GEORGIA
MUNICIPAL
ASSOCIATION

1785

Carl Vinson
Institute of Government
UNIVERSITY OF GEORGIA

The Harold F. Holtz Municipal Training Institute

GEORGIA MUNICIPAL ASSOCIATION

Carl Vinson Institute of Government
UNIVERSITY OF GEORGIA

The Harold F. Holtz
Municipal Training Institute

INFORMATION PRIVACY AND SECURITY BREACHES

Prevention and Response

GMA Cities United Summit 2024

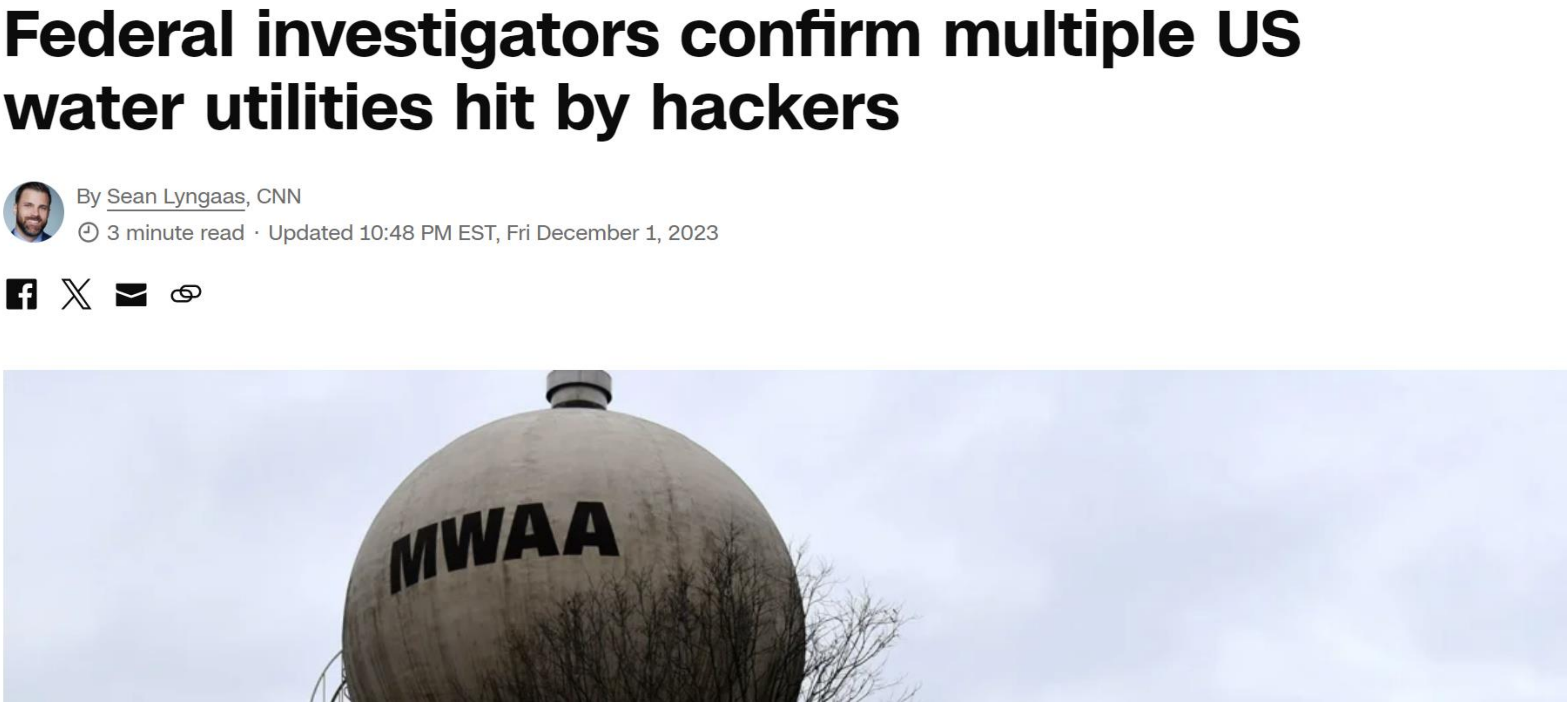
GEORGIA
MUNICIPAL
ASSOCIATION

Carl Vinson
Institute of Government
UNIVERSITY OF GEORGIA

The Harold F. Holtz
Municipal Training Institute

INTRODUCTIONS

What keeps you up at night?



Federal investigators confirm multiple US water utilities hit by hackers

By Sean Lyngaas, CNN

3 minute read · Updated 10:48 PM EST, Fri December 1, 2023

Now is the Time.

“Shields Up” – Nationwide alert.
ARPA SLFRF – Funding is Available.

Water Cities, Electric, Gas Cities – Additional Vulnerabilities but SAME ACTIONS required for all cities

March 1, 2022 – Statement by President Biden (Shields Up)

This is a critical moment to accelerate our work to improve domestic cybersecurity and bolster our national resilience. I have previously warned about the potential that Russia could conduct malicious cyber activity against the United States, including as a response to the unprecedented economic costs we've imposed on Russia alongside our allies and partners. It's part of Russia's playbook. Today, my Administration is reiterating those warnings based on evolving intelligence that the Russian Government is exploring options for potential cyberattacks.

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 broadly available for government services, including “modernization of cybersecurity, including hardware, software, and protection of critical infrastructure”
- ARPA SLFRF are available for cybersecurity investments in Water and Sewer Infrastructure and certain technology infrastructure investments associated with the pandemic or negative economic effects of the pandemic

“What We Urge You To Do Now”

City leaders must champion INCONVENIENT security measures, including critical IMMEDIATE ACTIONS required to obtain cyber coverage as well as longer term actions - inventory of data, identification of applicable laws, and policies and procedures

ARPA SLFRF funds are available for cybersecurity

Cities will be left without cyberliability coverage unless they take IMMEDIATE ACTIONS

A Word from GMA’s Executive Director and CEO

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

How do you serve as a Cybersecurity Champion?

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 for outsourced services

- GMA recommends contacting Kyle Bryans of MS-ISAC and immediate free membership in MS-ISAC
- GMA recommends contacting Stanton Gatewood of CISA to arrange for a free assessment

How Cities Can Obtain Additional No-Cost Skilled Resources

- CISA Assessments and Services
- MS-ISAC Services
- Still need a skilled IT resource! These are not substitutes!

GMA Cybersecurity: 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

DID YOU KNOW?

- The average data breach cost is expected to reach $5 million in 2023.

Source: http://www.tradearabia.com/news/IT_405446.html#:~:text=Threats%20from%20phishing%20and%20malicious,global%20leader%20in%20cyber%20protection

What could happen if . . .

