GEORGIA MUNICIPAL ASSOCIATION

CYBERSECURITY THREATS

Your Leadership Needed; Resources Available

October 4, 2022

Presenters

- Charles Kicklighter, Assistant Special Agent in Charge, Georgia Cyber Crime Center. Charles Kicklighter is a Special Agent (SA) with the Georgia Bureau of Investigation (GBI) and has been so employed since February 1998. Prior to becoming a Special Agent with the GBI, he had served as Chief of Police for the City of Wrightsville Police Department and a Patrol Officer for the Savannah Police Department. S/A Kicklighter is currently assigned to the GBI Cyber Crime Center (G3C) in Augusta, Ga. as the Assistant Special Agent in Charge (ASAC) and is also a Federal Task Force Officer (TFO) with the FBI Cyber Crime Task Force in Atlanta, Ga. He is a certified P.O.S.T. Instructor. and has a B.S. in Criminal Justice from Armstrong Atlantic University in Savannah, Ga.
- Sou Ford, Senior Vice President, Southeast Cyber Practice Leader. Sou Ford is responsible for overseeing and managing a team of cyber insurance professionals. She consults with clients on their cyber insurance needs and assists in designing and placing the coverage. Ms. Ford received her B. A. in Biology from Columbia University and has extensive experience in the healthcare, manufacturing, retail, hospitality, public entity and transportation industries.

Presenters

- Alison Cline Earles, Senior Associate General Counsel, CIPP/US. A graduate of Princeton University and Duke Law School, Ms. Earles joined Georgia Municipal Association in March 2014 after an extensive career in employee benefits and information privacy and security law – both in private practice with Alston & Bird and Benefits Law Group and for the Georgia Department of Community Health, where she served as Information Privacy and Security Officer for Georgia Medicaid and as counsel and Information Privacy and Security Officer for the State Health Benefit Plan. Ms. Earles leads information privacy and security efforts for GMA. She coordinates with General Counsel, the Chief Information Officer and executive leadership to complete security assessments and develop information privacy and security policies and procedures and training materials. She delivers information privacy and security training to GMA staff and city leaders and leads GMA's business continuity and disaster recovery planning. Ms. Earles was certified as an Information Privacy Professional by the International Association of Privacy Professionals in 2019.

Cybercrime is a serious threat

- Victim every 11 seconds – human factor
- Cybercrime is **more profitable than the global illegal drug trade**
- Estimated 2021 Damages were $20 billion
- 66% of businesses attacked weren’t confident they could recover
- Increasing sophistication, international actors – **very little that can be done after successful attack**
- Breach of Customer Personally Identifiable Information, Damage to Reputation, Customer Victims, Loss of Data, Loss of Audio/Video Recordings

Cybercrime is a serious threat

- Victim every 11 seconds – human factor
- Cybercrime is **more profitable than the global illegal drug trade**
- Estimated 2021 Damages were $20 billion
- 66% of businesses attacked weren’t confident they could recover
- Increasing sophistication, international actors – **very little that can be done after successful attack**
- Breach of Customer Personally Identifiable Information, Damage to Reputation, Customer Victims, Loss of Data, Loss of Audio/Video Recordings

Cyberattacks - a threat to Residents

- "The world took notice when a cyber attacker breached a Florida city's water treatment plant and tried to poison the water supply." https://www.forbes.com/sites/leemathews/2021/02/15/florida-water-plant-hackers-exploited-old-software-and-poor-password-habits/?sh=24c5da20334e
- "The water sector could be at particular risk and has been previously referred to by Cyberspace Solarium Commission Executive Director Mark Montgomery as critical infrastructure's "weakest link."" https://www-governing-com.cdn.ampproject.org/c/s/www.governing.com/security/water-systems-face-unique-challenges-from-russian-cyber-threats?_amp=true
- Florida city - Failure to patch/update - "Faced with the possibility of a broken piece of critical software, many organizations choose to continue running the outdated OS. This incident once again underscored just how risky that practice can be." Shared passwords; No firewall

