

INFORMATION SECURITY BREACHES

Immediate Actions for
Prevention & Response;
Cyberliability Questionnaires

October 7, 2021/ARPA slides revised January 10, 2022

Introductions

What Keeps You Up at Night?

Disclaimer

- This webinar is for informational purposes only, and is not legal advice or a substitute for legal advice. It is designed for municipal employers in Georgia. This webinar reflects the presenters' understanding of certain requirements of cybercoverage carriers and of cybersecurity provisions related to ARPA as they existed on October 15, 2021.

Prevention AND Response

- Cannot ever fully prevent, so MUST prepare for response
- Cities must be prepared to respond to attack and be able to continue business
- Cybersecurity cannot be an afterthought, it is a CORE part of city business
- ARPA State and Local Fiscal Recovery Funds (SLFRF) are available for “modernization of cybersecurity, including hardware, software, and protection of critical infrastructure”
- ARPA SLFRF are available for cybersecurity investments in Water and Sewer Infrastructure and investments made in response to the pandemic or negative effects of the pandemic

“What We Urge You To Do Now”

- City leaders need to understand some cybersecurity basics to ensure proper investments in cybersecurity
- City leaders must champion **INCONVENIENT** security measures
- Determine whether ARPA SLFRF funds are available for cybersecurity
- Cities will be left without cyberliability coverage unless they take **IMMEDIATE ACTIONS**
- Let’s learn some basics of cybersecurity language

Agenda

- Examples of Breaches, Ransomware Focus
- Upcoming Changes to Cyberliability Underwriting
- Key Terms on Underwriting Questionnaires
- Immediate Actions for Cities
- Investing in Cybersecurity: ARPA SLFRF
- Breach Response: the role of the Cyberliability Carrier
- GMA Resources: GIRMA Cyberliability Coverage & IT in a Box

What could happen if . . .

- Malware corrupted or encrypted all City data AND City
 - Had no policies or procedures for restoring data from backup servers
 - Had no plans in place to continue city business
 - Had plans in place, but plans were out of date and never practiced

Six days after a ransomware cyberattack, Atlanta officials are filling out forms by hand

By Kimberly Hutcherson, CNN

🕒 Updated 3:00 PM ET, Wed March 28, 2018



Advertisement

City of Atlanta Ransomware Attack

- **8** emergency contracts between March 22 and April 2 - **\$2,667,328** for incident response, digital forensics, extra staffing, infrastructure consulting
- **\$50,000** for crisis communications services
- **\$600,000** for incident response consulting from Ernst & Young
- <https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/>



City Services Interrupted

- Warrant issuances
- Water requests
- New inmate processing
- Court fee payments
- Online bill-pay programs across many city departments
- <https://www.beckershospitalreview.com/cybersecurity/atlanta-s-ransomware-attack-may-cost-the-city-17m.html>

What could happen if . . .

- Bad press
- Loss of trust
- Loss of information systems and disruption of business
- Legal fees
- Costs of investigations
- Cost of breach response
- Employment lawsuits
- Misuse of incident for political gain
- Oversight by outside parties
- Removal of leadership
- Invasion of privacy lawsuits
- Open records requests
- Disruption of election/loss of confidence in election results

Cyberattacks are a threat to the City's Core Business. . .

- “[Organizations] that view ransomware as a threat to their core business operations rather than a simple risk of data theft will react and recover more effectively.”
- “The threats are serious and they are increasing. We urge you to take these critical steps to protect your organizations and the American public.”
- - June 2, 2021 Memo to U.S. Businesses from Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technology “What We Urge You To Do To Protect Against The Threat of Ransomware”

Cyberattacks can be 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>
- 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

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

Major Changes to Cyberliability Underwriting

- Per Lockton:
- Minimum security standards will need to be evidenced to secure a quote. Those controls include:
 - Confirm that multifactor authentication is in place for all email, privileged accounts, and remote connections
 - Confirm the deployment of smart endpoint detection and response
 - Demonstrate effective backup air gapping and segregation (at any time, a copy of critical data is offline & offsite)

Major Changes to Cyberliability Underwriting

- 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

What do Cyber Policies Cover?



