LGR

LOCAL GOVERNMENT REVIEW

Putting Research Into Practice

SPECIAL SECTION OF *PM* MAGAZINE,
JULY 2021 — VOLUME 7.0

icma.org

Franchise Agreements Serving as Vehicles for Local Governments to Achieve Clean Energy Goals

New research from the National Renewable Energy Laboratory examines the intricacies of local governments using franchise agreements

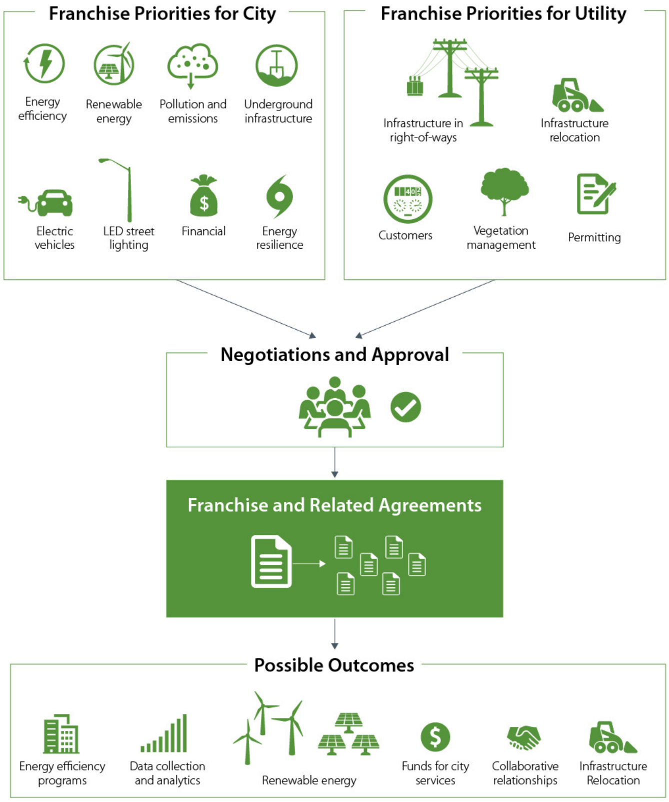
BY JEFFREY J. COOK

Improving sustainability has increasingly become a focus of local governments, with almost 50 percent of respondents in a 2015 ICMA survey identifying environmental protection as a priority in their jurisdiction.[1] New National Renewable Energy Laboratory (NREL) research focuses on one potential pathway for a local government and its electric service provider to partner and achieve joint clean energy goals: franchise agreements.[2,3,4] Franchise agreements are a negotiated contract between an authority having jurisdiction (AHJ) and an electric service provider, granting the utility the right to serve customers in the AHJ. The contract often specifies the period of service and a fee remitted back to the jurisdiction, and commonly includes stipulations regarding a utility's right of way to install and maintain electrical infrastructure.

Franchise agreements are often set for significant periods of time, sometimes upwards of 20 years, offering a rare opportunity for local government leaders to negotiate and create obligations for progress on long-term community sustainability goals.

Some local governments have incorporated other energy objectives into franchise agreements—or have signed agreements in parallel—that commit the AHJ and utility to work together to achieve joint energy goals. When franchise and related agreements are implemented, the local government and utility can deliver a wide variety of outcomes, including additional revenues for municipal services, new renewable energy projects, and more collaborative working relationships between parties (see Figure 1).

Figure 1. **Illustrative Example of a Franchise Agreement Partnership**



Franchise Priorities for City
Energy efficiency
Renewable energy
Pollution and emissions
Underground infrastructure
Electric vehicles
LED street lighting
Financial
Energy resilience
Franchise Priorities for Utility
Infrastructure in right-of-ways
Infrastructure relocation
Customers
Vegetation management
Permitting
Negotiations and Approval
Franchise and Related Agreements
Possible Outcomes
Energy efficiency programs
Data collection and analytics
Renewable energy
Funds for city services
Collaborative relationships
Infrastructure Relocation

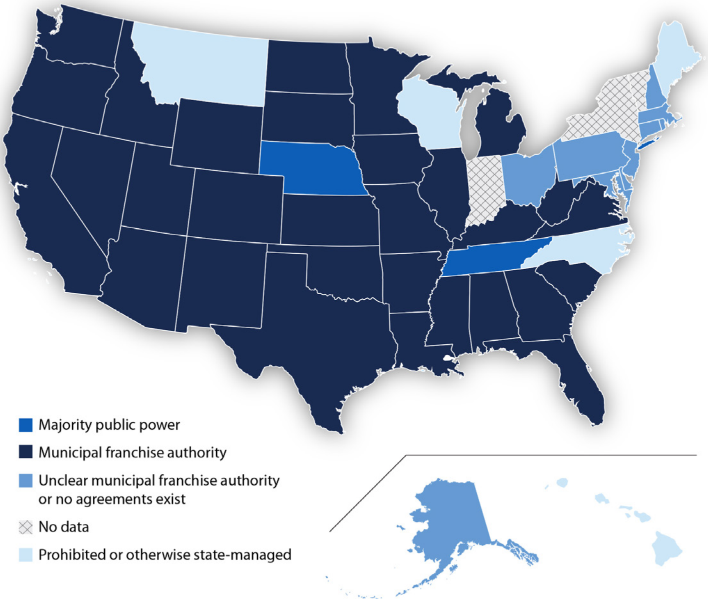
To better understand the potential for franchise agreements to serve as vehicles to achieve clean energy goals, NREL researched the extent to which municipalities have the authority to enter franchise agreements, how many have pursued additional energy objectives in or alongside their agreements, and to what effect these objectives have been pursued.

Franchise Authority and Energy Objectives

NREL used a two-pronged data collection approach to build a franchise agreement dataset that includes 3,538 municipalities. NREL began by searching for franchise agreements via public utility commission docket databases; municipal code databases, such as MuniCode and General Code; and other web-based searches. NREL augmented this secondary data collection with primary interviews with state public utility commissions, state municipal leagues, electric service providers, and municipalities.

From the data set, NREL concludes that municipalities in 30 states can legally pursue franchise agreements with their electric service providers (see Figure 2). Five states are prohibited from negotiating their own agreements (Hawaii, Maine, Montana, North Carolina, and Wisconsin), while two other states are majority public or municipal owned power, where cities may be unlikely to self-impose franchise agreements and related fees (Nebraska and Tennessee). NREL concludes that municipalities in 10 other states, largely in the competitive market eastern states, also do not have access to this opportunity. Finally, NREL had insufficient data to make definitive claims about Indiana, New York, and Vermont.[5]

Figure 2. **States Where Municipalities Can Pursue Franchise Agreements with Electric Service Providers**

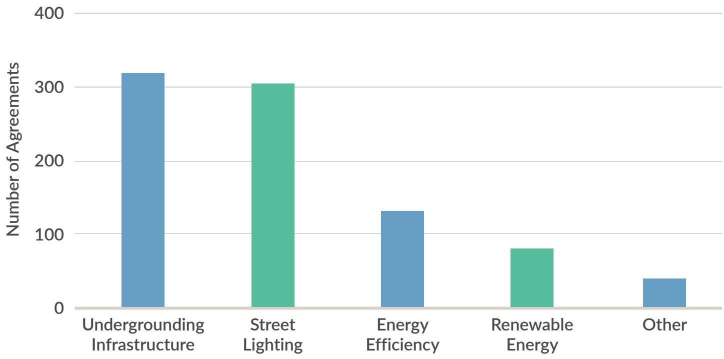


Majority public power
Municipal franchise authority
Unclear municipal franchise authority or no agreements exist
No data
Prohibited or otherwise state-managed

A total of 467 cities (13 percent of cities in the data set) were identified to have either adopted franchise agreements or a franchise-related agreement with one or more energy-related objectives. NREL coded these references into one of five categories: energy efficiency, renewable energy, street lighting, undergrounding infrastructure, and other (i.e., electric vehicles (EVs), service reliability, and infrastructure strengthening).

Two energy objectives—undergrounding infrastructure and street lighting—were the most common objectives referenced in franchise or related agreements, followed by energy efficiency, renewable energy, and other objectives (see Figure 3). Though references to energy efficiency and renewable energy are significantly lower, these have been increasing since 2006. Ultimately, most efficiency or renewable energy references are nonbinding or require electric service providers to inform municipalities of existing or upcoming energy-related programs. Even so, some cities and utilities have agreed to binding commitments, including providing funds to support certain municipal projects or programs.

Figure 3. **Energy Objectives Referenced in Municipal Franchise Agreements**



Over 1,200 cities in the data set have franchise agreements expiring between 2020 and 2040. Most existing franchise agreements have terms exceeding 20 years, so many of these jurisdictions may lack institutional knowledge of these agreements. NREL completed five case studies of cities that have successfully negotiated a franchise agreement that also addressed renewable energy including:

- Chicago, Illinois.
- Denver, Colorado.
- Sarasota, Florida.
- Minneapolis, Minnesota.
- Salt Lake City, Utah.

These five cities were selected for a variety of reasons, including geography, population, and utility variation. All five cities have also adopted unique energy stipulations in their agreements that demonstrate the wide variation across city approaches used. Here, we focus on the results of one case study: Sarasota, Florida, along with the aggregate lessons learned across all the case studies.

Case Study Snapshot: Sarasota, Florida

The city of Sarasota, Florida (population 57,000), is served by Florida Power and Light (FPL), and began discussing renewing its franchise agreement with FPL in 2008. The city had a keen interest in pursuing additional renewable energy generation to offset community load and a shorter franchise term (five years), while FPL was interested in pursuing a longer-term contract (30 years) that provided more investment certainty that excluded other energy objectives.

In 2010, the two entities signed a new 30-year franchise agreement, along with a separate Renewable Energy, Energy Efficiency, and Energy Sustainability Agreement (Renewable Energy Agreement) to codify FPL's clean energy commitments to the city.[6] This parallel agreement included a variety of energy projects addressing energy efficiency, renewable energy, and electric vehicles, among others.

Timeline

Sarasota, Florida Partnership Timeline

2008–2009

- FPL and Sarasota conduct franchise renewal negotiations

2010

- FPL and Sarasota sign 30 year franchise agreement and separate agreement relating to clean energy

2011

- 2 distributed PV projects installed
- 5 EV chargers installed
- Energy audits completed at all city facilities

2012

- LED lighting pilot project completed

2014

- 10 kW PV installed

2017

- 10 EV chargers installed
- 3 nonprofit energy makeovers completed
- Cumulative 456 home energy makeovers completed

2021

- FPL to replace initial 5 EV chargers

2026

- FPL to replace remaining 10 EV chargers

2031

- FPL to replace existing distributed PV systems

2040

- FPL to complete 1500 home energy makeovers
- FPL to complete 15 nonprofit energy makeovers
- Existing franchise agreement with FPL expires

FPL and Sarasota have been implementing these agreements for almost 10 years. Both entities provide biannual updates to the city commission on activities in relation to the Renewable Energy Agreement.

As required by the agreement, FPL has successfully:

- Deployed five EV charging stations in 2011 and added 10 more charging stations in 2017.
- Provided $2,000 for municipal personnel to attend a Leadership in Energy and Environmental Design course in 2011.
- Completed 27 energy education presentations at schools in Sarasota from 2011 to 2017.
- Conducted energy audits at all city facilities.
- Implemented 456 of 1,500 and five of 15 residential and nonprofit energy makeovers, respectively.
- Installed a 5-kW rooftop PV project at BayHaven Elementary in 2011, five pole-mounted solar panels at the city-owned Van Wezel Performance Arts Hall in 2012, and a 10-kW rooftop PV project at a nonprofit conservation education facility, Save Our Seabirds, in 2014.

Local governments can leverage franchise negotiations to help achieve their clean energy goals.

Lessons Learned for Negotiating Energy Objectives into Franchise-Related Agreements

Sarasota and the other four case study cities all had unique lessons learned related to their local context. Even so, NREL identified seven key takeaways transcending the five cases, including:

1. **Mutual understanding of authority and goals helped cities and utilities agree on energy-related terms in four of the five cases.** Excluding Chicago, interviewees from all cases noted the importance of understanding what was possible via a partnership between a city and utility. Emphasis on pilot projects or working together on enabling other higher-impact projects via franchise fee increases or enabling state legislation are all possible outcomes from these partnerships. Understanding opportunities and limitations up front can help cities and utilities successfully negotiate agreements.
2. **Utilities were willing collaborators with municipalities pursuing energy objectives in two of the five cases.** Interviewees in Minneapolis and Salt Lake City noted that city and utility personnel were aware of ongoing and contentious municipalization discussions and were interested in partnering to find common ground to avoid a similar situation. In addition, a growing list of utilities are interested in deploying more renewable energy to meet load, including Xcel Energy, who announced a 100 percent carbon-free energy goal by 2050 in 2018.[7] Other jurisdictions pursuing renewable energy objectives may benefit from partnering with more proactive utilities interested in similar goals.

LGR
LOCAL GOVERNMENT REVIEW
Putting Research Into Practice

JULY 2021 SPECIAL SECTION — VOLUME 7.0

Managing Editor
Cory Fleming
lgrfeedback@icma.org

Guest Editor
Lindsay Jacques

In the tradition of *The Municipal Year Book*, ***LGR: Local Government Review***—a special section of Public Management (*PM*)—presents key research findings and expert insights about local government issues and trends. ***LGR*** is published as new research findings and analyses become available.

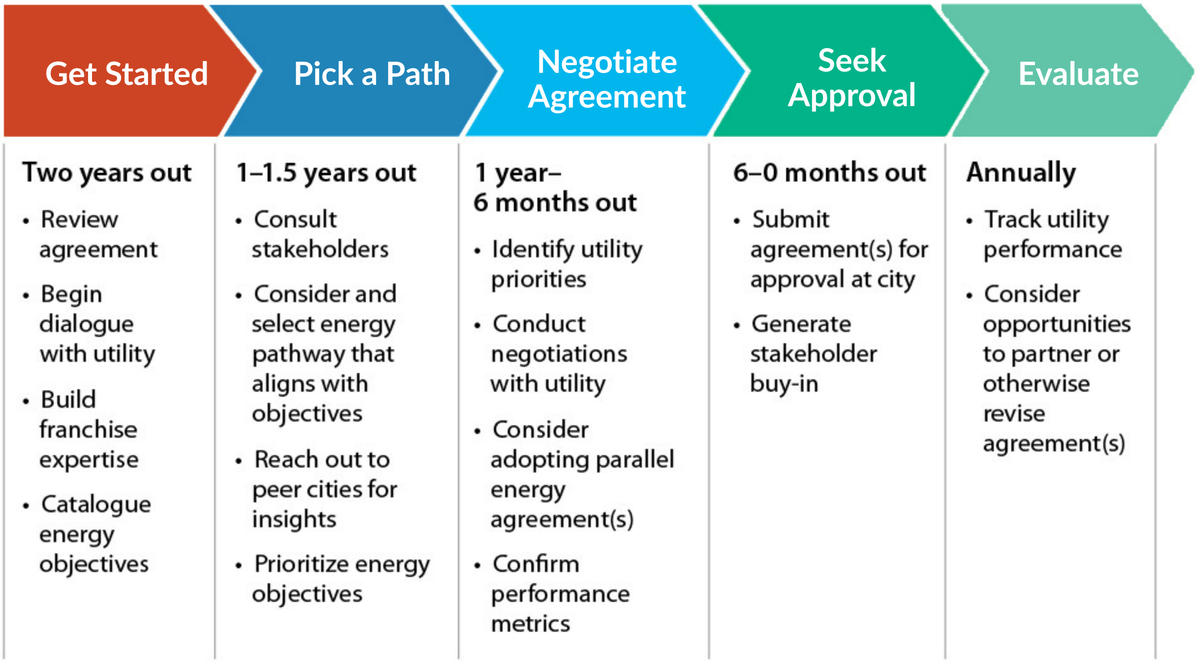
ICMA's intent is to contribute to the profession's collective understanding of practices, policies, and trends that have a significant impact on local governments, now and with an eye toward the future.

