CYBER SECURITY THREATS

Your Leadership Needed

City leaders, we call you to take action to ensure your city has the tools and resources to control the risk of cyber-attack and information security breaches. We have gathered information from cyber coverage carriers, national cyber security experts, the National League of Cities, and our own members to provide you with this list of actions and resources. We urge every city to take these actions NOW.

1. Champion and Invest in Cybersecurity

Learn about the urgency of immediate action to implement critical cybersecurity measures, communicate that federal funds can be used for this purpose*, and charge and empower city leaders to take action.

- YES YOU CAN discuss cybersecurity gaps, plans, action items, and budgeting needs in executive session (O.C.G.A. Section 50-14-3 (b)(5).)
- YES YOU CAN request preparation of cyber coverage questionnaire responses and reports showing status of cybersecurity goals – they are not subject to open records requests (O.C.G.A. Section 50-18-72 (a)(25)(A)(v).)

2. Engage a Skilled Cybersecurity Resource

Ensure that city leaders engage a skilled cybersecurity resource that can establish ongoing, automated security measures, monitor the measures, respond immediately to incidents, and implement / manage all cybersecurity measures below.

- If you don't already have a skilled cybersecurity resource, GMA recommends VC3 Cybersecurity and Technology Services (Contact Darin Jenkins at djenkins@gacities.com).
- GMA recommends utilizing these free federal resources:
  i. **MS-ISAC -** MS-ISAC is funded by the Department of Homeland Security and Department of Defense and their membership and services are free to local governments (Contact Kyle Bryans at kyle.bryans@cisecurity.org)
  ii. **CISA -** The Cybersecurity & Infrastructure Security Agency also provides valuable free resources to local government. (Contact CISA Cybersecurity Coordinator Stanton Gatewood at stanton.gatewood@cisa.dhs.gov)

3. Obtain Cyber Coverage

Ensure the city works with the cybersecurity resource to implement measures required to obtain cyber coverage (those marked with plus sign are currently required by many carriers to get a quote for limited coverage.) Revisit to request removal of limits after completion of all items.

- Multifactor authentication for administrator accounts, email, remote access +
- Monitored endpoint detection and response deployed on all computers and services +
- Administrative privileges are restricted on all computers +
- Administrative audit and mailbox logging are enabled on all Microsoft Exchange email servers (or enable comparable logging capability of non-Microsoft email servers) +
- Protective DNS Service in use +
- Prompt security updates and patching of operating systems, applications, and firmware
- Offline, offsite, current backups of critical data are available, monitored, and tested to ensure data can be restored
- Remote access to the local network available only through VPN
- All workers complete regular security awareness training and phishing tests
- City maintains and tests an incident response procedure through tabletop exercises
- Sensitive data is identified and encrypted at rest and in transmission
- A third party (not the cybersecurity resource) performs penetration tests of systems to identify vulnerabilities
- Sunsetting or removal of end-of-life hardware and software
- City has written policies and procedures to ensure that all of the above are implemented and enforced

GEORGIA MUNICIPAL ASSOCIATION

**American Rescue Plan Act - State and Local Fiscal Recovery Fund money can be used for cybersecurity now. Additional federal funds for cybersecurity will be available through the Bipartisan Infrastructure Law State and Local Cybersecurity Grant Program.*

If you have any questions about this document, please contact Alison Earles at aearles@gacities.com