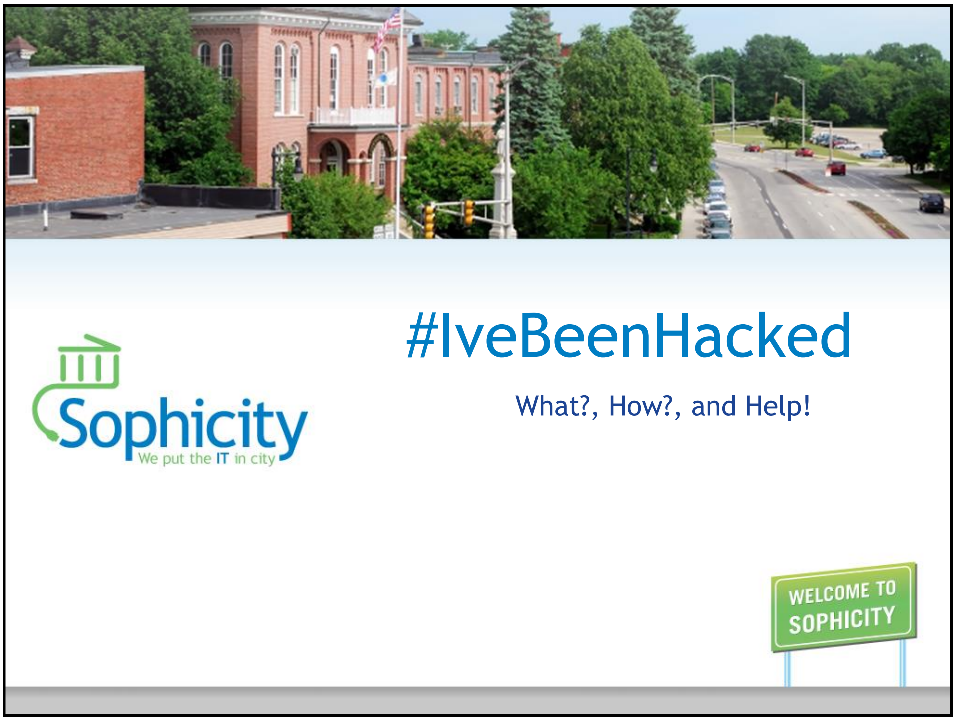


#IveBeenHacked

What?, How?, and Help!

Presenter

Dave Mims

CEO

davemims@sophicity.com
770-670-6940 x110

What we will cover

1. **What?** - What do I need to know?
2. **How?** – How have some real cities been impacted?
3. **Help!** – Best Practices and Common Issues.
4. **Take Aways**

Sophicity
We put the IT in city

What?

What do I need to know?

- Passwords
- Virus Attacks
- Data Backup
- Security Updates
- Physical Security
- City Websites

Sophicity
We put the IT in city

What? - Passwords

A study from a research company in California found:

- 1 out of 3 people had their passwords written down somewhere around their desk.
- Many used obvious passwords (child name, pet name, college mascot, birthdate, etc).
- Overall, researchers figured out passwords of half of the people in the study!

I changed all my passwords to "incorrect".
So whenever I forget, it will tell me "Your password is incorrect."

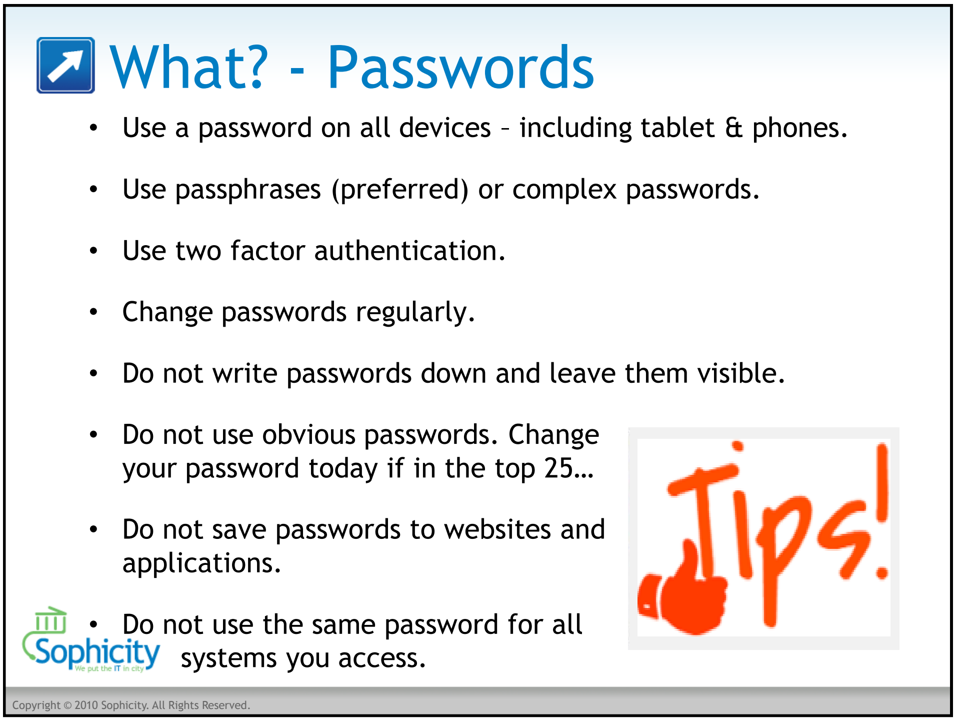
Half of all security breaches involve stolen or easily guessable passwords!

What? - Passwords

SplashData's annual **Worst Passwords List**, compiled from millions of **leaked** passwords during the year, shows people continue putting themselves at **risk**. For 2016:

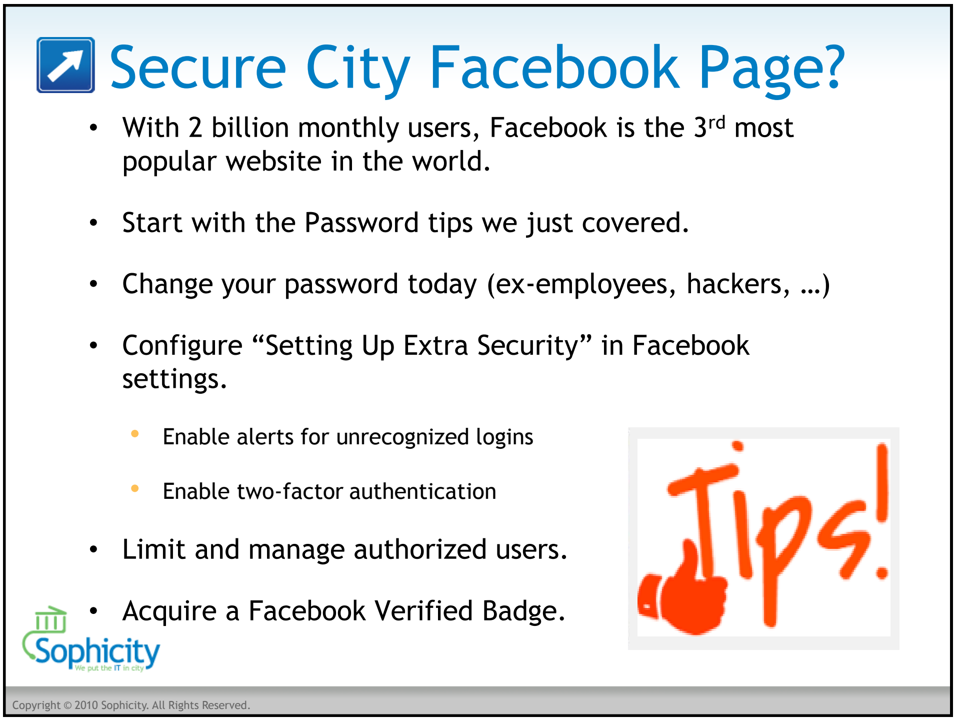
1. 123456	2. password	3. 12345	4. 12345678	5. football
6. qwerty	7. 1234567890	8. 1234567	9. princess	10. 1234
11. login	12. welcome	13. solo	14. abc123	15. admin
16. 121212	17. flower	18. passw0rd	19. dragon	20. sunshine
21. master	22. hottie	23. loveme	24. zaq1zaq1	25. password1

Remember, hackers are using **automated software** to look for holes. That automated software attempts common and weak passwords that are easy to crack.



What? - Passwords

- Use a password on all devices – including tablet & phones.
- Use passphrases (preferred) or complex passwords.
- Use two factor authentication.
- Change passwords regularly.
- Do not write passwords down and leave them visible.
- Do not use obvious passwords. Change your password today if in the top 25…
- Do not save passwords to websites and applications.
- Do not use the same password for all systems you access.



Secure City Facebook Page?

- With 2 billion monthly users, Facebook is the 3rd most popular website in the world.
- Start with the Password tips we just covered.
- Change your password today (ex-employees, hackers, …)
- Configure “Setting Up Extra Security” in Facebook settings.
  - Enable alerts for unrecognized logins
  - Enable two-factor authentication
- Limit and manage authorized users.
- Acquire a Facebook Verified Badge.

