# Bond Case Briefs

*Municipal Finance Law Since 1971*

---

## How Local Governments Can Prevent Cyberattacks.

The recent cyberattack on Atlanta, in which the municipal government's computers and related services were held hostage by a ransomware attack, is a reminder that local governments are particularly vulnerable to these and other cyberthreats.

Local governments of all sizes and locations now own and operate a wide and growing array of internet-connected technology systems: employee-issued laptops, motion sensors on light poles and under pavement, mapping and informational systems inside police cars, online citizen-engagement tools and much more.

Most local governments in the United States don't have a strong grasp of the policies and procedures they should implement to protect their technology systems from attacks. This is especially concerning because the threat of a cyberattack is the most important cybersecurity problem they face, according to a survey conducted by the organization I work for, the International City/County Management Association, and the University of Maryland, Baltimore County.

Forty-four percent of local governments report that they regularly face cyberattacks, on either an hourly or daily basis. More troubling is the high percentage of governments that do not know how often they are attacked (28 percent) or breached (41 percent). Further, a majority of local governments do not catalog or count attacks (54 percent).

This is not just an American problem. Last month, at a conference in Tel Aviv, Tamir Pardo, the former head of Mossad, Israel's national intelligence agency, said that most local government leaders around the world do not fully understand how serious a threat cyberattacks are and have not imaginatively assessed the consequences of inaction. He described cyberthreats as "soft nuclear weapons" that one day may be used to start and finish a war without firing a shot.

So what should local governments do to improve their cybersecurity apparatus to help prevent or mitigate damage from future attacks like the one experienced in Atlanta, or from those contemplated by Mr. Pardo?

First, local leaders must create a culture of cybersecurity that imagines worst-case scenarios and explores a range of solutions to mitigate threats to the ecosystem of local government technology. This should involve prioritizing funding for cybersecurity, establishing stronger cybersecurity policies and training employees in cybersecurity protocols. Success will require collaboration with local elected officials, internet-technology and cybersecurity staff members, department managers and end users.

Cybersecurity is more than just the I.T. department's problem. It must now also be a top priority along the entire chain of elected and appointed officials in and around local governments. Preventing and mitigating the effects of future attacks will require intergovernmental cooperation, because localities work together across state lines and collaborate with the federal government on crucial tasks like running elections, managing transportation and sharing intelligence.

Most technological advances are transforming local governments for the better, moving them from inefficient and costly paper systems to digital systems that allow for better analysis and understanding of policy decisions. The science of analytics and big data promises even greater leaps for local governments in evidence-based policymaking. These exciting developments may one day radically alter the ways that traditional local government services are financed, operated and managed.

But we cannot get lost in the excitement. We must actively prepare for cyberthreats of the sort that have been demonstrated in places like Atlanta. If smart cities and communities are the brightly lit days of the increasingly connected world of local government technology, cyberattacks are the dark and stormy nights. We don't need to halt technological deployments and evolution, but we do need to recognize that cybersecurity is an essential counterpart.

**The New York Times**

By Tad Mcgalliard

March 30, 2018

*Tad McGalliard is the director of research and policy at the International City/County Management Association.*