# Bond Case Briefs

*Municipal Finance Law Since 1971*

---

## How Transparent Should Government Be After a Cyberattack?

**City tech leaders and cybersecurity experts confront the tension between elected officials beholden to the public and IT bosses whose primary concern is limiting the information available to bad actors.**

Atlanta was one of the first major cities hit, waylaid by a costly ransomware attack. As headlines about what happened continued in the months to come, similar incidents besieged other government agencies across the country. There was Baltimore. There was the Colorado Department of Transportation, twice. There were half a dozen small cities in Massachusetts. There was Albany, N.Y.

In the past 18 months or so, cyberattacks on government have accelerated. Experts say this is an evolution wherein bad actors have moved from targeting individuals at random, to going after governments, school districts, companies, and other institutions, which often have more to lose and are thereby more lucrative. Another factor in the recent acceleration is that many of these entities have been traditionally underfunded in the realm of cybersecurity.

As such, public-sector IT leaders have begun to view a successful cyberattack as a matter of when, not if. Essentially, regardless of how well-prepared government is, a breach is still coming, and so a larger onus is now being placed on response, specifically on best practices for the aftermath of a cyberattack. Within this conversation, however, a major point of tension has arisen — transparency.

A question local government leaders must grapple with is this: How transparent should government be after a cyberattack? Should they tell citizens everything, or should they downplay incidents altogether, obscuring details under the assumption that any information on their vulnerabilities can and will be used against them?

It’s a complicated debate, and with this wave of cybercrime showing little sign of slowing, finding answers has become imperative.

Being as transparent as possible with citizens has evolved as of late, fueled by technology that enables easier sharing of data as well as more convenient lines of communication between government and the citizens it serves.

There is, perhaps, a growing expectation that local government should tell residents everything, provided it doesn’t infringe on the privacy of others. But what about emergency situations like cyberattacks?

In March, Albany was hit by a cyberattack on a Saturday. Thanks to an alert about the breach, the city had most major systems up and running again by Monday, except for getting birth, death and marriage certificates. City offices were closed Monday morning, though, as the city worked to ensure a full recovery.

Albany Mayor Kathy Sheehan was open with information throughout, announcing via social media

that an attack had occurred the same day she found out. On Sunday, she again took to social media to let residents know city officials had been working to prevent any interruptions in government service. Then on Monday, the city let residents know when it was open again.

It all seems innocent enough, but at a recent breakfast roundtable discussion about cybersecurity and cities, hosted during the CityLab DC summit, Sheehan said not everyone in City Hall agreed with that open approach.

“Our CIO would have preferred saying nothing at all,” Sheehan told a collection of other elected officials and IT leaders, the majority of whom had similar anecdotes to share.

Other CIOs in attendance agreed with the stance, or at least the desire to be able to maintain silence. But Sheehan felt obligated as an elected official to let the public know all that she could about what was happening. Moreover, she said her CIO and the rest of the IT staff had “done a phenomenal job” and she wanted the public to know that as well.

The reason for advocating silence, however, is in part a concern that a larger cybersecurity target will be put on local governments, and that bad actors will see detailed news of a successful defense as a challenge. Another layer is that releasing detailed information will help bad actors find a new vulnerability to exploit. Cyberattacks are, after all, a crime, and so some of the details will always be sensitive.

Brian Nussbaum, who is a fellow with New America’s Cybersecurity Initiative and an assistant professor of cybersecurity at the University of Albany, said a balance must be struck between giving citizens necessary info and obscuring the scope of defenses and recovery, noting that “it’s possible to describe in general what’s being done without being specific about what’s being done.”

Sometimes, Nussbaum added, public organizations withhold information not in the name of secrecy, but rather because they are still sorting out “second order effects,” which basically means assessing the problem and understanding the damage. For organizations like government or public health systems, which keep private data subject to regulations, this is paramount.

Nussbaum, however, was optimistic that more answers about transparency after a cyberattack will emerge as this particular challenge matures. As cybersecurity defenses, response plans and general knowledge evolves in the public sector, so too will best practices around what information to share with the public.

This is also far from a new tension within government.

“This is not an unusual problem in the abstract,” Nussbaum said. “Elected officials who are accountable to citizens often have impulses to do things that people in the business line don’t have the same incentives to want to do, because they are not directly talking to the citizens in the same way. I don’t think this is a problem that’s unique to local government cybersecurity, but rather a problem for government writ large.”

Gary Brantley, the Atlanta CIO, continues to oversee that city’s cybersecurity in the wake of its recovery. Also in attendance at CityLab DC, Brantley said his goal is always to share as much information as he can without compromising operations or inciting fear. One thing that gets lost, he added, is just how common failed attacks are.

“These attacks are widely unsuccessful,” Brantley said, “and that’s one thing we don’t talk about.”

BY LUCAS ROPEK, GOVERNMENT TECHNOLOGY | NOVEMBER 8, 2019 AT 3:01 AM