What? - Viruses

Computer viruses are **software programs** designed to spread and interfere. They will:

- **corrupt**, **delete**, and **steal** data
- use your access, email, social media, and messaging programs to **spread** itself
- hold your data hostage for **money** -- e.g. Ransomware!

Viruses can be disguised as attachments and links of, for example, funny images, greeting cards, online games, social media quizzes, or audio and video files.

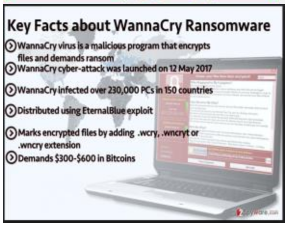
Sophicity
We put the IT in city

What? – Ransomware again!

$$$

- Current indications are that ransomware price demands are **increasing**.
- **World's biggest cyberattack** on May 2017, named WannaCry, sends 150 countries into disaster recovery mode.
- Future concerns (already proofed) are infrastructure targeting ransomware that put our industrial control systems and **municipal water supplies** at risk.

The easiest way for a hacker to get in is when **someone lets them in** the door.



Key Facts about WannaCry Ransomware

- WannaCry virus is a malicious program that encrypts files and demands ransom
- WannaCry cyber-attack was launched on 12 May 2017
- WannaCry infected over 230,000 PCs in 150 countries
- Distributed using EternalBlue exploit
- Marks encrypted files by adding .wcry, .wncryt or .wncry extension
- Demands $300-$600 in Bitcoins

Sophicity
We put the IT in city

What? - Viruses

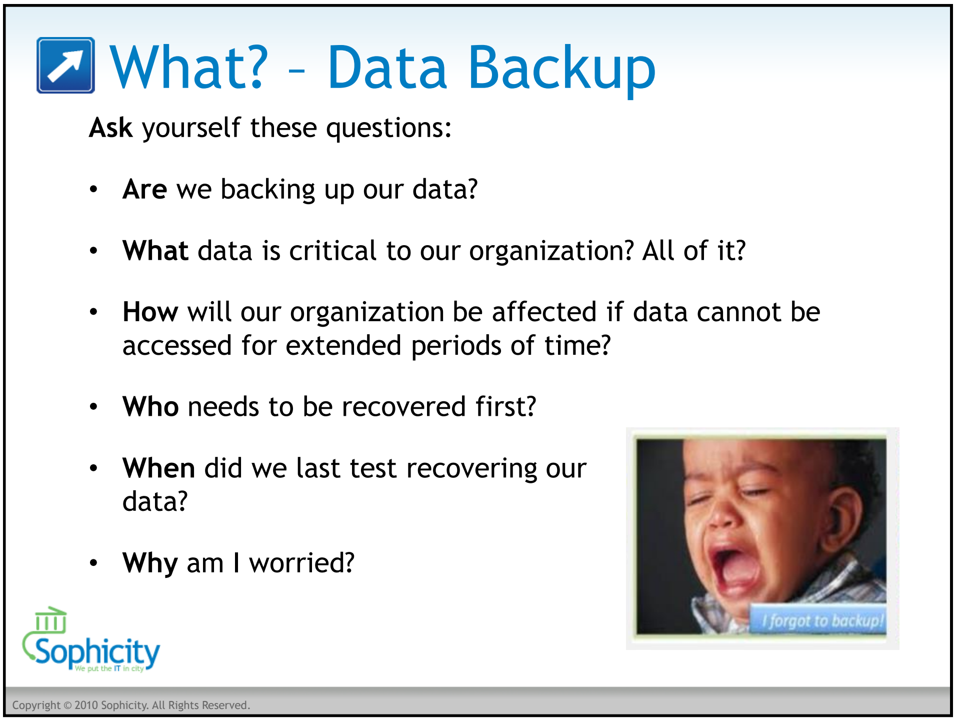
- **93%** of phishing emails are now ransomware!
- The average cost of a data breach is **$204 per lost record**!
- The average organization faces **1,400** cyberattacks in a **week**!
- A cyber breach can go undetected for **months**!

What do we do?

What? - Viruses

- Install **business class antivirus software** on every computer.
- Audit antivirus software regularly confirming installation and definitions are **up to date**.
- Keep computer updates and **patches** up to date.
- Train staff on common sources of viruses: **email attachments**, **websites**, and **online software**

People install viruses! We choose to download them. We trust too much.

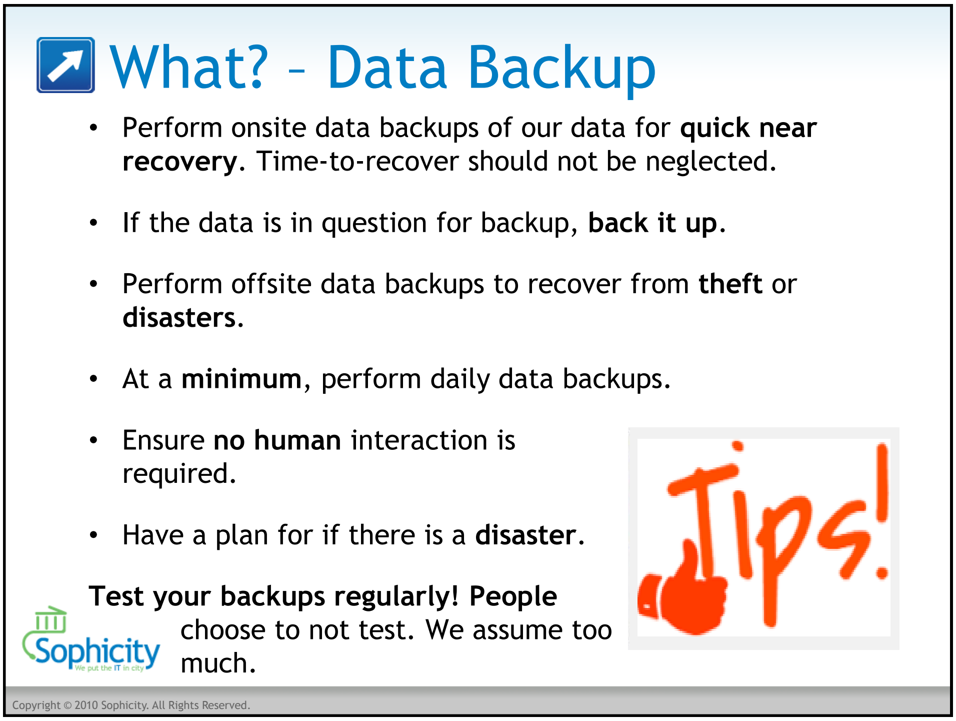


What? – Data Backup

Ask yourself these questions:

- **Are** we backing up our data?
- **What** data is critical to our organization? All of it?
- **How** will our organization be affected if data cannot be accessed for extended periods of time?
- **Who** needs to be recovered first?
- **When** did we last test recovering our data?
- **Why** am I worried?

I forgot to backup!
Sophicity
We put the IT in city



What? – Data Backup

- Perform onsite data backups of our data for **quick near recovery**. Time-to-recover should not be neglected.
- If the data is in question for backup, **back it up**.
- Perform offsite data backups to recover from **theft** or **disasters**.
- At a **minimum**, perform daily data backups.
- Ensure **no human** interaction is required.
- Have a plan for if there is a **disaster**.

Test your backups regularly! People choose to not test. We assume too much.

What? – Security Updates

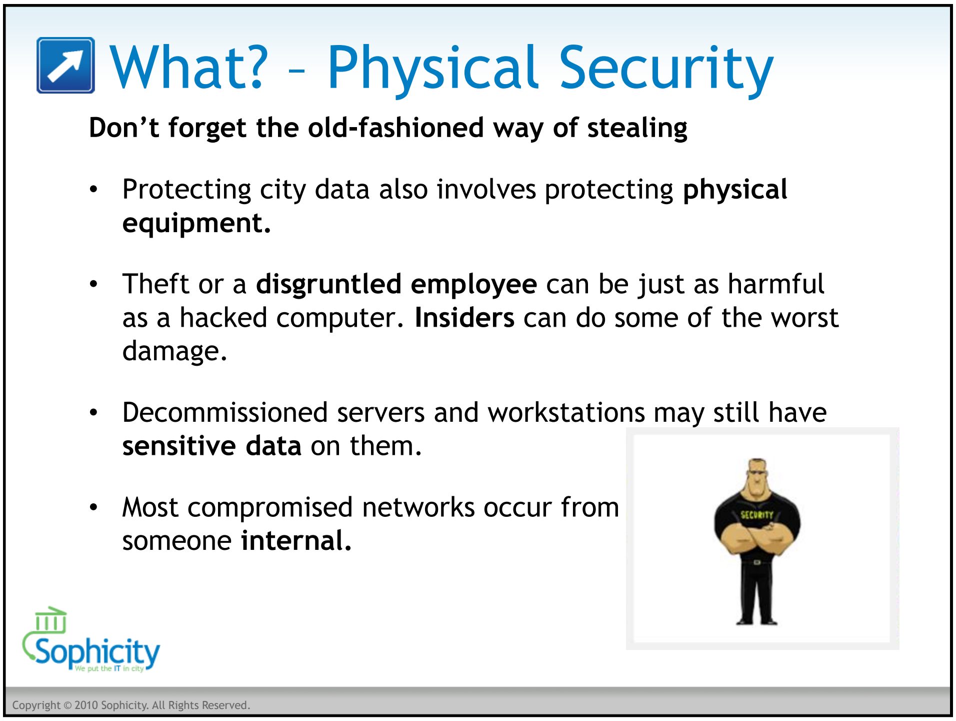
Studies show:

- Most cyber outbreaks can be prevented by keeping computers **up to date.**
- Applications (like Adobe Reader and Java) are **more likely** to be exploited than Operating Systems (like Windows).
- Most people **ignore** messages on their computers about installing updates.