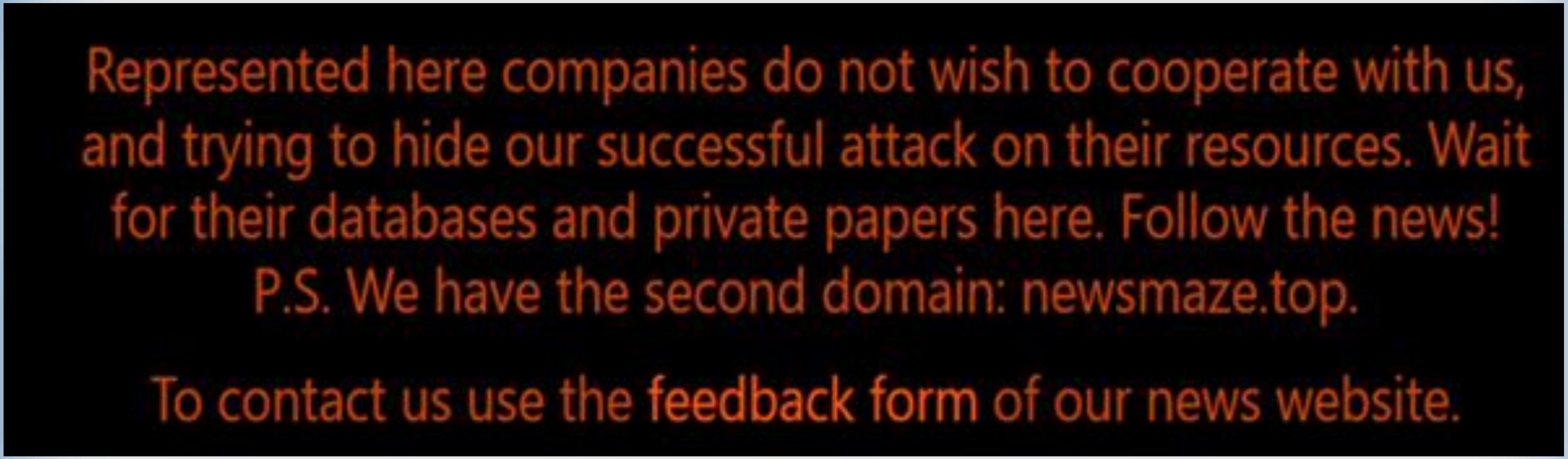
Threat Vectors

- Ransomware
- Business Email Compromise
- Phishing-vishing
- Denial of Service
- Malware
- Keyloggers
- Social Engineering
- ***Cyber attacks can have serious consequences for cities and their citizens***

Ransomware has changed

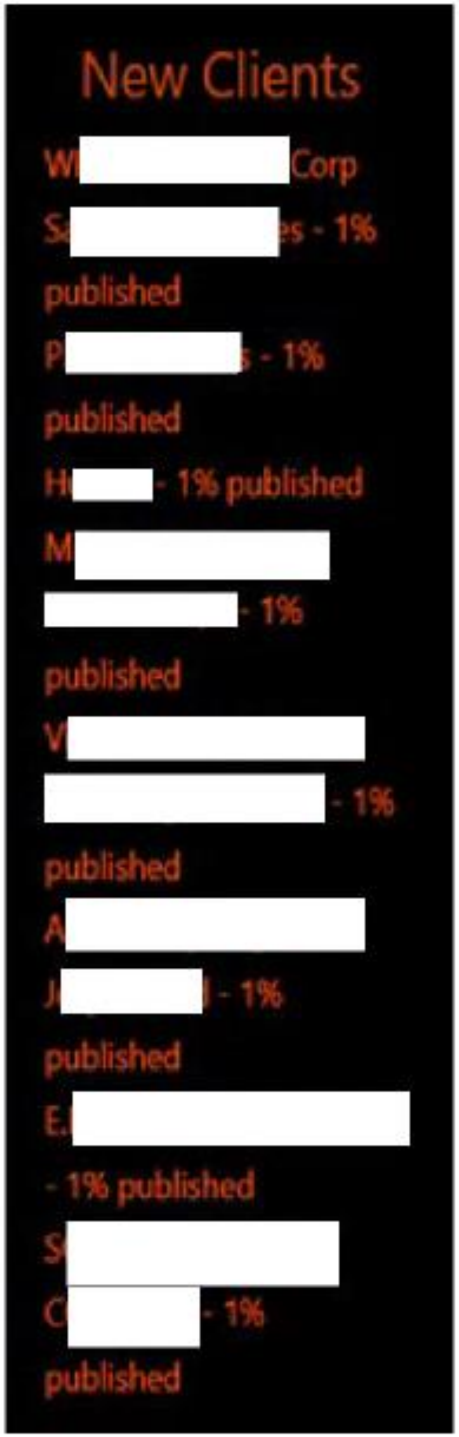
- Old Ransomware: Threat actor encrypts data and charges a ransom to give you the key. No data is taken.
- New Ransomware: Threat actor steals data AND encrypts data. Threat actor shows you stolen data and threatens to publish it or use it to cause further harm.
  - Breach response is required
  - May need to pay ransom even if you can restore completely from backup
- New Ransomware: “Ransomware as a service” makes it much easier for small actors
- Note - Paying ransom to entity on OFAC list is illegal – carrier may only reimburse after confirming legality of payment

