WHAT LOCAL GOVERNMENT OFFICIALS SHOULD KNOW AND DO ABOUT CYBERSECURITY

DONALD F. NORRIS AND LAURA MATECZUN

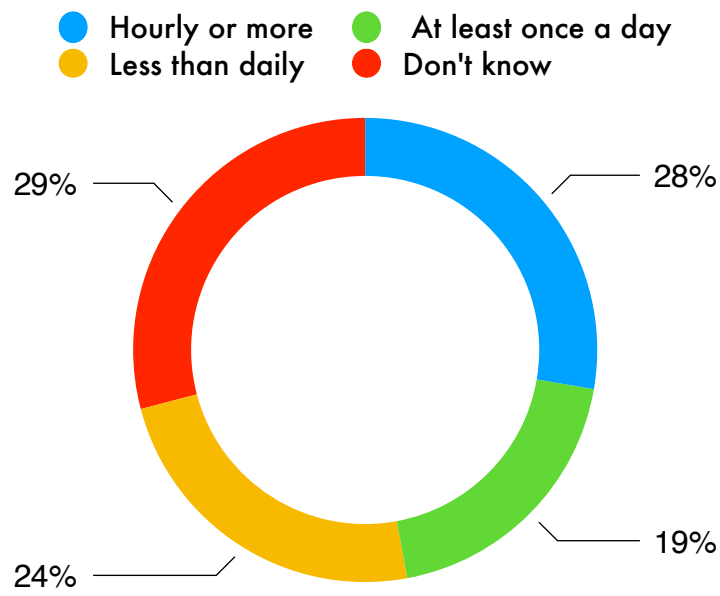
UNIVERSITY OF MARYLAND, BALTIMORE COUNTY

SCHOOL OF PUBLIC POLICY

TOP 5 THINGS LOCAL GOVERNMENT OFFICIALS NEED TO KNOW ABOUT CYBERSECURITY

1. Your local government is under constant or nearly constant cyberattack.

Findings from a focus group among top IT and cybersecurity staff in several Maryland local governments confirmed that attacks are constant.[1] Data from a recent survey show, however, that a sizable fraction of local governments did not know that they were under attack.[2] And, it may be that those who said their governments were under attack less than daily really did not know, either.



We define attack as: any attempt by any party to gain unauthorized access to any component of an organization's IT system for the purpose of causing mischief or doing harm.

2. The bad guys are really, really good at what they do.

Cyber criminals, state sponsored malicious cyber actors, terrorists, hacktivists, and others who bombard local government websites know what they are doing; know what they are after; are driven by motives such as financial gain, ideology and mischief; are numerous; and are relentless. Recent estimates suggest that cybercrime damages worldwide will cost $6 trillion by 2021.[3] And, things will only get worse.

3. **Even if your government maintains a high level of cybersecurity, it is very likely to experience adverse cyber events (incidents or breaches) from time to time.**

   Verizon defines an incident as: "Any event that compromises the confidentiality, integrity or availability of an information asset;" and a breach as: "An incident that resulted in confirmed disclosure (not just exposure) to an unauthorized party."[4]

   It is common to hear cybersecurity professionals say: "It is not if, but when will your organization be breached." Evidence from the survey found that more than one-third of local governments reported being breached. This said, there is no excuse for not maintaining high levels of cybersecurity, because not doing so will only make your government's cyber outcomes worse. Breaches can result in drastically reduced or effectively no service delivery with a loss of public trust. Public safety is at risk, with 911 and 311 service loss or disruption; residents may not be able to complete important transactions such as not being able to close on a house or pay water bills; and vulnerable populations dependent on city services are disproportionately affected.

4. **If your government does not maintain high levels of cybersecurity, it is almost (if not certainly) guaranteed to experience adverse cyber events.**

   At the worst, such events - especially breaches - can cause serious damage, disrupt service delivery, result in theft or loss of data, cost thousands if not millions of dollars to recover (think Baltimore 2019 - $18 million to recover from a ransomware attack), and prove downright embarrassing to local officials. Federal and state governments may need to step in if your local government is not prepared.

5. **Cybersecurity is YOUR RESPONSIBILITY, not solely or even primarily the responsibility of local government IT and cybersecurity staff.**

   Unfortunately, however, data from the survey show that, for the most part, local elected and top management officials do not view cybersecurity as an important part of their jobs. If they do not take an active role in cybersecurity and act as cybersecurity champions, everyone else in their local government will think: "If they don't care, why should I?"

---

[1] Norris, Donald F., Laura Mateczun, Anupam Joshi and Tim Finin. 2018. Cyber-Security at the Grassroots: American Local Governments and the Challenges of Internet Security. *Journal of Homeland Security and Emergency Management*.

[2] 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*.

[3] Morgan, Steve. 2019. 2019 Official Annual Cybercrime Report. Cybersecurity Ventures and Herjavec Group. https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

[4] Verizon. 2015. 2015 Data Breach Investigations Report. http://www.verizon.com/about/news/2015-data-breach-report-info

TOP 5 THINGS LOCAL GOVERNMENT OFFICIALS SHOULD DO ABOUT CYBERSECURITY

1. Play an active role in your government's cybersecurity.

Elected officials and top appointed managers must be proactive, not just reactive, regarding their government's cybersecurity. These leaders must practice cybersecurity and emphasize its importance throughout the organization. They should assure that: 1) their government adopt Cybersecurity plans; 2) establish by ordinance and fill the position of Chief Information Security Officer; 3) provide that Officer with sufficient authority to protect all aspects of their cities' IT infrastructure; and 4) require all departments and staff to follow cybersecurity requirements.

