



COLORADO
MUNICIPAL
LEAGUE

Managing Transparency Related Risks

Presented by Sam Light, CIRSA General Counsel 8.27.2020



Presentation Overview

- Transparency—in its broadest sense, access to government and government information—is a basic expectation and requirement for municipalities.
- Citizens expect access and openness & laws require it.
- But with these increasing expectations and requirements, and the “virtuality” of everything your cities and towns do, municipalities face ever increasing risks.



Presentation Overview

- In this presentation, we'll talk about some hot topics / trouble spots related to transparency:
 - Cyber Attack Risks
 - First Amendments Audits
 - Balancing Transparency & Confidentiality in Executive Sessions



Cyber Attack Risks - Trends

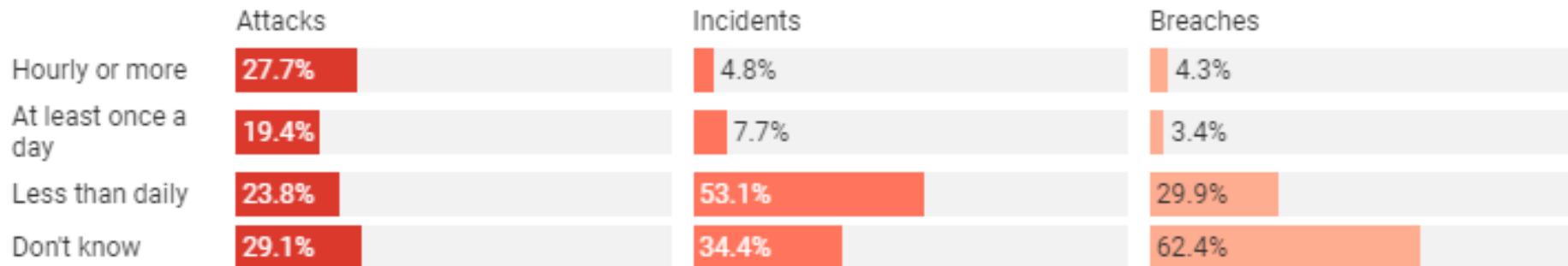
- Cyber attacks on local governments have risen significantly.
- According to one source, in the single year between 2018 and 2019, known incidents of ransomware or similar cyber attacks on local governments rose 58.5%.
- In line with the national trend, Colorado governments are not immune and are seeing more events. See <https://www.seculore.com/cyber-attacks-colorado> for a sampling of Colorado cyber events (with related news links).



Cyber Attack Risks - Trends

How frequently are local governments under cyberattack?

While many local governments know how often they're being targeted, a surprising number do not.



Attacks are attempts to gain unauthorized access to cause mischief or do harm. Incidents are events that compromise confidentiality, integrity or availability of a computer system. Breaches are incidents that result in confirmed disclosure of information to an unauthorized person.

Chart: The Conversation, CC-BY-ND • Source: [University of Maryland, Baltimore County](#) • [Get the data](#)



COLORADO
MUNICIPAL
LEAGUE

Cyber Attack Risks - Trends

- In addition to the general uptick in cyber attacks, municipalities particularly face increased risks. Why?
 - Municipalities collect and store a lot of personal information and other valuable data.
 - Hackers view governments as vulnerable; systems more accessible; easier targets.
 - Budgets for IT staff and resources can be tight.
 - Risk awareness lower?
 - Limited understanding of how cyber attacks occur and how to mitigate them?



Cyber Attack Risks - Trends

- Cyber attack events can have both internal and external impacts.
 - Internal (first-party):
 - Loss of system data & functionality
 - Down-time
 - Recovery expenses
 - Other
 - External (third-party):
 - Notice requirements (e.g., House Bill 18-1128 requirements)
 - Public relations expenses
 - Third-party liability claims
 - Other



Cyber Attack Risks – CIRSA's Experience

- In line with the national trend, we are seeing at CIRSA increases in the number and costs of cyber attacks against members, including particularly attacks via “social engineering fraud” and ransomware.
- Almost all of our members' losses in these areas have been since 2017.
- In addition, we are seeing a “tightening” of the market for cyber reinsurance and excess insurance.