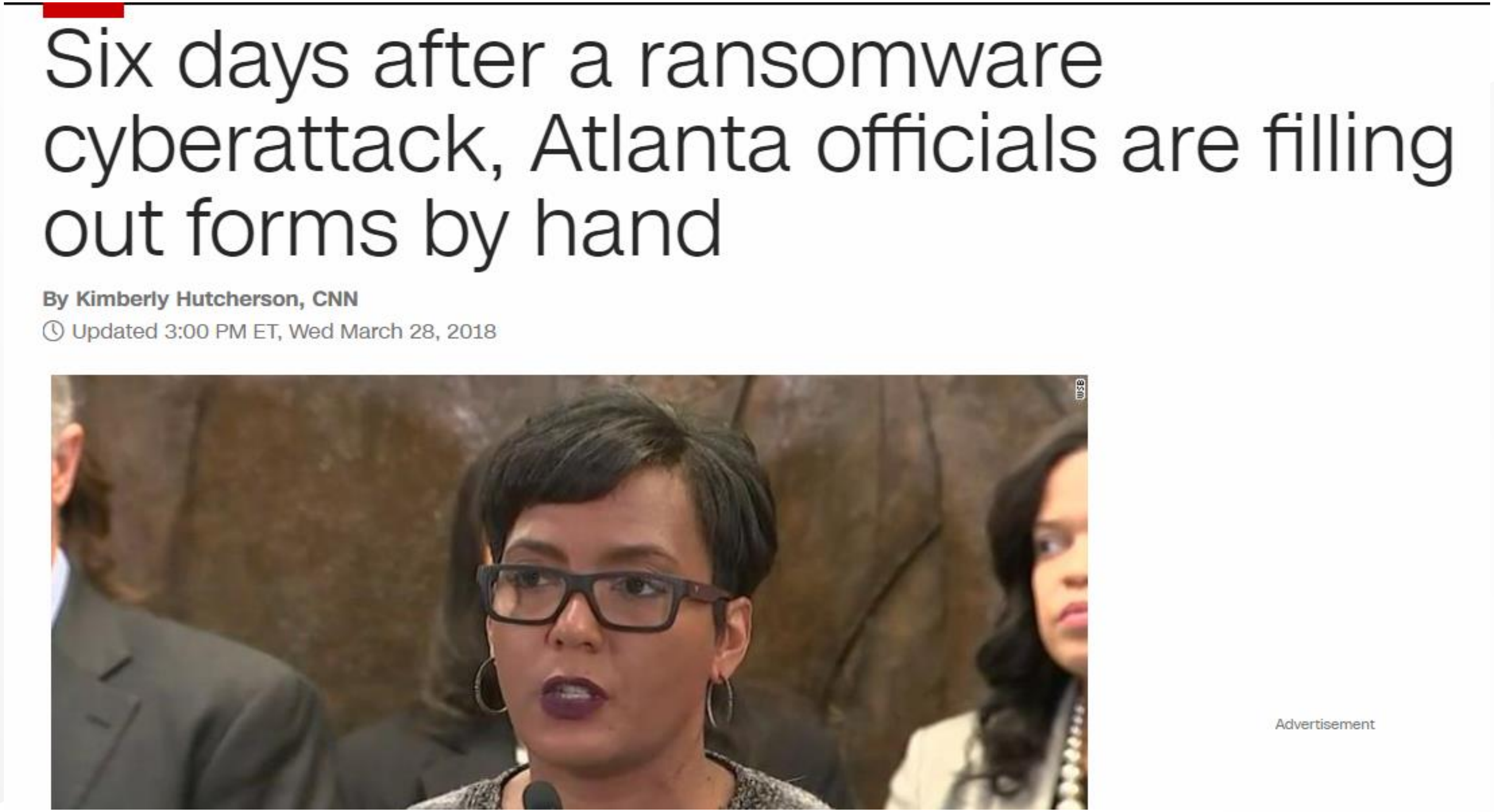
Malware corrupted or encrypted all City data AND City

- 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

DID YOU KNOW?

- 300,000 thousand new pieces of malware are created daily.

Source: https://techjury.net/blog/how-many-cyber-attacks-per-day/



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

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

What could happen if . . .

In addition, if city has or might have a HIPAA healthcare component:

- Penalties imposed by Department of Health and Human Services Office for Civil Rights
- Ongoing monitoring by HHS

In addition, if city accepts payment cards:

- Increased compliance obligations in order to keep taking the cards
- Liability for fraudulent transactions (card present)
- Worst case – loss of ability to accept the cards

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

- “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

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

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, as of May, 2023 actions marked with asterisk are required to get quote that includes ransomware coverage – Requirements are changing.

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

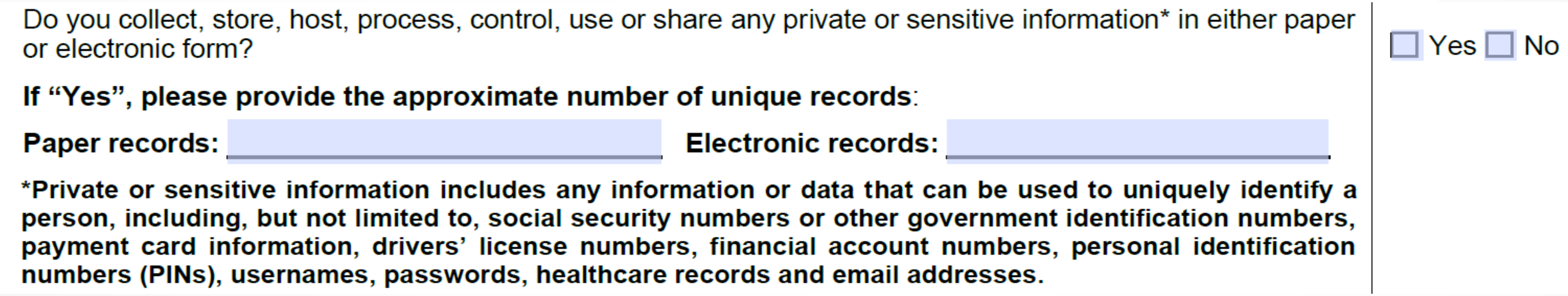
Sensitive Data is Identified and Encrypted at Rest and in Transmission

3rd Party Regularly Conducts Penetration Test for Vulnerabilities

Networks are Segmented as appropriate

End-of-Life software removed or segregated from rest of network

Cities Need to Get Ready for Cyberliability Insurance Questionnaires

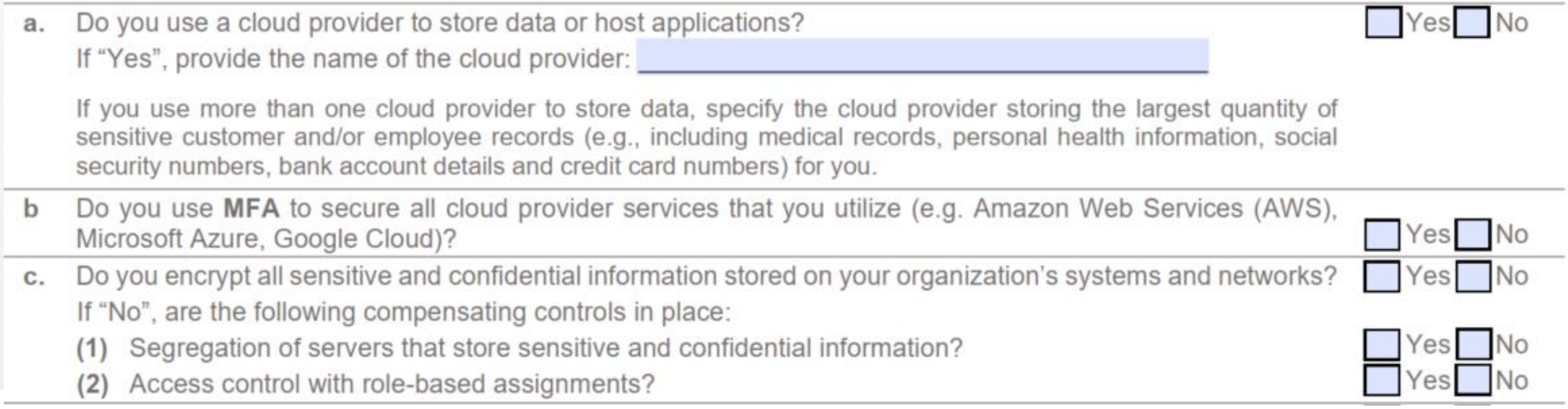


Do you collect, store, host, process, control, use or share any private or sensitive information* in either paper or electronic form? □ Yes □ No

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.**



a. Do you use a cloud provider to store data or host applications? □ Yes □ No

If "Yes", provide the name of the cloud provider: ____________________

If you use more than one cloud provider to store data, specify the cloud provider storing the largest quantity of sensitive customer and/or employee records (e.g., including medical records, personal health information, social security numbers, bank account details and credit card numbers) for you.

b Do you use **MFA** to secure all cloud provider services that you utilize (e.g. Amazon Web Services (AWS), Microsoft Azure, Google Cloud)? □ Yes □ No