What? – Security Updates

- Let those updates and security patches **run!** Patch management is an essential element of cyber protection.
- As **vulnerabilities** are found, vendors create a fix and make a patch available, but those patches still have to be deployed.
- If you have servers, make sure an **IT resource** is updating them.
- Upgrade any application, operating system, and hardware that has reached **end of life.**

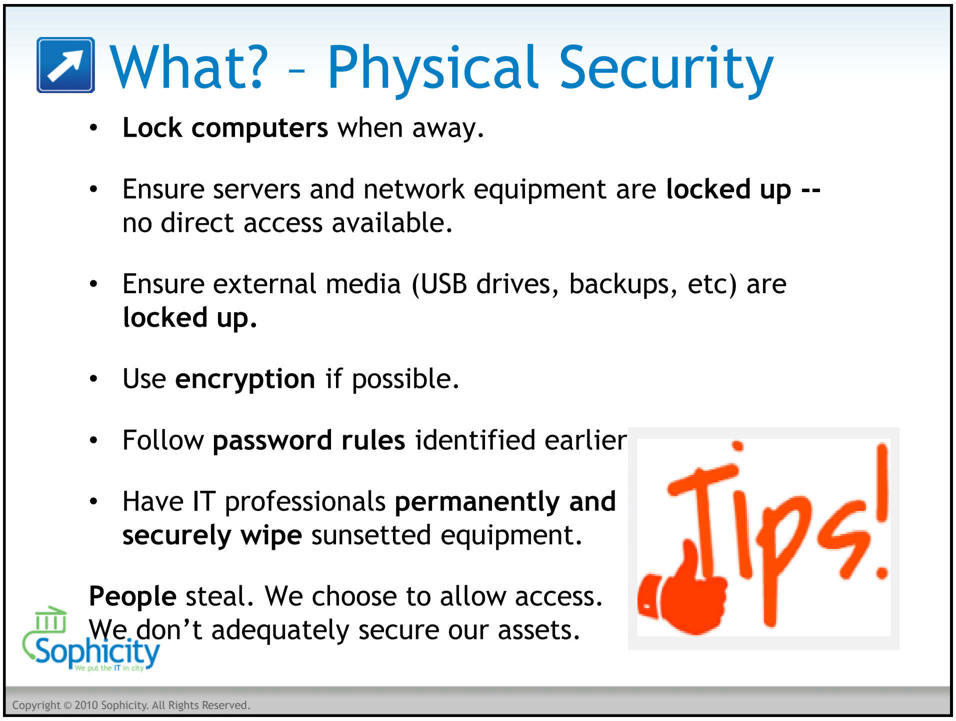
People ignore messages and warnings. We choose the risk. We are too impatient.



What? – Physical Security

Don’t forget the old-fashioned way of stealing

- Protecting city data also involves protecting **physical equipment.**
- Theft or a **disgruntled employee** can be just as harmful as a hacked computer. **Insiders** can do some of the worst damage.
- Decommissioned servers and workstations may still have **sensitive data** on them.
- Most compromised networks occur from someone **internal.**



What? – Physical Security

- **Lock computers** when away.
- Ensure servers and network equipment are **locked up --** no direct access available.
- Ensure external media (USB drives, backups, etc) are **locked up.**
- Use **encryption** if possible.
- Follow **password rules** identified earlier
- Have IT professionals **permanently and securely wipe** sunsetted equipment.

People steal. We choose to allow access. We don’t adequately secure our assets.

What? – City Websites

Today, when someone is interested in knowing more about your organization, **where do they go first?**

And if your website does not reflect your organization well, **what do they do?**

- Is our website **modern**?
- Is our website's **content current**?
- Is our website **secure**?

When did you personally last visit your organization's website? Could it be defaced and you **don't even know it**?

What? – City Websites

- Ensure the website is hosted by a **reputable provider.**
- Know **where** the website is hosted.
- Ask your website's host if they have been **audited** for potential risks by a third party.
- Follow **password rules** identified earlier.

People judge quickly. We choose how to make the first impression. We are too quick to settle for just *good enough* when it isn't really good enough.

How?

How have some real cities been impacted?

These are not **headlines** in the news. These are real cities and examples of what is seen **daily**. Cyber attacks are **costly**, **destructive**, & **embarrassing** for cities.

City #1: Virus initiates $90,000 transaction!

City #2: Virus deletes financial data!

City #3: Virus hacks city website!

Sophicity
We put the IT in city

How? – Virus $90K Xaction!

City #1: Real city that will remain anonymous.

- Finance officer gets a call from the city's bank.
- A transaction in the amount of **$90,000** was just attempted from her computer.
- Her computer was compromised by a virus. The virus allowed her computer to be **remotely controlled** by an outside party.
- Finance officer panicked. **What do I do?**

Sophicity
We put the IT in city

How? – Financial data gone!

City #2: Real city that will remain anonymous.

- **Finance server** became infected with a virus.
- City's data backup system **failed** to recover the data. **No one** had ever **tested** the backups!
- **Financial data lost**!

Data loss has **increased 400 percent** since 2012, while 71 percent of enterprises are not fully confident in their ability to recover after a disruption.

Search: 75032328
It's a great accounting program. Jenkins just downloaded it from deadlycomputervirus.com, sir.

Sophicity
We put the IT in city

How? – Website hacked!

City #3: Real city that will remain anonymous.

- **Citizens** visiting **the city's website** found nothing but advertisements. The website had been hacked and **all content replaced** with advertisements.
- The hacker **infiltrated** the **utility billing system** thru the online bill pay.

Citizen computers could have been infected with spyware/malware after visiting the city website. **Citizen information** may have been stolen.

Sophicity
We put the IT in city

Help!

1. Best Practices
2. Top 10 Most Common Issues
3. Take Aways

Best Practices

Guidelines for **best practices and policies** to mitigate potential **information security risks.**

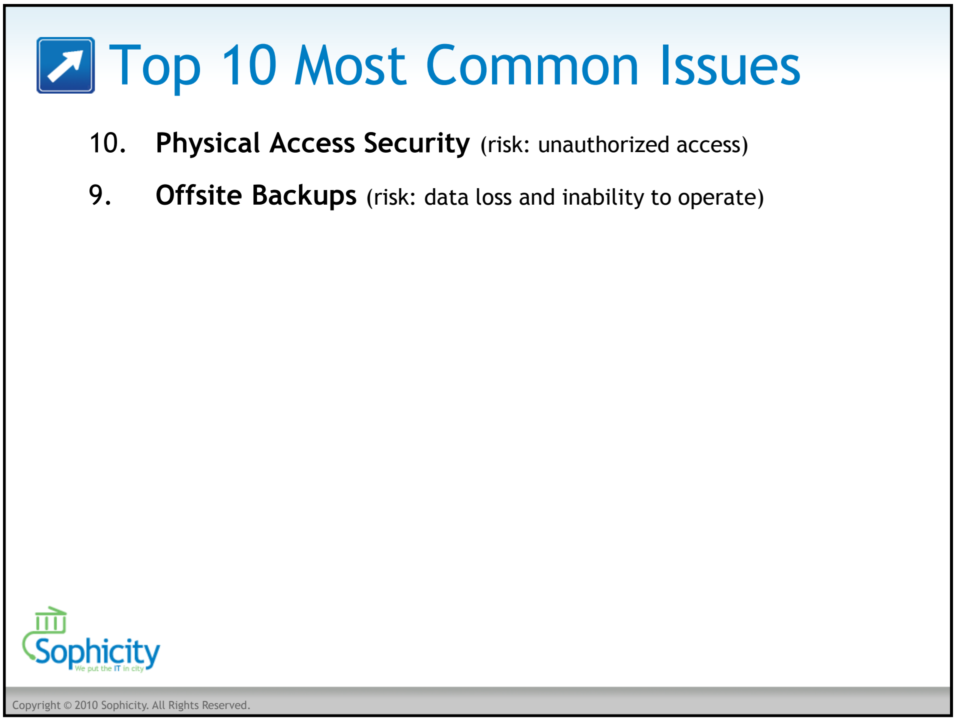
General Controls	Application Controls
• IS Management • Contract/Vendor Management • Network Security • Wireless Network Security • Physical Access Security • Logical Access Security • Disaster Recovery / Business Continuity	• Data Input • Data Processing • Data Output • Application Level General Controls