Security and
Privacy Liability
Insurance



Event Management
Insurance



Cyber Extortion
Insurance

Security and Privacy Liability Insurance

Provides coverage for Loss incurred as a result of a **Security Failure or Privacy Event**.

- **Privacy Event:** Failure to protect confidential information (by social engineering, phishing, or otherwise) that could result in identity theft.
- **Security Failure:** Failure or violation of security of a computer system.

Event Management Insurance

- Covers **Loss** insured incurs as a result of Security Failure or Privacy Event.
- Loss: expenses and costs
 - Investigation
 - PR Firm
 - To notify victims of the Security Failure or Privacy Event whose confidential information is the subject of the event.
 - To restore, recreate, or recollect electronic data or determine if this is not possible.

Cyber Extortion Insurance

- Covers Loss an insured incurs solely as a result of a **Security Threat** or **Privacy Threat**.
 - Privacy Threat: Threat or series of threats to unlawfully or publicly disclose confidential information for the purpose of demanding money, securities, or tangible property.
 - Security Threat: Threat or series of threats to commit an intentional attack against a computer system for the purpose of demanding money, securities, or tangible property.
 - Loss:
 - Money paid to end the threat (restrictions may apply - illegal payment to entity on OFAC list may not be covered).
 - Costs to conduct investigation.

Common Policy Features


Shared limit of liability between coverages.



Expenses erode the limit.



Loss must be reported “as soon as practicable.”
(Translation: **Now!**)



Costs should be incurred only with carrier approval.

Practical Advice

When claim is discovered, immediately report directly to carrier with copy to broker and to normal reporting mechanism.

Example: For GIRMA Members, report to AIG, Lockton, and Gallagher Bassett.

Claims should be reported as soon as discovered.

Vendors should only be used from carrier's approved panel.

Immediate Actions & Key Terms

- **Multifactor authentication** (because passwords alone are routinely compromised) – especially for remote access, email, and privileged accounts
- **Endpoint detection & response** (to hunt for malicious activity on a network and block it)
- **User Training & Phishing Tests**
- **Encryption** (so if data is stolen, it is unusable)
- **A skilled, empowered security team** (to patch rapidly, and share and incorporate threat information in your defenses).
- **Backup** your data, system images, and configurations, regularly test them, and keep the backups offline (and offsite).
- **Update and patch** systems promptly: This includes maintaining the security of operating systems, applications, and firmware, in a timely manner. Consider using a centralized patch management system.
- **Test Incident Response** – test your incident response plan
- **Penetration Test** - Use a 3rd party pen tester to test the security of your systems and your ability to defend against a sophisticated attack.
- **Segment Networks**

Cities Need to Get Ready for 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: _____

Cities Need to Get Ready for Cyberliability Insurance Questionnaires

End Point Security

17. Please indicate below the endpoint (*PC's, laptops, Smartphones, tablets, etc.*) security controls your Company is using:

- Password/passcode protected
- Encryption
- Firewalls enabled/turned on
- Traditional antivirus products on all endpoints
- Next generation antivirus on all endpoints

18. Who is primarily responsible for patching end points?

- A managed services provider
- The Company's IT department
- The user/employee

Email Security

19. Do you use Sender Policy Framework (SPF)?

20. How often is phishing training conducted to all staff:

- Never
- I don't know
- Semiannually
- Annually

21. Do you use an email filtering tool to detect and/or block SPAM, malicious links, and attachments?

22. Do you require multifactor authentication (MFA) to access email?

Cities Need to Get Ready for Cyberliability Insurance Questionnaires

Who monitors the Company's networks for intrusions or other unusual activity (*select one*)?