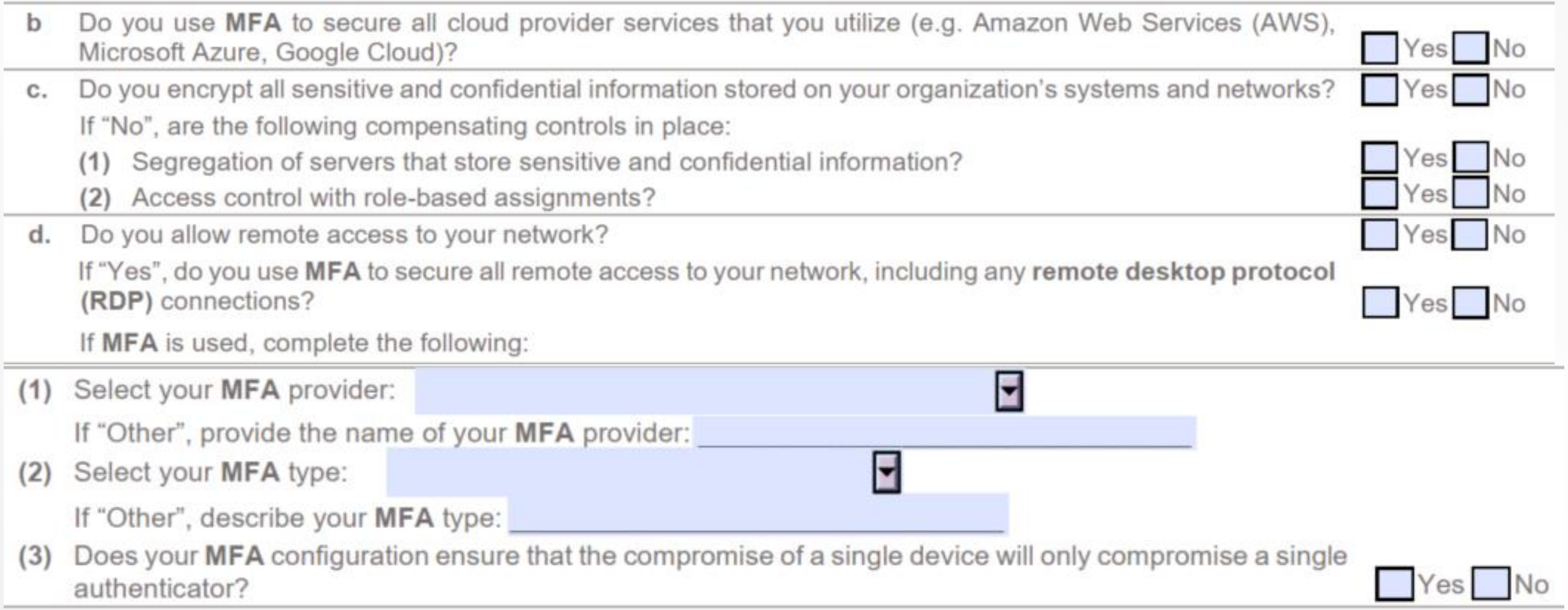
c. Do you encrypt all sensitive and confidential information stored on your organization's systems and networks? □ Yes □ No

If "No", are the following compensating controls in place:

(1) Segregation of servers that store sensitive and confidential information? □ Yes □ No

(2) Access control with role-based assignments? □ Yes □ No

Cities Need to Get Ready for Cyberliability Insurance Questionnaires



b Do you use **MFA** to secure all cloud provider services that you utilize (e.g. Amazon Web Services (AWS), Microsoft Azure, Google Cloud)? □ Yes □ No

c. Do you encrypt all sensitive and confidential information stored on your organization's systems and networks? □ Yes □ No

If "No", are the following compensating controls in place:

(1) Segregation of servers that store sensitive and confidential information? □ Yes □ No

(2) Access control with role-based assignments? □ Yes □ No

d. Do you allow remote access to your network? □ Yes □ No

If "Yes", do you use **MFA** to secure all remote access to your network, including any **remote desktop protocol (RDP)** connections? □ Yes □ No

If **MFA** is used, complete the following:

(1) Select your **MFA** provider: ▼

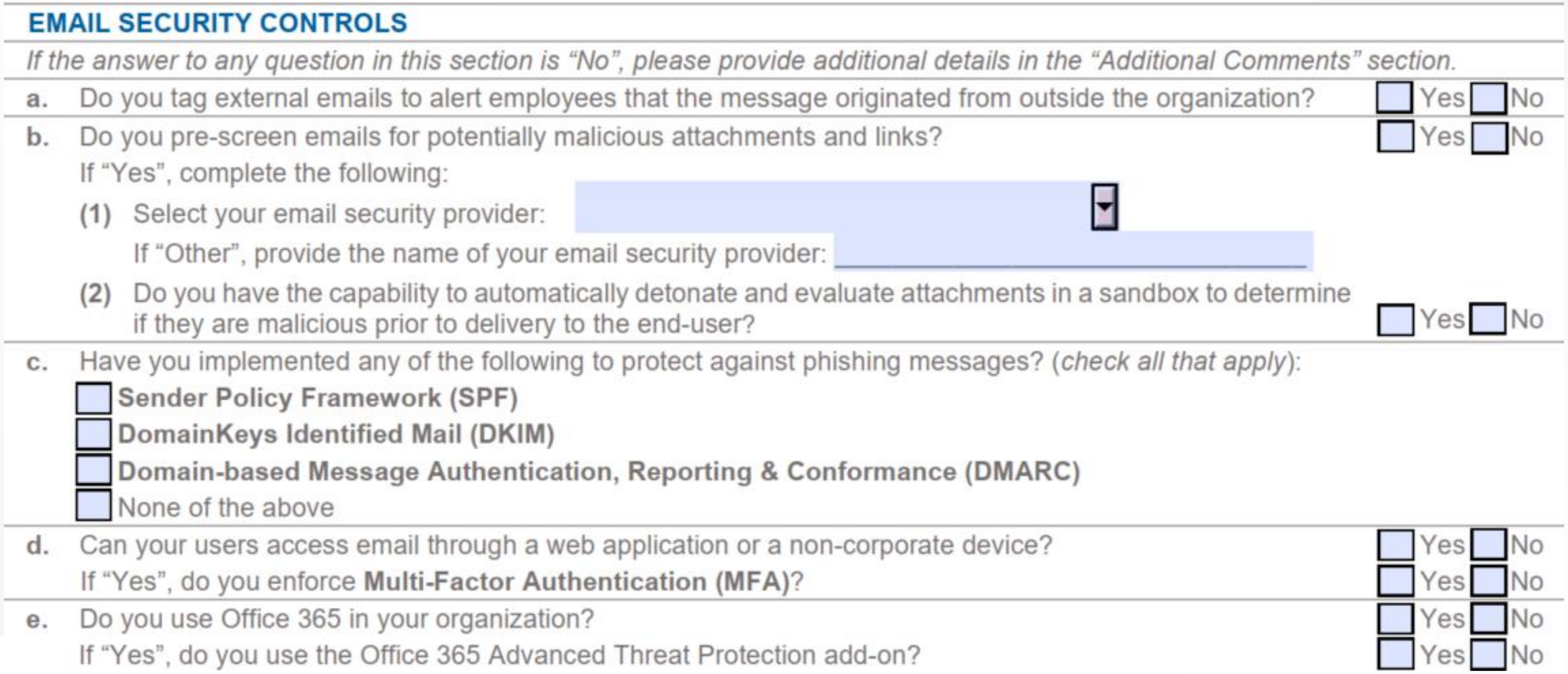
If "Other", provide the name of your **MFA** provider: ______________________

(2) Select your **MFA** type: ▼

If "Other", describe your **MFA** type: ______________________

(3) Does your **MFA** configuration ensure that the compromise of a single device will only compromise a single authenticator? □ Yes □ No

Cities Need to Get Ready for Cyberliability Insurance Questionnaires



EMAIL SECURITY CONTROLS

If the answer to any question in this section is "No", please provide additional details in the "Additional Comments" section.

a. Do you tag external emails to alert employees that the message originated from outside the organization? □ Yes □ No

b. Do you pre-screen emails for potentially malicious attachments and links? □ Yes □ No

If "Yes", complete the following:

(1) Select your email security provider:

If "Other", provide the name of your email security provider: ____________________

(2) Do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if they are malicious prior to delivery to the end-user? □ Yes □ No

c. Have you implemented any of the following to protect against phishing messages? (*check all that apply*):