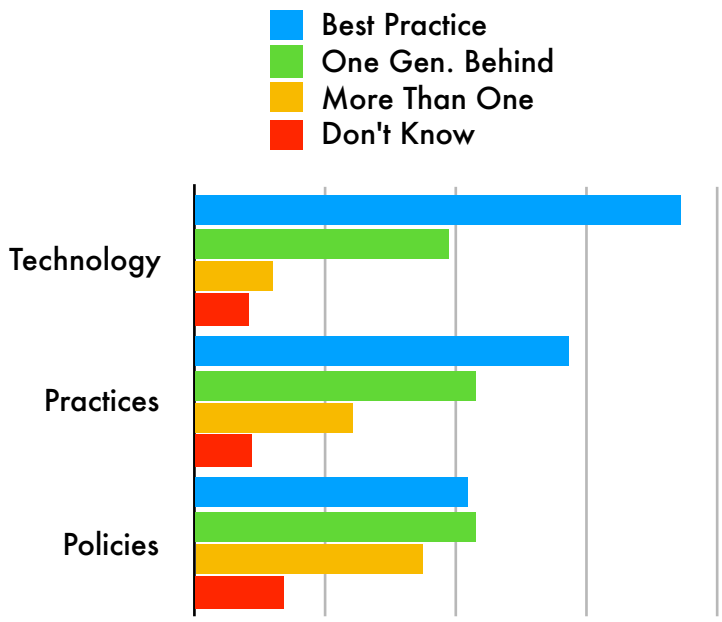
2. Learn the basics of cybersecurity so that you can ask the right questions of your cybersecurity staff.

It is not necessary that elected officials and top managers become cybersecurity experts, but they should learn the basics of this important field (call it Cybersecurity 101!) in order to know what questions to ask and what cybersecurity technology, policies and practices to insist be adopted. Here are just a few (but important) actions needed to facilitate high levels of cybersecurity:

- ensure proper cybersecurity staffing levels;
- implement regular cybersecurity awareness training for all staff and officials;
- ensure that cybersecurity responsibilities are added to all local government job classifications to make them official and enforceable;
- implement accountability measures regarding everyone's use of your IT assets;
- back up all systems all the time (and store back-ups off site);
- create continuity of operations and recovery plans;
- patch all systems as soon as patches are available; and
- implement dual factor authentication.

3. Listen to and support your cybersecurity staff.

Your cybersecurity staff are technical experts and should be tasked to advise top officials in an executive session at least annually, if not more often, about the ever-changing cyber threat landscape, how well your local government is positioned to meet cyber threats and what, if any, technologies, actions, tools, policies and practices are needed to ensure the highest level of cybersecurity. Listen to them. The charts below show the top three recommendations to improve cybersecurity from the respondents to the survey as well as their rankings of their governments' cybersecurity technology, practices and policies.



TOP 3 ACTIONS TO IMPROVE CYBERSECURITY

1. GREATER FUNDING
2. BETTER POLICIES
3. GREATER AWARENESS AMONG LOCAL GOVERNMENT EMPLOYEES

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*.

4. Adequately fund cybersecurity.

Evidence clearly says that lack of funding is the biggest barrier to local government cybersecurity. Local government leaders must ensure adequate, dedicated funding within either the local government or IT budget for this critical function. NASCIO found that nearly half of states do not have dedicated cybersecurity budgets, and those that do limit funding to 0 to 3 percent over their overall IT budget, compared to rates of 15 percent found in private industry.[5]

5. Insist on the creation and maintenance of a culture of cybersecurity throughout your local government.

A culture of cybersecurity starts when top officials in an organization fully embrace and support cybersecurity, insist that all others in the organization do so and ensure that all are held accountable for their practice of cybersecurity. Cybersecurity must be inculcated into the organization and must be seen by all parties, no matter their position, title or pay grade, as one of their most important jobs.

[5] National Association of State Information Officers (NASCIO). 2020. Ensure Dedicated Cybersecurity Funding for State and Local Governments with CIOs as Key Decisionmakers. https://www.nascio.org/wp-content/uploads/2020/01/NASCIO-Dedicated-Cyber-Funding-2020.pdf

The authors created this White Paper at the request of the Coalition for City CISOs (www.cityciso.org) to assist CISOs everywhere inform and educate local government officials and staff in the need for high levels of cybersecurity. We appreciate Coalition members' review of and comments on the White Paper before we finalized it. The White Paper is intended for open use. We ask users cite the White Paper as follows.

Donald F. Norris and Laura Mateczun. March 2020. *White Paper: What Local Government Officials Should know and Do about Cybersecurity.* Baltimore, MD: University of Maryland, Baltimore County. Coalition of City CISOs. The authors can be reached at: norris@umbc.edu and lam6@umbc.edu.

© 2020