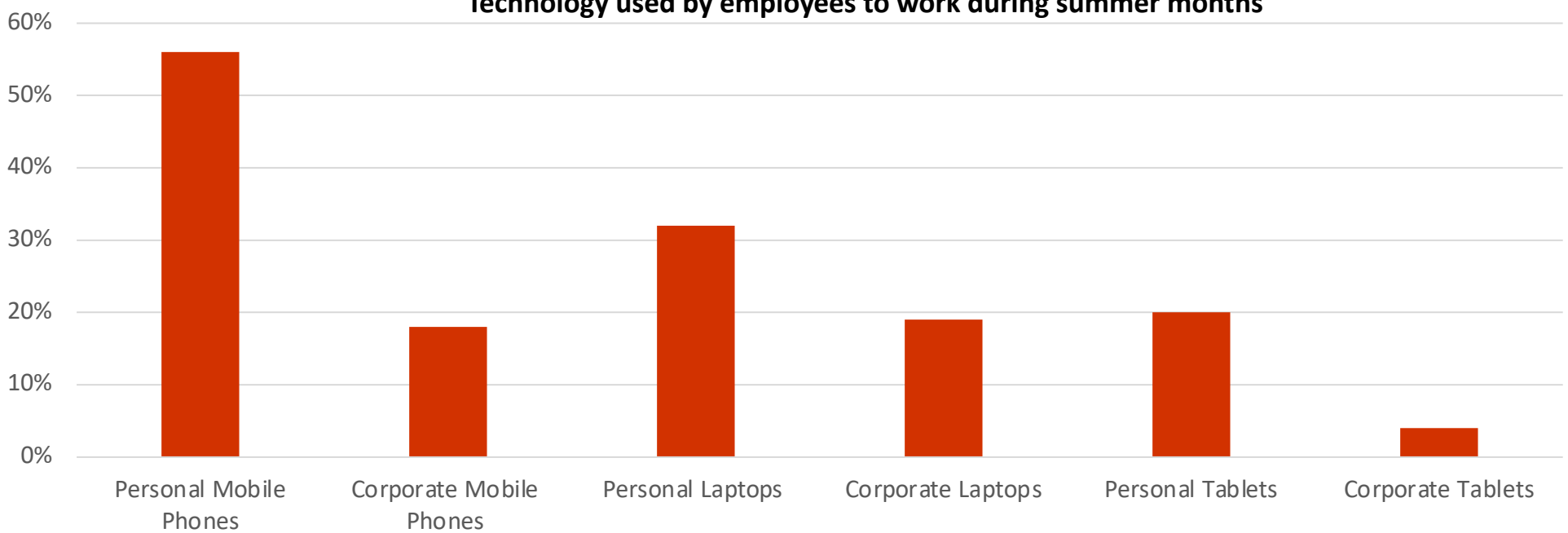ThreatX announced the findings from a 2023 survey on Cybersecurity Gaps During Summer Months, which sourced insights from 2,000 consumers ages 21+ across the US and UK. Respondents included 1,000 UK employees, whose data was broken out and analysed below. The data offers a better understanding of how employees during the summer are inadvertently increasing API and application risk with loosened cybersecurity practices. The results showcase how organisations, and specifically IT teams, are struggling to monitor and enforce BYOD (Bring Your Own Device) policies during summer months when more employees are traveling or working remotely.

1 56% of employees admit to relying solely on mobile devices while working from holiday destinations in the summer

Employees are using personal devices during the summer to access corporate data, which could enable cyber criminals to attack corporate networks, and makes it harder for IT teams to monitor BYOD policies – meaning mobile devices or the applications running on them could allow attackers to enter corporate networks through vulnerable APIs. **56% of employees admit to relying solely on their mobile devices** while working from holiday destinations in the summer, with **22% claiming that they are only slightly or not concerned about ensuring network connections** are secure when accessing company data, and **only 11% using a VPN** when traveling and working remotely.