LGR: Local Government Review is offered to ICMA members as a benefit of membership. Non-members can purchase digital copies of this special section from ICMA's online bookstore at bookstore.icma.org.

For information about advertising in this special section, contact Kyle Elgin at kyle.elgin@mci-group.com or 410-316-9866.

3. **The negotiation process took about two years to complete on average and unfolded over five stages in all five cases.** Either the city or utility initiated the process and cities began by reviewing their energy objectives and pathways (see Figure 4). Once a pathway is selected and objectives are prioritized, the jurisdiction can begin to negotiate the terms of the franchise and related agreements. In most cases, the AHJ will only need to secure the support of elected officials to approve the franchise agreement, but others may need to seek voter approval, as occurred in Denver. Once implemented, local government and utility personnel may work together to report on performance.
4. **Building internal, or pursuing external, expertise helped city personnel understand negotiation opportunities and limitations in all five cases.** Three of the five cities (excluding Minneapolis and Salt Lake City) sought third-party, often legal, expertise before negotiating their franchise agreements. Given these agreements exceeded 20 years, these cities lacked institutional knowledge of the previous negotiation process. If a jurisdiction cannot secure third-party support, they may still benefit from reaching out to other peers that have recently negotiated agreements, requesting information from municipal leagues to gain perspective on the process, and relying on internal career civil servants that may also have relevant legal and energy-related expertise.
5. **Negotiating franchise agreement length was one of the most contentious elements of the process in four of the five cases.** Two cities (Salt Lake City, Minneapolis) renegotiated franchise agreements with significantly shorter terms (five and 10 years, respectively) than the national average (20 years), while Denver had

Figure 4. Typical Timeline for Franchise Agreement Negotiations and Implementation



Get Started	Pick a Path	Negotiate Agreement	Seek Approval	Evaluate
Two years out	**1–1.5 years out**	**1 year–6 months out**	**6–0 months out**	**Annually**
• Review agreement • Begin dialogue with utility • Build franchise expertise • Catalogue energy objectives	• Consult stakeholders • Consider and select energy pathway that aligns with objectives • Reach out to peer cities for insights • Prioritize energy objectives	• Identify utility priorities • Conduct negotiations with utility • Consider adopting parallel energy agreement(s) • Confirm performance metrics	• Submit agreement(s) for approval at city • Generate stakeholder buy-in	• Track utility performance • Consider opportunities to partner or otherwise revise agreement(s)

the opportunity to exit their franchise agreement at 10 years. Shortening franchise agreements is one avenue to strengthen utility accountability to clean energy goals and provide flexibility given a rapidly changing power sector. However, these goals may conflict with the interest of the utility to secure long-term contracts that provide investment certainty. Several cities compromised on this issue by negotiating energy objectives into or alongside franchise agreements.

6. **Four of the five cities adopted separate franchise and clean energy agreements, as opposed to integrating energy objectives into the franchise itself.** Excluding Chicago, each city adopted a separate energy-related agreement that outlines the goals and partnership between the city and the utility. These agreements outline energy objectives, principles, and plans for implementation that often call on parties to commit staff, develop work plans, and complete regular (annual, biannual) progress reports. Utilities favor this approach because they view franchise agreements as purely related to access to the public right-of-way. Thus, local governments might consider using their franchise agreement negotiation as a starting point to develop a parallel agreement addressing renewable or other energy objectives.
7. **Collecting data and tracking agreement implementation performance is an essential, though ongoing, challenge in all five cases.** Four of the five cities (excluding Salt Lake City) have five or more years of implementation experience. Interviewees noted that at the outset of implementing a franchise or related agreement it may be unclear what data the utility and city should be collecting. This can make it challenging to design the monitoring and evaluation aspects of a franchise agreement that are essential to gauge impact. Establishing a clear but flexible data collection, management, and review process in or alongside the franchise agreement may help mitigate this issue and provide an avenue for more accurately tracking performance throughout the agreement life cycle.

Conclusion

In summary, local governments can leverage franchise negotiations to help achieve their clean energy goals. Whether individual cities pursue a similar approach to those outlined in the case studies will depend on their own internal decision-making processes, as well as their existing relationships and negotiations with their electric service providers. NREL's research provides guidance on how some local governments have approached these discussions, serving as a foundation for others to make more informed decisions.

Local governments interested in learning more about this opportunity should visit NREL's website and related franchise agreement data, which can be found here: https://www.nrel.gov/solar/municipal-franchise-agreements.html. PM

Endnotes

[1] International City/County Management Association. *2015 Local Government Sustainability Practices*, *2015 Summary Report*. Washington, DC: ICMA, 2016. https://icma.org/documents/icma-survey-research-2015-local-government-sustainability-practices-survey-report.

[2] https://www.sciencedirect.com/science/article/pii/S0038092X2031183X

[3] Cook, Jeffrey; Grunwald, Ursula; Alison Holm, and Alexandra Aznar. 2020. Wait, cities can do what? Achieving city energy goals through franchise agreements. *Energy Policy* 44: https://doi.org/10.1016/j.enpol.2020.111619.

[4] Jeffrey J. Cook, Alexandra Aznar, Bryn Grunwald, Alison Holm, Hand me the franchise agreement: municipalities add another policy tool to their clean energy toolbox, *Solar Energy*, Volume 214, 2021, Pages 62-71, ISSN 0038-092X, https://doi.org/10.1016/j.solener.2020.10.091. (https://www.sciencedirect.com/science/article/pii/S0038092X2031183X)

[5] The limited data collected from municipalities in these states suggest municipalities do not have this authority either.

[6] *Renewable Energy, Energy Efficiency and Energy Sustainability Agreement. 2010. Renewable Energy, Energy Efficiency and Energy Sustainability Agreement Between the City of Sarasota, Florida and Florida Power and Light Company.* https://www.sarasotafl.gov/home/showdocument?id=1008.

[7] Xcel Energy. 2018. "Xcel Energy aims for zero-carbon electricity by 2050." https://www.xcelenergy.com/company/media_room/news_releases/xcel_energy_aims_for_zero-carbon_electricity_by_2050.

JEFFREY J. COOK is a renewable energy market and policy analyst at the National Renewable Energy Laboratory. He has been on staff at NREL since 2014, and focuses on state and local policy, resilience, technology cost reduction, and distributed energy resource aggregation.

A New Tool to Advance Equity: Artists in Residence in Government

Inviting artists into government creates opportunities for new ways of approaching public service and engaging with the community

BY MALLORY RUKHSANA NEZAM AND JOHANNA K. TAYLOR

The events of 2020 increased our awareness of public health disinvestment and systemic inequity. Marginalized groups experienced more illness, received less medical assistance, and ultimately had less access to a vaccine. It is clear that we must build stronger and more collective government systems to prepare us for the future and protect our most valuable populations. What does this future look like? What must we change to get there? Across the country, communities are embedding artists into government to help tackle these questions, and to find creative ways to prepare for a future that is responsive to critical issues. These artists in residence in government programs (AIRG) are helping agencies spur innovative advancements to internal operations and are working incrementally to advance ways of equitably engaging with and serving constituents.

Through our research investigating AIRG programs operating across the United States in 2020, we have developed a set of typologies that detail how these programs are structured and how they operate within government contexts. Our research findings highlight the potential for internal systems change, specifically demonstrating incremental shifts towards equity and inclusion around both internal operations and dissemination of services. Each program is unique and responds to the distinct contexts of place, community, and government challenges and opportunities. This article draws out strategies and lessons for local governments interested in developing

Convened by Boston Artist in Residence Karen Young, Older and Bolder connects Age-Friendly Boston with the Department of Transportation to elevate the voices of elders of color. Photo courtesy of City of Boston, 2018.

AIRG programs within their own communities designed to respond to their unique contexts.

In this article we use examples of AIRG programs in Boston, Massachusetts, and Granite Falls, Minnesota, to present two cases of this work. Each AIRG program is organized around different, context-specific structures to meet similar goals of creating more just places and governments.

Artists bring others into the creative process, establishing safe spaces for government staff to take risks to cocreate new structures of operating internally, new methods of collaboration across departments, or new ways of engaging constituents.

Research Methodology

In 2020 and 2021, we interviewed (face-to-face and online) and surveyed 40 artists, government officials, nonprofit staff, and others connected to programs that embedded artists in government in 2020. We also reviewed relevant literature, including project documentation, final reports, and department evaluations. Three municipalities will be releasing evaluations of their AIRG programs in 2021: Boston,[1] Minneapolis,[2] and Los Angeles County.[3] Out of this research we produced a typology that provides an overall, broad view of how artists are embedded in government and a more detailed typology of the structures of AIR programs hosted by government agencies that incorporates nuances such as the preconditions for their development, program design considerations, implementation partner relationships, and program sustainability. The full typology is available in academic publications, and further work is forthcoming on our website.[4]

Granite Falls, Minnesota: Artist in Residence in a Small Town

In the town of Granite Falls in western Minnesota (population 2,260), a collaboration between artists and city officials gave rise to the first rural AIRG.[5] Beginning in 2017, Ashley Hanson, an artist and executive director of the Department of Public Transformation (DPoT), approached city staff, including the mayor, city manager and financial director with a proposal to bring an artist into city hall. Previously, Hanson herself had served as an artist in residence with a planning department, and then as a program manager for a city artist residency in St. Paul, Minnesota. She brought these direct experiences as a manager and artist in developing this new residency program.

Designed with a local cross-sector advisory group, the proposal for The Granite Falls City Artist-in-Residence program received unanimous approval from the city council.[6] The residency is managed through a joint effort between the arts nonprofit, DPoT, and the city of Granite Falls. Beginning in October 2020, in the midst of the Coronavirus pandemic, Dani Prados became the city's first artist in residence. The artist's role is to "design and implement arts and cultural strategies that increase civic participation and community engagement in city policy-making, planning, and public processes." Prados has both an office space at city hall and studio and living space provided by the DPoT. As this residency has only recently launched, we provide an introduction, but their website and communications will continue to provide information as the program evolves (publictransformation.org/cair).

Boston, Massachusetts: Cohort of Artists Working in Multiple City Departments

Boston Artists-in-Residence (AIR) was developed with the support of a grant from ArtPlace America as a strategic program implementing Boston Creates, the city's 10-year cultural plan launched in 2015.

Organized by the mayor's office of arts and culture, Boston AIR invites a cohort of artists for a one-year period to partner with departments across the city. The program has evolved with each iteration to learn from previous cohorts and respond to current city needs in order to strengthen the impact of the artists, government collaborators, and Boston residents. The third cohort was focused on racial equity and resilience through the work of seven artists who were collaborating with schools and city departments such as the library, planning, women's advancement, and new urban mechanics. The cohort met monthly to discuss challenges

An artist's methods welcome experimentation and iteration, an important perspective to bring inside of government, and a way to engage in new ideas.

and successes, collectively strategizing how to advance their individual work and respond to the underlying goals of resilience and racial equity.

The artists collaborated with government partners, and this collaboration and process of creation was the artwork just as much as any final event or product. Their work took many forms. For example, Nakia Hill worked with the mayor's office of women's advancement to elevate the voices of women of color in Boston through storytelling workshops about resilience, published writing by young girls, and conducted a survey about workplace experiences to explore racial bias and close the gap between government programs and women of color. One city partner commented that the work "opens the conversation about racial equity" and "sparks collective action in community members."[7]

Contextualizing Artists in Residence in Government

AIRG programs are increasingly common across the country and use many names including: Creative CityMaking,[8] Minneapolis; Public Artists in Residence,[9] New York City; Creative Strategist-Artist in Residence,[10] Los Angeles County; and Artists in Residence, Washington State Department of Transportation.[11] These programs are often part time and temporary, placing artists in government settings for a set period of time to address particular goals and often have the structural support of a municipal art department or partnering nonprofit. AIRG artists can work broadly across the city as a whole (as is the case with the Granite Falls program) or are embedded within one specific department, such as public health, planning, transportation, or sustainability (as was the case with Boston's program).

These programs have significant effects on enlivening agency culture, staff creativity, and community engagement approaches, which can all ultimately lead to more equitable government systems and processes. The artistic approach often attracts a wider or different range of individuals than the "usual suspects" and brings them into the creative process, establishing safe spaces for government staff to take risks to cocreate new structures of operating internally, new methods of collaboration across departments, or new ways of engaging constituents. An artist's methods welcome experimentation and iteration, an important perspective to bring inside of government, and a way to engage in new ideas. A theatre artist can use storytelling with residents of a particular neighborhood to elevate stories of the meaning of place that support planners in redesigning local infrastructure to meet community needs. A designer can engage spatial analysis to reimagine office spaces with government staff to increase aesthetic appeal and facilitate collaboration. AIRs can also focus on policy-specific outcomes, tying creative processes to policy agendas and strategic plans across departments. In this way, AIRG programs are mutually beneficial for both artists and government staff dedicated to the social good.

Preconditions that Lead to Success

Each AIRG program is unique and responds to regional contexts. Understanding the contextual preconditions of a specific place can pave the way for more successful and sustainable AIRG programs.

Political Will

In the case of the Boston Artist-in-Residence program, receiving high-level leadership support from the mayor's office paves a path forward for sustainability of resources, will, and program integrity. In the smaller local government context of Granite Falls, DoPT did a significant amount of work before the program started, meeting with individuals and building relationships within the local government that led to the unanimous approval of the city council. When actually developing the structure of their program, they engaged different community stakeholders through the advisory council—composed of a diverse representation of the population, from the city manager to indigenous tribe representatives to individuals from the local arts council—with ensured wide support from many sectors of the community. Receiving support from decision makers and those with political power, as well as community representation and approval throughout the process, has proven effective for both of these programs.