Cyber Attack Risks - Social Engineering Fraud

“**Social Engineering Fraud**’ means an intentional misrepresentation of fact or a willful, deliberate or fraudulent act committed with the intention of misleading an “employee” and resulting in the “theft,” transfer, dispersal or payment of funds to unauthorized persons.

It is also called **Impersonation Fraud** and defined as electronic, telegraphic, cable, teletype, telefacsimile, telephone or written instruction received and relied upon by you or your employee which was transmitted by a purported director, officer, partner... but was in fact fraudulently transmitted by someone else...



COLORADO
MUNICIPAL
LEAGUE

Social Engineering Fraud – What Does it Look Like?

From: Tami Tanoue <mgttoff@earthlink.net>
Sent: Tuesday, October 29, 2019 10:42 AM
To: Dianne Hall <dianneh@cirsa.org>
Subject: RE: Quick One...

How close are you to Target, Walgreens or CVS? I need some eBay gift cards sent out to a client today. I will reimburse you later today. Let me know how soon you can get them.

-----Original Message-----

>From: Dianne Hall <dianneh@cirsa.org>
>Sent: Oct 29, 2019 9:40 AM
>To: Tami Tanoue
>Subject: RE: Quick One...

>

>Sure

>

>

>

>-----Original Message-----

>From: Tami Tanoue
>Sent: Tuesday, October 29, 2019 10:40 AM
>To: Dianne Hall <dianneh@cirsa.org>
>Subject: Quick One...

>

>What are you up to? Can you get a task done right away?



COLORADO
MUNICIPAL
LEAGUE

Social Engineering Fraud – What Does it Look Like?




Mon 2/24/2020 6:12 AM

Cirsa.org <clopez@centralfreight.com>

Mail Update

To: cirsamembers@cirsa.org

 If there are problems with how this message is displayed, click here to view it in a web browser.

Office536

Dear Cirsamembers,

Due to recent server update, you are required to apply latest security update to enhance your email functionality.