- Nobody/we do not monitor
- Somebody in the Company's IT department
- A third party/managed security provider
- Somebody in the Company's IT department AND a third party/managed security provider

Are your firewalls configured according to the principles of least privileges?

Do you regularly review firewall rules and alerts?

Is multi-factor authentication required to remotely connect to the network?

When did the Company last have a comprehensive (*i.e. inclusive of vulnerability scanning and penetration test*) network security assessment conducted by a third party (*select one*)?

- Last 6 months
- Last 18 months
- Last 36 months
- Never

Does the Company maintain a formal program for evaluating the security posture of its vendors?

Cities Need to Get Ready for Cyberliability Insurance Questionnaires

Back-Up Security

30. Do you back up all mission critical systems and data?

If yes, please provide the following:

How Frequently do you back up? Daily/nightly Weekly Less frequently then weekly

Which of the following back-up solutions do you employ?

Local Network drives Tapes/disks Off-site Cloud

Which of the above are encrypted?

Local Network drives Tapes/disks Off-site Cloud

How quickly can you restore from back-ups? Same day 24-48 hours Longer

How frequently do you test your ability to restore from back ups?

Never Quarterly Semi-annually Annually

Cities Need to Get Ready for Cyberliability Insurance Questionnaires

Social Engineering

14. Indicate which of the following controls you have implemented with respect to electronic funds transfers:

- Callback procedures to verify funds transfer requests or changes to banking information
- Dual authorization for funds transfers greater than \$2,500
- Other (*please describe*) _____

City of Atlanta Ransomware Attack

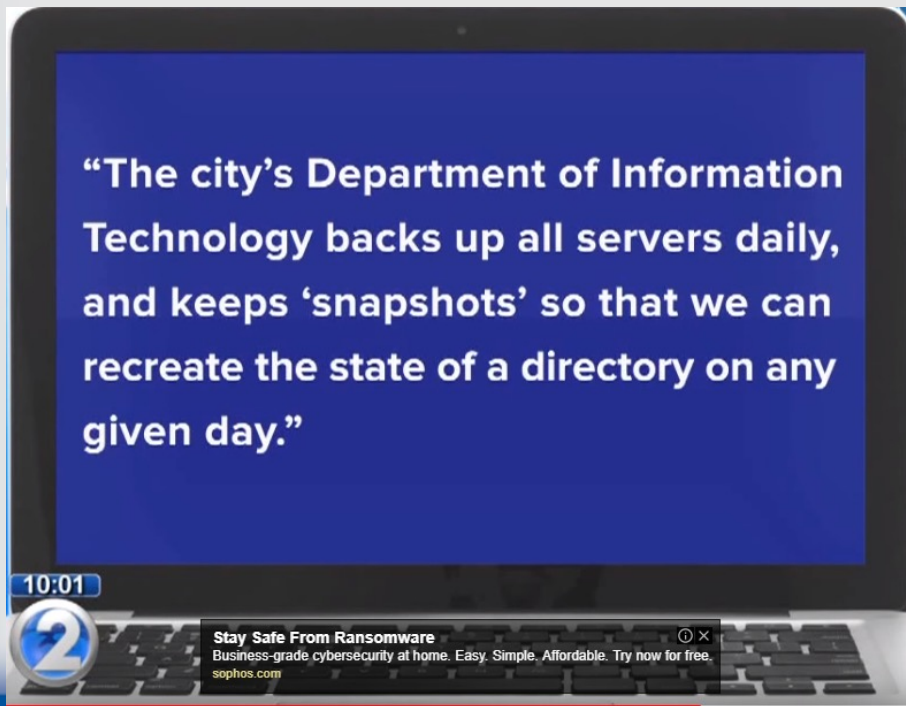
- "vulnerabilities identified . . . existed for so long the organizations responsible have essentially become complacent and no longer take action."
- "departments . . . do not have enough time or tools to properly analyze and treat the systems."

