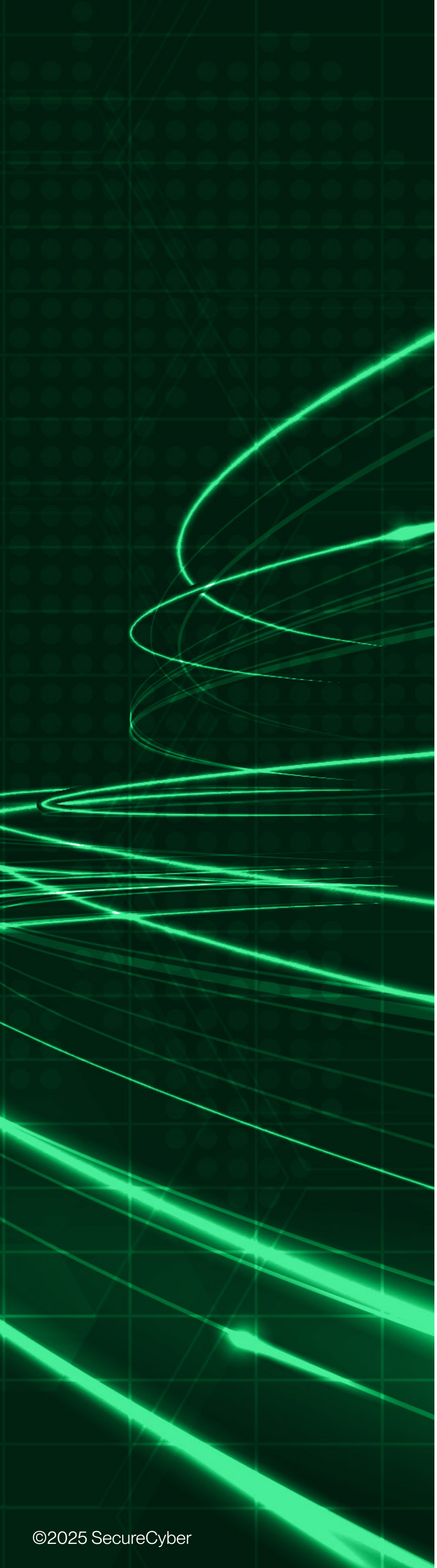

SECURECYBER™

Proven. Proactive. Personalized.

The Ultimate HB96 Cybersecurity Resource Guide for Local Governments:

Helping local government meet the requirements of HB96 to protect critical data, infrastructure, and recover in the event of a cybersecurity incident.

July 2025

SecureCyber exists to guide, protect, and defend in the daunting world of cyber warfare. We give you peace of mind that your organization, employees, and citizens are shielded from cyber threats. As an Ohio-based company, we are centrally located to manage and secure data and networks wherever you have locations.

www.securecyberdefense.com

Understanding the Threat Landscape

Ransomware: A Growing Threat for Local Government

- According to a report by the FBI's Internet Crime Complaint Center, government agencies were the third largest critical infrastructure sector targeted by ransomware attacks in 2023.
- In April last year, the Ohio state auditor reported at least 23 cyberattacks against government offices in the last 12 months.
- Recent ransomware attacks have crippled cities including Columbus, Cleveland, and Huber Heights compromising residents' personal information and slowing down services
- Local Governments are frequent cyberattack targets due to their political significance and the essential services they provide.

Case Study Snapshot:

(2024) On July 18, the City of Columbus was the victim of a ransomware attack. In this case, the attackers, known as the Rhysida ransomware group, sought to impair the city's IT infrastructure and possibly use ransomware to demand a sizeable payment of $1.9 million. Although the encryption attempt was unsuccessful, the attackers were able to exfiltrate a large amount of data, claiming to have taken 6.5 terabytes of data impacting 500,000 individuals.

A city employee was able to identify the attack vector as a file download from an internet domain. This download enabled the attackers to obtain access to the city's internal network. The City of Columbus' Department of Technology rapidly discovered the issue and cut off internet connectivity to prevent additional exposure.