Top 10 Most Common Issues

Top 10

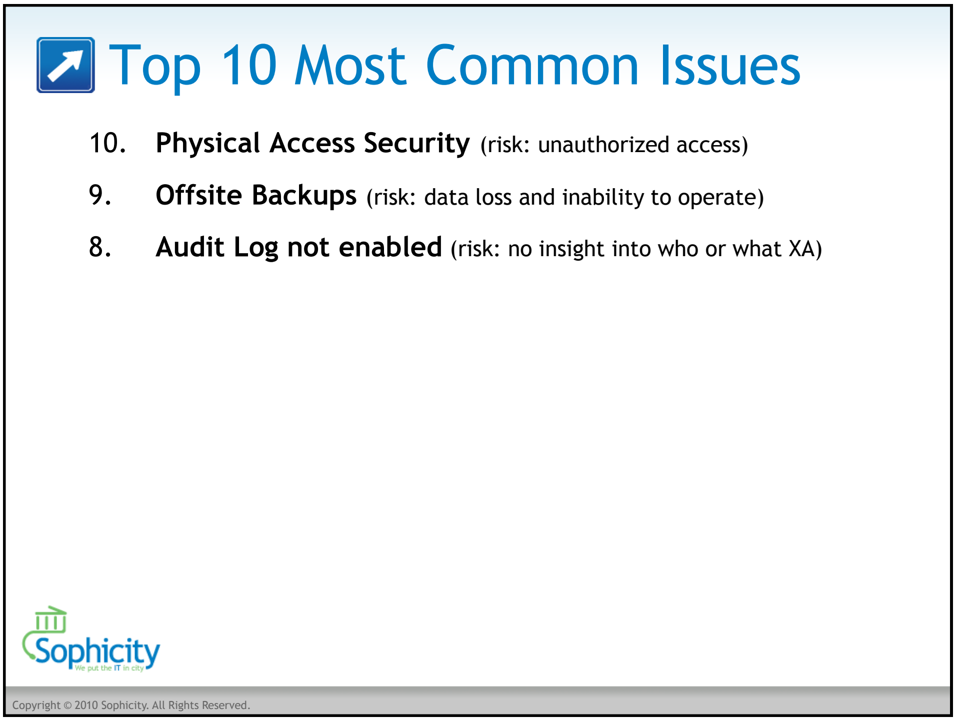
Top 10 Most Common Issues

10. **Physical Access Security** (risk: unauthorized access)



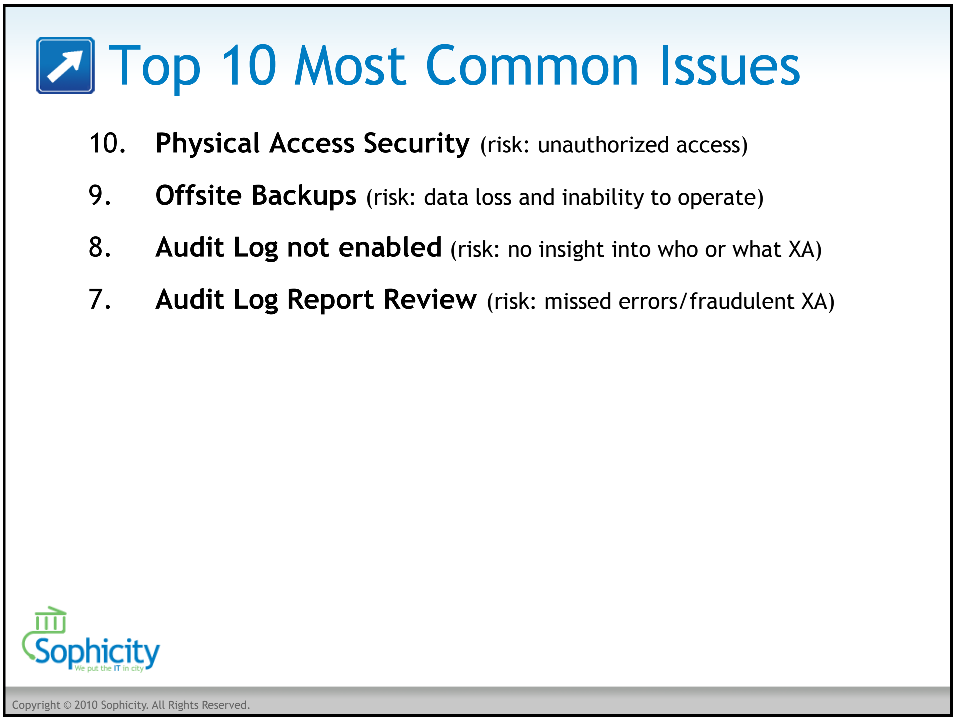
Top 10 Most Common Issues

10. **Physical Access Security** (risk: unauthorized access)
9. **Offsite Backups** (risk: data loss and inability to operate)



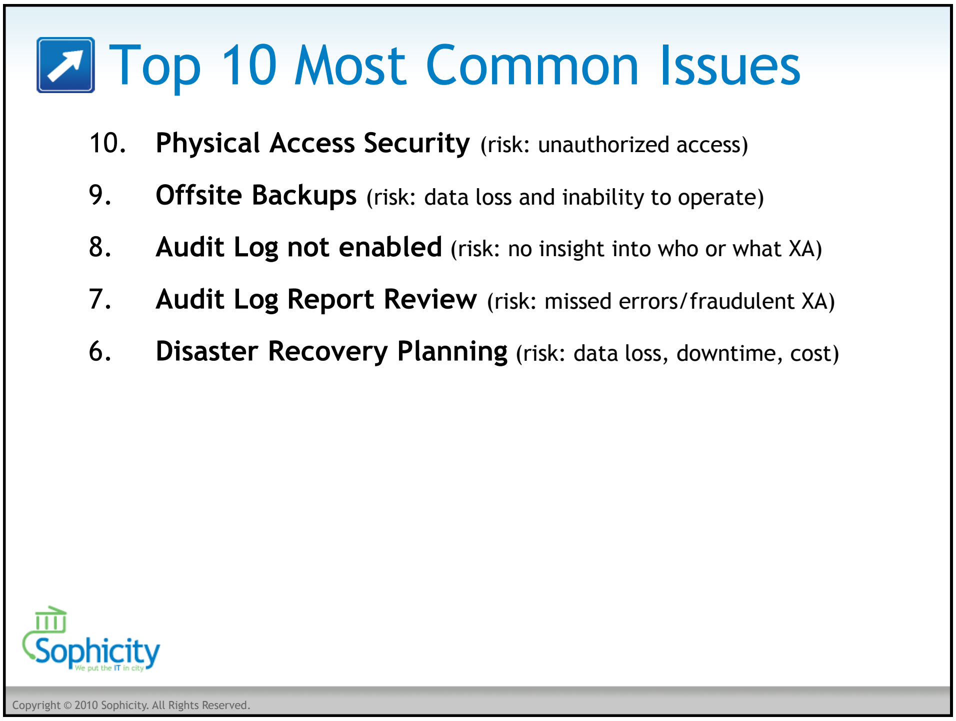
Top 10 Most Common Issues

10. **Physical Access Security** (risk: unauthorized access)
9. **Offsite Backups** (risk: data loss and inability to operate)
8. **Audit Log not enabled** (risk: no insight into who or what XA)



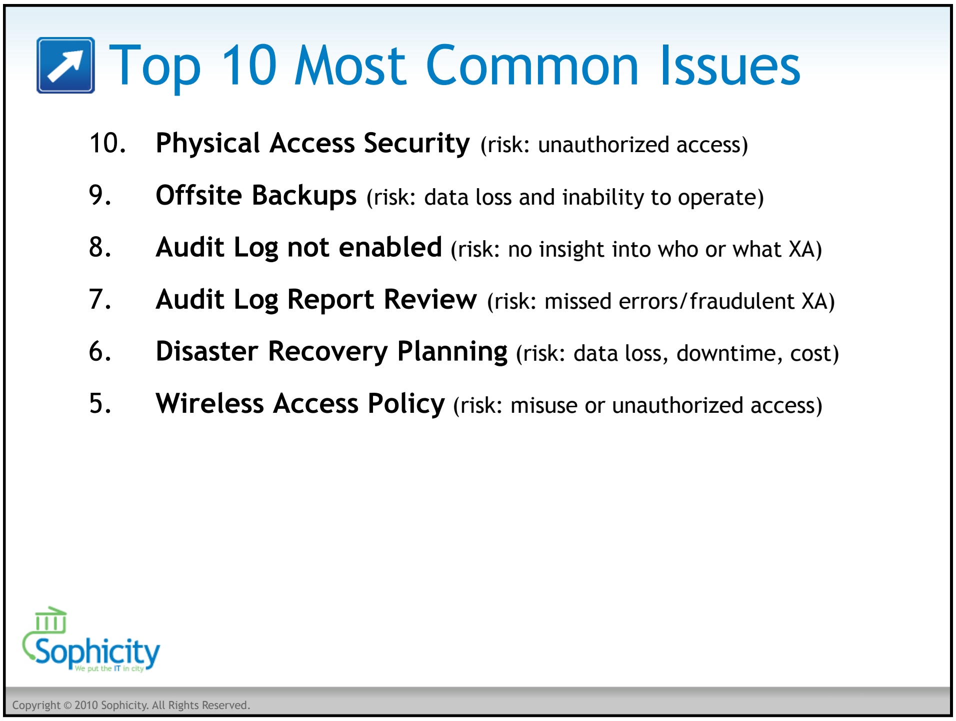
Top 10 Most Common Issues

10. **Physical Access Security** (risk: unauthorized access)
9. **Offsite Backups** (risk: data loss and inability to operate)
8. **Audit Log not enabled** (risk: no insight into who or what XA)
7. **Audit Log Report Review** (risk: missed errors/fraudulent XA)