Designing for Local Needs

Our research indicates that designing AIRG programs specific to the structural and cultural assets, opportunities, complexities, and challenges of a respective place will lead to more transformative impacts. There is no standard AIRG program model that will effectively work in every place. As Karin Goodfellow, director of public art for the city of Boston, explains, "I think we're finding it's also particular to where you are. What is your community? What's the structure of your government? Are you a county? Are you a city? It's all so different and unique and we have just had to adapt based on what's happening that year." In addition to using lessons from existing AIRG programs, Granite Falls conducted a community survey that helped inform the structure and focus of their program to address their unique needs.

Institutional Value of Equity

Because of the profound power of these residencies to abet cultural progress and inform the creation of more just systems, an institution's commitment to equity strengthens these programs. For example, the Creative Strategies Initiative in Seattle is built from a partnership between the Seattle Office of Arts and Culture and the Seattle Office for Civil Rights.[12] Built into the city's racial justice work, it is formally a "culture shift strategy."[13] Teams narrowly interested in founding an artist-in-residence program for aesthetic output will miss out on the creative problem-solving impacts of this work and artists' ability to nurture a culture shift.

Leveraging a Policy Window

Opportunities like a new cultural plan or a pro-arts elected official are frequently the occasions through which AIRG programs have been established. Boston AIR is not the only program established in conjunction with a new cultural plan. In Oakland, California, Cultural Affairs Manager Roberto Bedoya, housed in the economic and workforce development department, worked on a cultural plan[14] that paved the way for the funding and support for Cultural Strategists in Government,[15] which placed seven artists into five city departments for one year focused on civic belonging and well-being. In other cases, connecting AIRG work to goals in a city-wide strategic plan provides an opportunity to establish an AIRG program.

Takeaways for Local Government: Program Structures

A primary challenge for government staff is determining how to structure AIRG programs that will work best for their needs. As mentioned previously, rather than importing a program structure, successful programs build a structure based on local context. Some of the models below overlap in practice, but we have pulled out the most prevalent patterns from our research.

Cohort Models Produce Strong Results

Cohorts of artists completing AIRG programs simultaneously create a community of practice for artists embedded in government, which provides professional support and strengthens their work. Without the cohort support, a novel undertaking like this can lead the artist to feeling isolated in unfamiliar territory within a government setting. If the goal is an exchange of ideas and methods, structures that foster collaboration and support are important. These cohort structures range from inter-departmental—as in the case of Oakland,[16] Minneapolis, St. Paul, Boston, and Los Angeles County—to interagency and across state lines, as seen within two residency programs created by Transportation for America through Washington State Department of Transportation[17] and Minnesota Department of Transportation.[18]

Two-party Partnerships (Government Department + Arts Organization) Are Accessible

This is the most common structure used in establishing AIRG programs. These two-partner structures are accessible to most governments that can identify an arts organization that can serve as a partner. The city of Granite Falls partnered with the arts nonprofit, the Department of Transformation. DPoT manages the "human resources" components of the residency, offering its expertise in managing artists, producing artworks, and crafting a welcoming environment. The arts organization also serves as a liaison, able to translate between the artist and the department to ensure that collaborators understand one another and can connect productively.

Takeaways for Local Government: Strategies

Arising from the research, these strategies are for municipalities and agency partners to consider as they revise existing AIR programs or as they design and implement one for the first time.

Valuing Process Over Product

Typically, artists begin residencies with an onboarding period to help learn systems and create relationships with staff. This process of listening, learning, and relationship building takes concerted effort and time, yet it is essential for building awareness about the internal challenges and opportunities to pursue. The artist can then build on this initial dialogue through collaboration with staff across agencies and constituent communities. This process is the core of AIRG work. Perhaps a final product, such as a report or book or festival occurs as well, and is a celebrated output of the residency, but the process of creation is both an incremental opportunity for systems change and a part of the artwork. Within art fields, this collaborative and dialogue-driven artwork is known as socially engaged art or social practice.

In Boston, Victor Yang worked with Boston Public Health Commission staff and Youth Organizing Institute members to advance work around racial justice, finding pathways to elevate youth voices and build connections across generational divides and power hierarchies. This dialogic process aims to both heal and work for social change by suggesting more inclusive ways to connect government staff and youth of color.

Embrace Flexibility

AIRG programs embed art practices into traditional government work, which creates new opportunities of working together. This process of readjustment is vital in creating insightful projects, but it requires a willingness to pivot and adapt as things evolve. While pre-planning the program structure is beneficial for creating a solid foundation, a flexibility to adjust to unexpected factors supersedes that to deepen impact.

The Boston team recognizes that program flexibility and ongoing reflection is important, and took time to assess after each AIRG cohort to revise the program structure to better support artists and city staff, as well as to respond to Boston communities. In the first year, they partnered with Massachusetts College of Art and Design, which provided insight on how to set expectations and develop curriculum to use in establishing relationships between artists and city staff. From the lessons learned in the first cohort they pivoted to a thematic approach with the second round and connected AIRs with community centers. In the third cohort they found that they needed more clarity around the roles of each participant to create a stronger structure, supporting the underlying intrinsic goals of racial equity.

Each year they add more clarity around the roles of each participant, which in turn increases their shared abilities to be flexible and pivot the work as needed to create a stronger process. As Boston Program Manager Sharon Amuguni reflected in an interview, “I think it was great that we had the sense of structure and the sense of direction starting off, so we could then be flexible within.” Similarly, in Granite Falls, the new residency is set up without a specific project or role for the artist to fill. Instead, “her role will be to design and implement arts and cultural strategies that increase civic participation and community engagement in City policy-making, planning and public processes.”[19]

Pursue Equity-focused Work

The artists selected for these programs are typically skilled at community engagement work and are often BIPOC individuals. The Granite Falls City Artist-in-Residence program specifically lists the following in its selection criteria: “experience as a practicing artist, with a focus on community engagement; interest in, connections to, and / or experience working in and with community members from a diverse range of social, cultural, economic, and political backgrounds.”[20] It is also common that the artists in these roles possess deep connections to and trust within the communities the government serves. The possibilities for how artists can use their creative, social, and aesthetic practices to courageously engage community members, especially people of marginalized backgrounds, to craft new ways for the government to address harm and/or center their needs are incredibly powerful. This activity is different from many traditional community engagement practices in that they are uniquely designed for and are responsive to community needs, are often interactive, engage people in deep storytelling, and create opportunities to celebrate culture.

AIRG programs are mutually beneficial for both artists and government staff dedicated to the social good.

While government staff increasingly recognize that their work should be more equitable, they do not necessarily know how to approach this. Inviting artists into government creates opportunities for government staff to take risks and explore new ways of working. For many local governments, tackling issues of inequity is new and requires diving into unknown territory. The experimental and curious methodology of artists embedded into this system begets a courage to engage in the unknown. For Boston artist Victor Yang, change happens in intimate settings, on an interpersonal level. This human exchange may lead to future policy, or it could influence how staff think about their future work—change on both scales is important in evolving government systems on incremental levels.

Boston reorganized their AIR program with racial equity and resilience as an organizing principle, seeing it as more than a temporary theme but as how all work was grounded. In this way, it became a model for how all city operations can be organized to promote equity and address systemic inequity. Government staff recognized this goal. One participant reflected that working with an AIR project "deepened my sense for how richly diverse the Boston community is and how we need more ways to bring these stories to light. With regards to racial equity, an important thing that came up is heightened conversation about these issues, and that is the first step."[21] This was reinforced in the 2021 program evaluation, which found that the work increased the dialogue about implicit bias and race within the government.

Promote Cross-sector Collaboration for Maximum Impact

Embedding artists in government systems connects art and design across sectors to leverage creative methods for innovative ideas. One example: participants engage in dance movements to advance community participation in transportation planning. In Boston, many departments across the city have participated in the AIR program as Director of Public Art Karin Goodfellow reflected in a research interview:

> Part of this work is realizing that having that creative thinking, and having the practice of an artist, benefits all of our departments. I think one of the things I've seen that's helpful is that there's so much space for more collaboration and connection across departments. The partnership is great for people to come together and to do this work; to have an opportunity to talk to other colleagues that we'd potentially not interact with day to day.

Boston now invites government agencies to apply to host an AIR, demonstrating their interest and dedication to collaboration. Through this initial foundation, artist Erin Genia worked with the office of emergency management to develop cultural organizing strategies to sustain long-term health and safety beyond discrete moments of crisis. This work involved collaborating with indigenous leaders and cultural heritage bearers to confront colonial narratives as an ongoing cultural crisis that still impacts communities in Boston today. The work expanded the conception of emergency management beyond a blizzard or other immediate crisis to underlying emergencies of inequity that challenge residents, suggesting an expansion of the office's role in promoting equity in the city.

Building Equitable Futures

As we collectively build our post-pandemic futures, local government leaders can play a significant role in strengthening civic infrastructure and programs to make them more equitable and inclusive through innovative collaborations such as AIRG programs. These programs can make the work of extending civic capacity to experiment with innovative models more accessible. A Boston city staff member reflected that their AIRG experience expanded their connections to community partners while also supporting work to "revaluate how we think and who we engage in our advocacy efforts," which served to "inform our future work."[22] It is an opportunity for experimentation that can lead to lasting change.

Drawing on our interviews with artists and government staff across the country, we have identified the three most likely ways in which AIRG programs can support governments in advancing equity in our future post-pandemic society.

1. **Promoting Equity by Strengthening Community Engagement.** Embedding artists within civic systems creates local community engagement opportunities that are more creative, culturally responsive and heartfelt, building a solid foundation for future collaboration with constituencies.

2. **Experimentation for Innovation and Systems Change.** Inviting experimentation into a local government agency through intentional collaboration with an artist. Creative methods, such as storytelling or visual analysis

or movement, can break through processes that are no longer serving government needs to discover innovative new ways of working.

3. **Shepherding in the Culture Shift Required for Institutional Equity Work.** Changing behaviors and mindsets are important foundations to more equitable practices. Through their intentional process of getting to know staff and community members, listening, and staying curious, AIRG programs can set in motion a more deeply attuned way of working, which can give government a stronger foundation for the ultimate mission of its work in service of the community. Minnesota Department of Transportation Community Vitality Fellow Marcus Young models a relationship and trust-centered process of working in government, as he reflected in a research interview: “You have to build the relationship and trust…you must consider how to be a good guest…and you must start asking really good questions.”

Further research on AIRG programs and opportunities for engagement are forthcoming. Sign up for our newsletter or contact us to collaborate at www.cairlab.net.

Endnotes and Resources

[1] https://www.boston.gov/departments/arts-and-culture/boston-artists-residence-air

[2] https://www.minneapoliscreates.org/programs-overview#creativecitymaking

[3] https://www.lacountyarts.org/CreativeStrategist

[4] www.cairlab.net

[5] https://data.census.gov/cedsci/table?q=granite%20falls,%20mn&tid=ACSDP5Y2019.DP05

[6] https://www.publictransformation.org/cair

[7] https://www.boston.gov/departments/arts-and-culture/boston-artists-residence-air

[8] https://www.minneapoliscreates.org/programs-overview#creativecitymaking

[9] https://www1.nyc.gov/site/dcla/publicart/pair.page

[10] https://www.lacountyarts.org/CreativeStrategist

[11] https://wsdot.wa.gov/news/2019/03/22/washington-state-department-transportation-announces-selection-two-artists-serve

[12] https://www.seattle.gov/arts/programs/racial-equity/creative-strategies-initiative#:~:text=The%20Creative%20Strategies%20Initiative%20(CSI,interconnection%20of%20all%20living%20systems.

[13] http://www.seattle.gov/Documents/Departments/RSJI/18-21_RSJI_Strategic_Plan_4.6.19_FINAL.pdf

[14] https://cao-94612.s3.amazonaws.com/documents/oak070756.pdf

[15] https://www.oaklandca.gov/news/2019/citys-cultural-strategists-pilot-program-seeks-to-advance-equity-transform-government

[16] https://www.oaklandca.gov/news/2019/citys-cultural-strategists-pilot-program-seeks-to-advance-equity-transform-government

[17] https://wsdot.wa.gov/news/2019/03/22/washington-state-department-transportation-announces-selection-two-artists-serve#:~:text=With%20today's%20announcement%20that%20Kelly,artist%20in%20a%20statewide%20agency.

[18] http://www.dot.state.mn.us/fellowship/

[19] https://www.publictransformation.org/cair

[20] https://static1.squarespace.com/static/5cc1d1f0809d8e15634f1ebf/t/5e6420ba48344f67f7ab554f/1583620311031/CAIR_RFP_Final.pdf

[21] https://www.boston.gov/departments/arts-and-culture/boston-artists-residence-air

[22] https://www.boston.gov/departments/arts-and-culture/boston-artists-residence-air

Josh Nezam

MALLORY RUKHSANA NEZAM loves cities and believes we have the tools to make them more just and joyful. She is an independent consultant (Justice +Joy), scholar, and artist who specializes in creative placemaking/keeping/knowing. Nezam holds a master’s degree in design from Harvard University. She seeks to be in every room she’s not supposed to be in.

JOHANNA K. TAYLOR is an assistant professor at the Herberger Institute for Design and the Arts at Arizona State University. Her research explores questions of cultural equity through the intersection of art, community, policy, and place—including in her recent book, *The Art Museum Redefined: Power, Opportunity, and Community Engagement*. Before turning to academia, she spent over a decade working as an arts administrator.

To learn more from ICMA about partnering with artists, visit the ICMA resource, *Problem Solving Through Arts and Cultural Strategies: A Creative Placemaking Wayfinding Guide for Local Government Managers*.

https://icma.org/problem-solving-through-arts-and-cultural-strategies-creative-placemaking-guidance-local

A New Look at Local Government Cybersecurity in 2020

Recommendations for staying vigilant against persistent cyber threats

BY DONALD F. NORRIS

Introduction

Greenville, North Carolina; Torrance, California; New Orleans, Louisiana; and 22 cities in Texas were among hundreds of local government organizations that reported cyberattacks in just 2019 and 2020. Over the past decade, American local governments have increasingly become targets of cybercriminals and victims of ransomware attacks. Cybersecurity has become synonymous with disaster resilience, and local government managers must place an emphasis on preparing for cyberattacks against their organizations. This report analyzes the current landscape of cybersecurity in local government and is based on an extensive review of the literature since 2000; data from previously conducted surveys (2016, 2018, and 2020); and conversations with chief information security officers (CISOs) and other information technology (IT) officials from local governments in the United States.

According to the cybersecurity firm Emsisoft, in 2019, the United States experienced "...an unprecedented and unrelenting barrage of ransomware attacks that impacted at least 966 government agencies, educational establishments, and healthcare providers at a potential cost in excess of $7.5 billion."[1] Prominently included among organizations hit by ransomware attacks were 113 local and state governments and agencies. During the first two quarters of 2020, another 60 federal, state, and local governments and agencies were hit by ransomware attacks.[2]

These statistics include only ransomware attacks, but we know from prior research that local governments are under constant or nearly constant cyberattack from many directions.[3] Attacks include such vectors as email, phishing, spear phishing, brute force, zero day and denial, and distributed denial of service. See Table 1 for brief descriptions of these types of attacks and Appendix 2 for more information.

