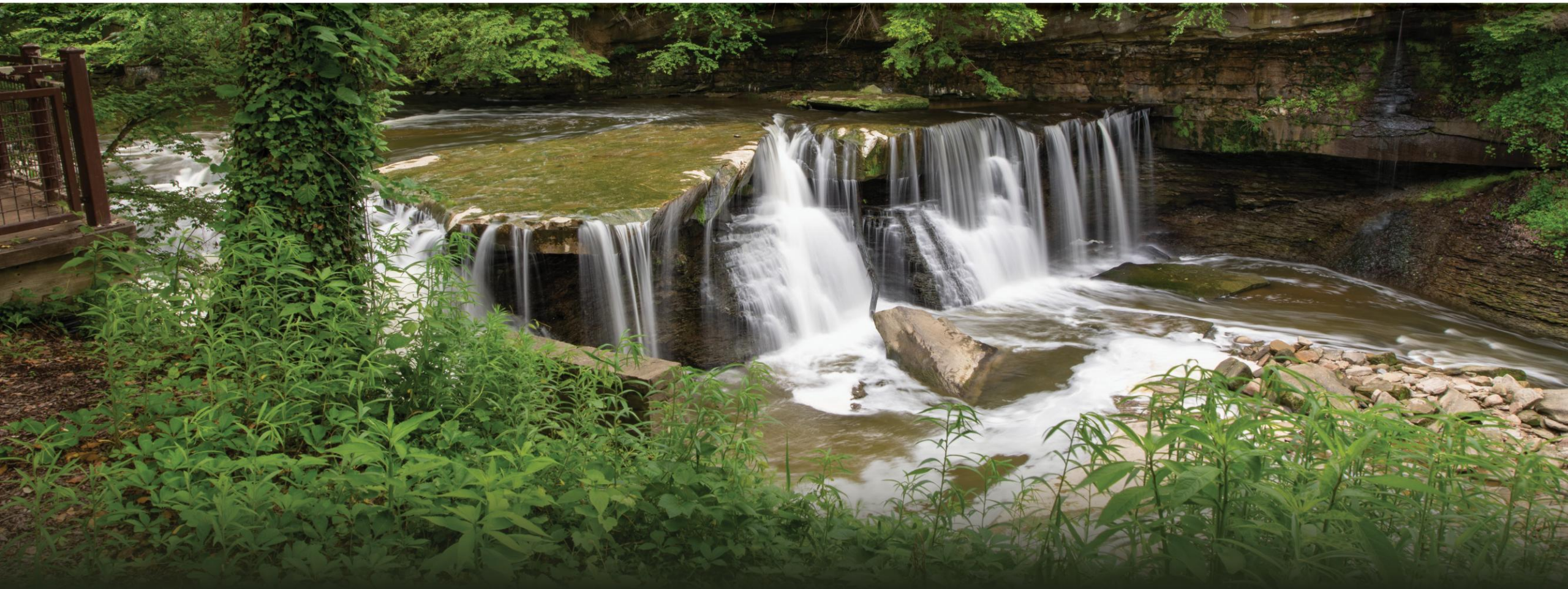
Your Time Your Place
CLEVELAND METROPARKS

HB 96 Ohio Cybersecurity Law

Priscila Rocha, Legal Counsel
Phillip Ruzicho, Cybersecurity Architect

May 21, 2026



The Cyber Threat

WHY CYBERSECURITY MATTERS

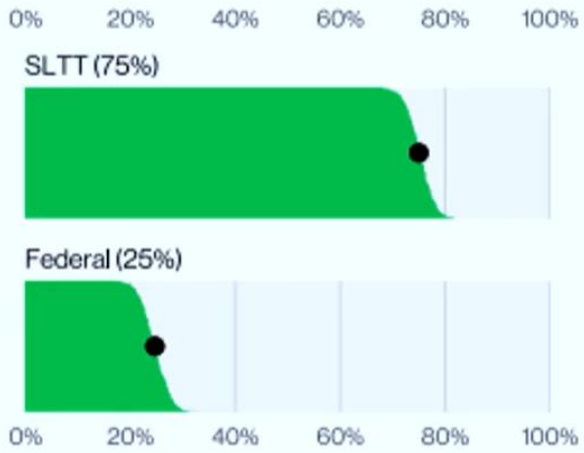


Figure 7. Ransomware victims by government level (n=312)

What's the common link in most data breaches? The human element.

60%

Human involvement in cybersecurity breaches remained about the same as the previous year – 60%.

Credential abuse and social actions – like phishing – were major factors in these types of breaches.