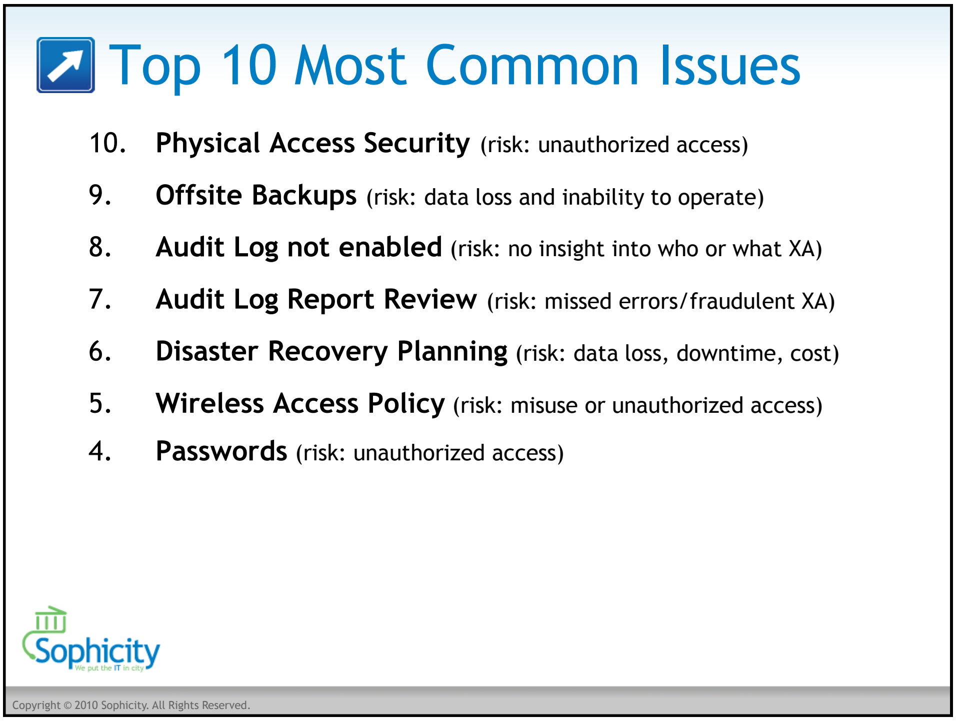
Top 10 Most Common Issues

10. **Physical Access Security** (risk: unauthorized access)
9. **Offsite Backups** (risk: data loss and inability to operate)
8. **Audit Log not enabled** (risk: no insight into who or what XA)
7. **Audit Log Report Review** (risk: missed errors/fraudulent XA)
6. **Disaster Recovery Planning** (risk: data loss, downtime, cost)



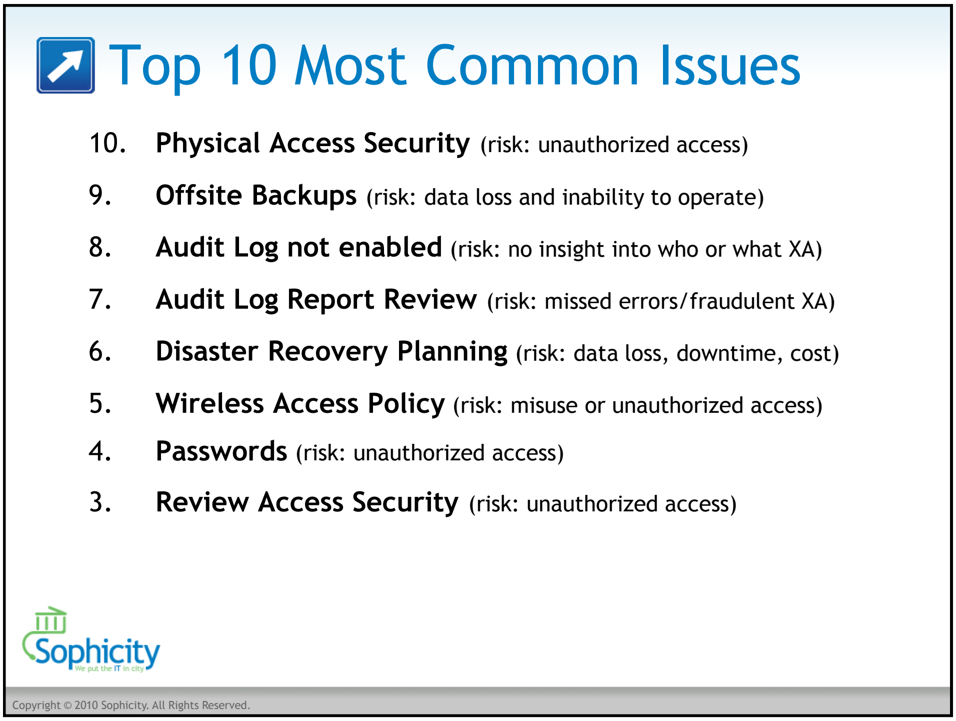
Top 10 Most Common Issues

10. **Physical Access Security** (risk: unauthorized access)
9. **Offsite Backups** (risk: data loss and inability to operate)
8. **Audit Log not enabled** (risk: no insight into who or what XA)
7. **Audit Log Report Review** (risk: missed errors/fraudulent XA)
6. **Disaster Recovery Planning** (risk: data loss, downtime, cost)
5. **Wireless Access Policy** (risk: misuse or unauthorized access)



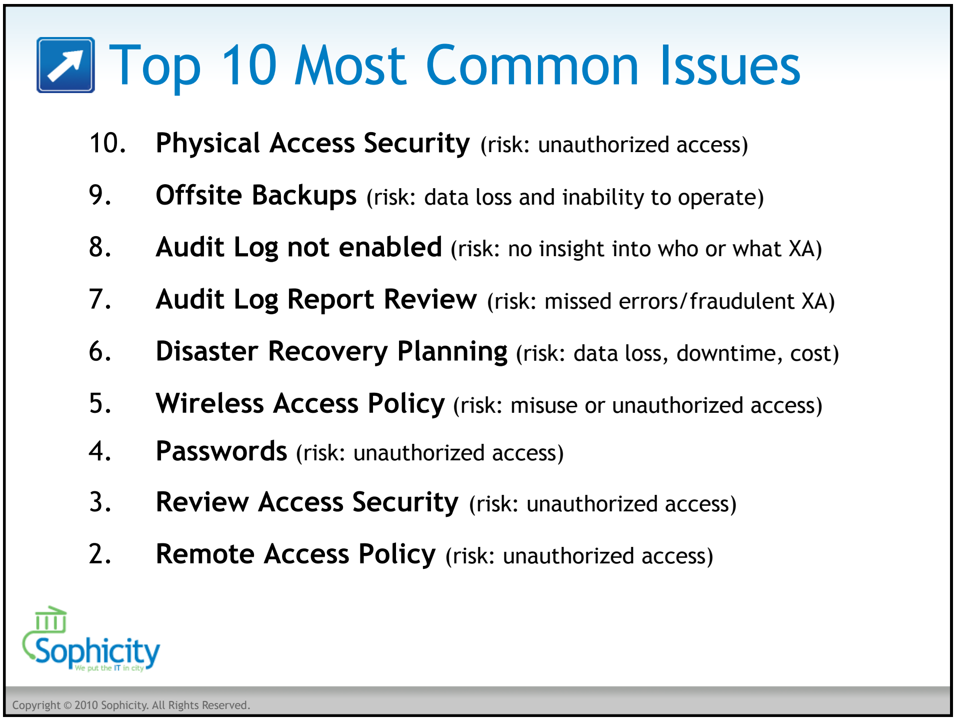
Top 10 Most Common Issues

10. **Physical Access Security** (risk: unauthorized access)
9. **Offsite Backups** (risk: data loss and inability to operate)
8. **Audit Log not enabled** (risk: no insight into who or what XA)
7. **Audit Log Report Review** (risk: missed errors/fraudulent XA)
6. **Disaster Recovery Planning** (risk: data loss, downtime, cost)
5. **Wireless Access Policy** (risk: misuse or unauthorized access)
4. **Passwords** (risk: unauthorized access)