Why This Matters to YOU

As a city administrator, you're responsible for protecting city, staff and citizen data. Cybersecurity isn't just an IT issue anymore — it's a business issue. Creating open lines of communication between city leadership and IT teams is a critical step in developing a cyber aware culture. The State of Ohio is requiring more transparency on security measures, recovery plans, threat monitoring, threat response methods, and training of administrative staff and employees because attackers are getting smarter and more determined.

What's The Impact?

- Compromised citizen records and sensitive HR files
- Lost access to city services
- Emergency incident response costs, loss of trust, and PR headaches
- Insurance costs and premium increases
- Damaged or compromised equipment to replace
- Legal costs and compliance penalties

What standards does HB96 Require?

- Encryption of data at rest an in transit
- Multi-factor authentication for system access
- Patch management to reduce known vulnerabilities
- Vendor oversight with cybersecurity requirements in contracts
- Documented incident response plan
- Annual compliance attestation to the state

Cybersecurity Crash Course for City Leadership

What Are the Most Common Risks?

- **Phishing Emails:** Trick staff and administrative staff into clicking malicious links or sharing usernames and passwords.
- **Hacking:** Unauthorized access to computer systems or data by students or external cyber criminals.
- **Malware:** Malicious software that infects a computer usually through suspicious email links or downloads from unsafe websites.
- **Ransomware:** Cyber criminals access and download sensitive information then encrypt (lock up) the data while requesting a ransom be paid to restore access or not sell the data to criminals.
- **Social Engineering/Impersonations:** A common approach used by cyber criminals is to mine data from social media accounts, understand the behaviors of executives, pull pictures of staff, logos, and school materials to impersonate known people to convince staff or students to share sensitive information or take action based on urgent requests.
- **Third Party Breach:** A third party platform or cloud provider that is breached allowing access to school systems through their API or network connection.

What's at Stake?

- **State of Ohio Violations:** Citizen privacy breach = legal exposure.
- **Reputation Damage:** The community and the media will be watching.
- **Loss of Critical Systems:** Losing critical systems and access to data can paralyze a city and its infrastructure for multiple weeks.
- **Financial Impact:** Paying a ransom, replacing damaged equipment, hiring incident response teams, increased cyber insurance costs, and downtime can translate into significant unplanned costs.

Must-Know Terms

Ransomware	Malware that locks systems and demands payment.
Phishing	Emails designed to trick staff into revealing login info.
Social Engineering	The tactic of manipulating, influencing, or deceiving a victim in using convincing information or identities in order to gain control over a computer system, or to steal personal and financial information.
Business Email Compromise	Impersonating school district leadership in emails to gain access to computer systems or for unauthorized financial payments.
Endpoint	Any device connected to the network (laptops, tablets, etc.).
Access Control	Controlling who needs access to specific systems and data.
Multi-Factor Authentication	Requiring two or more verified sign-in mechanisms to access protected systems or databases.
Patching and Updates	Software and system providers regularly provide security updates to their systems once they become aware of vulnerabilities. Timely patching provides increased security protections.
Threat Alerts	Alerts forwarded to IT teams from security systems indicating suspicious activity.
Zero Trust	Security model that assumes no device or user is safe by default.

SECURECYBER™
Proven. Proactive. Personalized.

City Leadership and IT Team Partnership Checklist

Start The Conversation: Identifying Potential Threats

Ask these questions in your next leadership meeting with your IT team. The goal is to help familiarize yourself with current practices and cybersecurity measures. The objective is to form a partnership to understand how cyber threats are being handled, what's needed to improve the city's cyber program, and how to achieve compliance with HB96 — not to put your IT team on the defensive.

Risk Awareness

1. What are the top 3 cybersecurity threats for our city right now?

   notes: ....

   ....

   ....

2. How are we monitoring for potential ransomware activity?

   notes: ....

   ....

   ....

3. How many cyber threats are we dealing with each day?

   notes: ....

   ....

   ....

4. What protections and reporting requirements do our service providers and platforms provide in the event of a breach?

   notes: ....

   ....

   ....

5. Have we mapped out the location of all sensitive citizen and staff information, where it's stored, and who has access to it?

   notes: ....

   ....

   ....

6. How are we managing system access and passwords?

   notes: ....

   ....

   ....