Table 1: Key Cyberattack Definitions

Malware: Malicious software installed that can encrypt data and files, block user access, exfiltrate data and files, etc.

Ransomware: Type of malware that encrypts sensitive data and files to then demand a ransom to unlock the encrypted information.

Phishing: A form of social engineering in which cybercriminals "go fishing" for victims by sending emails, seemingly from trusted parties, with promises, opportunities, or threats to deceive victims.

Spear phishing: Spear phishing is a more sophisticated form of phishing in which the cybercriminal uses just enough information to make the victim believe the email came from someone known to the victim or another trusted source.

Brute force: An attack method where an attacker uses a tool such as software to continuously "bang away" to gain access to a victim's computer, network, or IT system.

Zero-day: An attacker's identification of a weakness in a network or IT system, such as utilizing defects in outdated software versions.

Denial of Service (DoS): An attack that sends massive volumes of traffic to overwhelm an organization's website or server.

Distributed Denial of Service (DDoS): A type of DoS attack that uses multiple computers simultaneously to shut down a website or server to all users.

See Appendix 2 for expanded descriptions.

Cybercriminals can and do use all of these vectors to attack local government IT systems, hold them for ransom, exfiltrate data, and otherwise do damage.

The cost of cyberattacks is enormous, and it increases every year. A 2016 report estimated that cybercrime would have a worldwide annual cost of $6 trillion by 2021, a significant increase over the $3 trillion in 2015. "This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined."[4] Another source estimates that by 2025, cybercrime will cost the world economy $10.5 trillion and be equivalent to the third largest economy in the world after the United States and China. In the United States, two well-publicized cases of local government breaches—Atlanta, Georgia, in 2018, and Baltimore, Maryland, in 2019—cost those cities $15 million and $18 million, respectively. For more information, see the case studies of these attacks later in this report.

Why Are Local Governments Targeted?

The first factor is the sheer number of American local governments—90,075 units, of which 38,779 are general purpose governments, including 3,031 county governments, 19,475 municipal governments, and 16,253 town or township governments.[5] Except for the smallest of them, these governments have critical IT systems and cumulatively spend billions of dollars each year to support them. In 2019, *Government Technology* magazine estimated state and local government spending on IT for that calendar year at $107.6 billion.[6]

Second, America's local governments store considerable amounts of sensitive information, especially personally identifiable information (PII) such as names, addresses, driver's license numbers, credit card numbers, social security numbers, and medical information. In addition, they have contractual, billing, and financial information of the governments themselves. This information is valuable to cybercriminals because they can sell the data or hold it for ransom, and obtaining it is often the purpose of cyberattacks. Over the past few years, numerous local governments have reported the loss of PII and other sensitive data through data breaches and information exfiltration. As local governments move into the world of smart cyber physical systems in such domains as traffic, wastewater, electricity, etc., they place those and related systems at greater risk of physical harm and damage resulting from breaches, to say nothing of the impact on public trust.

Third, cybercriminals are very good at what they do. In recent years, the availability of low cost but effective hacking tools that require little technical knowledge has made it is relatively easy to get into the business of cybercrime, thus increasing the number and types of cybercriminals. This means that even inexperienced hackers can break into well-defended IT systems.[7] Poorly defended systems (research that colleagues and I conducted has shown that local governments systems, on average, are not well defended) are even easier to breach.[8] Cyberattacks are deployed by a variety of actors, including external actors (both individuals and organizations), malicious insiders, nation states, hacktivists, and terrorists. Perhaps the clearest contemporary example of this is the well-documented ongoing Russian government interference in U.S. elections.

Fourth, local governments operate under financial constraints, sometimes severe ones, that limit their ability to acquire and implement state of the practice cybersecurity technology, policies, and practices. Financial limitations also mean that most, if not all, local governments cannot compete with the private sector in hiring and retaining qualified cybersecurity staff. The top three barriers to effective cybersecurity reported in a 2016 nationwide survey were inability to pay competitive salaries to cybersecurity employees (58.6%); insufficient number of cybersecurity staff (53.1%); and lack of funds (52.8%). All three involved funding or lack thereof.[9]

Last, the Internet of Things (IoT), a global phenomenon that permits electronic devices of various kinds to connect to the internet for various purposes, has introduced new vulnerabilities and risks for local governments. This is especially true of local governments endeavoring to create “smart cities” by deploying internet-connected devices to provide, monitor, or manage such services as public transit, solid waste collection, traffic lights, traffic congestion management, water meter reading, potable water provision, security cameras, and many more. By one estimate, in 2018, there were seven billion IoT devices worldwide, 26.7 billion in 2019, 31 billion in 2020, and a projected 75 billion by 2025.[10]

For local governments, the spread of IoT devices greatly increases the “attack surface” that makes them vulnerable to cyberattacks. Moreover, the devices may be numerous and heterogeneous, with different manufacturers, capabilities, and interfaces. The result is a system that is inherently difficult to monitor and update as new security vulnerabilities are discovered. Other risks are that the devices can be disabled, have their sensor data stolen or modified, or have their activator functions used inappropriately to cause damage.

For these and perhaps other reasons, it is critical that local governments, especially their top elected and appointed officials, understand:

- The cyberthreats that their governments face.
- The actions they should take to protect their information assets from attack and to mitigate the damage after successful attacks.
- The gaps between the actual cybersecurity practices of local governments and the cybersecurity threats that they face.
- The barriers that their governments encounter when deploying cybersecurity.

Local officials must also provide their support for their cybersecurity technology, practices, policies, and staff needed to ensure that the highest levels of cybersecurity are maintained throughout their organizations.

Findings

This section presents findings from a survey conducted in 2020 among a cohort of CISOs in 14 mainly larger U.S. local governments with a population range of 220,000 to 3,979,576: Boston, Massachusetts; Chicago, Illinois; Dallas, Texas; Detroit, Michigan; Fairfax County, Virginia; Los Angeles, California; Memphis, Tennessee; Nashville, Tennessee; San Francisco, California; and Seattle, Washington.

The survey asked a series of questions on the structure of cybersecurity operations, types of attacks and attackers, cybersecurity policies, barriers to trainings, awareness, and support within local governments. (See Appendix 1 for the full list of questions.)

This author expressly thanks the members of the recently formed Coalition of City CISOs (https://cityciso.org/) for their support of and participation in this survey.[11] A *CISO* is defined here as the main employee responsible for the organization’s cybersecurity practices and policies. Depending on the size of the local government, this can be in a position entirely dedicated to cybersecurity or could be an IT or other staff member with cybersecurity as only one of their duties.

This section also compares findings from the 2020 survey with the results of two nationwide local government cybersecurity surveys (conducted in 2016 and 2018). The section unfolds as follows: First, it presents basic information about the responding governments’ cybersecurity operations. Second, it discusses cybersecurity attacks and attackers. Third, it addresses cybersecurity policies, barriers to cybersecurity, cybersecurity training, and awareness of and support for cybersecurity among various parties in these governments.

The Structure of Cybersecurity Operations

Organization

The great majority of local governments in the 2020 survey (71.4%) responded that their CISO or other officials responsible for cybersecurity reported to the chief information officer (CIO), while 14.3% reported to the chief technology officer (CTO) or the city or county manager, respectively. This is not surprising since CISOs are often viewed as subordinate to top IT officials, such as CIOs and information technology directors (ITDs). There is an emerging trend, mainly within the corporate world, for CISOs to be elevated to positions equivalent to CIOs and to report directly to the CEO. According to a 2018 survey conducted by PWC, 40% of firms worldwide said that their CISOs reported directly to the CEO.[12]

While this trend has yet to make much headway among local governments, there are good arguments for having the CISO report directly to the top elected and/or appointed official. This would elevate the importance of cybersecurity throughout the organization and improve the CISO's ability to communicate directly with the top officials in the local government.

The survey also asked if the CISOs had total control over their local governments' cybersecurity. Nearly two-thirds (64.3%) said they had total responsibility while just over one-third (35.7%) said it was divided. It then asked, if responsibility is divided, among what offices (see Table 2). The division of cybersecurity responsibility was somewhat different among these local governments. In 7.1%, each department had a cybersecurity official who "matrixes" to the CISO. In 21.4%, certain agencies or departments are responsible for their own cybersecurity. And in 7.1%, IT is divided into two groups, and the leaders of each report to the CIO. One government's CISO had responsibility for cybersecurity but reported that "...my counterpart is able to appeal my recommendations."

Organizations, including local governments, generally structure their cybersecurity in one of three ways: centralized, decentralized, and federated. In a centralized system, there is a single office or department for cybersecurity for the entire organization. In a decentralized system, each department is responsible for its own cybersecurity. In a federated model, there is a mix in which the CISO is responsible for some elements of cybersecurity and individual departments are responsible for others.[13]

Dividing cybersecurity responsibility is generally considered a poor practice because it means that the CISO is not totally in charge of this function, and therefore cannot set the rules for all units and end users, and is not able to hold all units and end users accountable for their cyber behavior. One of the CISOs in the survey indicated that he had to work with over 50 units in his local government that had individual cybersecurity authority. If one unit does not properly set cybersecurity policy and practice, the whole organization can be at risk. Such a structure makes it unnecessarily difficult to manage cybersecurity.

Staffing

Cybersecurity in local governments involves, among other things, managing in-house staff, cybersecurity contractors, and end users. The numbers of in-house staff reported from the 2020 survey varied considerably with 7.1% reporting no cybersecurity staff and 7.1% with 24 in-house staff. The number of cybersecurity staff was not proportional to local government population, although larger governments tended to have more cybersecurity staff. Among the jurisdictions in the sample with populations from 220,000 to just under 700,000, the number of in-house cybersecurity staff ranged from zero to 12. Among the group with populations between 700,000 and less than one million, their range was similar from 0 to 14. Among the jurisdictions greater than one million, one had seven, one had nine, one had 12, and one had 24.

The situation with cybersecurity contractors was rather different from that of in-house staff, with half of the governments reporting that they had no contractors. Among the jurisdictions with populations between 220,000 and 700,000, two had zero cybersecurity contractors, two had one, one had two and one had six. Three jurisdictions between 700,000 and a million had zero contractors, and one had four. Among those with populations greater than one million, two had zero, one had four and one had eight. Overall, the data suggest that, with one or two exceptions, these local governments do not have sufficient cybersecurity personnel to properly maintain high levels of cybersecurity.

Table 2. Responses to the Question, "If responsibility is divided, among what offices?"

- My team is the only cybersecurity team within [my city]. However, we have a decentralized IT organization and I do not have cybersecurity authority over other technology groups (i.e., [names units over which CISO has no control]).
- Sister agencies are independent. [Provides short list of them.]
- IT is split into two groups. While I have all of Cyber, both groups report to the CIO. Therefore, my counterpart is able to appeal my recommendations.
- There are some operational components to cybersecurity [names a couple] that are held by certain departments [names three].
- Each department has a department information security officer who matrixes to the city CISO.

Next, the survey inquired about the number of end users in these governments. The range of was from 2,200 to 45,000. As might be expected, these numbers generally corresponded to the size of the local government, with larger governments having more and smaller ones having fewer end users, although there is not a precise match.

For current purposes, what is perhaps most important is not the number of end users but the percent of end users that fall under the CISO's responsibility. In all but 21.4% of local governments, 100% of end users fell under the responsibility of the CISO. A total of 7.1% reported 25%, 7.1% responded 60% and 75%, while 7.1% did not report.

The fact that all end users do not fall under the responsibility of the CISO means that these cities' cybersecurity is more at risk than it should be. This is because end users of a government's IT system who are not under the CISO's responsibility do not have to follow the same rules as those under such responsibility (indeed, they may operate under different rules altogether); they are not required to take the same training; and they cannot be held accountable for their cybersecurity actions as can end users under the CISO's responsibility.

Funding

As previous studies have shown, lack of adequate funding is a major barrier to achieving high levels of cybersecurity.[14] The 2020 Deloitte-NASCIO Cybersecurity Study (based on a survey of state CISOs) found the same among state governments. Three of the top five barriers involved funding: lack of funding, lack of cybersecurity staff and lack of dedicated budget.[15] Consequently, the survey asked about the level of cybersecurity spending. According to the same report, most states spend under 3% of their IT budgets on cybersecurity, which is far less than financial institutions and federal agencies. By contrast, according to Gartner, average spending by U.S. businesses on cybersecurity is between 5% and 8% of companies' IT budgets.[16] Moreover, only about one-third of states have formally established cybersecurity budgets.

Among the local governments in the 2020 survey, the average spending was 4.09% of the IT budget, and the range was between zero and 10.0%. A total of 57.1% of these governments spent less on cybersecurity (as a percent of their IT budgets) than Gartner found among U.S. businesses, while 35.7% were within or greater than Gartner's estimate. A total of 42.9% spent less than NASCIO found among state governments while 57.1% spent more. These responses tend to confirm that funding for cybersecurity is inadequate or not on par for at least some of these local governments. This is not surprising because studies of IT and government, e-government and cybersecurity among local governments have consistently produced similar results. As local governments across the nation have learned the hard way, inadequate spending on cybersecurity often results in the predictable—breaches and the high cost associated with them.

Outsourcing

Last, the survey inquired about whether and to what extent local governments outsourced cybersecurity. Half of the respondents said that their governments outsourced cybersecurity partially, and half said they did not outsource at all. None outsourced cybersecurity completely. The functions that were partially outsourced are found in Table 3. These findings are somewhat consistent with findings from the 2016 survey where 60.5% did not outsource, 31.3% outsourced partially, and 8.2% outsourced totally. In their 2018 survey, Hatcher, et al., found that 50.9% outsourced at least some of their cybersecurity functions, while 38.8% did not and 10.3% did not know.[17] Of those that outsourced, 35.7% outsourced all cybersecurity.

Given the passage of time since those surveys, one might have expected greater adoption of outsourcing in the 2020 survey, especially among a sample of local governments that consists mostly of large to among the largest U.S. local governments, where presumably the need for cybersecurity is greater and budgetary resources are also greater. One might also have expected that larger jurisdictions that devote relatively small numbers of in-house staff to cybersecurity would have taken greater advantage of outsourcing. Neither of these results were evident from the survey.

Table 3. Responses to the Question, "If you outsource cybersecurity, what principal functions are outsourced?"

- PCI scanning and penetration testing.
- We use contractors and a number of vendor tools to monitor the network.
- 24/7 monitoring of cyber threats.
- 24/7 monitoring of our IPS.
- IT operation; SOC (security operation center).
- Some is outsourced [no list provided].
- Some monitoring and vulnerability scanning.