Top 10 Most Common Issues

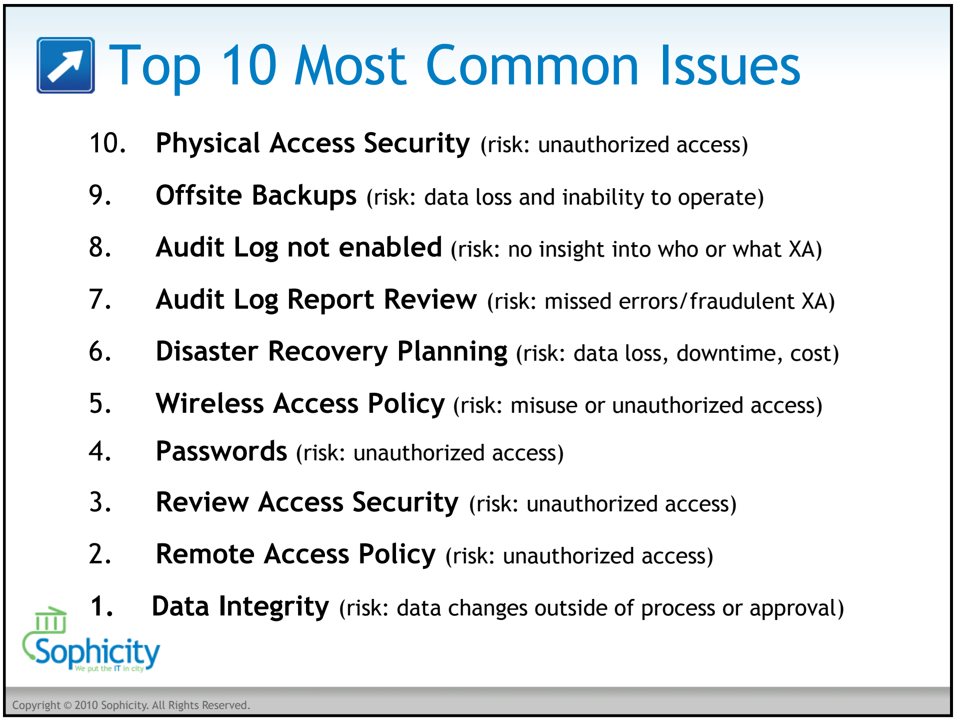
10. **Physical Access Security** (risk: unauthorized access)
9. **Offsite Backups** (risk: data loss and inability to operate)
8. **Audit Log not enabled** (risk: no insight into who or what XA)
7. **Audit Log Report Review** (risk: missed errors/fraudulent XA)
6. **Disaster Recovery Planning** (risk: data loss, downtime, cost)
5. **Wireless Access Policy** (risk: misuse or unauthorized access)
4. **Passwords** (risk: unauthorized access)
3. **Review Access Security** (risk: unauthorized access)



Top 10 Most Common Issues

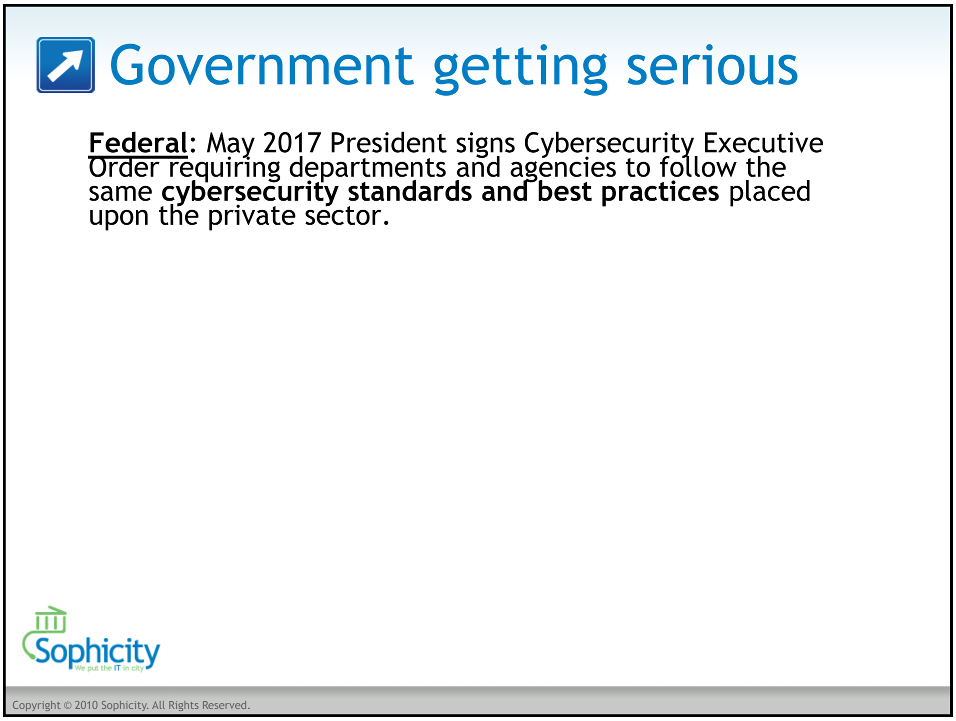
10. **Physical Access Security** (risk: unauthorized access)
9. **Offsite Backups** (risk: data loss and inability to operate)
8. **Audit Log not enabled** (risk: no insight into who or what XA)
7. **Audit Log Report Review** (risk: missed errors/fraudulent XA)
6. **Disaster Recovery Planning** (risk: data loss, downtime, cost)
5. **Wireless Access Policy** (risk: misuse or unauthorized access)
4. **Passwords** (risk: unauthorized access)
3. **Review Access Security** (risk: unauthorized access)

2. **Remote Access Policy** (risk: unauthorized access)



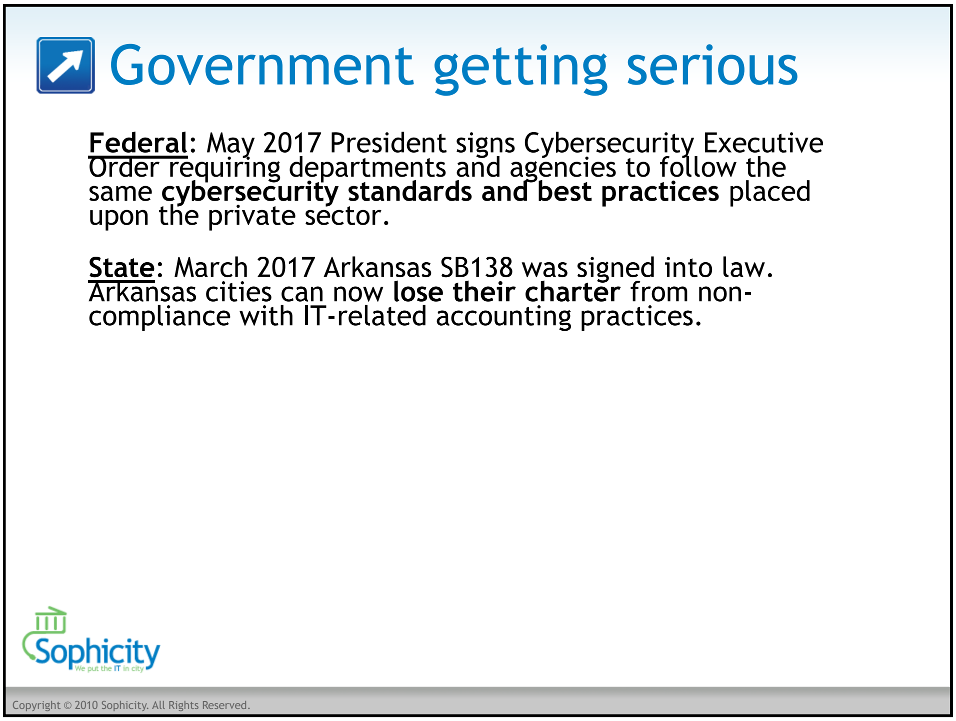
Top 10 Most Common Issues

10. **Physical Access Security** (risk: unauthorized access)
9. **Offsite Backups** (risk: data loss and inability to operate)
8. **Audit Log not enabled** (risk: no insight into who or what XA)
7. **Audit Log Report Review** (risk: missed errors/fraudulent XA)
6. **Disaster Recovery Planning** (risk: data loss, downtime, cost)
5. **Wireless Access Policy** (risk: misuse or unauthorized access)
4. **Passwords** (risk: unauthorized access)
3. **Review Access Security** (risk: unauthorized access)
2. **Remote Access Policy** (risk: unauthorized access)
1. **Data Integrity** (risk: data changes outside of process or approval)



Government getting serious

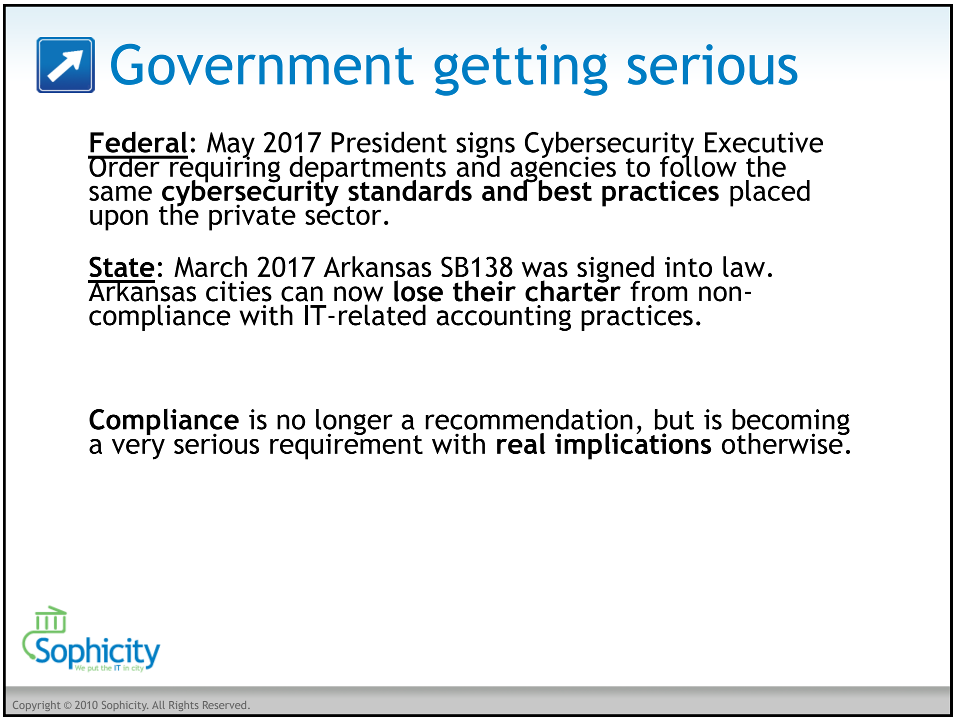
<u>Federal</u>: May 2017 President signs Cybersecurity Executive Order requiring departments and agencies to follow the same **cybersecurity standards and best practices** placed upon the private sector.