Darkweb example of new Ransomware



Represented here companies do not wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news! P.S. We have the second domain: newsmaze.top.

To contact us use the feedback form of our news website.



New Clients

W[redacted] Corp

S[redacted]es - 1% published

P[redacted]s - 1% published

H[redacted] - 1% published

M[redacted]

[redacted] - 1% published

V[redacted]

[redacted] - 1% published

A[redacted]

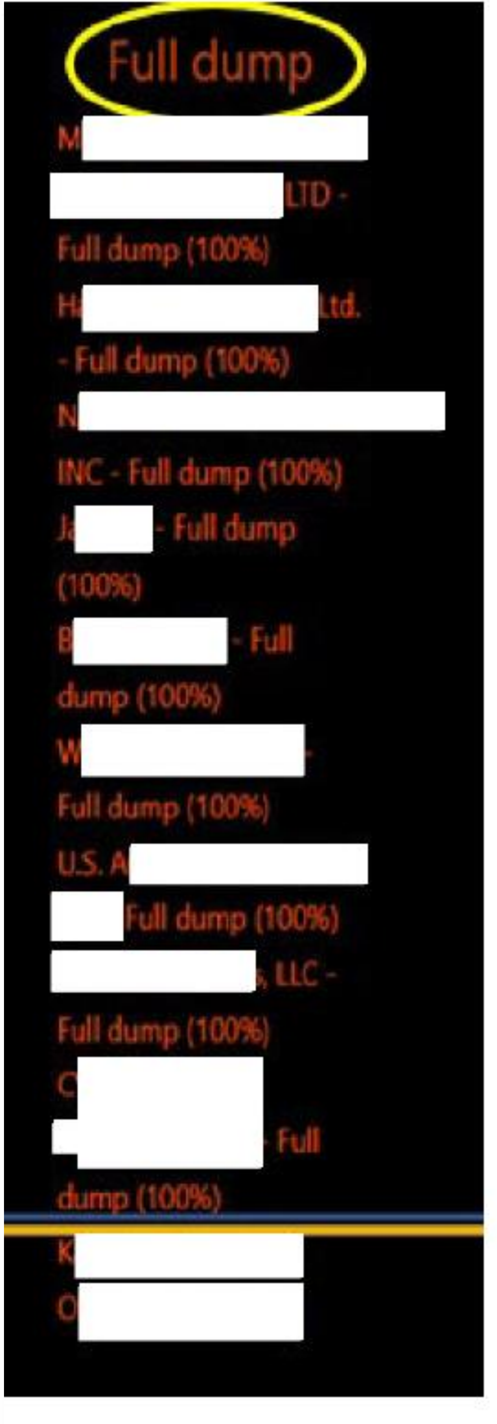
J[redacted] - 1% published

E.[redacted]