Update Now

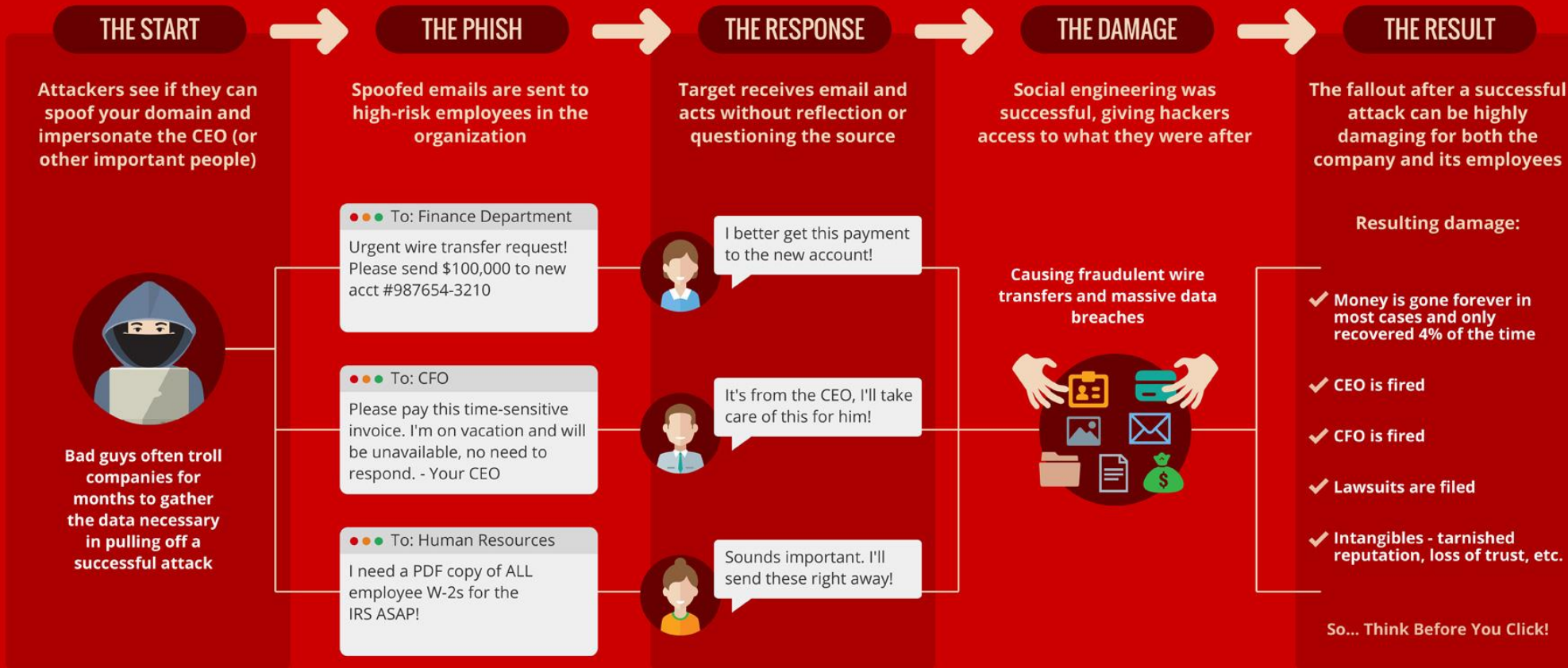
Be aware that, [Cirsa.org](#) will not be responsible for any loss of data should this warning be neglected.

Kind regards,
[Cirsa.org](#)



COLORADO
MUNICIPAL
LEAGUE

HOW CEO FRAUD IMPACTS YOU



Cyber Attack Risks - Ransomware

Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

Users are shown instructions by the attacker for how to pay a fee to get the decryption key.

Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at
KurtSchweickardt@protonmail.com
or
KurtSchweickardt@tutanota.com

BTC wallet:
14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk

Ryuk
No system is safe



COLORADO
MUNICIPAL
LEAGUE

Cyber Attack Risks - Ransomware

- Ransomware attacks are costly and time-consuming.
 - From 2017-2020, the estimated reported ransom paid per event in municipalities was \$125,697.
 - The average downtime that results from a ransomware attack is 9.6 days.
 - Where ransom is not paid, recovery costs are significant.



Tips for Managing Cyber Attack Risks

- Scrutinize e-mails closely, particularly the ones that seem a bit off; e.g.:
 - Familiar name but unfamiliar address and/or unfamiliar attachments
 - Odd grammar, odd timing, etc.
 - Review in a reading pane before opening (no reflexive double-clicking)
- Don't use open public wi-fi.
- Don't use your cell phone for sensitive stuff.
- Restrict or prohibit use of portable storage devices.



Social Engineering Red Flags



FROM

- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they **were not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.



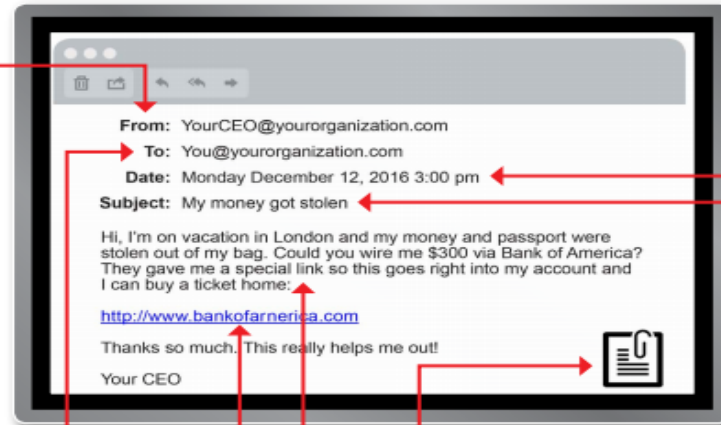
TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.



HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?



SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?



ATTACHMENTS

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt file**.



CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd or illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

More Tips for Managing Cyber Attack Risks

- Use strong passwords and change them regularly.
- Keep systems up to date:
 - Don't ignore software updates – install them!
 - Use/maintain anti-virus and firewall protection.
- Make regular backups.
- Report odd messages/events to IT – don't just reboot and move on!
- Don't install/download programs/apps on a whim.
- Appropriately resource any incident (e.g., specialized legal, etc.).



First Amendment Audits

- Nationwide and in Colorado, there is a trend of citizens conducting “First Amendment Audits” by visiting public places to record, and often livestream, their interactions with public officials and staff.
- First Amendment Audits aren’t really about making new laws; rather, they are the latest trend by which citizens are “testing” officials’ and staff’s knowledge of long-standing laws—particularly the First, Fourth and Fifth Amendment.
- Auditors’ recording of police in the streets has been going on for a while, and as you may have experienced, they recently have taken to visiting more places, including to your city or town hall....



First Amendment Audits

YouTube

Search



Hickman KY. City hall ILLEGALLY DETAINED AND FORCED TO ID. 1st amendment audit BIG FAIL.

16,272 views

495 82 SHARE SAVE

First Amendment auditors believe that such audits “[p]romote transparency and accountability in public officials.”

“We have no interest or intention in breaking any law. We stand strong for freedom and the constitution, and do so in a responsible and professional manner. It is our goal to create free and open discussion whenever possible in an effort to educate those willing to learn.”



COLORADO
MUNICIPAL
LEAGUE



Coppell,Tx.-City Hall-"You can't record this GET OUT!!!"
22K views • 1 week ago



Westminster,Co.-CITY HALL-"You're creating a..."
18K views • 1 week ago



Arvada,Co.-"In this day and age people might ATTACK..."
11K views • 1 week ago



Littleton,Co.-SETTING THE JUDGE STRAIGHT!-...
35K views • 1 week ago



Dallas,Tx.-CITY COMPLAINT-"When you..."
11K views • 1 week ago



Dallas,Tx.-BELLIGERENT TYRANT SECURITY-...
62K views • 2 weeks ago



Dallas,Tx.-"Comply with my orders or I will remove you!-...
64K views • 2 weeks ago



Lakewood,Co.-"You're not allowed to record here!-...
26K views • 2 weeks ago



Lone Tree,Co.-Flipping the script-"You got ID on you?"
40K views • 2 weeks ago



Dallas,Tx Constables Precinct 5-"Take them they..."
62K views • 2 weeks ago



NNP, NNH, Daymond Chief Jones News Media...
5.8K views • 2 weeks ago



Greenwood Village,Co.-"It's just SUSPICIOUS when we..."
23K views • 2 weeks ago



Aurora,Co.-Detention Center-"I've never been in..."
11K views • 2 weeks ago



Coppell,Tx.-"You must identify if you're going to..."
36K views • 2 weeks ago



Dallas,Tx.-West End Bus Station-Copwatching
6.9K views • 2 weeks ago



Edgewater,Co.-"It's policy recording isn't allowed..."
46K views • 3 weeks ago



Centennial,Co.-FAILED INTIMIDATION-"Look no..."
24K views • 3 weeks ago



Ness City,Ks.-"We don't have Complaint Forms here"-...
10K views • 3 weeks ago



Patrick Roth
62,437 subscribers



COLORADO
MUNICIPAL
LEAGUE



COLORADO
MUNICIPAL
LEAGUE

First Amendment Audits

- These visits can be unexpected stressors for officials and employees and understandably can make people uncomfortable—when's the last time you were videotaped at your desk by someone you've never met?
- And they can raise legal issues that probably don't come up in our day-to-day operations:
 - Can they really say “#(@*#^%%”?
 - Can they really videotape our employees while they work?
 - Can they really go anywhere in city/town hall?



