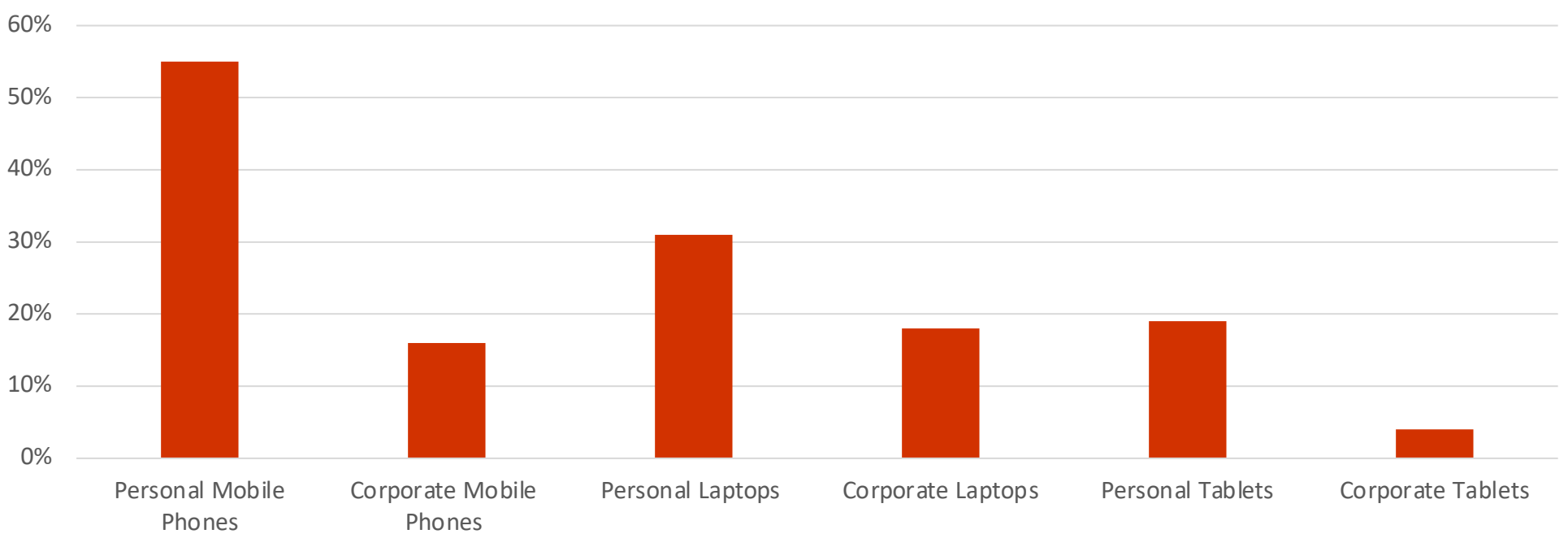


ThreatX announced the findings from a 2023 survey on [Cybersecurity Gaps During Summer Months](#), which sourced insights from 2,000 consumers ages 21+ across the US and UK. The data offers a better understanding of how employees during the summer are inadvertently increasing API and application risk with loosened cybersecurity practices. The results showcase how organizations, 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.

## 55% of employees admit to relying solely on mobile devices while working from vacation destinations in the summer

**1** 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 hackers to enter corporate networks through vulnerable APIs. **55% of employees admit to relying solely on their mobile devices** while working from vacation destinations in the summer, with **25% claiming that they aren't concerned about ensuring network connections** are secure when accessing company data, and **only 12% using a VPN** when traveling and working remotely.