□ **Sender Policy Framework (SPF)**

□ **DomainKeys Identified Mail (DKIM)**

□ **Domain-based Message Authentication, Reporting & Conformance (DMARC)**

□ None of the above

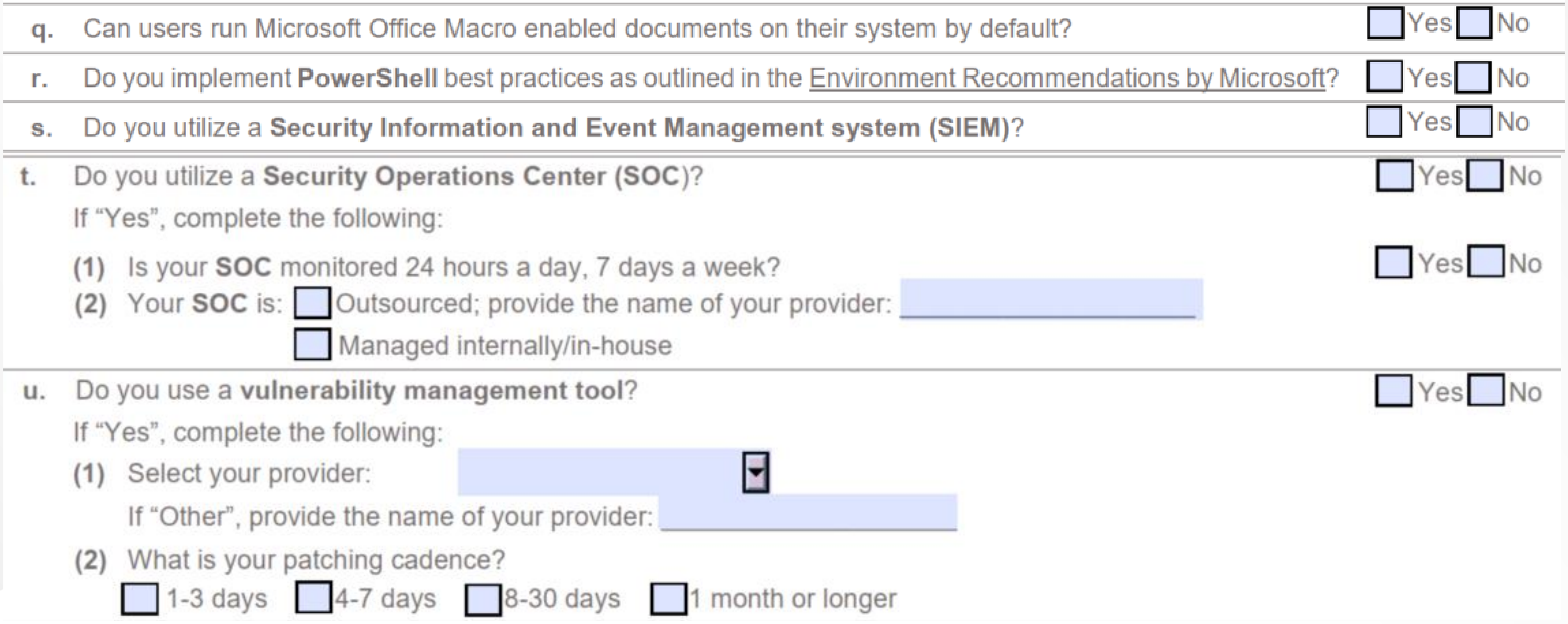
d. Can your users access email through a web application or a non-corporate device? □ Yes □ No

If "Yes", do you enforce **Multi-Factor Authentication (MFA)**? □ Yes □ No

e. Do you use Office 365 in your organization? □ Yes □ No

If "Yes", do you use the Office 365 Advanced Threat Protection add-on? □ Yes □ No

Cities Need to Get Ready for Cyberliability Insurance Questionnaires



q. Can users run Microsoft Office Macro enabled documents on their system by default? □ Yes □ No

r. Do you implement **PowerShell** best practices as outlined in the Environment Recommendations by Microsoft? □ Yes □ No

s. Do you utilize a **Security Information and Event Management system (SIEM)**? □ Yes □ No

t. Do you utilize a **Security Operations Center (SOC)**? □ Yes □ No

If "Yes", complete the following:

(1) Is your **SOC** monitored 24 hours a day, 7 days a week? □ Yes □ No

(2) Your **SOC** is: □ Outsourced; provide the name of your provider: ____________

□ Managed internally/in-house

u. Do you use a **vulnerability management tool**? □ Yes □ No

If "Yes", complete the following:

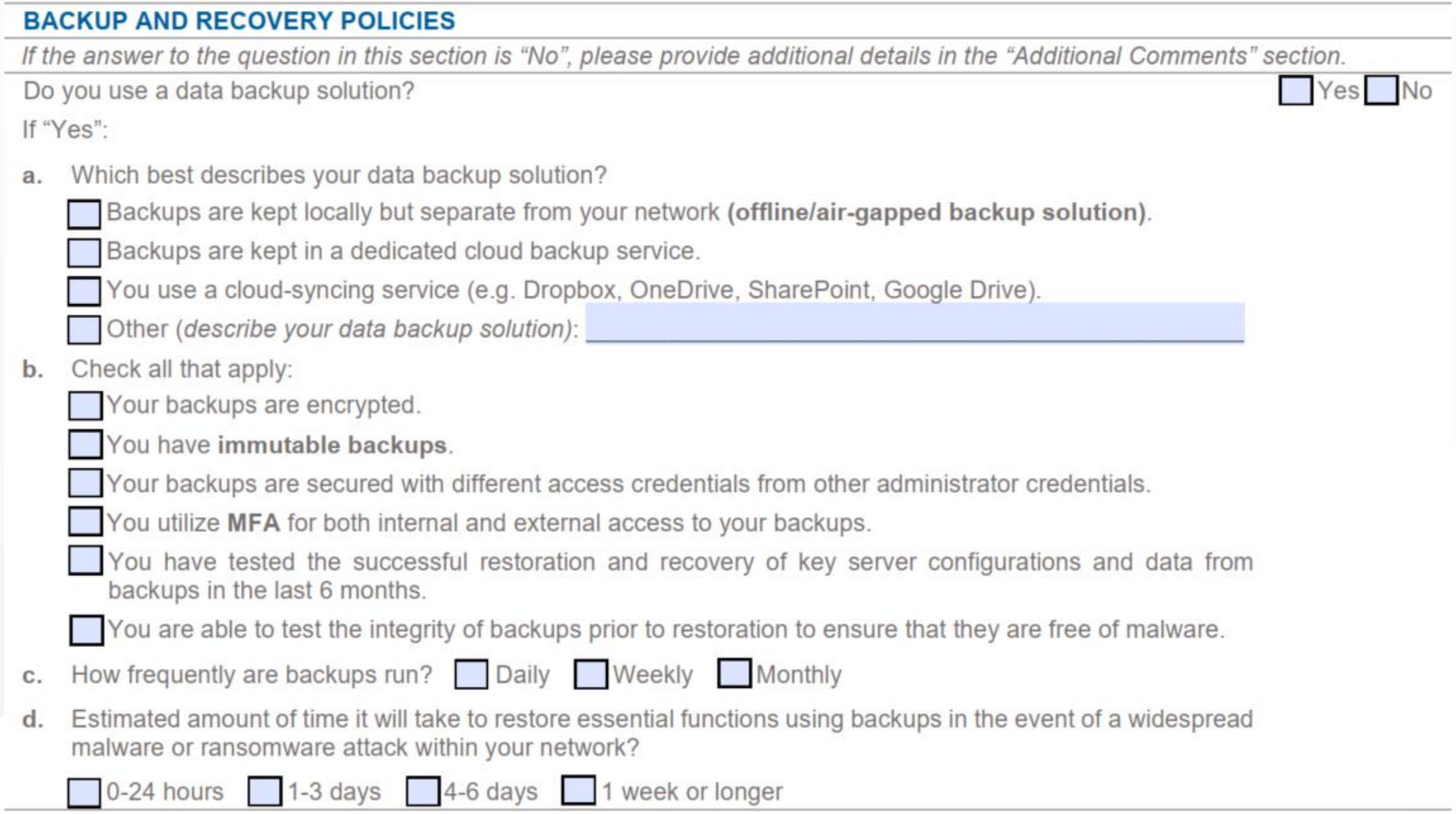
(1) Select your provider: ____________

If "Other", provide the name of your provider: ____________

(2) What is your patching cadence?

□ 1-3 days □ 4-7 days □ 8-30 days □ 1 month or longer

Cities Need to Get Ready for Cyberliability Insurance Questionnaires



BACKUP AND RECOVERY POLICIES

If the answer to the question in this section is "No", please provide additional details in the "Additional Comments" section.

Do you use a data backup solution? □ Yes □ No

If "Yes":

a. Which best describes your data backup solution?

□ Backups are kept locally but separate from your network **(offline/air-gapped backup solution)**.

□ Backups are kept in a dedicated cloud backup service.

□ You use a cloud-syncing service (e.g. Dropbox, OneDrive, SharePoint, Google Drive).

□ Other (*describe your data backup solution*): ____________________

b. Check all that apply:

□ Your backups are encrypted.

□ You have **immutable backups**.

□ Your backups are secured with different access credentials from other administrator credentials.

□ You utilize **MFA** for both internal and external access to your backups.

□ You have tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months.

□ You are able to test the integrity of backups prior to restoration to ensure that they are free of malware.

c. How frequently are backups run? □ Daily □ Weekly □ Monthly

d. Estimated amount of time it will take to restore essential functions using backups in the event of a widespread malware or ransomware attack within your network?