Outsourcing is seen by many observers as an important way to improve cybersecurity in organizations, especially in smaller ones with limited cybersecurity staffing and funding capabilities. A total of 85% of participants in a recent Deloitte survey said that they had "…some level of reliance on vendors and managed service providers to provide cybersecurity operations, with 66% of those outsourcing between 21% and 66% of cybersecurity operations.[18]

Local governments can contract with cybersecurity vendors for some or all of their cybersecurity needs and, in doing so, have access to the skills, expertise, and experience of literally hundreds of cybersecurity professionals or more. As the chief security officer in a Maryland county noted: "Google has 2,000 security engineers…I've got four."[19] Outsourcing also transfers some or much of the responsibility for securing critical data and information from the local government to the vendor. However, one source notes that many CISOs are "uncomfortable" having their data handled by anyone or organization outside of their organization, and therefore, this may account for the rather slow adoption of outsourcing.[20]

Attacks and Attackers

Cyberattacks

This section discusses attacks and attackers against U.S. local governments. The first question concerned the frequency of cyberattacks. Both the 2016 survey and earlier research found that local governments are under constant or nearly constant attack.[21] Those findings are largely confirmed in this survey. Just over half of respondents said constantly, more than a quarter said hourly, and 14.3% said daily. Unlike the 2016 survey, none of the governments in the 2020 survey said that they did not know how frequently they were under cyberattack. This finding represents a welcome improvement, although may be attributed to the small sample size. If local governments (or any organizations, for that matter) do not know whether they are under cyberattack, they have opened the door to cyberattacks. All local governments must implement technologies and policies, such as those outlined later under the "cybersecurity policies" section, that allows them to be continually aware of their cyber environment and the risks they face.

The survey then asked whether these governments had experienced "incidents" or "breaches" during the previous year, using Verizon's definition of those terms.[22] An *incident* is "an event that compromises the confidentiality, integrity or availability of an information asset." A breach is "an incident that resulted in confirmed disclosure (not just exposure) to an unauthorized party." Only 7.1% of the governments reported no incidents in the past year and 7.1% did not know; 21.4% of governments responded they had one incident; 14.3% said two incidents; 28.6% said three incidents; and 21.4% said more than five incidents. These responses confirm that the bad guys not only attack often, but that they also get through local governments' defenses, and confirm that local governments need sufficient resources to better protect their information assets.

Half of the local governments in the 2020 survey had not experienced breaches in the past year. However, the remainder had experienced between one and more than three breaches. Once again there is confirmation that the bad guys are really good at what they do and that local governments need to improve their ability to protect their information assets. The number of governments (21.4%) that experienced multiple breaches is troubling, especially among a set of governments with mostly large populations and more resources opportunities to protect their information assets.

Local governments are not only under constant or nearly constant attack, but the frequency of attacks is increasing. The 2016 survey found that about one third of local governments (32.5%) experienced the same number of attacks in the past year, compared to slightly over one-third (34.4%) that experienced about the same number. Nearly all governments responding to this survey (13 or 92.9%) said attacks had become more frequent over the past year, and only 7.1% said that they had remained about the same. This suggests, at least for this subset of local governments, a significant increase in the number of attacks, which is consistent with reporting across all or nearly all sectors of the economy. Cyberattacks are steadily increasing.

Cybercriminals

A question in the 2020 survey asked whether local governments could determine the types of attackers they were facing. The 2016 survey asked a similar question and found that 41.6% of governments could determine their attackers and 58.4% could not. Information from the 2020 survey shows a substantial increase in those that can determine their attackers' identities. Two-thirds could determine their attackers' identities, while 28.6% could not and one was unsure. Separately, one responding CISO said: "Attribution is not a critical factor to us. In most cases, we can take educated guesses, but we do not dedicate cycles to attribution." The increase in the fraction of governments that are able to identify attackers noted in this survey could be the result of this particular sample of local governments, and therefore, may not be representative of the broader population of local governments, especially smaller ones.

The local governments in the 2020 survey said that they were most often attacked by external actors-organizations (35.7%), followed by hacktivists/spammers (21.4%), nation states (14.3%), 7.1% external actors/individuals, and 14.3% did not provide answers. This is somewhat similar to findings from the 2016 survey in which 71.0% said external actors/organizations, 60.7% external actors/individuals, and 29.0% nation states. It also tracks well with other sources regarding types of attackers over time.

The survey next asked if the pattern of attacks had changed over the past year. A total of 71.4% respondents said it had remained the same, while 28.6% said it had changed. The changes observed by the latter were increased sophistication of spear and whale phishing, increased phishing, a focus on ransomware and breach of vendors, and use of commodity malware and attacks tied to the social justice movement (see Table 4). That so many local governments in the 2020 survey responded "remained the same" is somewhat surprising given the dramatic increase in ransomware attacks recently, as well as an increasing emphasis that attackers have placed on breaching third parties in order to get to their ultimate attack destinations.

Table 4. Responses to the Question, "If the pattern has changed, please describe the changes."

- Phishing emails are the biggest threat, and the biggest change is more targeted and sophisticated spear phishing and whale phishing.
- Focus on ransomware and breach of vendors.
- More sophisticated use of commodity malware. Increase in attacks tied to social justice movement.
- Broader attempt at phishing has occurred.

The local governments in the 2020 survey experienced phishing and spear phishing the most among all attack vectors in the past year. This was followed by zero-day brute force and other (35.7% each), Distributed Denial of Service or DDoS (21.4%), and Denial of Service or DOS (7.1%).

The most frequent cyberattack purposes that these governments identified were: (1) ransom, (2) theft of money, (3) theft of PII; (4) theft of confidential records, and (5) hacktivism. A total of 21.4% of governments did not know (which is somewhat surprising and not fully consistent with what one might expect from a sample of mainly large governments). The increase in ransomware attacks is consistent with national data as noted earlier. Four of the top five attack purposes identified by the 2016 survey were somewhat similar to the information gained from the 2020 survey, although not in the same order: (1) ransom—59.4%, (2) mischief—37.6% (in last place in 2020), (3) PII—27.7%, (4) hacktivism—27.7%, and (5) theft of money—20.8% (much more prominent in 2020).

When asked if the attack purposes had changed during the previous year, 78.6% of respondents said no, 7.1% said yes, and 14.3% did not know. One respondent who said yes added that the change was a "rise in attacks recently tied to the social justice movement."

Case Studies

Now we examine two examples of cities that experienced breaches to their IT systems and faced ransomware demands: Atlanta, Georgia; and Baltimore, Maryland. Their experiences are typical of what can happen to local governments of every type and size that do not place a high priority on cybersecurity and follow through with adequate funding and staffing.

Atlanta, Georgia

Population: 506, 811
Area: 133 sq. miles
Median Family Income: $59,948
Poverty Rate: 20.8%
City Budget: $661.4 million

Atlanta saw its computer system taken over by a ransomware attack that was discovered on March 22, 2018, but potentially had been going on longer. Atlanta's attackers, whom the U.S. Justice Department said were two Iranians, used ransomware known as SamSam in a "brute force" attack against the city's IT system.[23] In such an attack, the hacker repeatedly runs passwords against elements of an IT system until it finds a match and, finding one, inserts the malware into the system. Such attacks can occur over weeks or even months. Whatever method is employed, hackers often succeed, get into a target's system, remain there until caught, and do their damage.

The city initially reported that the attack had taken down the municipal court system, the city's email, water and traffic ticket payment systems, and wi-fi at Hartsfield-Jackson International Airport.[24] Dashboard camera videos from police cars were destroyed.[25] Later, officials discovered that financial, customer relationship management, and service desk systems had been affected along with the data associated with them, and several years' worth of officials' and employees' correspondence had been lost.[26] The hackers demanded a ransom in Bitcoin equal to about $51,000, but the city chose not to pay and instead began to remove the virus and get the system back up and running. No small task, it turned out.

In April, the city shelled out $2.7 million for contracts with cybersecurity and communications firms to assist in the recovery effort.[27] Later, the city estimated recovery costs at $9.5 million, and later still, the full cost of the recovery, not including lost city productivity, was estimated to be $17 million.[28,29] By June 2018, about one-third of software programs the city relied on were partly or completely unusable. And, as much as a year later, work was still ongoing to fully restore the city's systems and data and also to establish a solid cybersecurity program.[30]

What went so wrong in Atlanta? The answer appears to be at once simple and complex. The simple answer is found in three reports on the city IT system from the city auditor. These reports—dated 2010, 2014, and January 2018—found numerous weaknesses and vulnerabilities in the system, including up to 2,000 "severe vulnerabilities" found by monthly vulnerability scans. Many of the vulnerabilities were over a year old and the report found "no evidence of mitigation of the underlying issues."[31] The January report also found evidence of "ad hoc and undocumented [security] processes," and almost 100 servers using a version of Windows that Microsoft no longer supported.[32] These findings strongly suggest that Atlanta's IT department was guilty of cybersecurity malpractice. Indeed, one cybersecurity expert suggested as much by saying that negligence was likely involved.[33]

The complex part, which partially excuses the IT department, is found in the then-new mayor's acknowledgement that cybersecurity had not been a city priority. The auditor's reports had not gained traction with city elected officials or top management or their findings would have resulted in efforts to fix the broken system. Doing this, however, is not simple, especially in local governments. Cybersecurity is expensive and competes with many other needs, both real and perceived. To complicate matters, local governments never have enough money to meet all needs and must prioritize, especially in times of severe recession (such as the Great Recession that began in December 2007). This is where politics (or making choices in order to govern) gets into the game. And politicians almost always favor funding of "visible" programs like education and public safety over "invisible" things like cybersecurity—until there is a breach with its corresponding cost and chaos.

Lessons Learned

The city of Atlanta had done a respectable job analyzing their IT systems for vulnerabilities through periodic audits that generated reports detailing how and where to strengthen their systems. However, these reports were left largely on the shelf, without enough action taken to close identified gaps in their cybersecurity. Without taking advantage of this knowledge and taking steps to address their IT cybersecurity issues, they left themselves and their community at risk and ultimately paid the price. Some steps a local government can take to elevate the cybersecurity issues in their community may include:

- After conducting an audit, create an action plan in response to an audit's findings, including prioritized short- and long-term goals on how to address known vulnerabilities.
- Assign staff time to each goal and create progress reports to distribute to top staff and elected officials.
- Update and appeal to top management and elected officials through presentations detailing priority goals, resources needed, and examples of the consequences of inaction from comparable organizations that had been subject to cyberattacks.

Baltimore, Maryland

Population: 593,490
Area: 80.94 sq. miles
Median Family Income: $50,379
Poverty Rate: 21.2%
City Budget: $3.5 billion

Baltimore has the distinctly undesirable reputation of having been successfully hacked twice in as many years—2018 and 2019. The first hack occurred on March 25, 2018, and involved a ransomware attack on and takedown of the city's computer assisted dispatch (CAD) system that supports Baltimore's 911 emergency dispatch and 311 non-emergency phone systems. Fortunately for Baltimore, city IT and cybersecurity staff were able to identify the problem quickly, and according to the city's CIO, Frank Johnson, "isolate and take offline the affected server, thus mitigating the threat."[34] The system was restored in less than 24 hours. The city later revealed that the hack occurred because staff were working on part of the IT system and had disabled a firewall accidentally and exposed a port (opening to the internet) for 24 hours. The hackers found the opening they needed quickly.[35]

Baltimore struggled to learn from this experience. On May 7, 2019, the city discovered that it had been hacked again, and this attack was of far greater consequence and cost. Baltimore's IT system was infected through a phishing attack by yet-unknown cybercriminals using the Robbinhood ransomware, which had successfully penetrated the city of Greenville, North Carolina, a month earlier.[36]

The hacker(s) took over nearly all of Baltimore's IT infrastructure and demanded a ransom of 13 bitcoin (around $76,000) to release the city's systems and data. The city refused to negotiate, and it took months before the system was fully up and running. During that period, several services were either fully or partially disabled, including water billing (which was not fully functional for several months), property taxes, parking tickets, email, and voicemail. Real property sales were interrupted for several weeks because the city's system that handles property transfers was offline.[37,38] Then, of course, there is the embarrassment factor.

In retrospect, few if any lessons had been learned from the 2018 attack. What is worse is that the immediate cause of the 2019 breach could have been easily fixed. According to cybersecurity expert Herb Lin of Stanford University, if Baltimore had installed a patch that Microsoft made available in 2017, the entire episode could have prevented.[39]

Additionally, after the 2018 breach, Baltimore had an opportunity to buy cybersecurity insurance in the aftermath of the 911 hack, which it decided against. This is unfortunate for at least two reasons. First, in the process of purchasing the insurance, the city almost certainly would have had to conduct a vulnerability analysis to qualify for the insurance. Such an analysis might have found the weakness that permitted the attack to succeed. Second, the cybersecurity insurance would likely have covered at least some of the estimated $18 million that the attack has cost the city.

What allowed this hack to occur? First, for years the city had underinvested in cybersecurity. The CIO had warned city officials months earlier to purchase cybersecurity insurance and that their IT system was essentially a disaster waiting to happen, as it was underfunded and employees lacked adequate cybersecurity training.[40,41] The CIO was fired, some think as a scapegoat, over this incident.

Next, Baltimore's IT system consisted largely of old technology, improperly managed and underfunded. According to local technology writer Sean Gallagher, Baltimore's IT system consisted of "a dangerously ill-prepared, kludged together municipal IT system" with a "chaotic jumble of operating systems," whose IT staff were "overworked, underpaid, and dramatically underfunded." Gallagher also noted that the "city does not have a full handle on its vulnerability management or patch management or keeping up to date with things."[42] If these observations are true, then it was only a matter of time before a serious breach occurred.

Lessons Learned

Baltimore, among many local governments, let their cybersecurity practices lag behind as their IT systems grew. Failing to learn from their mistakes, they had to bolster their cybersecurity practices after it was too late—and much more expensive. To avoid the pitfall Baltimore found itself in, local governments can consider:

- Reaching out to local governments in their state that have suffered from a cybersecurity attack and discuss what steps they have taken to learn from and better prepare themselves in the future.
- Investigating cybersecurity insurance that fits organizational needs before a breach occurs, coupled with an analysis of IT systems and their current vulnerabilities. Organizations such as the Cybersecurity and Infrastructure Security Agency and the Center for Internet Security are good places to start to learn more about insurance options for local governments.
- Creating a schedule for updating IT systems, with reminders for staff and individual users responsible for installation.
- Staying aware of the cyberthreats impacting other organizations and looking for ways to actively protect your organization from similar threats.

Case Study Conclusion

What conclusions can be drawn from the from Atlanta and Baltimore experiences? In retrospect, these successful cyberattacks are not terribly surprising. This is, in part, because many local government officials, if not most, do not fully understand the need for cybersecurity, and therefore do not provide adequate funding for cybersecurity.[43] This seems to have been abundantly true in Atlanta and Baltimore.

Both cities experienced ransomware attacks, both attacks took down important city services, both were costly in terms of recovery, both cities had a history of under-investing in already vulnerable IT systems, and both attacks brought considerable municipal embarrassment. The primary lessons that should be drawn here are that local government officials must fully understand the need for and provide adequate direction and funding for high levels of cybersecurity. Failure to do so will result in predictably similar and detrimental outcomes.