VERIZON DBIR

The Blueprint for an Attack

How Public Data Fuels Modern Cyberattacks

- **Case 1: Open-Record Contract Weaponization (Cabarrus County, NC / City of Ocala, FL, 2019)**
  - Threat Actor: Corporate Impersonation Fraud Syndicates
  - The Source: Mandated public disclosures of active vendor contracts and finance staff directories.
  - The Impact: $3.2M in public funds diverted via fraudulent electronic payment routing forms.
  - The Vulnerability: Public compliance records provided a pre-built social engineering blueprint, bypassing technical controls entirely.
- **Case 2: Human Recon (MGM Resorts, 2023)**
  - Threat Actor: Scattered Spider
  - The Source: Employee bio and role details found on LinkedIn.
  - The Impact: A 10-minute "vishing" call to the Help Desk led to a $100M loss.
  - The Vulnerability**:** Attackers used easily accessible personal info to bypass standard help desk security questions.

The Blueprint for an Attack Continued

AI-Driven Cyberattacks

- **Case 3: AI-Driven Directory Scraping (Ohio Local Governments)**
  - Threat Actor: AI-Accelerated Fraud Syndicates
  - The Source: Online employee directories and organizational charts required by state Sunshine laws.
  - The Impact: Automated harvesting of rosters led to targeted "Whaling" campaigns and urgent Ohio Auditor of State alerts.
  - The Vulnerability: Generative AI scaled open-source intelligence, turning static transparency registries into active target-acquisition catalogs.

PHISHING, SOCIAL ENGINEERING, AND PUBLIC INFORMATION USED FOR CYBER ATTACKS

Publicly available government records and personnel information are routinely harvested by attackers to build believable pretexts for spear-phishing and targeted social-engineering attacks.

Organizational Charts & Staff Directories

- Attackers can download or request public staff rosters, meeting minutes, or org charts to see who holds authority.
- They then impersonate a manager (via spoofed email or phone) and pressure subordinates into sending sensitive data, approving wire transfers, or granting access.

Public Procurement & Technology Disclosures

- Procurement records (contracts, RFPs, purchase orders) often reveal the exact software and hardware a government entity uses.
- Adversaries study these documents to identify unpatched systems or software with known vulnerabilities.
- Once they know a county still runs an older firewall or outdated version of Microsoft Exchange, attackers can craft exploits or phishing emails that appear to come from the vendor.

Meeting Agendas, Calendars & Reports

- Public calendars and meeting agendas can reveal when key staff are traveling, when IT systems will be down for maintenance, or when sensitive initiatives are being discussed.
- Attackers time spear-phishing campaigns to coincide with absences ("while the CIO is out of office"), increasing the chance of success.

Personnel Records & Licenses

- Public record disclosures (licenses, pay scales, credential lists) can expose personal emails, dates of birth
- This data feeds identity theft, tailored phishing ("We need to update your HR file")

Takeaway

Every public disclosure, from contracts to calendars, can be weaponized. Agencies must treat public records as part of their **attack surface**, carefully redacting sensitive details and balancing transparency with security.

HB 96: Key Cyber Mandates for Local Governments

Under the new law, RC 9.64, local government entities must:

- Implement a cybersecurity program
- Obtain approval from their legislative body for ransomware payments
- Report cybersecurity incidents within specific timeframes to DPS and AOS

Law also includes:

- Public records exemption

Develop Cyber Program

Local Governments Must:

- Establish a cybersecurity program that:
  - Safeguards data and systems
  - Ensures confidentiality, integrity, and availability of data and systems

Follows best practices like:

- National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF)
- Center for Internet Security (CIS) controls

NIST Cybersecurity Framework 2.0

A flexible, scalable framework that helps any organization, from a global corporation like Parker Hannifin to a local government agency like Cleveland Metroparks, identify cybersecurity gaps and build a prioritized plan to close them.

The 6 Core Functions:

GOVERN
Set policy, assign roles & define risk tolerance

IDENTIFY
Map assets, data, and cybersecurity risks & gaps

PROTECT
Implement controls to limit the impact of incidents

DETECT
Continuously monitor for threats and anomalies

RESPOND
Contain incidents and communicate with stakeholders

RECOVER
Restore services and apply lessons learned

How It Works:

1. Assess current state → 2. Identify gaps → 3. Score & prioritize → 4. Build action plan → 5. Repeat & improve

Works the same way whether you are a park district or a Fortune 500 corporation. The framework scales to your resources and risk profile.