□ 0-24 hours □ 1-3 days □ 4-6 days □ 1 week or longer

City of Atlanta Ransomware Attack

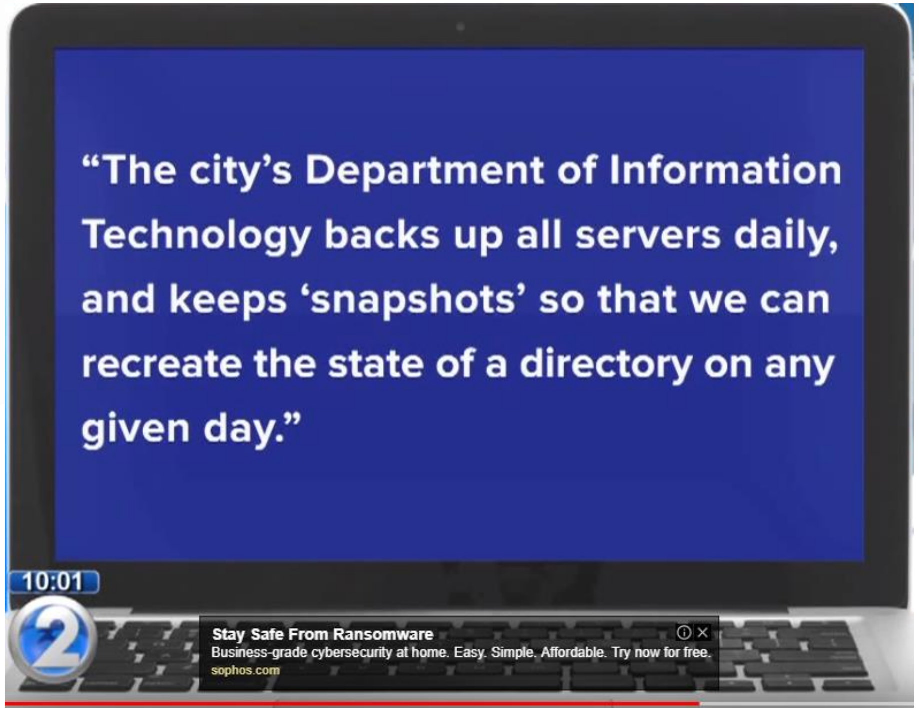
- "vulnerabilities identified . . . existed for so long the organizations responsible have essentially become complacent and no longer take action."
- "departments . . .do not have enough time or tools to properly analyze and treat the systems.“

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

Power of Good Backup

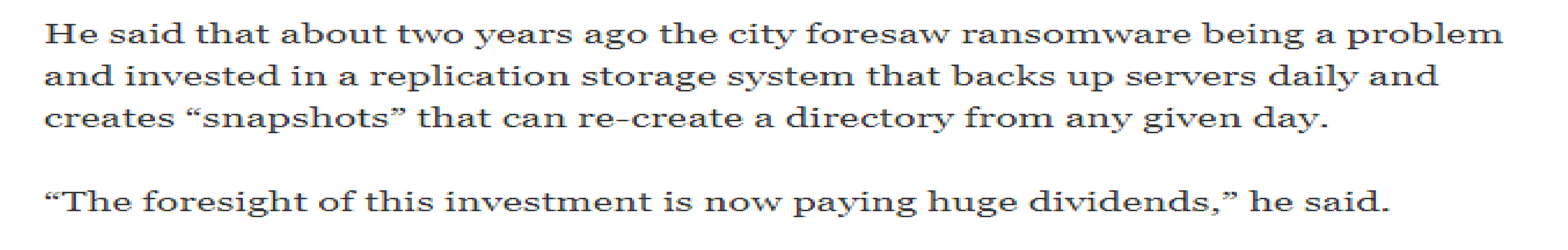
Honolulu Fire Dept. – no ransom, files backed up, up and running swiftly (September, 2016)

https://www.youtube.com/watch?v=b9d4sXENACs



"The city's Department of Information Technology backs up all servers daily, and keeps 'snapshots' so that we can recreate the state of a directory on any given day."

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-Infects-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

<u>Phishing (most common)</u>

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

- <u>Pretexting</u>
- 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

Emergency Contracting Example - 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/

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)

Prevention: Essential Investment

Identifying a PHISH – sample training

- Generic subject and greeting
- Spelling, grammar, or fact mistakes
- Odd looking characters (like 1 instead of l)
- ANY request for an URGENT response
- ANY request that has an explicit or implicit threat
- ANY request for sensitive information or username/password

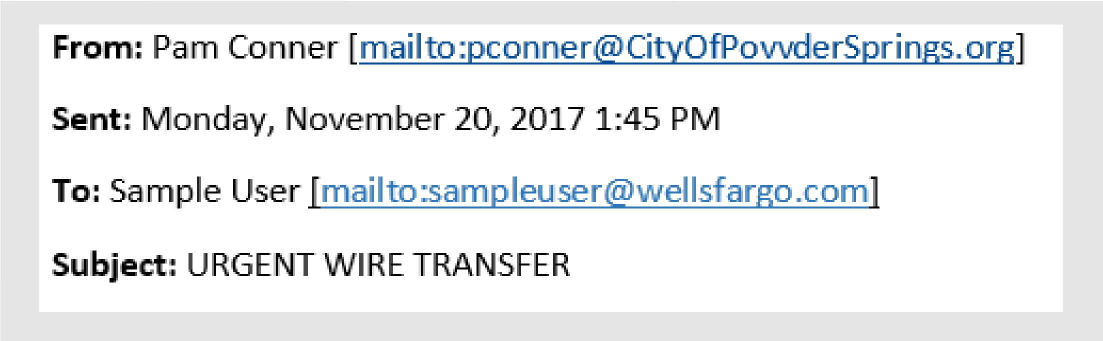
Any message that addresses you with the wrong name
Always hover over the url to see the full address
Check to make sure the text of the link matches the url when you hover

- https://www.dhs.gov/sites/default/files/publications/2018_AEP_Vulnerabilities_of_Healthcare_IT_Systems.pdf

DID YOU KNOW?

- 95% of successful cyberattacks start in email

Identifying a PHISH – sample training

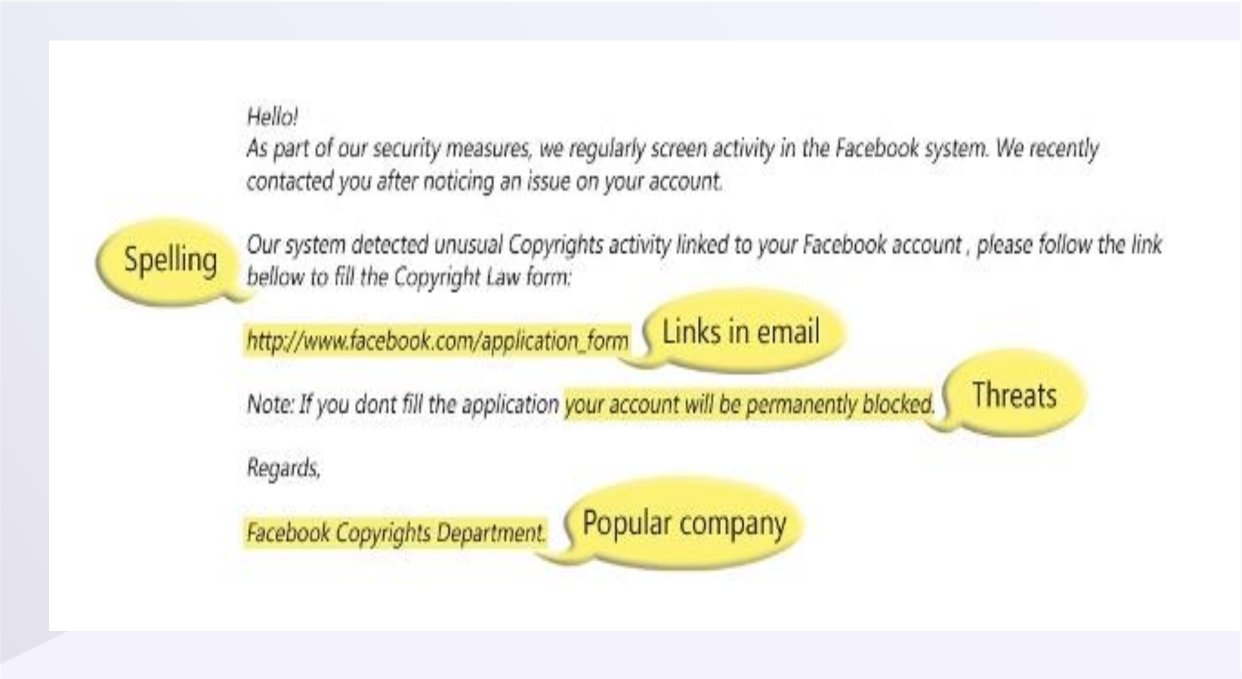


From: Pam Conner [mailto:pconner@CityOfPovvderSprings.org]

Sent: Monday, November 20, 2017 1:45 PM

To: Sample User [mailto:sampleuser@wellsfargo.com]

