Public Law Update – New Law Allows Legislative Bodies to Meet in Closed Session on Cybersecurity Threats

RELATED PRACTICES

California City Attorney
Public Law

RELATED PEOPLE

Charles H. Abbott

On September 14, 2024, Governor Newsom signed AB 2715, which amends the Ralph M. Brown Act ('Brown Act") and allows legislative bodies to hold a closed session about threats relating to cybersecurity. This new law takes effect on January 1, 2025.

The Brown Act generally requires legislative bodies to hold open meetings, ensuring transparency in their decision-making process. Under limited circumstances, however, the Brown Act allows closed sessions, which are private sessions excluding the public and press. Government Code Section 54957 permits a closed session to discuss threats to security of public buildings, essential public services, or the public's right to access these buildings or services.

AB 2715 adds language to Section 54957 to clarify that a public entity may hold a closed session to discuss threats "to critical infrastructure controls or critical infrastructure information relating to cybersecurity." Subsection (a)(2)(A) defines "critical infrastructure control" to include the computer networks and systems so critical that their incapacity or destruction would have a "debilitating impact on public health, safety, economic security, or a combination thereof." And Section (a)(2)(B) defines the "critical infrastructure information" to mean any actual, potential, or threatened interference with or incapacitation of the critical infrastructure through a physical or computer-based attack.

AB 2715 explicitly permits a public entity to have private conversations with technological and security experts before a cyberattack occurs. Specifically, the public entity can keep private the hardware and software it employs to prevent an attack. The new law also allows a public entity to work with those experts in private on a strategy to restore critical infrastructure after a ransomware attack. A private session permits a public entity to discuss openly the infrastructure impacted and the process to restore that infrastructure without fear of disclosure to the very threat actors who caused the disruption.

Cyberattacks on a public entity's computer infrastructure are on the rise. Reports suggest that cyberattacks on the public sector rose 40 percent in 2023. These attacks have real consequences for public

entities. Ransomware disrupts City services and often results in personal information leaked to the Internet.

Not only does a cyberattack require a public entity to seek legal expertise about mitigation, notification and labor relations, but the leak often results in litigation. Public entities have legal immunities and particular arguments, unavailable to private businesses, to combat class-action lawsuits. Burke's expertise in public law and data breach provides governmental entities with a unique perspective to address the wide-ranging issues arising from cybersecurity threats and an attack.
