Cybersecurity & The Workplace

Bob Robenalt
Partner
rrobenalt@fisherphillips.com
614-561-5003

Workforce Threat Landscape (2025)

- People remain the No. 1 attack vector or target
  - credential theft,
  - phishing,
  - misuse.
- Ransomware targets HR/Payroll databases.
- Leaks of Personal Identifiable Information – Artificial Intelligence and Generative AI information created in databases such as SaaS (software as a service).
- Concerns over leaks of PII (personal identifiable information) and PHI (personal health information).

Common Cyber Threats

- Business Email Compromises: actors impersonating HR or leadership to change employee banking information to reroute payments
- Data delivery: inadvertently sending confidential employee data to the wrong individual
- Third-Party Vendor Risks: payroll processors and benefits platforms
- AI Deepfakes: actors impersonate job candidates to obtain sensitive roles or pass identity checks;
- AI-generated or manipulated images can trigger Title VII liability.

Why HR is a Cyber Target

- HR manages sensitive personal data (SSNs, bank accounts, medical information, etc.)
- Threat actors know that HR teams manage this information, and tend to target systems containing HR data to quickly exfiltrate known sensitive data

Workforce Threat Landscape (2025)

- Employee hybrid work expands the potential for cyber attacks:
  - Employees working on home networks
  - Use of personal devices

How Companies are combating the threat:

- Multi-Factor Authentication or MFA
- User to provide 2 or more verification factors when logging-in

Anatomy of a Data Breach

Cybersecurity refers to the type of targeted cyberattack where a scammer impersonates a trusted contact to trick the organization into sending sensitive information or money.

1. Phishing or credential-stuffing hits an HR or payroll admin account.
2. Movement of the data into payroll or time-clock systems.
3. Data exfiltration; ransomware or payroll redirection
4. BEC – Business Email Compromise - missed pay cycles, tax filings, benefits enrollment,

Spotlight: Biometrics & Time-Keeping

- High-frequency risk: finger/face scans for clock-in/clock-out.
- Common gaps
  - Employer fails to provide written policy
  - Obtain consent, and
  - Does not keep a retention schedule.
- Key controls: narrowly-scoped purpose, vendor indemnity, deletion deadlines, alternate authority.
- Litigation posture: class exposure for technical violations should be treated as priority control.

Spotlight: AI Deepfakes and Effective Controls

- Video interview impersonation: pre-scheduled, liveness checks, randomized challenge prompts, secondary ID proofing, post-interview notarized identity attestation for sensitive roles.
- Voice-cloned payroll or HR directives: out-of-band verification for any changes; mandatory 24-hour hold for DD changes; staff training on voice cloning per FTC guidance
- Employee-targeted deepfake harassment: explicit ban in anti-harassment policy on AI-generated content of co-workers.
- Disinformation about HR programs or union/collective activity: crisis comms templates; "source of truth" channels; adopt provenance technologies where feasible.

Drafting Clinic: Handbook Insert (Acceptable Use Policy + GenAI)

- Employees must use company-approved systems for HR transactions; personal AI/chat tools may not be used to process or store employee data.
- Use of GenAI for recruiting, performance, or scheduling requires prior written approval and logging of prompts/outputs.
- Multi-factor authentication is mandatory for HR, payroll, and time-keeping systems; sharing credentials is prohibited.
- Monitoring is limited to legitimate business purposes and will not interfere with protected concerted activity.

Best Practices for HR Team

- Train & Test: ongoing phishing training
- Verify Requests: confirm bank change requests with a second channel, preferably calling the employee
- Limit Access: limit access to HR data to only where necessary
- Secure: if sending sensitive employee information via email, password protect the document
- Vendor Due Diligence: assess the security posture of your vendors
- Incident Response Testing: understand HR's role in the event of an incident

Ohio House Bill 96: Cybersecurity for Public Entities

The Ohio Legislature passed House Bill 96 which creates new cybersecurity requirements for local governments. The bill was signed into law by Governor DeWine on June 30, 2025, and the law became effective on September 30, 2025.

The Bill set forth 3 requirements, mandating that each political subdivision do the following:

1. Create and implement a basic cybersecurity program;
2. Report cyber incidents to the Ohio Cyber Integration Center and the Ohio Auditor of the State; and
3. Pass a resolution before paying any ransomware demand.