Subject: URGENT WIRE TRANSFER



Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

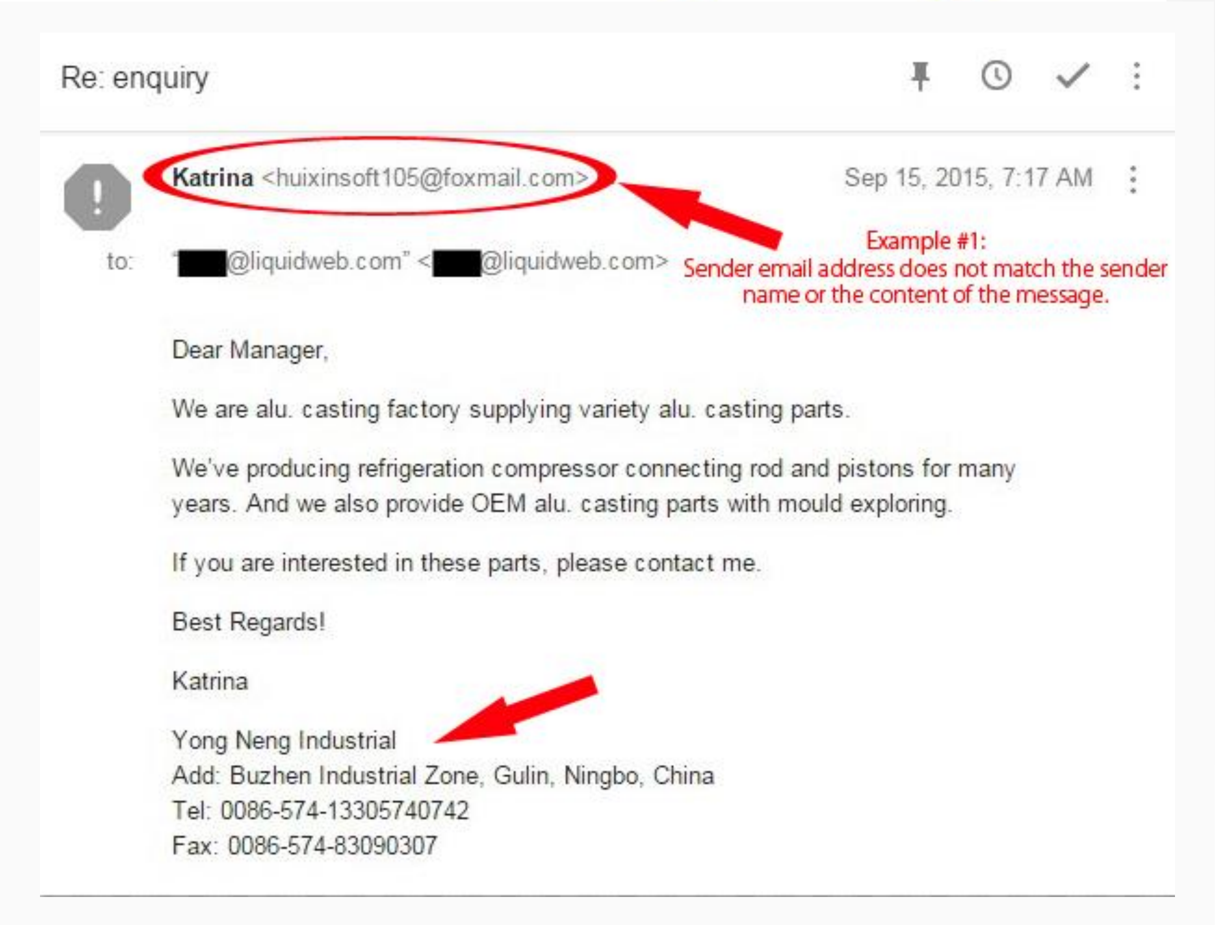
Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link bellow to fill the Copyright Law form:

http://www.facebook.com/application_form

Note: If you dont fill the application your account will be permanently blocked.

Regards,

Facebook Copyrights Department.



Re: enquiry

Katrina <huixinsoft105@foxmail.com>   Sep 15, 2015, 7:17 AM

to: "[redacted]@liquidweb.com" <[redacted]@liquidweb.com>

Example #1:
Sender email address does not match the sender name or the content of the message.

Dear Manager,

We are alu. casting factory supplying variety alu. casting parts.

We've producing refrigeration compressor connecting rod and pistons for many years. And we also provide OEM alu. casting parts with mould exploring.

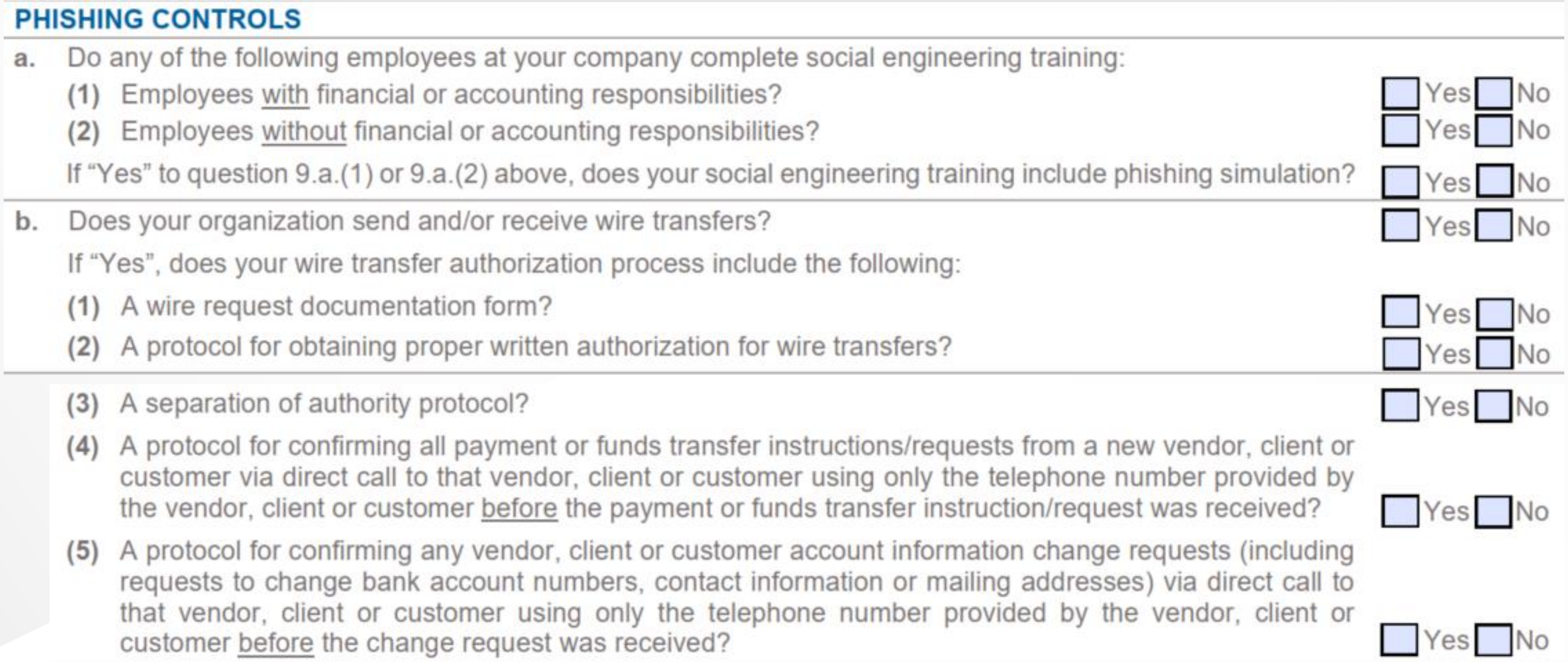
If you are interested in these parts, please contact me.

Best Regards!

Katrina

Yong Neng Industrial
Add: Buzhen Industrial Zone, Gulin, Ningbo, China
Tel: 0086-574-13305740742
Fax: 0086-574-83090307

Preventing Theft Due to Pretexting



PHISHING CONTROLS

a. Do any of the following employees at your company complete social engineering training:

(1) Employees <u>with</u> financial or accounting responsibilities? □ Yes □ No

(2) Employees <u>without</u> financial or accounting responsibilities? □ Yes □ No

If "Yes" to question 9.a.(1) or 9.a.(2) above, does your social engineering training include phishing simulation? □ Yes □ No

b. Does your organization send and/or receive wire transfers? □ Yes □ No

If "Yes", does your wire transfer authorization process include the following:

(1) A wire request documentation form? □ Yes □ No

(2) A protocol for obtaining proper written authorization for wire transfers? □ Yes □ No

(3) A separation of authority protocol? □ Yes □ No

(4) A protocol for confirming all payment or funds transfer instructions/requests from a new vendor, client or customer via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer <u>before</u> the payment or funds transfer instruction/request was received? □ Yes □ No

(5) A protocol for confirming any vendor, client or customer account information change requests (including requests to change bank account numbers, contact information or mailing addresses) via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer <u>before</u> the change request was received? □ Yes □ No

HIPAA – Why it Matters and Why it Doesn’t!