- 1% published

S[redacted]

C[redacted] - 1% published



Full dump

M[redacted]

[redacted] LTD - Full dump (100%)

H[redacted] Ltd. - Full dump (100%)

N[redacted]

INC - Full dump (100%)

J[redacted] - Full dump (100%)

B[redacted] - Full dump (100%)

W[redacted] - Full dump (100%)

U.S. A[redacted]

[redacted] Full dump (100%)

[redacted], LLC - Full dump (100%)

C[redacted] - Full dump (100%)

K[redacted]

O[redacted]

Threat actor steals data AND encrypts data. Threat actor shows you stolen data and threatens to publish it or use it to cause further harm.

If Hit with Ransomware – Cybercoverage Carrier Perspective

- Disconnect/Isolate Infected Computer from the Network
- Notify IT
- Notify Cybercoverage Carrier and follow instructions
  - Immediate access to forensic team
  - Immediate access to breach counsel
- Pre-negotiated rates for response services
- Resources available to purchase new equipment, meet breach notification obligations, meet legal obligations
- Secure Computer Logs
- Don't Panic
- Generally advised to not pay ransom

If Hit with Ransomware – Law Enforcement Perspective

- Disconnect/Isolate Infected Computer from the Network
- Notify IT
- If Utility – per HB 156 notify GEMA within 2 hours of detection. 1-800-TRY-GEMA; GEMA.Georgia.gov (Reports, Records not subject to public inspection)
- Report to IC3.gov – the FBI Internet Crime Complaint Center; Report to CISA.Gov
- Secure Computer Logs
- Don't Panic
- Advised to not pay ransom

Cybercrime - Prevention is King

- Law Enforcement can do very little due to international actors and sophistication of tools.
- Prevention/mitigation of harm is KING
  - Backup your data offsite & offline/Healthy backups
  - Multi-factor Authentication
  - Update Software
  - Incident Response Plan (That’s Practiced)
  - Cybersecurity Awareness Training for Staff with Fake Phishing attempts

Cybersecurity Measures Work

- Georgia city (3,000 – 6,000 population) avoids data loss after 3rd ransomware attack in one year
- Officials were successful in restoring city infrastructure because of data backups
- First 2 attacks were successful

Major Changes to Cyberliability Underwriting Due to Need for Prevention

- Basic measures required to get a quote that includes ransomware coverage. Even if city can secure coverage, coverage may be limited if sufficient security controls are not in place
  - Deductibles
  - Ransomware sub-limits
- Cyberliability questionnaires are far more detailed
- City will need IT expertise to complete questionnaire
- Review of answers by city attorney is recommended
- Inaccurate responses can cause denial of claims
- Cyberliability coverage is an ESSENTIAL source of expertise and protection for city assets
- *Per Lockton, actions marked with asterisk in “Your Leadership Needed” are required to get quote that includes ransomware coverage – Requirements are changing.

New GMA Cybersecurity Videos

Cybersecurity Threats: Your Leadership Needed - on the New GMA Website Cybersecurity Landing Page

Three Steps of “Your Leadership Needed”

1) Sound the alarm & champion investments in necessary protections; 2) Use skilled, knowledgeable people and the right materials; 3) do what is necessary to obtain and keep insurance for WHEN, not IF, you are attacked.

Cybersecurity Threats: Leadership Needed

- Step One. Champion and Invest in Cybersecurity –
  - learn about the urgency of immediate action to implement critical cybersecurity measures,
  - communicate that ARPA SLFRF money can be used for this purpose
  - charge and empower city leaders to take action,
  - request and review reports from city leaders about progress
- Note: New laws allow for Executive Session meetings about cybersecurity and exemption of cybersecurity related reports and portions of contracts from open records