Technology used by employees to work during summer months



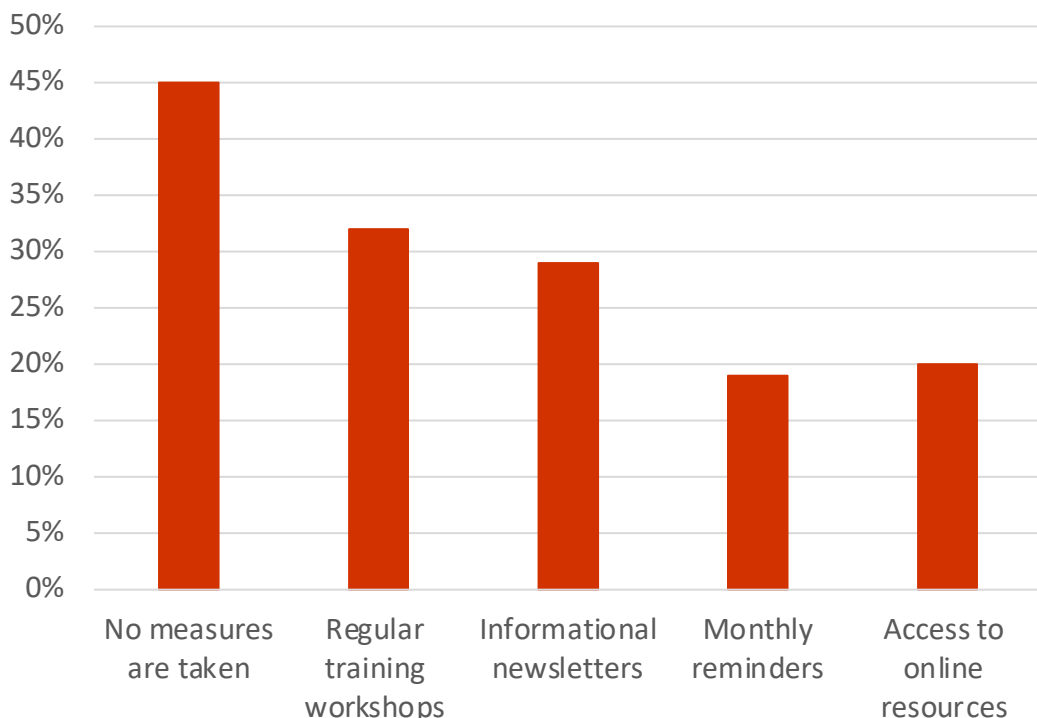
## 45% of employees in the US and UK said their employer takes no specific measures to educate and remind employees on security best practices during the summer.

**2** 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. **45% of employees in the US and UK said their employers take no specific measures to educate and remind employees on security best practices** during the summer, with only **24% of UK respondents receiving access to online cybersecurity trainings** and **even less (17%) in the US**.

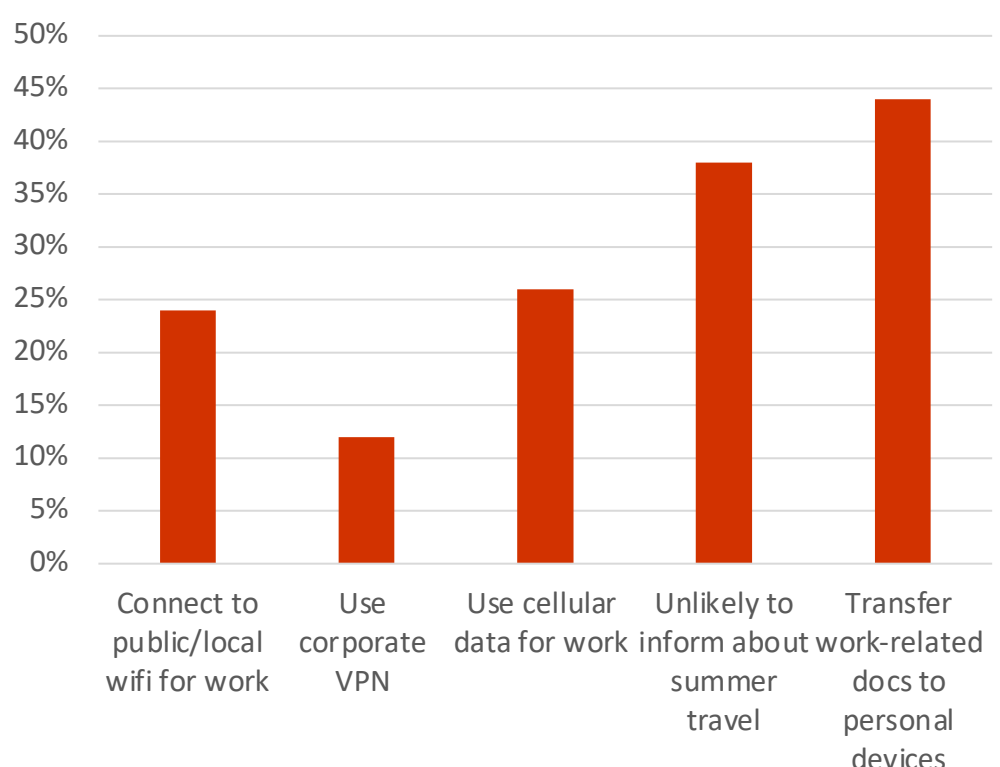
## 33% of employees are less likely to worry about cybersecurity best practices while working in the summer

**3** **33% of employees are less likely to worry about cybersecurity best practices** while working in the summer. What's more, **38% 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



Loosened cybersecurity behaviors during summer



\*Source: June 2023 Dynata survey of 2,000 US and UK based consumers ranging from 21+ years of age.