

Bond Case Briefs

Municipal Finance Law Since 1971

State and Local Security Adjusting to Shifting Cyber Threats, Insurance Requirements.

State and local governments are under the radar no more. Although security has always been taken seriously, many governments didn't consider going as far as taking out cybersecurity insurance because they didn't feel they were lucrative enough targets to attract the persistent attention of cyber threat actors.

But any added sense of security from being perceived as relatively inconsequential targets is quickly eroding. The attacks this summer on the [City of Columbus, Ohio](#), and the [New Mexico public defender's office](#) were notable on their own, but they also continued a trend. Malware attacks and ransomware incidents targeting state and local governments increased by [148% and 51%](#), respectively, from 2022 to 2023, and show no signs of slowing down.

At the state level, CISOs are facing this increasingly pernicious threat, with nearly 40% of them saying they don't have the IT budgets or resources to protect systems that are heavy with legacy equipment, [according to a report](#) released Sept. 30 by Deloitte and the National Association of State Chief Information Officers (NASCIO).

[Continue reading.](#)

Route Fifty

By Paul Underwood,
VP of Security, Neovera

November 12, 2024