Why CSF 2.0:

- Vendor-neutral and sector-agnostic. Adopted by government agencies and private industry alike
- Adds GOVERN as a 6th function, elevating cybersecurity as an enterprise-level risk management priority
- Enables Current vs. Target Profile scoring so organizations can quantify gaps and sequence investments

Who Must Comply and When

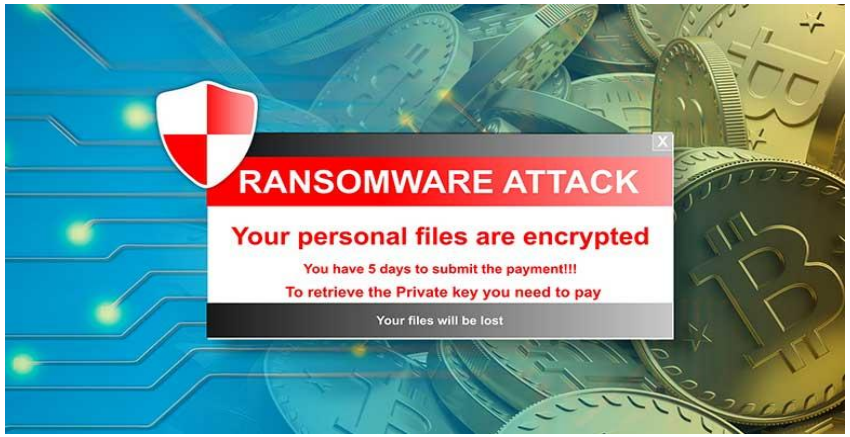
Applies to all political subdivisions under the state:

- "Political subdivision" means a county, township, municipal corporation, or other body corporate and politic responsible for governmental activities in a geographic area smaller than that of the state
- Implementation due dates:
  - Cities & Counties: January 1, 2026
  - All Other Entity Types: July 1, 2026

Incident reporting requirements are effective as of September 30, 2025

Auditors will test compliance in FY26 Local Government Audits

Ransomware Payment Restrictions



New Requirement

Local governments may not pay or comply with ransomware demands unless:

- A formal resolution or ordinance is passed by board
- The resolution must justify why payment is in the best interest of the jurisdiction

Cyber Incident Reporting Requirements

After a Cyber or Ransomware Incident, Local Governments Must Notify:

Ohio Department of Public Safety (DHS/OHS)

- Within 7 days
- To be submitted to the **Ohio Cyber Integration Center (OCIC)**

Ohio Auditor of State (AOS)

- Within 30 days

HB 96: Public Records Exemption

Records related to:

- Cybersecurity programs
- Cyber Incident reports
- Cyber-related procurement documents

Are NOT public records under RC 149.43

This protects the confidentiality of sensitive systems

What is a Public Record

"Records" includes any document, device, or item, regardless of physical form or characteristic,

- including an electronic record, created or received by or coming under the
- jurisdiction of any public office, which serves to document the
- organization, functions, policies, decisions, procedures, operations, or other activities of the office

* Unless excluded from the definition by law

Exemptions

ORC 149.433	Infrastructure Records Security Records
ORC 9.64	Cybersecurity records

Cybersecurity Records

Ohio Revised Code 9.64(E)

Any records, documents, or reports related to the cybersecurity program and framework are not public records

The reports of a cybersecurity incident or ransomware incident are not public records

Cybersecurity Records

Ohio Revised Code 9.64(F)

A record identifying cybersecurity-related software, hardware, goods, and services,

- that are **being considered for procurement, have been procured, or are being used** by a political subdivision,
- including the **vendor name, product name, project name, or project description**, is a security record
- Not a public record

Examples

MODEL NUMBERS AND DESCRIPTIONS OF COMPUTER EQUIPMENT ON PURCHASE ORDERS

EMPLOYEE ID NUMBERS

CYBERSECURITY VENDOR NAMES AND SERVICES

CYBERSECURITY INSURANCE DOCUMENTS

EMPLOYEE TITLES ON HR LISTS

Cybersecurity Policy Update

BOARD OF PARK COMMISSIONERS OF THE
CLEVELAND METROPOLITAN PARK DISTRICT
POLICY STATEMENT

SUBJECT: Cybersecurity Policy

EFFECTIVE DATE: June 18, 2026

I. Purpose

This Cybersecurity Policy establishes the framework, guidelines, responsibilities, and behavioral standards required to protect Cleveland Metroparks' information systems, data, and technology assets. This policy applies to all employees, volunteers, interns, vendors, contractors, affiliates, and third parties who access organizational systems or data. This Policy is based on the National Institute of Standards and Technology Cybersecurity Framework ("NIST CSF 2.0 standards") and its core functions and is issued in accordance with Ohio Revised Code § 9.64 and other relevant laws and regulations. Supplemental NIST-aligned standard operating procedures and supporting policies are maintained separately by the Information Technology Services (ITS) department and are hereby incorporated by reference into this Cybersecurity Policy.

II. Scope

This policy applies to:

1. All full-time, part-time, temporary, and seasonal employees
2. Contractors, consultants, affiliates, and third-party vendors with access to systems and data
3. Volunteers and interns with access to systems and data
4. All devices (Cleveland-Metroparks-owned and personal) used to access Cleveland Metroparks systems and data
5. All information systems, applications, cloud services, and data repositories maintained or used by Cleveland