Government getting serious

Federal: May 2017 President signs Cybersecurity Executive Order requiring departments and agencies to follow the same **cybersecurity standards and best practices** placed upon the private sector.

State: March 2017 Arkansas SB138 was signed into law. Arkansas cities can now **lose their charter** from non-compliance with IT-related accounting practices.

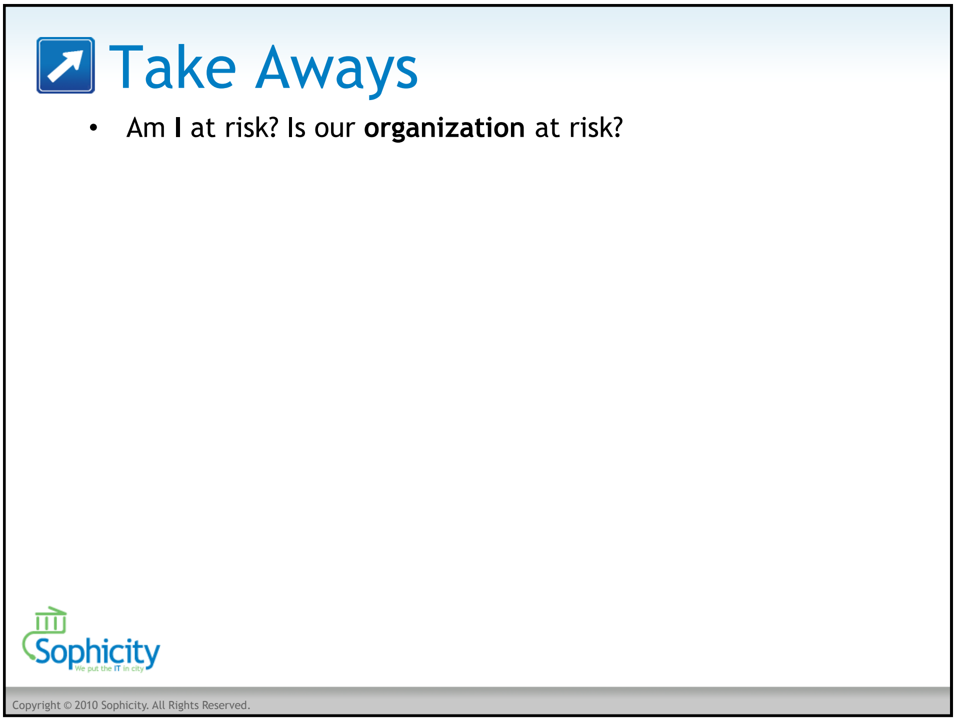


Government getting serious

Federal: May 2017 President signs Cybersecurity Executive Order requiring departments and agencies to follow the same **cybersecurity standards and best practices** placed upon the private sector.

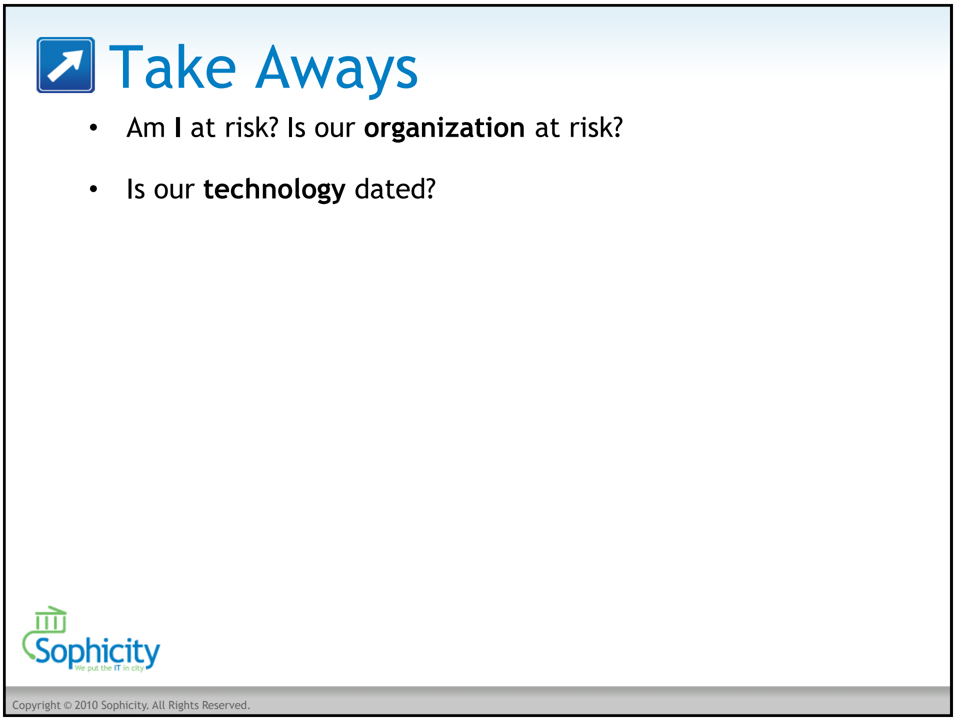
State: March 2017 Arkansas SB138 was signed into law. Arkansas cities can now **lose their charter** from non-compliance with IT-related accounting practices.

Compliance is no longer a recommendation, but is becoming a very serious requirement with **real implications** otherwise.



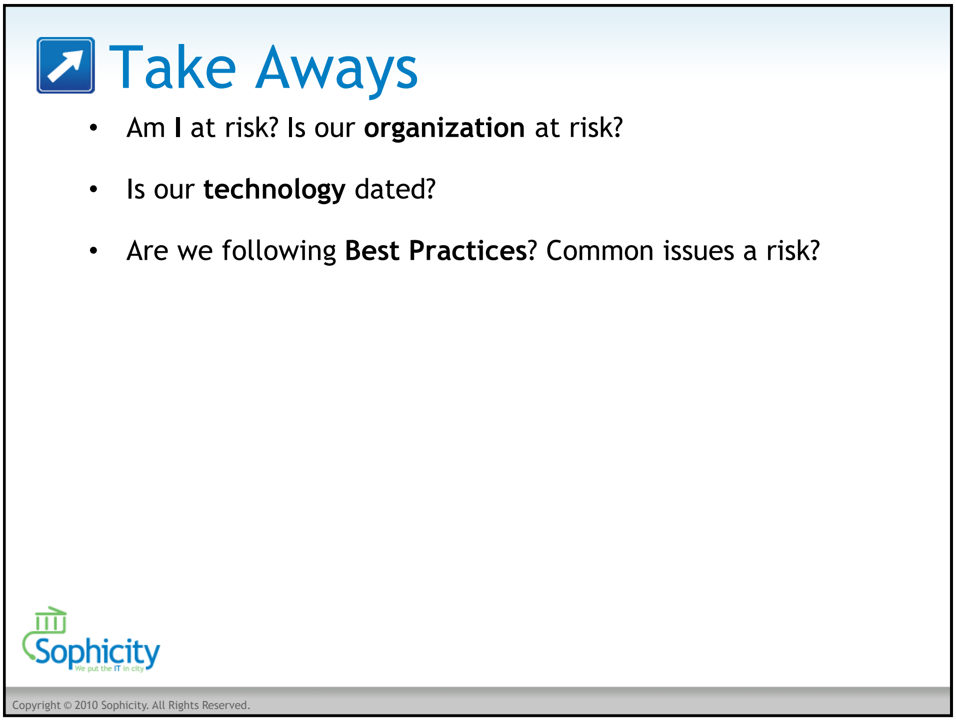
Take Aways

- Am **I** at risk? Is our **organization** at risk?