Why every city should designate itself a “Hybrid Entity.”

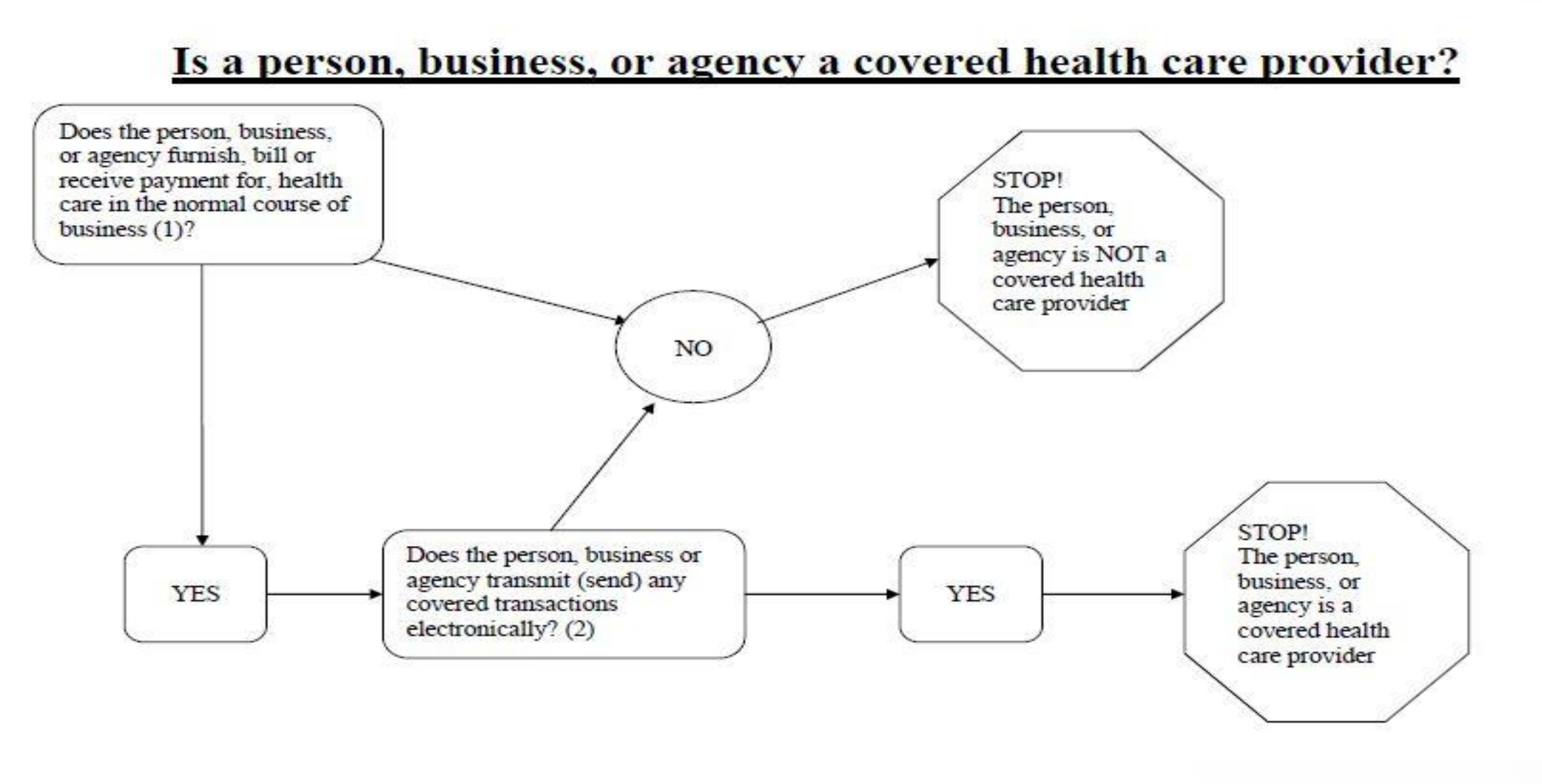
HIPAA

Health Plans

- If city has a Self-Insured health plan (other than GMEBS);
- If a third party administers city’s medical flexible spending account plan
- If city offers ONLY a fully-insured health plan or the GMEBS health plan: privacy and security of limited information they have (enrollment, summary health information) is not regulated by HIPAA when it is in their hands. Still . . . Must protect enrollment information and use Summary Health Information only for permitted purposes.

HIPAA

Healthcare Providers



Is a person, business, or agency a covered health care provider?

Does the person, business, or agency furnish, bill or receive payment for, health care in the normal course of business (1)?

NO

STOP! The person, business, or agency is NOT a covered health care provider

YES

Does the person, business or agency transmit (send) any covered transactions electronically? (2)

YES

STOP! The person, business, or agency is a covered health care provider

HIPAA

Examples of Hybrid Designations

- –City of Greenwood, Indiana (employer “hands on” PHI for health plan)
- –City of Williamsburg, Virginia (employer “hands off” PHI for health plan)

See Handouts

HIPAA covered information

- Any unauthorized use or disclosure of Protected Health Information (even inadvertent) must be analyzed to see if breach occurred
- If breach occurred, mandatory reporting to HHS OCR
- Also mandatory notification to affected individual
- Incident response procedure must include legal review

Breach Response

Laws govern breach response (confirmed disclosure of data to unauthorized person)

- Applicable Laws (City of Monroeville, ex. of knowing what law applies)

Response

- Incident Response (includes Tech response)
- Breach Response
- Role of Elected Officials in Prevention and Response
- Role of Cybercoverage Carrier in Breach Response

Our Case Study

- City of Monroeville, PA

City of Monroeville

- Dispatch center involved was not a HIPAA healthcare component
- Disastrous incident response
- Political use of information privacy and security incidents
- Bad press

City of Monroeville, PA 2014

- Ambulance dispatches were sent to a former Monroeville police chief after he had terminated employment
- Generic usernames and passwords were created to access a database of 911 callers' medical information, giving anyone with that information the ability to anonymously access personal medical records

Privacy IS a BIG DEAL

- City attorney - “Who thinks it is a violation? So far, the vote is the assistant chief. And he’s practicing law without a license.
- I don’t see it. . . .The only lessons learned out of this mountain out of a molehill is we’re taking names off this list that don’t have any reason to be on there anymore.
- This isn’t a big deal.”

City of Monroeville

HHS determined no HIPAA breach because the dispatch center was not a HIPAA covered entity.

- –$50,000 in legal fees,
- –Investigation by HHS,
- –Investigation by PA Attorney General
- –Months of bad publicity

- –http://www.wtae.com/investigations/Complaint-alleges-police-chief-received-shared-info-from-911-call/16880170

City of Monroeville

- Employment drama
- Council drama
- Council #1 overtaken by Council #2
- Council #1 demanded resignation of City Manager who refused to fire Police Chief in charge at time of breach, appointed new City Manager
- Council #2 fired new City Manager, who sued – settlement

City of Monroeville

Cole (Chief at time of breach)

Demoted

Suspended

Fired

Sued

Rehired

Pascarella (Asst. Chief at time of breach)
Promoted
Resigned
Rehired as Lt.
Fired
Sued
Settlement

What Can We Learn?

- Information security incident response procedure and clear commitment to security from mayor, council, city attorney and city manager could have resolved the incident proactively
- HIPAA hybrid designation could have prevented investigations by HHS and PA Attorney General
- Enforcement of access control policies and procedures could have prevented the disclosures in the first place

Actions for Breach Prevention and Response

- Remember what we can do TODAY – backups, Endpoint Detection and Response, training and phish testing, password policies, MFA
- Complete an Information inventory + risk assessment
- Make a HIPAA “hybrid entity” designation (and similar identification of other laws that apply to information)
- Maintain policies and procedures: training, enforcement, incident response, breach response
- All Contracts should include information privacy and security provisions whenever vendor accesses/maintains/uses confidential information

Actions for Breach Prevention and 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)

Elected Officials Must Champion Information Privacy and Security

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 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 Info Privacy and Security

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

- Treasury guidelines allow recipients to report using their funds for revenue replacement for the full amount of their award, up to $10 million.
- If using funds under the revenue replacement category, funds may be used for any government service, including cybersecurity, hardware, software, and protection of critical infrastructure.
- Rember 12/31/2024 is the deadline to obligate ARPS SLFRF; 12/31/2026 is the deadline to spend.