First Amendment Audits

Can they really say “#(@*#^%%”?

- Well, yes. The First Amendment protects the free speech rights of individuals and the press, and municipalities can be liable for retaliating against a person who’s engaging in protected speech, or for improper restrictions on speech.
- Offensive, profane or vulgar speech is protected, and cannot be restrained on that basis alone.
- Fighting words are not protected: Narrow, limited to: “[E]pithets (1) directed at the person of the hearer, (2) inherently likely to cause a violent reaction, and (3) playing no role in the expression of ideas.”
- Obscene speech is not protected.
- Good First Amendment Auditors generally know where the line is drawn!



COLORADO
MUNICIPAL
LEAGUE

First Amendment Audits

Can they really videotape our employees while they work?

- Well, yes. The right of persons in public places to make video recordings is generally well-established.
- Colorado is a single-party consent state. Thus, consent of the subject being taped is not required.
- Under two Colorado statutes (C.R.S. 16-3-311 & 13-21-128), persons have the express right to record peace officers, and officers and their employers can be liable for unlawful destruction, damage, or seizure of a recording, or for retaliating against a person making a recording.
- “You can’t record here” isn’t an appropriate approach.



First Amendment Audits

Can they really go anywhere in city/town hall?

- The public areas of public buildings are public spaces open to the public (whew...that's a lot of public).
- For these areas, there's not a legal basis for "trespassing" against a person in open areas of a public building hours and there's no requirement the visitor demonstrate they are there for "official business."
- A First Amendment Audit is not the first time to tell the visitor a publicly accessible area is "off limits." Rather, non-public areas should be secured and marked in advance.
- And confidential information should be shielded from view/recording.



First Amendment Audits

- First Amendment auditors can be less than compassionate; yet, they generally understand their rights, and recognize when their rights are being infringed.
- There are hero/villain themes to these videos and related comment threads.
- With preparation, training and the proper approach, your entity will be a hero!



COLORADO
MUNICIPAL
LEAGUE

First Amendment Audits

- At CIRSA our members have seen First Amendment audit activity in Council/Board chambers, on the sidewalk, at crime scenes, in parks, at festivals, fairs and other events, and now in city/town hall.
- We can't be certain where it will go next, but we can be prepared whenever it occurs:
 - Train front-line staff on options and techniques for dealing with auditors.
 - De-escalate—even embrace. Audit visits with kind and welcoming hosts often go well (and look good too!).
 - Clearly delineate your public / non-public areas.
 - Take appropriate steps to guard confidential areas and information.



Balancing Transparency & Confidentiality in Executive Sessions

- While transparency is a basic expectation and requirement, there are times when confidentiality is not only entirely defensible under the law, but also in furtherance of the interests of your municipality and its citizens.
- But, the discretionary right to keep certain discussions in confidence must be used carefully.
- Apart from legal risks, toeing too close to the line on these issues can also take a toll in terms of political capital and trust.
- And frequent testing of where the line is located can place significant stress on the organization, its leaders and staff.



Balancing Transparency & Confidentiality – Executive Sessions

- Recent Colorado Court of Appeals decision, *Guy v. Whitsett*, (2020 WL 3088844) is good reminder of difficulty and risks in striking the right balance.
 - Executive sessions for “legal advice” and “personnel matters.” The motions for those sessions referenced these topics and the statutory citations but no further detail of the subject matter to be discussed.
 - Town asserted that attorney-client privilege (ACP) and privacy interests in personnel matters prevented the Town from further identifying the topics to be discussed.
 - Court of Appeals disagreed, holding ACP is not waived by disclosing the subject matter, and OML outweighed employee’s privacy interests (in this case, the Town Manager).