<https://www.cbsnews.com/news/atlanta-warned-cyber-vulnerabilities-audit-shows/>



Power of Good Backup

- Honolulu Fire Dept. – no ransom, files backed up, up and running swiftly (September, 2016)
- <https://www.youtube.com/watch?v=b9d4sXENACs>



Power of Good Backup – Mark Wong, Honolulu Director of IT

He said that about two years ago the city foresaw ransomware being a problem and invested in a replication storage system that backs up servers daily and creates “snapshots” that can re-create a directory from any given day.

“The foresight of this investment is now paying huge dividends,” he said.

<https://www.govtech.com/em/safety/Ransomware-Virus-Infests-Department.html>

Prevention – Training Staff

- Phishing
- Run test campaigns to see who “takes the bait,” conduct training.
- Assume repeat “victims” will fall prey in real life and develop strategies
- Require staff to report phishing attempts
- Pretexting
- Provide role-specific training to Human Resources, Finance staff, and other users who will be targets based on privileges or access to data.

Prevention – Training on Social Attacks

- Phishing (most common)
- Attacker tries to get recipient of email, text, to “take the bait” by clicking on a link or opening an attachment
- Link goes to location that requests username and password or opens malware
- Malware leads to data corruption/loss
- Pretexting
- Attacker impersonates organization leader (CEO, other executive) and requests valuable information
- Malware not involved
- Targets: Human Resources, Finance Staff

Verizon Report 2018, p. 11

Role of Cyberliability Carrier in Breach Response

- Immediate access to expertise
- Forensic teams to determine what data was compromised; breach response attorneys to determine legal obligations for notification and reporting; assistance to help city pay ransom if it chooses to do so; Call center and crisis response services; identity theft tools; assistance with required notifications
- No need for emergency contracting

Actions for Breach Response

- Make sure incident response procedure is up to date and reviewed by city attorney to ensure compliance with applicable laws
- Make sure you understand your role (if any) in incident response communication (prepared communications should be part of the plan)

City Leaders Must Champion Immediate Actions



City Leaders Must Champion Immediate Actions

- Each city leader can champion for investments in cybersecurity (staffing, tools, training) in his or her own field of influence – ARPA SLFRF may be available!
- Security is INCONVENIENT – consistently message the importance of training, MFA, etc.
- Baltimore – council member unable to persuade:
 - “. . . in his previous role as councilman he tried to convince the Pugh administration to make cybersecurity a higher priority, to no avail.”
- <https://www.usatoday.com/story/news/nation/2019/05/24/hackers-hit-vulnerable-cities-like-baltimore-ransomware-attacks/1211611001/>

City Leaders Must Champion Immediate Actions

- Janne Lindqvist, assistant professor of electrical and computer engineering at Rutgers University:
“government officials often think of securing computer systems as an added cost, not an inherent part of their duty to protect residents.” “A general problem, and not just for cities, is that no one wants to pay for security, and nobody knows what security looks like.”
- Lindqvist said **proper protection would involve backing up all the systems and deploying a strategy for bringing them back online after an attack.** That’s not a cheap endeavor.

ARPA SLFRF – Revenue Replacement

- ARPA SLFRF money may be used for government services, including “modernization of cybersecurity, including hardware, software, and protection of critical infrastructure” ***up to the amount of revenue lost due to COVID.*** (Appendix 1, eligible use category 6.0 Revenue Replacement; 6.1 Government Services)
- **Final Rule: city may elect “standard” revenue loss of \$10 million.**
- **This is the EASIEST and most CLEAR-CUT way to spend ARPA funds on cybersecurity**

ARPA SLFRF – Technology Infrastructure

- The Final Rule enumerates “technology infrastructure” as an eligible use under the “Effective Service Delivery” Category:
- “Technology infrastructure resources to improve access to and the user-experience of government information technology systems, including upgrades to hardware and software as well as improvements to public-facing websites or to data management systems, to increase public access and improve public delivery of government programs and services (including in the judicial legislative, or executive branches.)” Final Rule p. 188

ARPA SLFRF – Capital Expenditures on Technology Infrastructure Due to Pandemic

- The Final Rule enumerates capital expenditures on “technology infrastructure” as an eligible use under the Administrative Needs Caused or Exacerbated by the Pandemic Category:
- [Treasury] is clarifying that capital expenditures such as technology infrastructure to adapt government operations to the pandemic (e.g., video-conferencing software, improvements to case management systems or data sharing resources) . . . are eligible.” Final Rule p. 190
- If spending more than \$1 million on capital expenditures, a written justification is required.