Cybersecurity Threats: Leadership Needed

- Step Two. Engage a Skilled Cybersecurity Resource
  - Able to establish ongoing, automated security measures
  - Able to monitor the measures, respond immediately to incidents
  - Able to implement / manage “must have” cybersecurity measures
  - Able to receive, understand, and act on cyber alerts
- GMA recommends VC3 technology services
  - GMA recommends immediate free membership in MS-ISAC
  - GMA recommends contacting CISA to arrange for a free assessment and identification of free resources

Cybersecurity Threats: Leadership Needed

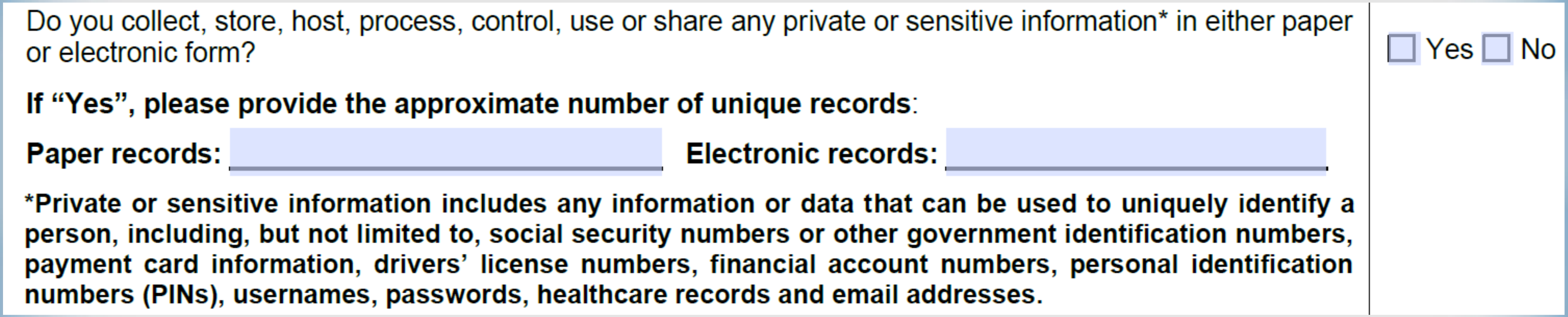
- Step Three. Obtain Appropriate Amount of Cyberliability Coverage that Includes Coverage for Ransomware (City must work with Skilled Security Resource to Complete Action Items to Get Coverage)

- Note: These Actions required to get coverage are the same basic cybersecurity measures recommended by the GBI, the FBI, and the Department of Homeland Security

Immediate Actions & Key Terms

- **Multifactor authentication** for remote access, email, and privileged accounts*
- **Endpoint detection & response on all endpoints** (hunts for and blocks malicious activity)*
- **Offline, offsite, current backups of critical data** are available, monitored, and tested to ensure data can be restored*
- **Administrative privileges are restricted** on all computers*
- **Administrative audit and mailbox logging** are enabled*
- **Protective DNS Service** in use*
- **Prompt security updates and patching** of operating systems, applications, and firmware
- **Remote access available only through VPN**
- **All Workers Complete Regular Security Awareness & Phishing Tests**
- **Documented Incident Response Plan* is regularly tested**
- **Sensitive Data is Identified and Encrypted at Rest and in Transmission**
- **3rd Party Regularly Conducts Penetration Test for Vulnerabilities**
- **Networks are Segmented as appropriate**
- **End-of-Life software removed or segregated from rest of network**