Balancing Transparency & Confidentiality – Executive Sessions

- The takeaway for reducing risks in this area? Court expects you will attend to both the letter of the law and its spirit of transparency. Regarding the letter of the law, be sure:
 - The executive session is for an authorized topic.
 - To make a complete announcement and motion prior to the executive session. This must include the topic, the specific statutory citation that authorizes the session and “identification of the particular matter to be discussed in as much detail as possible without compromising the purpose for which the executive session is authorized.”
 - To stay on topic in the session; participants must self-regulate on this point.



Balancing Transparency & Confidentiality – Executive Sessions

- Regarding the spirit of transparency:
 - Use executive sessions sparingly, only as absolutely necessary.
 - Take appropriate opportunities immediately before and after session to share publicly appropriate information about the context of the session; e.g.,
 - Before the session, remind everyone publicly of the “ground rules.”
 - After the session, remind the audience that any matter requiring the body’s action will appear on a future agenda for public discussion prior to any decision.



Sources & Reference Material

- CIRSA Liability Loss Alert: *Colorado Court of Appeals Weighs in on the Calling of Executive Sessions – You’ll Want to Read This!*, https://www.cirsa.org/wp-content/uploads/2020/07/Liability-Article_Executive-Sessions.pdf.
- CIRSA Articles: *If it’s Spring it Must be First Amendment Audit Season*, <https://www.cirsa.org/news/if-its-spring-it-must-be-first-amendment-audit-season/>, and *First Amendment Audits Coming to Your Town*, <https://www.cirsa.org/news/first-amendment-audits-coming-to-your-town/>.
- CIRSA Article: *Data Privacy and House Bill 18-1128: New Requirements to Protect Personal Information*, <https://www.cirsa.org/news/colorado-house-bill-18-1128/>.
- KnowBe4, Whitepaper: *The Economic Impact of Cyber Attacks on Municipalities*, <https://www.knowbe4.com/hubfs/Cyber-Attacks-on-Municipalities-White-Paper.pdf>.
- Donald F. Norris, Laura Mateczun, Anupam Joshi & Tim Finin (2020), *Managing Cybersecurity at the Grassroots: Evidence from the First Nationwide Survey of Local Government Cybersecurity*, *Journal of Urban Affairs*, <https://www.tandfonline.com/doi/full/10.1080/07352166.2020.1727295>.
- ICMA, *Checklist for Cyber-Secure Remote Work*, https://icma.org/sites/default/files/ICMA%20Remote%20Work%20Cybersecurity%20Checklist_0.pdf.
- The Conversation, *Local Governments’ Cybersecurity Crisis in 8 Charts*, <https://theconversation.com/local-governments-cybersecurity-crisis-in-8-charts-94240>.



Speaker Bio

Sam Light is General Counsel for the Colorado Intergovernmental Risk Sharing Agency (CIRSA). Previously Mr. Light was a partner with the Denver law firm of Light | Kelly, P.C., specializing in municipal and other public entity law, insurance law and defense of public entities and elected officials. Sam is a frequent speaker on municipal law and has practiced in Colorado since 1993.



COLORADO
MUNICIPAL
LEAGUE

Colorado Intergovernmental Risk Sharing Agency



- CIRSA is a Colorado public entity self-insurance pool for property, liability, and workers' compensation coverages.
- Formed by in 1982 pursuant to state pooling laws. Not a for-profit insurance company, but rather an entity created by IGA of our members. CIRSA is owned, controlled, and governed by Colorado municipal interests.
- Total membership today stands at 281 member municipalities & affiliated entities:
 - 278 are members of the Property/Casualty pool
 - 141 are members of Workers' Compensation pool
- We have the largest concentration of liability-related experience and knowledge directly applicable to Colorado municipalities.
- Visit our website: www.cirsa.org.



COLORADO
MUNICIPAL
LEAGUE



THANK YOU



COLORADO
MUNICIPAL
LEAGUE