Take Aways

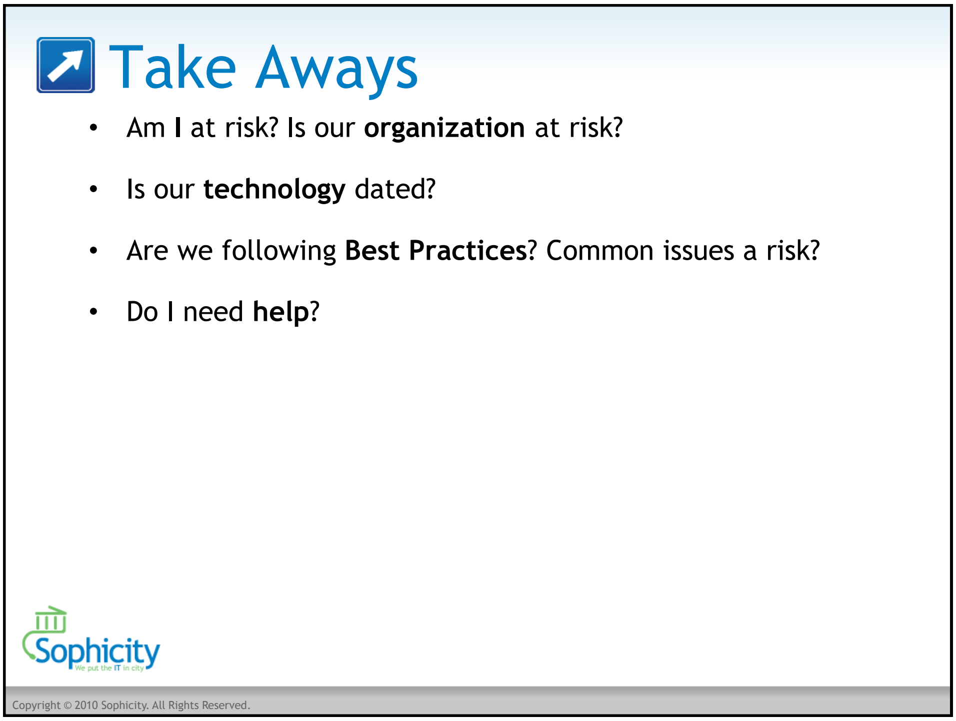
- Am **I** at risk? Is our **organization** at risk?
- Is our **technology** dated?



Take Aways

- Am **I** at risk? Is our **organization** at risk?
- Is our **technology** dated?
- Are we following **Best Practices**? Common issues a risk?

Sophicity
We put the IT in city



Take Aways

- Am **I** at risk? Is our **organization** at risk?
- Is our **technology** dated?
- Are we following **Best Practices**? Common issues a risk?
- Do I need **help**?

Sophicity
We put the IT in city

KLC’s IT in a Box

Who guarantees IT services based on your expectations?

WE DO!

New City Website
Modern fresh design. We manage the content. Accept online payments.

Data Backup
Unlimited offsite data backup storage for disaster recovery. Indefinite retention for data backup archiving. Realtime monitoring. Quarterly testing.

Document Management
Protect city records. Apply record retention schedules.

Email
Separate personal and city business. Share calendars. Includes Microsoft Office Professional Plus.

Open Records Requests
Be prepared for FOIA and Open Records Requests. We will help the clerk process them.

Video Archiving
No more buying additional onsite storage for squad car and body camera videos!

Policy & Compliance
Formally adopt best practices and policies to address information security risks.

Vendor Management
No more frustrating calls with vendors. We got it.

Helpdesk
24x7. We are always there when you need help.

Server, Desktop,& Mobile Management
Guard against cyber attack. Keep your computers patched, protected, and healthy.

Certified
Experienced certified senior engineers. We are GCIC certified.

Sophicity
We put the IT in city

Recap

What? – We’ve covered ‘What you need to know’?

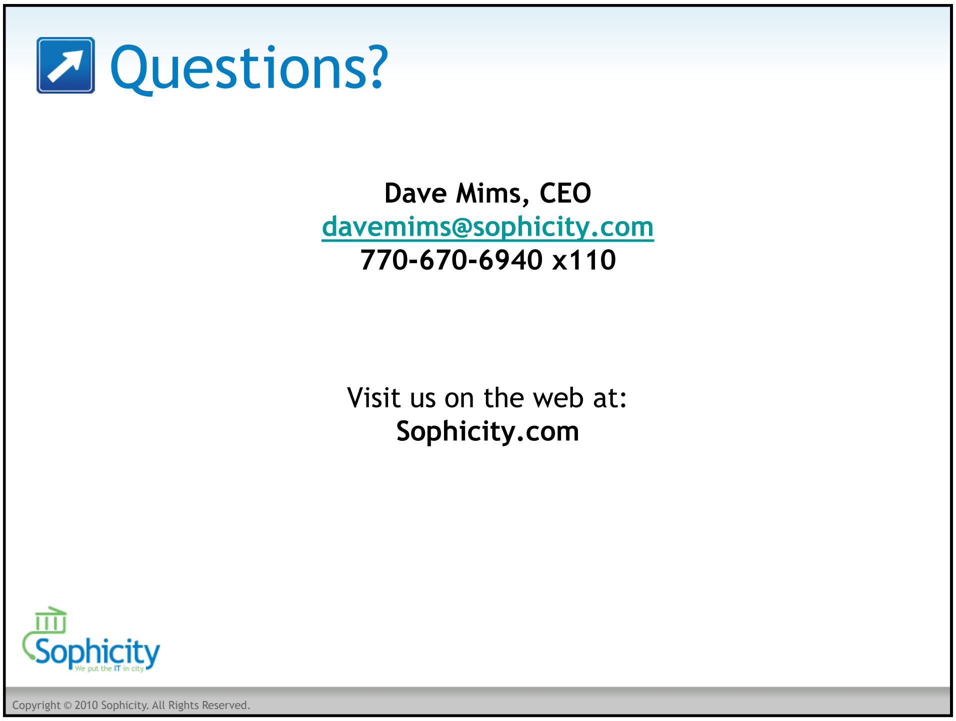
How? – We’ve covered ‘How some real cities have been impacted’?

Help! – We’ve covered ‘Best Practices and Common Issues’!

Know cyber crimes affect all organizations, not just big ones.

Don’t be an easy target. Don’t be a victim. Don’t be front page news. -- Take action! Be alert! Be proactive!

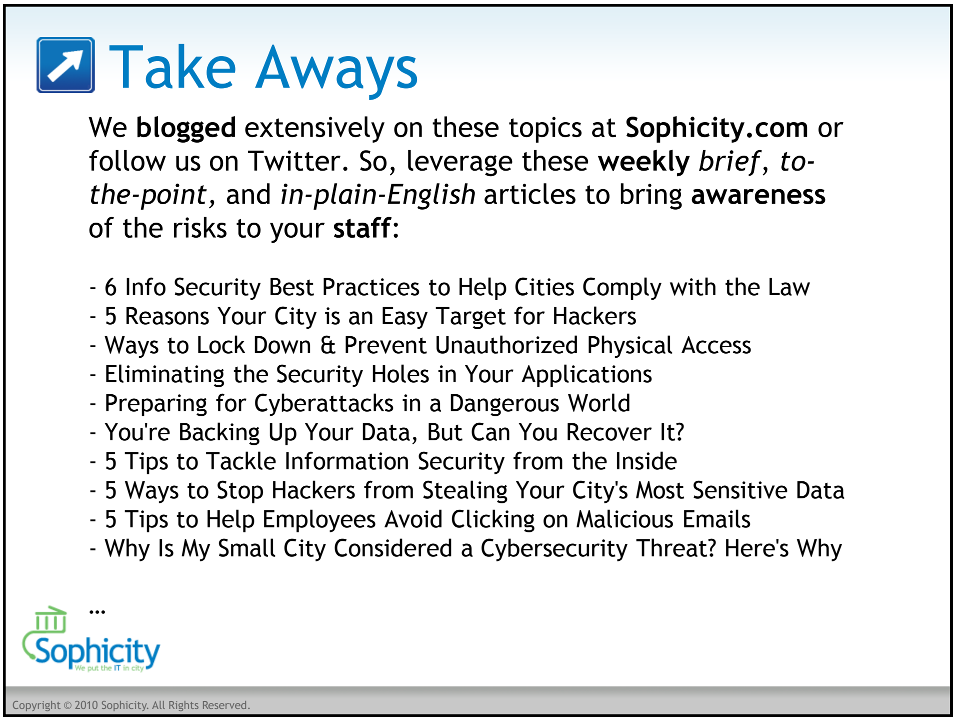
Sophicity
We put the IT in city



Questions?

Dave Mims, CEO
davemims@sophicity.com
770-670-6940 x110

Visit us on the web at:
Sophicity.com



Take Aways

We **blogged** extensively on these topics at **Sophicity.com** or follow us on Twitter. So, leverage these **weekly** *brief*, *to-the-point*, and *in-plain-English* articles to bring **awareness** of the risks to your **staff**:

- 6 Info Security Best Practices to Help Cities Comply with the Law
- 5 Reasons Your City is an Easy Target for Hackers
- Ways to Lock Down & Prevent Unauthorized Physical Access
- Eliminating the Security Holes in Your Applications
- Preparing for Cyberattacks in a Dangerous World
- You're Backing Up Your Data, But Can You Recover It?
- 5 Tips to Tackle Information Security from the Inside
- 5 Ways to Stop Hackers from Stealing Your City's Most Sensitive Data
- 5 Tips to Help Employees Avoid Clicking on Malicious Emails
- Why Is My Small City Considered a Cybersecurity Threat? Here's Why

…