Cybersecurity Program Requirements

Political subdivision should adopt a program that safeguards the political subdivision's data, information technology and information technology resources.

The term "political subdivision" includes the county commissioners, township trustees, city council, etc.

Cybersecurity Resolution. Under the law, each political subdivision is required to pass a resolution adopting a cybersecurity program.

Each program is required to be consistent with generally accepted best practices for cybersecurity.

Cybersecurity Program Requirements

CAUTION: It is a best practice not to include the specific program information in the public resolution.

- Including the specifics of the program in the public resolution could serve to tip off cyber attackers and provide the attackers with information that may help them target the system.

Best Practices: In developing a compliant program, the political subdivisions are required to utilize best practices such as NiST Cybersecurity Framework, CSF, and CIS Controls.

Cybersecurity Program Requirements – Best Practices

These "best practices" for the program may include, but are not limited to, the following:

- Identify and address the critical functions and cybersecurity risks of the political subdivision.
- Identify the potential impacts of a cybersecurity breach.
- Create Specify mechanisms to detect potential threats and cybersecurity events.
- Specify procedures for the political subdivision to establish communication channels, analyze incidents, and take actions to contain cybersecurity incidents.
- Establish procedures for repairing infrastructure impacted by a cybersecurity incident and maintaining security after the incident.

The OCIC, O-PCI, and Cyber Reserves will be able to assist local governments in assessing cyber risk and begin to develop a cyber program.

Cybersecurity Program Requirements – Cybersecurity Training

Training is **not required by law** but is **strongly recommended** to enhance cyber risk reduction.

The Cyber Training Program should include a training component to ensure staff are prepared to recognize and respond to common cyber threats.

Subdivisions are encouraged to take advantage of **free training offered through the Ohio Persistent Cyber Improvement (O-PCI) program.** This program is offered by the Ohio Cyber Range Institute.

This training should equip staff with critical knowledge and skills to better defend against cyber attacks.

Cybersecurity Program – Cyber Incident Notification Requirements

Reports and Notifications. The law sets out new reporting requirements following a cybersecurity or ransomware incident.

Following all such incidents, local governments must notify both of the following:

- The Executive Director of the Division of Homeland Security within the Ohio Department of Public Safety, in a manner prescribed by the executive director, as soon as possible but not later than seven days after the political subdivision discovers the incident, and
- Ohio's Cyber Integration Center (OCIC)

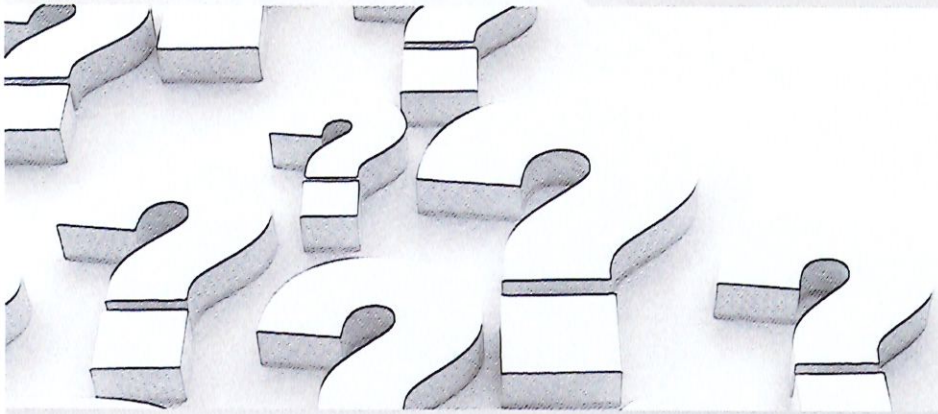
Cybersecurity Program – Documentation and Reports

Under this section, a reportable "Cybersecurity incident" means any of the following:

- A substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network.
- A serious impact on the safety and resiliency of a covered entity's operational systems and processes;
- A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services;

Importantly, any records, documents, or reports related to the cybersecurity program, and the reports of a cybersecurity incident or ransomware incident are **not** public records under section 149.43 of the Revised Code.

Final Questions



Thank You

Presented by:
Bob Robenalt Phone: (614) 561-5003
Email: rrobenalt@fisherphillips.com