Along with the reasons discussed earlier, the Atlanta and Baltimore examples should demonstrate clearly why it is crucial that local governments and the officials leading them understand the many cybersecurity threats they face. Failure to do so places their communities at increased risk of experiencing otherwise preventable cybersecurity problems. This understanding should, at a minimum, encompass the following:

- The cyberthreats that these governments face.
- The actions they should take to protect their information assets from attack and to mitigate the damage after successful attacks.
- The gap between those actions and the need for high levels of cybersecurity at the grassroots.
- The barriers that these governments encounter when deploying cybersecurity.

Understanding these issues will enable local officials not only to see why cybersecurity is crucial to their government's digital well-being, but will help ensure that cybersecurity has their full support and is adequately funded and properly managed.

Cybersecurity Policies, Barriers to Cyber Training, Awareness, and Support

This section addresses a variety of topics including cybersecurity policies, barriers to cybersecurity, training, and awareness and support, all of which are important to local governments being able to maintain high levels of cybersecurity.

Cybersecurity Policies

Cybersecurity consultants and the professional literature strongly recommend that organizations equip themselves with and carefully implement a number of cybersecurity policies in order to provide high levels of cybersecurity. Perhaps the best guide to what a good cybersecurity policy should look like is the 2018 National Institute of Standards and Technology (NIST) Cybersecurity Framework. This document describes the principal elements of a cybersecurity policy that, if adopted, will enable organizations, including local governments, to develop and implement cybersecurity policies that work for them and meet their specific needs. It is built around five core functions: identify, protect, detect, respond, and recover, as briefly described by NIST on the right.

The document is a rather brief, non-technical starting point to begin building your local government's cybersecurity practices. It should be read by all top officials in local governments and followed by their technology staff in developing the local government's cybersecurity policies. After each policy is developed, it should be carefully reviewed by top elected and appointed officials and then formally adopted. Policies should be reviewed and updated periodically to adapt to the ever-changing cybersecurity environment. And they should be scrupulously implemented, and all parties in the local government should be held accountable for their cyber behavior accordingly.

Local governments may wonder where to find example cybersecurity policies that they can use to craft their own. Perhaps the best starting point would be other local governments, especially larger governments that are more likely to have adopted policies. This is perhaps the easiest way to begin, and resources like ICMA Connect (icma.connectedcommunity.org) provide a platform to ask for and share examples from other local government organizations. Second, there are consulting and security firms that may share templates and can be hired to help local governments develop such policies. Third, there are online templates that may be of use. Last, some membership organizations may have guidance on how to create cybersecurity policies and cyber staff who might be able to provide advice like state municipal leagues, county associations, and township organizations.

According to a report from the security firm McAfee, *Grand Theft Data*, "...people inside organizations caused 43% of data loss, one-half of which was accidental. Improved cybersecurity policies can help employees... better understand how to maintain the security of data and applications."[45] Cybersecurity policies are important, among other things, because they:

NIST Cybersecurity Framework Core Functions

Identify: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify function are foundational for effective use of the framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome categories within this function include asset management, business environment, governance, risk assessment, and risk management strategy.

Protect: Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome categories within this function include identity management and access control, awareness and training, data security, information protection processes and procedures, maintenance, and protective technology.

Detect: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect function enables timely discovery of cybersecurity events. Examples of outcome categories within this function include anomalies and events, security continuous monitoring, and detection processes.[44]

Respond: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome categories within this function include response planning, communications, analysis, mitigation, and improvements.

Recover: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome categories within this function include recovery planning, improvements, and communications.

National Institute of Standards and Technology. April 16, 2018. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Pages 14–15. Verbatim.

- Establish cyber roles and responsibilities for all parties in an organization.
- Describe proper and responsible cybersecurity practice and list actions that are neither proper nor responsible.
- Set the rules of behavior around several consequential cybersecurity matters, including but not limited to password management, software patching, cyber risk management, incident response planning, use of external (including personal) devices on an organization's IT system, and policies for vendor and contractor use of an organization's IT system.

The following section examines whether local governments in the 2020 survey had adopted seven important cybersecurity policies (Table 5) and respondents' perceptions of the effectiveness of those policies. It also compares adoption rates and perceptions of effectiveness with those reported in the 2016 survey.w

Table 5. Seven Important Cybersecurity Policies for Local Governments

- Formal cybersecurity policy.
- Password management policy.
- Policy regarding applying software patches.
- Cyber risk management plan.
- Incident response/disaster recovery/business continuity plan.
- Policy on use of external devices (e.g., cell phones/flash drives).
- Policy for vendors, contractors, cloud services.

Policy Adoption

Of the local governments surveyed, 78.6% had fully adopted formal cybersecurity policies, which is considerably higher than the 2016 survey, and 21.4% had partially adopted. Similarly, 78.6% of governments had also fully adopted password management policies, slightly higher than those recorded in 2016; 21.4% had partially adopted, and 21.4% had not adopted. A total of 71.4% had fully adopted policies regarding software patches, while 21.4% had partially adopted and 7.1% had not adopted this policy.

Overall, 57.1% of governments had fully adopted cyber risk management plans, while 21.4% had partially adopted them, and 21.4% had not adopted them. Similarly, 57.1% of governments fully adopted incident response plans/

disaster recovery/business continuity plans, while 35.7% had partially adopted them, and 7.1% had not adopted. Almost half (42.9%) had adopted policies on the use of external devices (54.2% in the 2016 survey), while 28.6% had partially adopted them, and 28.6% had not adopted them. Last, 42.9% of governments had adopted policies for vendors and cloud contractors (this figure was 27.6% in 2016), 42.9% had partially adopted, 7.1% had not adopted, and 7.1% did not know.

Overall, these data show that larger percentages of the governments in the 2020 survey had adopted cybersecurity policies than in the 2016 survey, although this is likely attributed to the small number and relatively large population of the sample size in the 2020 survey. This said, too many had adopted too few policies or had adopted them only partially. The latter is not terribly surprising since only 44% of firms worldwide had adopted cybersecurity policies.[46]

Aside from the full adoption of two important policies, these responses reveal a surprising lack of full policy adoption among the responding governments, especially since these governments are, for the most part, large in size with potentially adequate budgetary resources that follow population size, and trained professionals managing their cybersecurity.

The lack of full adoption, in turn, likely means that these governments are not able to derive the full benefits of these policies, their implementation, or enforcement. These responses do not enable us to know how much "partial" adoption meant to the respondents, and this could be important in understanding the policies perceived effectiveness.

Policy Effectiveness

Next, the survey asked about the perceived effectiveness of the policies. Almost half (42.9% of respondents said that their password management policies were highly effective (compared to 56.3% in 2016), 21.4% said somewhat, and 7.1% said not very. Overall, 28.6% said their formal cybersecurity policies were highly effective (versus 19.2% in 2016), and 7.1% said not very. Another 28.6% said that their software patching policies were highly effective, 57.1% said somewhat, and 7.1% each said not very and not at all.

A total of 21.4% respondents said that their incident response plans were highly effective (compared to 21.1% in 2016), 64.3% said somewhat, and 7.1% each said not very and not at all. When asked about the effectiveness of their cyber risk management plans, 14.3% said highly effective (versus 19.2% in 2016), 42.9% said somewhat, 28.6% said somewhat, and 14.2% said not at all. A total of 14.3% said their policies on the use of external devices was highly effective (compared to 42.1% in 2016), 57.1% said somewhat, 7.1% said not very, 14.3% said not at all, and 7.1% did not know. Finally, 14.3% said their policies for vendors, etc., were highly effective (versus 36.5% in 2016), half said somewhat, 14.3% said not very, 7.1% said not at all, and 14.3% did not know.

For the most part, responses to the questions of policy effectiveness in both the 2016 survey and 2020 survey do not inspire confidence that the policies are working as needed to achieve their objectives. "Somewhat effective" and "not very effective" responses suggest that the policies (and/or their enforcement) contain gaps that are likely to allow problems of cybersecurity practice and management to occur, potentially serious problems. Consider, for example, the policy on applying software patches where only 28% of respondents said that this policy was highly effective. That suggests that too often software patches are not applied in a timely manner, if at all. The literature tells us that failure to apply software patches as soon as possible after they are released by vendors is a major reason that cybercriminals are able to breach local government IT systems, as illustrated in the Baltimore case study. What these data cannot reveal, however, is why the respondents rated the effectiveness of these policies so low, and further research will be needed to find answers to these questions.

Barriers to Cybersecurity

Previous research has uncovered a number of barriers to local government achievement of high levels of cybersecurity. For example, the 2016 survey found that the top four barriers were inability to pay competitive salaries (58.6%), insufficient number of staff (53.1%), lack of funds (52.8%), and lack of adequately trained staff (46.0%). Notably, all of these barriers are somewhat or totally related to funding. The results of the current survey are reasonably consistent with those of the 2016 survey in that the two top barriers were lack of funds (78.6%) and lack of adequate/adequately trained staff (71.4%). All other listed barriers received 21.4% or fewer responses.

The 2020 survey also asked what three things local governments needed to do or possess to be able to achieve the highest levels of cybersecurity. The top three from the 2016 survey were greater funding (54.7%), better cybersecurity policies (38.3%), and greater cybersecurity awareness among local government employees (35.3%). From the current survey, 57.1% of respondents identified funding and half identified staffing as the top two needs, which are consistent with the top two barriers previously identified. The third need was leadership buy-in, the lack of which is a common complaint among cybersecurity officials. Until local governments affirmatively address these and perhaps other barriers—especially funding, staffing, awareness, and support—they cannot expect to improve their cybersecurity outcomes or more effectively protect their information assets.

Cybersecurity Training

The survey also inquired about what types and frequency of training the governments provided to various officials and staff. The literature tells us that training is essential to achieve an understanding of and support for the need for cybersecurity and also to ensure effective end user cyber hygiene within organizations. Therefore, the survey asked if the governments provided mandatory cybersecurity training (and how frequently) to the mayor/elected county executive, city/county councilmembers, city/county manager/ administrators, department heads, and average end users.

A little over three-fourths (78.6%) responded that their governments provided mandatory cybersecurity training annually to the mayor/elected county executive, city/county councilmembers, department heads, and average end users. Fewer (71.4%) said that they provided annual cybersecurity training to the city/county manager/ administrator. Additionally, 7.1% said training is conducted at some other period of time for all of those parties, and 7.1% did not know. Finally, 14.3% of these governments did not provide training to any of these end users.

These findings may indicate a substantial improvement over the 2016 survey where 20–50% did not provide training at all and another 8–14% did not know if training was provided. They are heartening because other research shows that a considerably lower proportion of organizations provide any training at all. For example, in its 2018 survey, PWC found that 48% of corporations worldwide provided cybersecurity training to its employees.[47]

Kudos to the local governments that provided annual mandatory training, as they are more likely to see improved cyber outcomes. Those that did not provide such training at all or provided it in a time frame greater than at least every three years, are almost guaranteeing that their cyber outcomes will be more difficult and should consider instituting mandatory cybersecurity training or increasing its frequency.

Awareness of and Support for Cybersecurity

The literature also tells us that in order to maintain high levels of cybersecurity, organizations need to ensure that all parties within them are aware of the need for cybersecurity and support it. The 2016 survey found that 61.7% of top managers were moderately/exceptionally aware of the need for cybersecurity; among department managers, 42.3% were moderately/exceptionally aware; and 32.0% of elected executives were moderately/ exceptionally aware.

The 2020 survey also asked about the awareness of and support for cybersecurity among these local governments' mayor/elected county executive, city/ county councilmembers, city/county manager/ administrator, department heads, and average end users. Respondents did not believe that the officials and staff in their governments were highly aware of the need for cybersecurity. In only one case (mayor/elected county executive) did a majority of respondents (57.1%) believe that incumbents in this office were highly or mostly aware of the need for cybersecurity. And 35.7% of respondents said these office holders were only somewhat/a little aware, and 7.1% said not at all aware.

Perceptions of cybersecurity awareness of the remaining officials and staff were bleak. Half of respondents each said that their city/county manager/ administrator was highly/mostly aware, 28.6% said somewhat/a little, 7.1% said not at all, and 14.3% didn't know. Half responded that department heads were highly/ mostly aware, while 42.9% said somewhat/a little and one said not at all. Additionally, 42.9% said that city/county councilmembers were highly/mostly aware; 50% said somewhat/a little and one said not at all. Finally, 42.9% responded that end users were highly/mostly aware, half said somewhat/a little, and 7.1% said not at all.

In theory, awareness of the need for cybersecurity among local government officials and staff should lead them to provide support for it. In the 2016 survey, respondents said that 54.0% of top managers provided strong/full support for cybersecurity. This was followed by 35.0% of elected executives and 33.0% of department managers. The results from 2016 suggest otherwise—that awareness does not necessarily lead to support because in each case respondents said that the amount of support provided by various officials and staff was lower than their degree of awareness.

The 2020 survey paints a different picture than the 2016 findings. Perhaps due to increasing cyberattacks on local governments and heightened awareness due to high profile attacks, such as those seen in Atlanta and Baltimore, its results are more positive, showing that the respondents on the whole felt that most of the parties in their governments provided a good deal of support for cybersecurity. Over three-fourths (78.6%) of respondents said that the mayor/elected county executive was highly/ mostly supportive of cybersecurity, 14.3% said somewhat/a little, and 7.1% said not at all. Next, 71.4% respondents said that department heads were highly/mostly supportive, 21.4% said somewhat/a little, and 7.1% said not at all. This was followed by city/county managers/administrators with 57.1% reporting highly/mostly, 21.4% somewhat/a little, one not at all, and 14.3% didn't know. Average end users came next with 57.1% of respondents saying highly/mostly, 35.7% somewhat/a little, and 7.1% not at all. City/county councilmembers fared the worst when half of respondents said highly/mostly, 42.9% said somewhat/a little, and 7.1% said not at all. In the 2016 survey, one respondent of a small jurisdiction noted "cybersecurity is a moving target and infrastructure can become outdated quickly, so that understanding and support from top-level officials needs to improve."

Other research confirms, however, that top officials in organizations are often not engaged in cybersecurity at high levels. For example, the 2018 PWC survey found that only 44% of corporate boards "... actively participate in their company's overall cybersecurity strategy."[48] Likewise, cybersecurity expert Charles Cresson Wood has concluded, based on his extensive cybersecurity consulting experience, that regardless of type, size, sector, or other characteristics of organizations, top management is not sufficiently well informed about or committed to cybersecurity. This is partly because cybersecurity competes with (and often loses to) other organizational needs. Nevertheless, Wood argued that top executives and managers should understand and fully support cybersecurity and should not allow information security to be the domain of technologists alone.[49] Local government officials should take heed of these findings and endeavor to ensure higher levels of awareness of and support for cybersecurity from all parties in their organizations, especially from top elected and appointed officials.