Sample Cyberliability Insurance Questionnaires



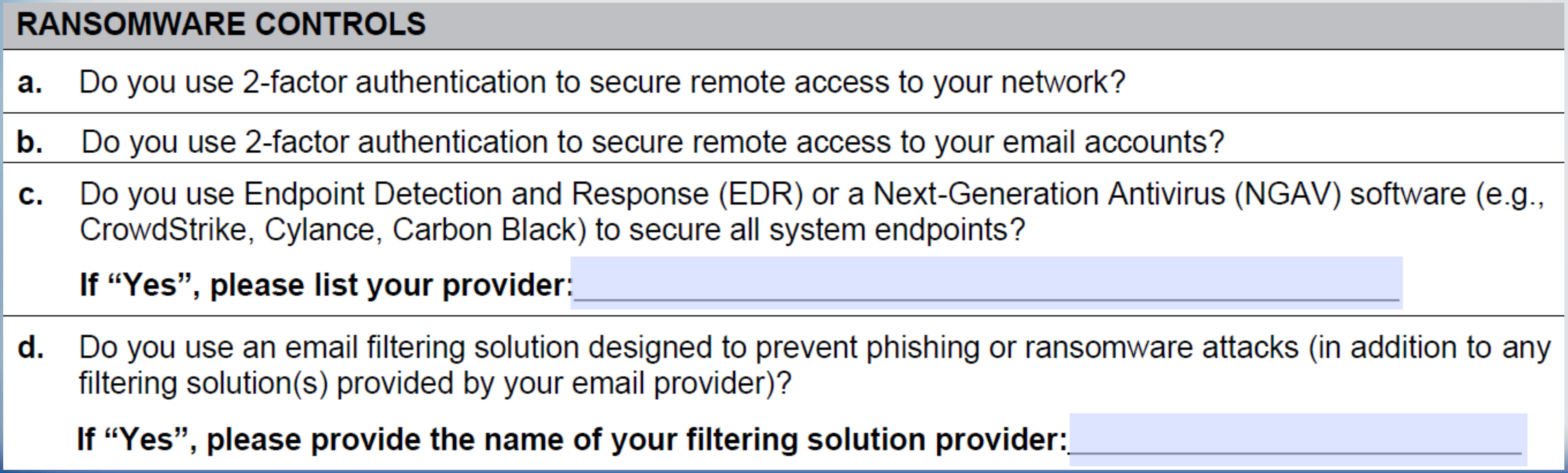
Do you collect, store, host, process, control, use or share any private or sensitive information* in either paper or electronic form?

□ Yes □ No

If "Yes", please provide the approximate number of unique records:

Paper records: **Electronic records:**

***Private or sensitive information includes any information or data that can be used to uniquely identify a person, including, but not limited to, social security numbers or other government identification numbers, payment card information, drivers' license numbers, financial account numbers, personal identification numbers (PINs), usernames, passwords, healthcare records and email addresses.**



RANSOMWARE CONTROLS

a. Do you use 2-factor authentication to secure remote access to your network?

b. Do you use 2-factor authentication to secure remote access to your email accounts?

c. Do you use Endpoint Detection and Response (EDR) or a Next-Generation Antivirus (NGAV) software (e.g., CrowdStrike, Cylance, Carbon Black) to secure all system endpoints?

If "Yes", please list your provider:

d. Do you use an email filtering solution designed to prevent phishing or ransomware attacks (in addition to any filtering solution(s) provided by your email provider)?

If "Yes", please provide the name of your filtering solution provider:

GMA Resources

- GIRMA - Cyber coverage included with property and liability coverage at no extra cost, but excess ransomware coverage is recommended
- GIRMA Crisis Management
- VC3 Information Technology Services
- *Cybersecurity Threats: Leadership Needed*
- GMA Website/Cybersecurity Minute

Learn More

- Webinar October 24, 2022 3:30 – 4:30 *Cyber Attacks = Perilous Waters: Resources to Guard Your City and Keep it On Course*
- Cybersecurity champions Dr. Arlene Beckles, Councilmember, City of Norcross and Gibb Cotton, Chief Technology Officer, City of Griffin, will describe why and how they are defending their cities. Learn about resources available to cities, including free federal resources, and how you can discuss cybersecurity vulnerabilities and plans in executive session, keep related documents private, take advantage of available resources, and follow the steps in GMA's *Cybersecurity Threats: Your Leadership Needed* to reduce the risk of cyberattack and minimize the harm when a cyberattack occurs.
- Representatives of MS-ISAC and CISA, two governmental organizations that provide free cybersecurity resources to cities, will participate in the discussion and answer questions.

Questions?

Alison Cline Earles

Senior Associate General Counsel

678-651-1028

aearles@gacities.com