Technology used by employees to work during summer months

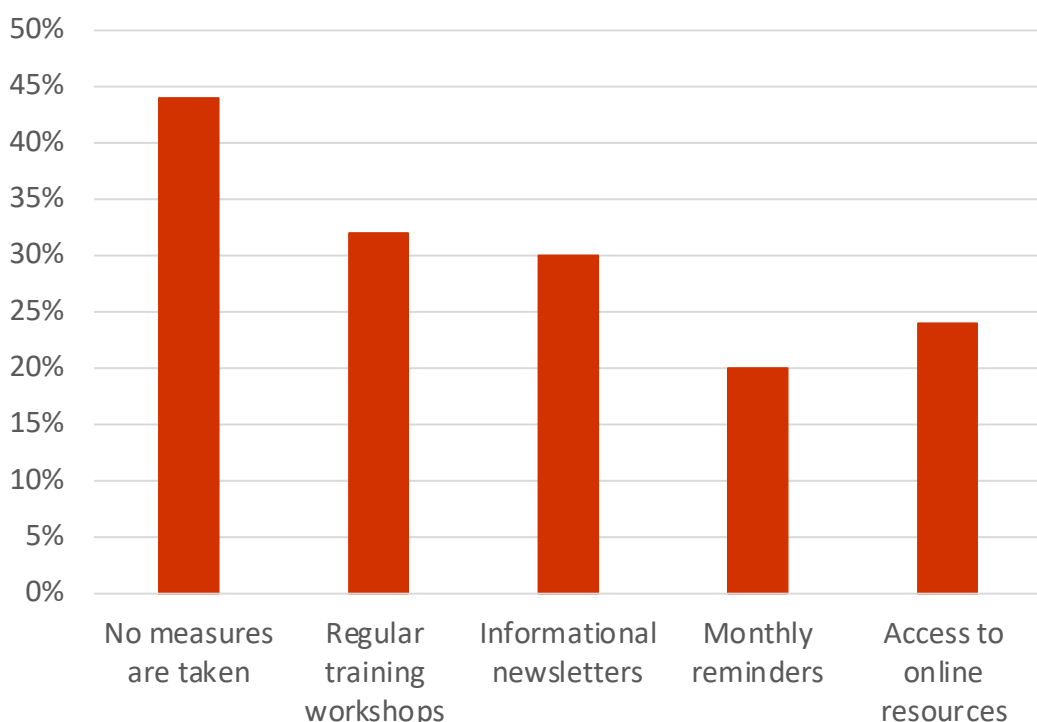| Technology	Percentage
Personal Mobile Phones	56%
Corporate Mobile Phones	18%
Personal Laptops	32%
Corporate Laptops	19%
Personal Tablets	20%
Corporate Tablets	4%

2 44% of employees in the UK said their employers take no specific measures to educate and remind employees on security best practices during the summer

The data reveals that it's more important than ever for businesses to develop a security program that emphasizes training and instills heightened security awareness during summer months. **44% of employees in the UK said their employers take no specific measures to educate and remind employees on security best practices** during the summer, with **32% receiving regular workshops and only 24% receiving access to online cybersecurity trainings.**
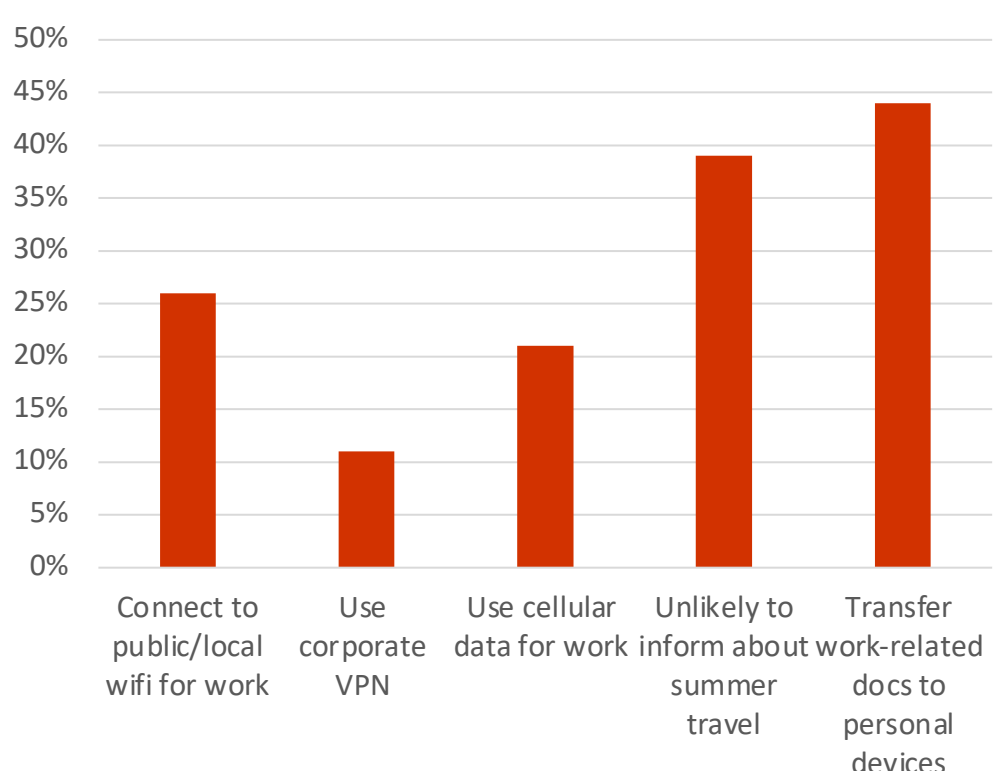
3 44% of employees are less likely to worry about cybersecurity best practices while working in the summer

44% of employees are less likely to worry about cybersecurity best practices while working in the summer. What's more, **39% admit to not updating employers when working from new locations**. With this in mind, it is important organizations strengthen the visibility and security by tracking, monitoring, and uncovering vulnerable API and applications.

Cybersecurity trainings available to employees over the summer

Training	Percentage
No measures are taken	44%
Regular training workshops	32%
Informational newsletters	30%
Monthly reminders	20%
Access to online resources	24%

Loosened cybersecurity behaviours during summer

Behaviour	Percentage
Connect to public/local wifi for work	26%
Use corporate VPN	11%
Use cellular data for work	21%
Unlikely to inform about summer travel	39%
Transfer work-related docs to personal devices	44%

*Source: June 2023 Dynata survey of 2,000 US and UK based consumers ranging from 21+ years of age. This infographic is reflective of the 1,000 UK respondents, exclusively.