Conclusion

Local governments that do not provide high levels of cybersecurity place their IT systems, the data stored in those systems, and their very ability to provide critical public services at unnecessary risk. Lack of adequate cybersecurity and/or poor cybersecurity hygiene in organizations often allows cybercriminals to breach their IT systems and cause great harm and cost. Successful cyberattacks can and do result in the loss of or the inability to access (in the case of ransomware attacks) critical data and files, loss of sensitive information (such as PII), loss of money, disruption of public service delivery, high costs to recover and, of course, the embarrassment factor. The examples of Atlanta and Baltimore make this perfectly clear.

Therefore, all local governments, regardless of size, must take whatever actions needed to ensure the highest levels of cybersecurity. But even if they do, the cybercriminals are relentless and very good at what they do, and the risk of being compromised is never gone. Similar to the adages often used in emergency management, there is a common saying in the field that it isn't whether you will be breached, but only a question of when. Local governments must understand their cyber vulnerabilities, be mindful of the fact that they can easily suffer breaches, be fully prepared to continue operations during a successful cyberattack and have concrete plans for recovery. These practices are commonly known as cyber resilience.

According to MITRE, "Cyber resiliency (also referred to as cyber resilience) is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources." Local governments considering ways to achieve cyber resiliency might think of doing so in the ways analogous to how they prepare for and recover from natural disasters. Know the types of potential adverse events; know how to deal with them when (not if) they occur; have concrete plans for continuing critical operations; have concrete plans for recovery in place; and practice, practice, practice.

To summarize the key findings of the 2016 survey and 2020 survey, as well as the literature and the practice, the structure of cybersecurity operations among responding local governments was largely unremarkable and generally followed established patterns among organizations. The numbers of cybersecurity staff reporting to these officials varied considerably. While larger governments, on average, had more cybersecurity staff, the relationship was not precise to population and the same can be said for cyber contractors.

The numbers of end users in these governments also varied a great deal, but the numbers were more closely aligned with the governments' populations. In most jurisdictions, all end users fell under the CIO's responsibility, but in 21.4%, they did not. Local government budget allocations for cybersecurity varied considerably, between less than 1% to 10%, as a fraction of the IT budget. They averaged 4.09%, which is slightly higher than the average for state governments, but below the private sector. Last, half of these governments outsourced some cybersecurity functions and half did not outsource cybersecurity at all.

Responses to the 2020 survey and others confirm that local governments are under constant or nearly constant cyberattack. Moreover, the frequency of attacks had increased in the past year. Most respondents said that the attackers had not changed over the past year. External actor-organizations were the leading type of attacker and phishing/spear phishing were the leading attack vector. Ransom, theft of money, and theft of PII were the principal attack purposes, which had not changed over the past year. All but one responding government had experienced an "incident" over the past year and half had been breached, including 28.6% that had been breached once and 7.1% each that had been breached twice, three times, and more than three times. This information suggests at least two things. First, the bad guys are good at what they do, and they do it more frequently every year. Second, even large (presumably with more budgetary resources) local governments are evidently not doing enough to protect their information assets, as can be seen by the number of breaches experienced in the past year by the responding local governments.

Overall, the local governments in the 2020 survey had not done as good a job as needed in the adoption of cybersecurity policies. Only three of the subject policies had been adopted by substantial majorities of these local governments, and the respondents' perceptions of the effectiveness of the policies bears this out. Fewer than half of respondents said that any policy was highly effective. Anything less than highly effective suggests varying degrees of ineffectiveness—an undesirable cybersecurity outcome.

Consistent with the literatures on IT and local government, local e-government, and local government cybersecurity, respondents to this survey named lack of funding and lack of staff as their top two barriers to effective cybersecurity. Responses from the 2020 survey on local government cybersecurity budgets demonstrate that cybersecurity is substantially under-funded in several of them.

The top needs for achieving cybersecurity were similar to the barriers identified—funding and staffing—but at least some of the respondents added one of considerable interest: leadership buy-in. Solid majorities of these governments required annual cybersecurity training for listed parties. Only 14.3% did not and 7.1% provided training in a different time period. This finding is of great importance because training of local officials and staff is highly recommended as a way to improve cyber hygiene and outcomes in organizations.

Respondents were not sanguine about the level of cybersecurity awareness among most parties in their local governments. Surprisingly, however, majorities of respondents (including large majorities in the cases of the mayor/elected executive and department heads) felt that most parties provided good support for cybersecurity.

Recommendations

Based on the evidence accumulated in this study, the first recommendation is that elected officials and top management of local governments must, within budgetary limitations, provide adequate funding for cybersecurity, including funding for adequate staffing for this important function. Staffing should be a combination of both internal staff and contracting services to best fit local governments specific needs. Failure to adequately fund and staff cybersecurity will almost certainly lead to adverse cyber outcomes (again, think Baltimore and Atlanta), which in turn will lead to unnecessary and significant costs to local governments.

Second, in order to improve cybersecurity outcomes, local governments should fully adopt and implement the policies discussed earlier. In the absence of fully adopted and implemented policies, local governments cannot achieve high levels of cybersecurity and will almost certainly pay the price for failing to do so. These policies should also align with the recommendations of the NIST Framework introduced earlier.

Recommendations for Small Local Governments

Small local governments often lack the budgetary resources to provide the hardware, software, and personnel needed to establish and maintain high levels of cybersecurity. Here are a few hints for overcoming these limitations.

1. To the extent budgetarily feasible, hire a qualified cybersecurity professional as chief of cybersecurity. If you are unable to hire additional staff, designate an existing role as the CISO, and make sure that the designee is properly trained in cybersecurity and has the support of top local officials.
2. Partner with other local governments, either a county, neighboring jurisdictions, or school districts to share cybersecurity costs.
3. Consider outsourcing some or all cybersecurity.
4. Seek help from area colleges and universities.
5. Contact the state or local National Guard to learn what support the latter may be able to provide. There are 59 guard cyber units across the nation and its territories with approximately 4,000 cyber operational personnel that may be available as a resource when planning for and responding to cybersecurity events. [50]
6. Contact national organizations that serve local governments that often have useful resources. For example, ICMA publishes works on cybersecurity for local governments and also provides training through its Cybersecurity Leadership Academy. The National League of Cities (NLC) publishes a variety of papers on cybersecurity (e.g., "Protecting Our Data: What Cities Should know about Cybersecurity"). The National Association of Counties (NACo) offers webinars on cyber (e.g., NACo Cyberattack Simulation). The National Association of State Chief Information Officers (NASCIO) provides useful publications for both state and local government (e.g., "Stronger Together: State and Local Cybersecurity Collaboration").
7. Consider participating in the Multi-State Information Sharing and Analysis Center (MS-ISAC), whose mission is "to improve the overall cybersecurity posture of the nation's state, local, tribal, and territorial governments through focused cyber threat prevention, protection, response, and recovery." [51]
8. Consider participating in state and regional organizations that provide cybersecurity support, such as the Michigan Cyber Civilian Corps, the Massachusetts Mass Cyber Center, or the Los Angeles Cyber Lab.

Tips on How to Manage Challenges of the Increasing Number of Employees Working from Home

1. If possible, the local government should have a telework policy requiring employees to work from home using only laptops (and other devices) issued and cleared by the local government. In this case, employees must not use the work-issued laptops for personal purposes.
2. If this is not possible, the local government should assist employees in making sure that their home computers/networks (and other devices as applicable) are secure.
3. Local governments must ensure that their IT systems and networks have sufficient bandwidth to accommodate these employees who are working from home for necessary frequent updates, such as those needed for antivirus and system patches.Consider if there are limitations in the network to plan around.
4. Local governments must ensure that their IT system and networks are secure and are being constantly monitored through detection systems, such as ransomware protection software .
5. Every party must understand that the cybersecurity rules at work apply when working from home.
6. Employees need to make sure that whatever devices are being used to work remotely (laptop, desktop, etc.,) are physically secure and cannot be used by others (friends, family, etc.) Employees must keep their laptop physically secure at all times when traveling.
7. As always, employees should utilize cybersecurity best practices and practice proper cyber hygiene. IT staff should send period reminders and conduct remote spot-checks on random employees to see if they are following instructions when possible.
8. Employees working from home should understand that they could be targeted by cybercriminals at any time and be especially mindful of phishing and spear phishing attacks and any anomalies that may occur with their home or work-issued computers.

Third, local governments must ensure that their cybersecurity policies are implemented properly and that they are effective. Periodically, they should be revisited, revised, and re-implemented appropriately. They should also be continuously monitored for effectiveness using appropriate methods or metrics.

Most of the local governments in the 2020 survey mandate that top elected officials, councilmembers, top administrators, department heads, and end users take cybersecurity training. However, respondents generally did not rate the results of the training highly. Thus, a fourth recommendation is for these governments to revise their cybersecurity awareness training, especially focusing on cybersecurity awareness and support, as well as appropriate cyber hygiene or behavior. This revision should include updated training on proper work from home conduct.

Fifth, all parties within local governments, including elected officials, top managers, and all employees and contractors, must be held accountable for their cyber actions and behavior.

This means, at a minimum, when someone violates policy regarding the use of the local government's IT system, that individual will lose certain system privileges and receive appropriate "counseling" and further training. In the event of further violations, the individual could lose all privileges and potentially be terminated. (Of course, termination of employment would not apply to elected officials.)

A final recommendation draws on academic and professional literature and is commonly found within the cybersecurity field itself. All local governments should establish and maintain a culture of cybersecurity within their organizations. A culture of cybersecurity means the following, at the minimum: top leadership, including both elected and appointed officials, must fully understand and support cybersecurity and not just at a rhetorical level.

They must:

1. Understand that cybersecurity is not solely the responsibility of the technologists, they have an active role to play in it, and they must embrace that role.
2. Provide the funding needed for effective cybersecurity.
3. Practice proper cyber hygiene themselves.
4. Promote cybersecurity throughout the organization as "job one" for everyone.
5. Insist that all parties are held appropriately accountable for their cyber actions.

If top officials fail to insist on such a culture and fail to act appropriately in their own cyber responsibilities, those under them will almost certainly think, "If they don't care about cybersecurity, why should I?" Top leadership buy-in will make all parties in an organization respect the importance of cybersecurity and their own cyber responsibilities and will make it more likely that they will practice proper cyber hygiene, thus improving cyber outcomes throughout the organization.

DONALD F. NORRIS is professor emeritus of public policy at the University of Maryland, Baltimore County (UMBC). He retired from UMBC in 2017 after serving 27 years as director of the Maryland Institute for Policy Analysis and Research and 10 years as director of the UMBC School of Public Policy. Norris was the founding editor-in-chief of the *International Journal of Electronic Government Research* and he specializes in information technology in government organizations, including e-government and cybersecurity.

This report was completed as part of ICMA's Local Government Research Fellowship program. ICMA Research Fellows are practitioners and academics that conduct action-oriented research addressing important trends, drivers, and issues facing local governments. Their work advances ICMA's strategic priority to provide thought leadership and resources that support members and other local government stakeholders in creating and sustaining thriving communities throughout the world.

Appendix 1:
2020 Survey Questions for CISO Interviews

1. As the official in charge of your local government's cybersecurity, whom do you report to:

   CIO or equivalent
   CTO or equivalent
   ITD or equivalent
   Mayor
   City/county manager/administrator
   Other

2. Is your local government's cybersecurity totally under you (or your office's) control or is it divided?

   Totally my responsibility
   Divided

2a. If responsibility is divided, among what offices?

3. How many cybersecurity staff (local government employees) report to you (by population group)?

4. How many cybersecurity contractors report to you?*

5. What percentage of end users fall under your responsibility as head of cybersecurity?

6. What percentage of your IT budget is allocated to cybersecurity?

7. Does your local government outsource cybersecurity?

   Yes, outsourced completely
   Yes, outsourced partially
   No, do not outsource at all

7a. If you outsource cybersecurity, what principal functions are outsourced?

8. How often is your local government subject to cyberattack?

   Constantly
   Hourly
   Daily
   Don't Know

9. How many times has your information system experienced an "incident" in the past year?

   None
   Once
   Twice
   Three times
   Four times
   Five times
   More than five times
   Don't know

10. How many times has your IT system or any element of it been breached in the past year?

    None
    Once
    Twice
    Three times
    More than three times
    Don't know

11. Have cyberattacks gotten more or less frequent over the past year?

    More frequent
    About the same
    Less frequent
    Don't know

12. Are you able to determine the types of attackers?

    Yes
    No
    Don't know

12a. If you are able to determine the types of attackers, are they (check all that apply):

    External actors – organizations
    External actors – individuals
    Nation states
    Hacktivists/spammers
    No answer

13. Has the pattern of attacks changed or remained the same over the past year?

    Changed
    Remained the same
    Don't know

13a. If the pattern has changed, please describe the changes.

14. What are the principal attack vectors (check all that apply)?

    Phishing or spearheading
    DOS
    DDoS
    Man in the middle
    Zaro day
    Brute force
    Other

15. Which is/are the most frequent vector(s) you experienced in the past year? If more than one, list in order of frequency.

    Phishing
    Spearheading
    Vulnerabilities
    Email
    Brute force
    Ransomware
    Vendor breaches
    DDOS
    Compromised credentials
    Insider threats

16. What are the principal purposes of the attacks you experience in the past year (check all that apply)?

    Ransom
    Theft of Money
    PII
    Hacktivism
    Confidential records
    Mischief
    Espionage
    Don't know

17. Which is/are the most frequent attack purpose(s) you experienced in the past year? If more than one, list in order of frequency.

    Ransom
    Data theft/theft/monetary gain
    PII/credential theft
    Defacement
    Hacktivism
    EFT
    Invoice information
    No answer

18. Have the purposes of the attacks changed in the past year?

    Yes
    No
    Don't know

19. Has your local government adopted any of the cybersecurity policies listed below?

    Formal cybersecurity policy
    Password management policy
    Policy regarding applying software patches
    Cyber risk management plan
    Incident response/disaster recovery/business continuity plan
    Policy on use of external devices (e.g., cell phones/flash drives)
    Policy for vendors, contractors, cloud services

20. How effective, if at all, are these policies?

21. What are the three top barriers your local government faces in being able to achieve the highest levels of cybersecurity?

    Lack of funds
    Lack of adequate staff**
    Lack of leadership buy-in/support
    Lack of collaboration
    Procurement process
    Governance

22. What are the three things your local government needs to do to possess or be able to achieve the highest levels of cybersecurity?

    Funding
    Staffing
    Leadership buy-in/commitment
    Awareness/training
    Continuity of operations/ disaster recovery/ incident response
    MFA (Multifactor authentication)
    No answer

23. Does your local government require mandatory cybersecurity training for any of the following (mayor/elected county executive, city/county councilmembers, city/county manager/administrator, department heads, average end user) and if so, how often?

    No
    Annually
    Every 2 years
    Every 3 years
    Other time period
    Don't know

24. In your opinion, how aware are the following parties (mayor/elected county executive, city/county councilmembers, city/county manager/administrator, department heads, average end user) of the need for high levels of cybersecurity?