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 Commentary, 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."

City Leaders Must Champion Info Privacy and Security

“Make the pitch” exercise

Selling the Process

Benefits of acting NOW

- It is the right thing to do!
- Control the process of protecting the information to limit expense and change corporate culture
- Prevent or limit investigations by analyzing legal obligations in advance
- Prevent breaches!
- Manage Public Relations for any breaches that occur

Keeping a Clean House to Reduce and Manage Risk – The Information Inventory and Risk Assessment

Information Inventory/RA

- What information should be protected, with access limited to those who need it?
- What laws establish protections and govern what happens if mis-used or improperly disclosed/accessed?
- Who gets it? Where does it go? How is it stored?
- How is it currently protected from improper use, disclosure or corruption?
- What is risk of improper use, disclosure or corruption?
- What changes are appropriate?

Information Inventory/RA

- See Handout
- Should result in secure destruction of unnecessary PPHI, updates of contracts
- Will form the basis for procedures/training
- Will form the basis for access controls for electronic information
- Interviews will provide buy-in and promote awareness

Contract Provisions

- Insist that all contracts with vendors handling sensitive information include provisions requiring the vendor to protect the information, follow industry standards, and pay for costs associated with breach response.
- Special rules for HIPAA business associates and payment card software/hardware vendors

Breach Response – Check the Source of the Obligations

HIPAA privacy and security requirements

- Extensive breach response requirements

Payment Card Industry Data Security Standards (for ANY CITY that takes credit cards)

- Breach response is included in contract

Sources of City Info P&S Obligations

- **GA Criminal Justice Information System Network policies**
- **GA Personal Identity Protection Act** OCGA 10-1-910 (notification of breach of security of personal information)
- **GA SSN Protection Law** O.C.G.A 10-1-393.8 forbids publicly posting or displaying SSNs, requiring individuals to transfer unencrypted SSNs over an unsecured connection or to use SSNs to access web sites, unless a PIN or password is also required. Exceptions for applications and enrollment, creating changing or terminating a contract or policy, for verifying SSN
- **Georgia Emergency Management Act** requires reporting by utilities of certain cyber incidents to GEMA and, once rules released, will require reporting by cities
- **Critical Infrastructure Protection rules** require utilities to report some attacks (beyond scope of this presentation)
- **Payment Card Industry Data Security Standards** (if city accepts payment card payments)
- **HIPAA** (for covered components only)

Payment Card Industry (PCI) Data Security Standards (DSS)

- PCI DSS are minimum requirements for protecting customers’ payment card information. PCI DSS were created by the five major payment card brands.
- No law requires PCI DSS compliance.
- Contractual obligation to comply
- City likely affirms its compliance in a contract.

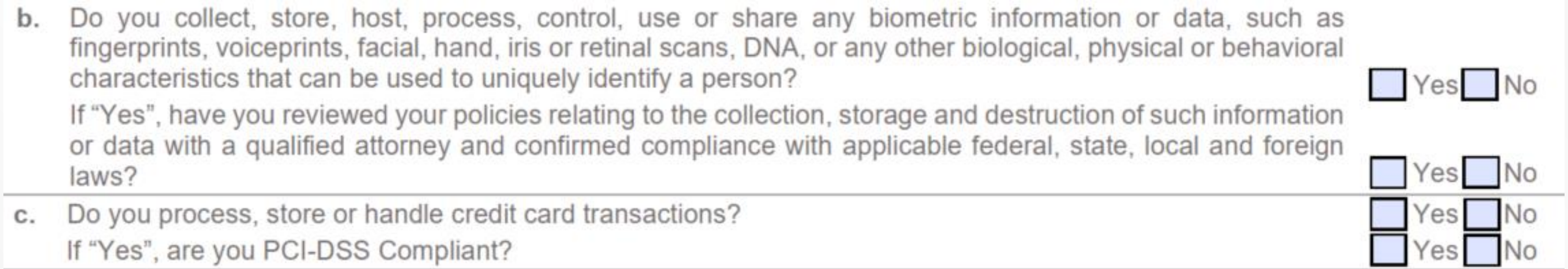
PCI DSS

- Merchant account agreement should outline fines if city is noncompliant, any duty to certify compliance
- Noncompliant + breach in security = card replacement costs, possible fines, forensic audits, reputation damage, additional compliance validation requirements, finally termination of merchant account and placement on dreaded **“Terminated Merchant File”**
- Lawsuits may use lack of compliance with PCI DSS standards to demonstrate negligence

PCI DSS

- City is responsible for protecting cardholder data at the point of sale, and as it flows into the payment system. The best step to reduce exposure is to not store *any* cardholder data.
- Compliance with the PCI standards includes protecting:
  - Card readers
  - Point of sale systems
  - Store networks & wireless access routers
  - Payment card data storage and transmission
  - Payment card data stored in paper-based records
- Self-Assessment Questionnaires will provide a guide
- Ensure agreements with payment processing vendors clarify responsibilities

Cyberliability Insurance Companies care about PCI DSS



b. Do you collect, store, host, process, control, use or share any biometric information or data, such as fingerprints, voiceprints, facial, hand, iris or retinal scans, DNA, or any other biological, physical or behavioral characteristics that can be used to uniquely identify a person? □ Yes □ No

If "Yes", have you reviewed your policies relating to the collection, storage and destruction of such information or data with a qualified attorney and confirmed compliance with applicable federal, state, local and foreign laws? □ Yes □ No

c. Do you process, store or handle credit card transactions? □ Yes □ No

If "Yes", are you PCI-DSS Compliant? □ Yes □ No

DID YOU KNOW?

- 2022: The average cost of a data breach was $3.80 million.
- 2023: The entire cost of cyberattacks is $6 trillion.
- 2025: cybercrime will cost the world $10.5 trillion yearly.

Source: https://techjury.net/blog/how-many-cyber-attacks-per-day/

Georgia Personal Identity Protection Act

- Georgia Personal Identity Protection Act O.C.G.A. Section 10-1-910 passed in 2005 defines personal information and requires breach notification if it is compromised; expanded in 2007
- Cities may be considered “data collectors” subject to the law, and its vendors subject to law as well
- Reasonable to follow HIPAA guidance when determining whether an event compromised the security, confidentiality, or integrity of the information
- No penalties or independent cause of action, but could be used to demonstrate negligence

GPIPA

(2) “Data collector” means any state or local agency or subdivision thereof including any department, bureau, authority, public university or college, academy, commission, or other government entity; provided, however, that the term “data collector” shall not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes or for purposes of providing public access to court records or to real or personal property information.

GA Emergency Management Act

- OCGA 38-3-22.2 Reporting of cyber events to GA Dept. of Homeland Security (probably not required until rules are issued about what must be reported and reporting mechanism.)
- Per GEMA memo, reporting to head of GEMA facilitates information sharing and access to guidance from GTA's Office of Information Security

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

- Use the term “incident” – not “breach.” “Breach” is only used after determination that incident compromised the privacy and security of the information
- HIPAA breach notification/risk of harm tools are very helpful
- www.hipaacow.org has excellent tools
- Document all actions taken to investigate and minimize harm
- Consider establishing contract with credit monitoring company
- All contracts with vendors handling PPHI should include breach provisions and indemnification
- Obtain legal review to determine whether notification to individuals or other entities is mandated by law or contracts

Elected Official During Incident Response

- Exercise

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

Other Questions to Take Back to the City

- Does the city have information privacy and security policies and procedures that include incident reporting and breach response? How often does the city provide security awareness training? Do the city's contracts contain information privacy and security provisions?
- Does the city have an incident response plan with prepared communications? What role, if any, are council members to play?

GMA Resources

- GIRMA Cyber coverage
- GIRMA Crisis Management
- VC3 Information Technology Services
- *Cybersecurity Threats: Leadership Needed*
- GMA Website/Cybersecurity

1. Name examples of attacks that target users.

2. You receive an email from your boss’s boss at 4:00 p.m. on a Friday telling you to urgently buy gift cards. What do you do?

3. Name examples of actions you can take to champion cybersecurity.

4. Who needs to comply with PCI-DSS and why?

5. Why is Cyberliability Insurance important?

Questions?

Alison Cline Earles, CIPP (US), CIPT

Senior Associate General Counsel, Georgia Municipal Association

aearles@gacities.com

678-651-1028