Mobile Security Index 2022: Public Sector

Spotlight

Key findings from extensive research into mobile-device security for local, state and federal government agencies, and education providers

Mobility is key to transformation.

Almost three-quarters of public-sector respondents said that mobile-based services are essential to accelerating the digital transformation of public services. Despite the imperative to transform, public-sector organizations are struggling. A large majority (86%) of respondents to our Mobile Security Index (MSI) survey from these organizations said that the public's expectations for self-service are putting great pressure on their budgets.

But mobile devices can be a threat.

That could help to explain why so many said that they had suffered a mobile-related compromise in the preceding 12 months. Nearly half (49%) of public-sector respondents said a mobile-related incident at their organization had led to lost data or downtime. That compares to just 27% of manufacturers and 34% of retail and hospitality companies.

The contributing factor most often cited by public-sector respondents was network threats, such as rogue base stations, insecure Wi-Fi or denial-of-service attacks. Over half (52%) of public-sector respondents affected said that this type of threat was at least partially to blame.

The fallout for public-sector organizations was often severe. Nearly three-quarters (73%) of those suffering a compromise said the consequences were major—and 61% of those said the consequences were lasting. Putting further pressure on already stretched resources, over two-fifths (42%) said remediation was "difficult and expensive."

Of public-sector organizations that experienced a compromise, 44% suffered reputational damage and 35% faced regulatory penalties.

49%

Almost half of public-sector respondents said their organization had suffered a mobile-related compromise in the past 12 months.

84%

Most public-sector respondents said organizations need to take the security of mobile devices more seriously.

87%

The vast majority of public-sector respondents said employee expectations for remote/flexible working are forcing them to reevaluate how they do things.

verizon✓

Mobile devices are an entry point, but not always the target.

The impact of mobile-related attacks wasn't limited to the devices themselves. Two-fifths of public-sector respondents that had experienced a mobile-related compromise said that cloud-based systems were affected as a result.

This highlights how important securing mobile devices is to reducing an organization's risk, yet only a third (34%) of public-sector respondents said their mobile security defenses were "very effective." That's despite most (68%) spending more in the previous 12 months than the year before. Reasons for increased spend included more devices (54%), more users (50%) and users doing more with their devices (48%).

2x

Almost twice as many public-sector respondents said their organization had suffered a mobile-related compromise in the past 12 months[1] as in our 2021 survey.

Lessons have been learned.

A lot has changed in the past couple of years. For many organizations, enabling users to work from home was crucial to maintaining services. Across all the public-sector organizations in our survey, an average of just 42% of employees now work from a government agency facility most (over 80%) of the time.

The ability to respond to changing expectations and unforeseen events is now crucial to strategy. Over three-quarters (77%) of public-sector respondents said being able to take a future crisis in stride is key to their planning and investment.

That includes being able to offer employees flexibility in where they work and what devices they can use. Five out of six (84%) public-sector respondents said this will be important to attracting the best new talent.

Organizations want to make security easier.

Looking ahead, 71% of public-sector respondents said they expect mobile security spend to increase in the coming 12 months. The two most frequently mentioned reasons for this were increased awareness of threats (60%) and increasing threats (58%).

Maintaining device security is not a trivial endeavor. Public-sector respondents' stated objectives for the additional spend over the next 12 months revolve around improving existing capabilities rather than innovation. This included increasing the security of existing user activities (55%); integrating the security management of phones, tablets and laptops (54%); and increasing automation to reduce the burden on the IT team (52%).

Find out more.

The fifth edition of the Verizon Mobile Security Index is available now. It's based on a survey of over 600 professionals responsible for the procurement, management and security of mobile devices. In addition to data and insights from Verizon, the report features contributions from other leading cybersecurity practitioners, including Absolute, Check Point, IBM, Ivanti, Jamf, Lookout, Netskope, Proofpoint and Thales.

The 2022 report features deep dives on key threats like phishing, ransomware and inappropriate use. It's also packed with actionable recommendations—from how to secure a bring-your-own-device (BYOD) setup to how to create an effective incident response program. The insights in this report, combined with the concise how-to guides, could help you transform your mobile device defenses and protect your users, your constituents and your organization's reputation.

Read the full report at
verizon.com/mobilesecurityindex

[1] A successful attack that results in a system's defenses being rendered ineffective. This could involve data loss, downtime, other systems being affected or no detrimental effects at all. It could be malicious or accidental.

verizon