Public sector cybersecurity: What to watch out for

The U.S. government – whether federal, state or local – remains a high-profile target for information theft and cyber disruption.

Analysis from the Verizon 2023 Data Breach Investigations Report (DBIR) found that Public Administration accounted for 20% of incidents, more than any other sector. Almost a fifth (17.8%) of these had confirmed data disclosure.[1]

Where do cyber threats come from?

Collusion: There was evidence of internal and external actors working together in 16% of Public Administration breaches – much higher than the 2% for the overall data set.[2]

Mobile workers: Half (49%) of public sector workers say their organization suffered a mobile-related compromise in the past 12 months, according to the Verizon 2022 Mobile Security Index (MSI): Public Sector report. That's compared to just 27% of manufacturing and 34% of retail and hospitality respondents.[3]

Networks: In over half (52%) of mobile breaches, network threats such as rogue base stations, insecure Wi-Fi or denial-of-service attacks were responsible.[4]

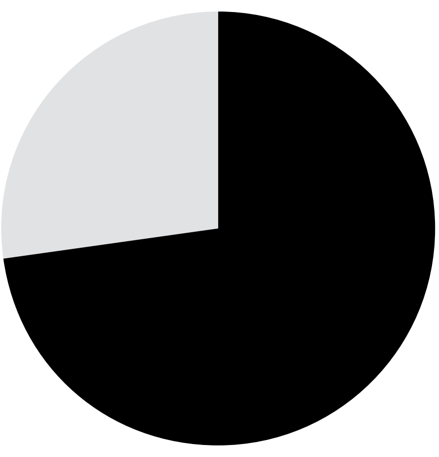
Ransomware: In 2022, 106 state or municipal governments/agencies were hit by ransomware, a 38% increase from 2021. Data was stolen in at least a quarter (25%) of incidents.[5]

Spies: This is the sector where espionage motivation is the highest.[6]

What is the impact?

An estimated 822 U.S. government entities have suffered data breaches between 2014 and 2022, impacting 175 million records. The estimated cost stands at $26 billion.[7]

According to the MSI, when public sector agencies suffered mobile-related compromises:[8]



73%

said the consequences were major.

61%

indicated the consequences were lasting.

44%

suffered reputational damage.

42%

said remediation was "difficult and expensive."

35%

faced regulatory penalties.

How Verizon can help.

Verizon has worked hand in hand with the public sector to help mitigate cyber risk for decades. Consider how the following could help you better serve your constituents and communities:

The Verizon Threat Research Advisory Center (VTRAC) can help you regain control and mitigate cyber threats from your networks, applications and devices.

Mobile device management (MDM) solutions can reduce the risks encountered by an increasingly remote workforce. They can enable remote enforcement of security policies and detection of non-compliant devices.

Cyber risk monitoring provides a 360-degree view of your security posture to help identify security gaps and areas to prioritize.

The DBIR provides cybersecurity insights sourced from cyber experts' analysis of breaches and incidents from around the world. Find the results of the 2023 DBIR, including a special section on the public sector, at verizon.com/dbir.

verizon✓

The author of this content is a paid contributor for Verizon.

[1] Verizon 2023 Data Breach Investigations Report.

[2] Ibid.

[3] Verizon, Mobile Security Index 2022: Public Sector.

[4] Ibid.

[5] Emsisoft, The State of Ransomware in the US: Report and Statistics 2022.

[6] Verizon 2023 Data Breach Investigations Report.

[7] Comparitech, Government breaches – can you trust the US Government with your data?, November 2022.

[8] Verizon, Mobile Security Index 2022: Public Sector.