City Leadership and IT Team Partnership Checklist (continued)

Current Protections

1. Do we have multi-factor authentication (MFA) in place for all citizen and staff logins?

   notes:

2. Are city devices filtered and monitored for unsafe behavior?

   notes:

3. How often do we update and patch our software?

   notes:

4. What cybersecurity protections are provided with the platforms and cloud providers the city uses? Is this detailed in their contracts?

   notes:

5. Are our security devices up-to-date? What is needed?

   notes:

6. How frequently do we run vulnerability tests?

   notes:

7. Are we running our own security program or do we use a partner?

   notes:

8. What are the cybersecurity responsibilities of our outside IT providers? What responsibilities are covered in their contract?

   notes:

Education/Training

1. What is the current cybersecurity training and certification levels of the IT staff or our IT providers?

   notes:

2. What type of online safety training are we providing our staff?

   notes:

3. What cybersecurity skill/certification training and is our IT staff taking?

   notes:

4. Do we regularly conduct phishing attempts and provide training on how to recognize phishing and social engineering?

   notes:

City Leadership and IT Team Partnership Checklist (continued)

Incident Response

1. Do we have a documented incident response plan if we get hit with ransomware?

   notes:

2. How often do we practice this and make updates?

   notes:

3. Do we have a documented recovery plan and projected timelines should we experience a full-system shutdown?

   notes:

4. What breach reporting responsibilities do our outside platforms and cloud providers have?

   notes:

Compliance and Reporting

1. Are we compliant with current cybersecurity protocols (NIST/CIS)?

   notes:

2. What cyber metrics should we share with the city commission, and how often?

   notes:

3. How do we store threat data and vulnerability testing information?

   notes:

4. How do we document improvements to our cybersecurity program?

   notes:

How Cyber-Ready Are We?

Work with your IT team to understand each area.

Score each area as:

✓ Green (Confident) ⚠ Yellow (In Progress) ⊗ Red (Needs Attention)

Area	Score	Notes
Staff cybersecurity training		
MFA for staff/admin accounts		
Offsite backup systems and testing		
Endpoint protections on laptops and mobile devices		
Privileged access to sensitive systems		
Daily monitoring of cyber threats/alerts		
Security updates and patch schedule		
Cyber insurance coverage		
Annual security evaluation such as penetration testing		

Next Steps Based on Your Score

Mostly Green

Refine and improve reporting.
You're ahead of the curve.

Mix of Yellow / Red

Focus on top 3 weaknesses. Prioritize training and response plans. Examine gaps in security equipment and monitoring to set a budget and improvement plan. Consider bringing in an independent consultant.

Action Plan + Follow-up

Action Items

Your 30-Day Cyber Confidence Plan

1. Schedule a meeting with your IT lead using the checklist to assess your current posture.
2. Identify 3 significant risks for your city's systems.
3. Implement the essentials (MFA, patch management, encryption, and centralized logging).
4. Update policies and incident response plans to comply with HB96.
5. Prepare your reporting and documentation process.
6. Share your current status with your leadership team and agree on next steps.
7. Reinforce staff and administrative team's role in maintaining data security, awareness of phishing and social engineering, and minimizing risky online behaviors.
8. Set up regular progress meetings with your IT staff.
9. Establish a regular reporting schedule with your city commission.
10. Engage a trusted partner if you don't have the resources or cyber expertise.

Next Steps

Congratulations on completing the Cybersecurity Workbook for Local Governments! By working through each step and implementing the recommendations, you've taken a significant step toward protecting your city from cyber threats. Remember, cybersecurity is an ongoing process since cyber criminals frequently change their tactics. Stay informed about emerging threats, regularly review and update your security measures, and continue to educate your staff about cybersecurity best practices.

Want Support?

SCAN ME

Schedule a 1:1 consultation with our cybersecurity specialists to review and support your cyber readiness plan.

Ohio Civic Shield from SecureCyber is an all-in-one solution that gives municipalities the tools, expert guidance, and documentation needed to meet and stay compliant with the mandates and reporting requirements of HB96 — efficiently, affordably, and with local support.

SECURECYBER™

Proven. Proactive. Personalized.