ARPA SLFRF – Capital Expenditures on Technology Infrastructure

- Examples of Capital Expenditures:
 - Firewall Equipment;
 - Wireless infrastructure equipment;
 - Computers, Servers;
 - Software licenses that are NOT subscription based
- Examples of Operational Expenditures:
 - Penetration Testing
 - Cloud-based data storage
 - Cloud-based backup services
 - Firewall monitoring services
 - Security Awareness and phish testing service subscription

ARPA SLFRF – Water & Sewer

- Consistent with DWSRF and CWSRF, ARPA SLFRF money may be used for cybersecurity needs related to water and sewer infrastructure. Final Rule P. 272. The EPA has published lists of cybersecurity actions to protect water and sewer infrastructure.
- It is likely that the eligible use category would be Appendix 1, eligible use category 5.15
Drinking water: Other water infrastructure or 5.5
Clean Water: Other Sewer Infrastructure

ARPA – Water & Sewer Infrastructure Cybersecurity

- “. . . consistent with the . . . DWSRF, Fiscal Recovery Funds may be used for cybersecurity needs to protect water or sewer infrastructure, such as developing effective cybersecurity practices and measures at drinking water systems and publicly owned treatment works.” Interim Final Rule, p. 60; Final Rule, p. 272.
- DWSRF Eligibility Handbook describes cybersecurity assessments, and cybersecurity effective practices or measures as eligible expenses: “Security inspections and exercises (including physical infrastructure and cybersecurity assessments)” p. 31 “Develop cybersecurity effective practices or measures” p. 33
- [EPA water security guide for states](#) lists specific cybersecurity steps to protect water and sewer infrastructure
- [EPA Incident Action checklist](#) also lists specific actions utilities must take: “As with any critical enterprise or corporation, drinking water and wastewater utilities must evaluate and mitigate their vulnerability to a cyber incident and minimize impacts in the event of a successful attack.”

Information Privacy/Security Incident Response

- Written process for information privacy or security incident reporting and response
- Staff and vendors to report incidents to specified individual or email
- Designated incident response team (might include city attorney, IT support vendor)

Information Privacy/Security Incident Response

- Written process for information privacy or security incident reporting and response
- Staff and vendors to report incidents to specified individual or email
- Designated incident response team (might include city attorney, IT support vendor)

GMA Resources

- GIRMA Cyber coverage
- GIRMA Crisis Management
- IT in a Box

Immediate Actions & Key Terms

- **Multifactor authentication [IT in a Box – all levels]**
- **Endpoint detection & response [IT in a Box – all levels, IT in a Box installs and monitors]**
- **User Training & Phishing Tests**
- **Encryption**
- **A skilled, empowered security team [IT in a Box]**
- **Backup** your data, system images, and configurations, regularly test them, and keep the backups offline (and offsite) – **[IT in a Box Gold and Add-On]**
- **Update and patch** systems promptly **[IT in a Box all levels]**
- **Test Incident Response Policy [IT in a Box Gold includes policy help]**
- **Penetration Test**
- **Segment Networks [IT in a Box can help]**

Questions?

Alison Cline Earles

Senior Associate
General Counsel,
CIPP/US

Georgia Municipal
Association

aeearles AT symbol
gacities.com

678-651-1028

James Westbury

Claim Manager &
Coverage Counsel,
Georgia Municipal
Association

jwestbury AT symbol
gacities.com

404-640-3003