    Highly/Mostly
    Somewhat/A Little
    Not at all
    Don't know

25. In your opinion, how supportive of the need to maintain high levels of cybersecurity are the following parties (mayor/elected county executive, city/county councilmembers, city/county manager/administrator, department heads, average end user)?

    Highly/Mostly
    Somewhat/A little
    Not at all
    Don't know

Appendix 2:
Key Cyberattack Vocabulary and Brief Descriptions

Local government officials should know the principal types of cyberattacks that their governments are likely to face. There are numerous types of cyberattacks, and this appendix discusses eight key vocabulary associated with the most common types of attacks.

Malware: Malware is malicious software installed after an attacker has penetrated a victim's IT system that can do one of several damaging things, such as encrypting data and files, blocking user access to systems or components of systems, exfiltrating data and files, and more. Significant examples of malware used against local governments include Atlanta, Georgia (2018); and Baltimore, Maryland (2018 and 2019).

Ransomware: Ransomware is an especially nefarious form of malware that is increasingly used in cyberattacks. It is typically delivered via social engineering, most often in phishing or spear phishing emails. Once the malware has penetrated an organization's IT system, the objective is to find and encrypt sensitive data and files and possibly lock down or seriously degrade an organization's entire IT infrastructure, likely paralyzing and preventing it from conducting its regular business. In the case of local governments, ransomware prevents them from providing essential serves to their residents and businesses. The cybercriminal then demands a ransom, usually in the form of Bitcoin or some other cryptocurrency, to release the system and its files and data. The threat is that if the organization does not pay the ransom, the cybercriminal will leave the data and files encrypted or the entire system locked down.

In the early years of ransomware attacks, many organizations paid the ransom to get their systems back because paying ransom is considerably cheaper than paying to restore an IT system. The consensus on whether to pay ransomware has shifted in recent years, although not totally, and organizations increasingly refuse to pay ransom. Today, it is commonly thought that paying ransom is a bad idea because it compensates cybercriminals for their criminality and encourages them to continue ransomware attacks. An article in ProPublica argued that paying ransom "...fuels the rise in ransomware attacks."[52] Also, if these attacks work and profit cybercriminals, as demonstrated by ransom payments, the criminals will be incentivized to continue attacking.

At its annual meeting in 2019, and at the urging of then-mayor Jack Young of Baltimore, the U.S. conference of mayors adopted a resolution urging their members not to pay ransom if their IT systems were victims of a ransomware attack.[53] Also, the U.S. Treasury Department now advises that, under some circumstances, organizations that pay ransom could face major legal penalties. Certainly, federal law enforcement advises against and frowns on paying, and this is increasingly true of state and local law enforcement.

It is never clear that paying ransom will actually result in the cybercriminal releasing the system. Nor is it clear that the criminal won't change their name and/or IP address and re-attack after payment since the criminal already knows the organization's vulnerability and willingness to pay. Hence, paying ransom entails some risk, not in the least because in some circumstances, paying ransom is illegal.[54,55] Today, the best advice to local governments is to not pay ransom and instead use the money you would have paid (and more if needed) to further enhance your cybersecurity to prevent breaches.

To prevent ransomware attacks from crippling their IT systems, local governments should continually scan their systems for malware, train their employees to never open suspicious emails, and regularly back up their systems.

Phishing: Phishing is a form of social engineering in which cybercriminals "go fishing" for victims by sending emails, seemingly from trusted parties, with promises, opportunities, or threats the attackers hope victims will fall for. Phishing and spear phishing (below) are perhaps the most common types of cyberattacks in today's cyber environment. According to one source, early in the COVID-19 pandemic phishing attacks increased 667%.[56] A report by the Anti-Phishing Working Group (APWG) showed that phishing attacks increased in an almost linear fashion throughout 2020 and totaled more than 200,000 monthly attacks in the fourth quarter.[57]

A common phishing attack, which many people have received (and which dates back to the late 1990s), is an email from someone in Nigeria promising the targeted party (the potential victim or victim) a large amount of money. The attacker asks the victim for their bank account details so that the attacker can transfer the money. Of course, the transfer never happens, and the scammer later steals funds from the victim's account. There are variations of this attack, some including URLs or attachments in the email that, if the victim clicks on or opens, will give the attacker access to the victim's computer and all of the information in it.

Spear phishing: Spear phishing is a more sophisticated form of phishing in which the cybercriminal uses just enough information to make the victim believe the email came from someone known to the victim or another trusted source. For example, the victim might receive an email with an attachment or URL that appears to be from their colleague or a trusted source that reads something like: "Hey [Name of Recipient]]! Have you seen this announcement from the city council? You'll want to read this." Given this scenario, many a victim has been tricked into opening the attachment or clicking on the URL. The same result occurs as with phishing—the victim's computer and all of the information in it are wide open to the attacker. In the 2020 survey, responding CISOs said that phishing and spear phishing were the most common attacks that they experienced.

Brute force: Brute force is a method that cybercriminals use to break into IT systems. The term brute force refers to the way an attacker "bangs away" at a victim's computer, network, or IT system using, for example, specifically designed software to guess a password that will enable them to penetrate the system. Once penetration has been achieved, the attacker can then install malware. It was a brute force attack that resulted in the 2018 Atlanta breach and the installation of ransomware.

Zero-day: Like brute force, a zero-day exploit is an attacker's identification of a weakness in a network or IT system, typically a previously unknown defect in software that had not been found and patched. Once the weakness has been identified, the attacker uses it to break into the system and install malware.

Denial of Service (DoS): A DoS attack occurs when an attacker sends massive volumes of traffic to an organization's website or server, so much so that the website or server cannot handle the traffic, essentially shutting down the server or website so that no one can use it. This can be done for no malicious reason, such as when the University of Maryland Baltimore County (UMBC) website went down because of a traffic overload that occurred when its president was interviewed on the television show 60 Minutes. DoS attacks can also be totally malicious, for example, to demand money to stop the attack.

Distributed Denial of Service (DDoS): A DDoS attack is a DoS attack on steroids. It is an attack on a server or website by many different computers simultaneously for the purpose of shutting it down to all users. According to Bloomberg News, the U.S. Department of Health and Human Services was hit by a DDoS attack in March 2019 and was "... part of what people familiar with the incident called a campaign of disruption and disinformation that was aimed at undermining the [HHS] response to the coronavirus pandemic and may have been the work of a foreign actor."[58]

Endnotes and Resources

[1] Emsisoft Malware Lab a. 2020 (December 12). The State of Ransomware in the US: Report and Statistics 2019. https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-andstatistics-2019/.

[2] Emsisoft Malware Lab b. 2020 (July 8). State of Ransomware in the US: Report and Statistics for Q1 and Q2 2020. https://blog.emsisoft.com/en/36534/state-of-ransomware-in-the-us-report-and-statistics-forq1-and-q2-2020/.

[3] Norris, Donald F., Laura Mateczun, Anupam Joshi and Timothy Finin. 2018. Cybersecurity at the grassroots: American local governments and the challenges of Internet security. *Journal of Homeland Security and Emergency Management*. 15(3): 1-14; and Norris, Donald F., Laura Mateczun, Anupam Joshi and Tim Finin. 2019. Cyberattacks at the grassroots: American local governments and the need for high levels of cybersecurity. Public Administration Review. 76(6): 895-904; Norris, Donald F., Laura Mateczun, Anupam Joshi and Tim Finin. 2021, forthcoming. Managing cybersecurity at the grassroots, Evidence from the first nationwide survey of local government cybersecurity. *Journal of Urban Affairs*. https://www.tandfonline.com/doi/full/10.1080/07352166.2020.1727295.

[4] Cybersecurity Ventures. 2015. Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021. https://cybersecurityventures.com/hackerpocalypse-cybercrimereport-2016/.

[5] U.S. Census Bureau. 2018. 2017 Census of Governments. Table2. Local governments by type and state: 2017 [CG1700ORG02]. https://www2.census.gov/programssurveys/gus/tables/2017/cog2017_cg1700org02.zip

[6] Government Technology. 2019. 2019 Spending Forecast for the State and Local IT Market. https://www.govtech.com/budgetfinance/2019--Spending-Forecast-for-the-State-and-Local-ITMarket.html.

[7] Secureworks. 2017. 2017 State of Cybercrime. https://www.secureworks.com/resources/rp-2017-state-of-cybercrime.

[8] Norris, et al., 2019.

[9] Norris, et al., 2019.

[10] Mayyan, Gilad David. 2020 (January 13). The IoT rundown for 2020: Stats, risks, and solutions.

[11] The author acknowledges support for this survey from the recently established Coalition of City CISOs (https://cityciso.org/) whose members constitute the majority of respondents to the survey.

[12] PWC. 2018. Strengthening Digital Society Against Cyber Shocks: Key Findings from the 2018 Global State of Information Security Survey. https://www.pwc.com.br/pt/global-state-of-information-security-survey-2018/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks.pdf.

[13] 2020 Deloitte-NASCIO Cybersecurity Study. 2020. https://www2.deloitte.com/content/dam/insights/us/articles/6899_nascio/DI_NASCIO_interactive.pdf.

[14] Norris, et al., 2019.

[15] Deloitte-NACIO, 2020.

[16] Nash, Kim S., 2019 (December 30). Tech Chiefs Plan to Boost Cybersecurity Spending. https://www.wsj.com/articles/tech-chiefs-plan-to-boost-cybersecurity-spending-11577701802.

[17] Hatcher, et al., 2020.

[18] Deloitte. 2019. The Future of Cyber Survey 2019: Cyber Everywhere. Succeed anywhere. https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cyber-survey.html.

[19] Norris, et al., 2018.

[20] Deloitte. 2019.

[21] Norris, et al., 2018.

[22] Verizon, 2015.

[23] Colorado Computer Support. 2018. The City of Atlanta Held Hostage by Cybercriminals. https://www.coloradosupport.com/the-city-of-atlanta-held-hostage-by-cybercriminals/.

[24] Blinder, Alan, and Perlroth, Nicole. 2018. A Cyberattack Hobbles Atlanta, and Security Experts Shudder. https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html.

[25] Freed, Benjamin. 2018. Atlanta was not prepared to respond to a ransomware attack. https://statescoop.com/atlanta-was-not-prepared-to-respond-to-a-ransomware-attack.

[26] Freed, 2018.

[27] Deere, Stephen. 2018. Feds: Iranians led cyberattack against Atlanta, other U.S. entities. https://www.ajc.com/news/local-govt--politics/feds-iranians-led-cyberattack-against-atlanta-other-entities/xrLAyAwDroBvVGhp9bODyO.

[28] Kearney, Laila. 2018. Atlanta officials reveal worsening effects of cyber attack. https://www.reuters.com/article/us-usa-cyber-atlanta-budget/atlanta-officials-reveal-worsening-effects-of-cyber-attack-idUSKCN1J231M.

[29] Deere, 2018.

[30] Freed, 2018.

[31] Deere, 2018.

[32] Freed, 2018.

[33] Deere, 2018.

[34] Rector, Kevin. 2018. Baltimore 911 dispatch system hacked, investigation underway, officials confirm. https://www.baltimoresun.com/news/crime/bs-md-ci-911-hacked-20180327-story.html.

[35] Rector, 2018.

[36] Duncan, Ian and Zhang, Christine. 2019. Analysis of ransomware used in Baltimore attack indicates hackers needed 'unfettered access' to city computers. https://www.baltimoresun.com/politics/bs-md-ci-ransomware-attack-20190517-story.html.

[37] Chokshi, Niraj. 2019. Hackers Are Holding Baltimore Hostage: How They Struck and What's Next. https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html.

[38] Gallagher, Sean. 2019. Baltimore ransomware nightmare could last weeks more, with big consequences. https://arstechnica.com/information-technology/2019/05/baltimore-ransomware-nightmare-could-last-weeks-more-with-big-consequences.

[39] Ropek, Lucas. 2019. Over a Month On, Baltimore Still Grappling with Hack Fallout. https://www.govtech.com/security/over-a-month-on-baltimore-still-grappling-with-hack-fallout.html.

[40] Duncan and Zhang, 2019.

[41] Gallagher, 2019.

[42] Gallagher, 2019.

[43] Norris, et al., 2019, 2020.

[44] National Institute of Standards and Technology. 2018. *Cybersecurity Framework Version 1.1*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[45] McAfee. 2020. How Cybersecurity Policies and Procedures Protect Against Cyberattacks. https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/cybersecurity-policies.html#:~:text=A%20cybersecurity%20policy%20sets%20the,data%20breaches%20are%20potentially%20costly.

[46] PWC 2018.

[47] PWC, 2018.

[48] PWC, 2018.

[49] Wood, Charles C. 2010. Preface. In Whitman, Michael E. and Herbert J. Mattord. 2010. *Management of Information Security*, 4th ed. Stamford, CT: Cengage Learning.

[50] Olenick, Doug., 2020 (September 15). National Guard Cybersecurity Units Ready to Protect Election. BankInfoSecurity. https://bankinfosecurity.com/national-guard-cybersecurity-units-ready -to-protect-election-a-14990.

[51] Multi-State Information Sharing and Analysis Center. Home Page. https://www.cisecurity.org/ms-isac/.

[52] Dudley, Renee. 2019 (August 17). The extortion economy: how insurance companies are fueling a rise in ransomware attacks. https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks.

[53] Duncan, Ian. 2019 (July 10). U.S. mayors group adopts resolution proposed by Baltimore, vowing not to pay ransoms to hackers. Baltimore, MD: *Baltimore Sun*. https://www.baltimoresun.com/politics/bs-md-ci-mayors-ransom-20190710-cznelxwcg5hiziiqmubtg2elju-story.html.

[54] CISOMAG. 2020 (October 5). Paying ransom is now illegal! U.S. Dept of Treasury warns. https://cisomag.eccouncil.org/paying-ransom-is-now-illegal-u-s-dept-of-treasury-warns/#:~:text=U.S.%20Dept%20of%20Treasury%20Warns&text=The%20U.S.%20Department%20of%20the,to%20cybercriminals%20is%20now%20illegal.&text=Ransomware%20payments%20may%20also%20embolden,future%20attacks%2C%E2%80%9D%20OFAC%20said.

[55] KrebsOnSecurity. 2020 (October 1). Ransomware victims that pay up could incur steep fines from Uncle Sam. https://krebsonsecurity.com/2020/10/ransomware-victims-that-pay-up-could-incur-steep-fines-from-uncle-sam/.

[56] Muncaster, Phil. 2020 (March 26). #COVID19 Drives Phishing Emails Up 667% in Under a Month. https://www.infosecurity-magazine.com/news/covid19-drive-phishing-emails-667/.

[57] Anti-Phishing Working Group (APWG). 2021 (February 9). Phishing Activity Trends Report 4th Quarter 2020. https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf.

[58] Stein, Shira and Jennifer Jacobs. 2019 (March 16) Cyber-attack hits u.s. health agency amid covid-19 outbreak. https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response.