 35%
  - 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%)
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).

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

- 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%

Mean: 14

<table>
<thead>
<tr>
<th>Country</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK</td>
<td>12</td>
</tr>
<tr>
<td>US</td>
<td>14</td>
</tr>
<tr>
<td>Australia</td>
<td>16</td>
</tr>
</tbody>
</table>

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

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.

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

- All the time: 25%
- Most of the time: 39%
- About half of the time: 20%
- A quarter of the time: 8%
- Hardly ever: 9%

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.

<table>
<thead>
<tr>
<th>Statement</th>
<th>Strongly agree</th>
<th>Agree</th>
<th>Neither agree nor disagree</th>
<th>Disagree</th>
<th>Strongly disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>I am confident in our ability as an organization to identify malicious links on mobile devices</td>
<td>40%</td>
<td>48%</td>
<td>8%</td>
<td>3%</td>
<td></td>
</tr>
<tr>
<td>The number of different ways in which mobile devices are being attacked is increasing</td>
<td>40%</td>
<td>46%</td>
<td>10%</td>
<td>4%</td>
<td></td>
</tr>
<tr>
<td>Attacks on mobiles are becoming more frequent and more sophisticated</td>
<td>40%</td>
<td>46%</td>
<td>10%</td>
<td>4%</td>
<td></td>
</tr>
<tr>
<td>I am confident in our ability as an organization to prevent attacks on mobile devices via malicious links</td>
<td>39%</td>
<td>45%</td>
<td>12%</td>
<td>3%</td>
<td></td>
</tr>
<tr>
<td>The frequency of malicious text messages is increasing</td>
<td>39%</td>
<td>42%</td>
<td>12%</td>
<td>3%</td>
<td></td>
</tr>
<tr>
<td>It is not possible to be prepared for all the different types of security attacks on mobiles currently out there</td>
<td>15%</td>
<td>38%</td>
<td>21%</td>
<td>21%</td>
<td>9%</td>
</tr>
<tr>
<td>It is not possible to keep up with the evolution of mobile security attacks</td>
<td>13%</td>
<td>25%</td>
<td>29%</td>
<td>31%</td>
<td>8%</td>
</tr>
</tbody>
</table>

Q10. How much do you agree or disagree with the following statements: Please select one answer per row.
Demographics
S1. What country do you live in? Please select one answer only

Base: 617
### Region

<table>
<thead>
<tr>
<th>Region</th>
<th>US</th>
<th>UK</th>
<th>Australia</th>
</tr>
</thead>
<tbody>
<tr>
<td>South</td>
<td>29%</td>
<td>Greater London 22%</td>
<td>Victoria 49%</td>
</tr>
<tr>
<td>Northeast</td>
<td>21%</td>
<td>South East 13%</td>
<td>New South Wales 27%</td>
</tr>
<tr>
<td>Midwest</td>
<td>21%</td>
<td>West Midlands 11%</td>
<td>Queensland 14%</td>
</tr>
<tr>
<td>West</td>
<td>15%</td>
<td>North West 11%</td>
<td>South Australia 5%</td>
</tr>
<tr>
<td>Southwest</td>
<td>9%</td>
<td>South West 10%</td>
<td>Western Australia 2%</td>
</tr>
<tr>
<td>Mid-Atlantic</td>
<td>4%</td>
<td>Yorkshire/Humberside 7%</td>
<td>Tasmania 1%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>North East 7%</td>
<td>Northern Territory 0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>East of England 6%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wales 5%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>East Midlands 5%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Scotland 3%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NI 0%</td>
<td></td>
</tr>
</tbody>
</table>

**Base:** 204 / 204 / 209
S5. What industry sector is your organization in? Please select one answer only

Base: 617

- 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

S6. How many employees are there in your organization? Please select one answer only

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

Base: 617
S7. What best describes the area you work in? Please select one answer only

Base: 617
S8. Which of these titles best describes your job? Please select one answer only

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

Base: 617
S9. Are you responsible for or actively involved in the management and control of your organisation’s IT security? Please select one answer only.

- Yes, I am fully responsible: 76%
- Yes, I am involved: 24%

Base: 617