Published on *The National Law Review* https://natlawreview.com

Municipal Group News: Municipalities Under Connecticut's New Cybersecurity Strategy

Article By:

Burt Cohen

Kari L. Olson

On July 10, 2017, Governor Dannel Malloy, along with Chief Information Officer Mark Raymond and Chief Cybersecurity Risk Officer Arthur House, released Connecticut's initial Cybersecurity Strategy. The goal of the Cybersecurity Strategy "is to strengthen the awareness and resilience of public and private entities to reduce the likelihood and severity of large cyber attacks." The Strategy focused on five essential sectors in the State: Connecticut State Government; Municipalities; Business(emphasizing critical infrastructure, financial services, insurance and defense); Higher Education; and Law Enforcement and Security. "These sectors were selected because of their statewide importance, as well as their special status as both prime targets and prime defensive players in the event of a major incident. They matter, and cyber adversaries know that."

The Strategy discusses in depth what it refers to as "our shared vulnerability." As the Strategy points out, "[n]ational experts confirm that almost everyone . . . has been or will be penetrated – banks, utilities, hospitals, schools, manufacturing and services firms and national, state and local governments." Municipalities have a treasure trove of private information about their employees, their students, their residents, and their ongoing law enforcement duties that makes local governments susceptible targets for compromise by cyber attacks. The Strategy notes several municipal cyber incidents that have caused disruption to important public services, such as mass transit, and the havoc that could be caused by loss of critical communications to emergency services. Accordingly, the principles of the Strategy apply to local governments, noting that even a single cyber incident can have devastating consequences and that executives in the both government and business have to make cybersecurity a persistent priority.

The Strategy addresses key municipal cyber concerns.

From a legal perspective, municipalities are subject to Connecticut's Data Breach law, enacted in 2015, codified in Conn. Gen. Stat. § 36a-701(b), which requires notification to both impacted residents and the Connecticut Attorney General. The Strategy then states that "[i]n response, many municipalities have implemented written information security plans (WISPs), documenting the measures they are taking to protect the integrity of the information they collect and maintain." Once considered a "best practice," WISPs are now an essential element for cyber planning in the private

sector, and some jurisdictions, such as Massachusetts, require them. And to the extent that municipalities rely on third-party providers for services to residents, students and employees, municipal governments have a legal duty to ensure that those vendors are also following the appropriate protocols and practices to maintain the confidentiality of personally identifiable information obtained as part of that relationship.

From an operational perspective, the Strategy lists some "initial strategic objectives" for municipalities:

1. Increase civic awareness of cyber dangers; identify "prevention measures"; investigate cyber breaches; and prosecute cyber crimes.
2. Joint efforts to make cyber defense "a shared learning experience" and cost-sharing.
3. Embrace collaboration with the State Department of Administrative Services and its Bureau of Enterprise Systems and Technology, which provides security protocols for the executive branch of State government.
4. Assess municipal cyber security efforts in other states.

The Strategy notes that the Connecticut Police Chief's Association has no cybersecurity strategy and each municipal police department addresses cybercrime as necessary but without adequate resources and procedures. There is a general statement that police capabilities should be strengthened, but this may not be possible without federal grants.

The Connecticut Cybersecurity Strategy may be downloaded at www.ct.gov/ctcyberlibrary.

The key take-aways for municipal leaders from the State's Strategy involve:

1. Development of a written information security plan for all levels of municipal government.
2. Ongoing training for employees on cybersecurity, security awareness and best practices on protecting confidential information.
3. Regular briefing of chief elected officials on cyber threats, risks, mitigation efforts and workforce needs.
4. Development of a culture of cyber-awareness not only by local government but also through the public education system and other municipal and civic organizations.
5. Working with other State and local governmental agencies on cyber-risks and incident reporting.

In summary, the Connecticut Cybersecurity Strategy is a thoughtful and well-researched document, although it may be more aspirational in certain parts. Municipalities are clearly considered a key participant in the implementation of the Strategy. Although cybersecurity is a complex problem, some relatively simple measures can lead to enhanced municipal preparation, awareness and response when cyber attacks strike.

National Law Review, Volume VII, Number 200