ECKERT SEAMANS ATTORNEYS AT LAW

April 2026

Cybersecurity, Data Protection & Privacy Update

Ohio Updates Cybersecurity Requirements for Public Entities including Counties, Townships and Municipal Corporations

By Matthew H. Meade and Xander B. Silva

On June 30, 2025, Ohio Governor Mike DeWine signed Ohio's new cybersecurity law, Ohio House Bill 96, later codified into law as Ohio Revised Code, Chapter 9, Section 9.64 "Political Subdivision Cybersecurity" (the "OH PSC Law" and "PSC Law"). The OH PSC Law became effective on September 30, 2025, and implements significant changes to the responsibilities local governments have when responding to cyber-attacks. The PSC Law, in part, was enacted in response to the increased number of cybersecurity incidents involving Ohio public sector entities. The OH PSC Law aims to create a framework that beefs up the preparedness and response procedures of Ohio political subdivisions who are the victims of cybersecurity incidents.

Overview of Changes for Ohio Political Subdivisions:

The OH PSC Law creates new legal requirements related to how Ohio political subdivisions implement their cybersecurity policies, respond to cybersecurity incidents including ransomware incidents, and respond to ransom demands.

A "Political subdivision" is defined as: "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." (OH Rev Code § 9.64(A)(2))

The PSC Law requires local entities to (i) implement a cybersecurity program, (ii) obtain approval from their legislative body when paying ransomware extortion payments, and (iii) abide by certain reporting requirements and timeframes for cyber incidents.

Cybersecurity Program Requirement:

Under the PSC Law all political subdivisions must implement a cybersecurity program. The requirement aims to ensure local entities maintain the integrity, confidentiality, and availability of its information. According to a 2025 presentation given by CyberOhio, Ohio counties and cities had until January 1, 2026, to adopt a cybersecurity program while all other political subdivisions have until July 1, 2026 (https://dam.assets.ohio.gov/image/upload/v1753899779/cyber.ohio.gov/New_Cyber_Law_Presentation.pdf).
The cybersecurity program must:

- Identify and address critical functions and cybersecurity risks;
- Identify potential impacts of a cybersecurity breach;
- Specify mechanisms to detect potential threats and cybersecurity events;
- Specify procedures for communication channels, incident analysis, and containment for cybersecurity incidents;
- Establish procedures for post-incident security to ensure infrastructure is secure and properly repaired after an incident; and
- Establish cybersecurity training requirements for employees.

It is important to note the PSC Law states that records related to cybersecurity programs and cybersecurity incident reports are not public records. Therefore, these programs and reports are not subject to open records requests. (OH Rev Code § 9.64(E)).

Obligation to Obtain Approval of Ransomware Payments:

Another key provision of the OH PSC Law (OH Rev Code § 9.64(B)) changes how local entities must act if they decide to pay a ransom to a cybercriminal by mandating transparency. The provision explicitly prohibits political subdivisions from paying or otherwise complying with ransomware extortion demands unless they first receive approval from their legislative authority. The legislative authority must formally approve payment or compliance with ransom demands in a resolution or ordinance that states why complying with the ransom demand is in the best interest of the political subdivision. No guidance is provided in § 9.64(B) as to what would meet the standard of what is "in the best interest of the political subdivision."

Reporting Requirements When Responding to a Cybersecurity Incident or Ransomware Incident:

The final major change the PSC Law implements on Ohio political subdivisions relates to reporting requirements for a cybersecurity incident or a ransomware incident. "Cybersecurity incident" is defined as "… any of the following:

a. A substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;

b. A serious impact on the safety and resiliency of a covered entity's operational systems and processes;

c. A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services;

d. Unauthorized access to an entity's information system or network, or nonpublic information contained therein, that is facilitated through or is caused by:

   i. A compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or

   ii. A supply chain compromise." (OH Rev Code § 9.64(A)(1)).

It is important to note that the definition of cybersecurity incident does not mention or refer to personal information or a breach of the security of the system.

A "Ransomware incident" is defined as:

> "a malicious cybersecurity incident in which a person or entity introduces software that gains unauthorized access to or encrypts, modifies, or otherwise renders unavailable a political subdivision's information technology systems or data and thereafter the person or entity demands a ransom to prevent the publication of the data, restore access to the data, or otherwise remediate the impact of the software." (OH Rev Code § 9.64(A)(3)).

After a cybersecurity incident or a ransomware incident public entities including counties, townships and municipal corporations shall notify both of the following:

(1) The executive director of the division of homeland security within the 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;

(2) The auditor of state, in a manner prescribed by the auditor of state, as soon as possible **but not later than thirty days** after the political subdivision discovers the incident.

Incidents can be reported to Homeland Security's Ohio Cyber Integration Center (OCIC) here:
https://homelandsecurity.ohio.gov/ohio-cyber-integration-center/reporting-guidance

Incidents can be reported to the Auditor of the State here:
https://ohioauditor.gov/fraud/docs/CybersecurityReportingForm.pdf

Ohio Revised Code, Chapter 9, Section 9.64 is available here:
https://codes.ohio.gov/ohio-revised-code/section-9.64

Sources:

Ohio Revised Code, Chapter 9, Section 9.64

CyberOhio, New Cybersecurity Requirements Presentation:
https://dam.assets.ohio.gov/image/upload/v1753899779/cyber.ohio.gov/New_Cyber_Law_Presentation.pdf

ECKERT SEAMANS ATTORNEYS AT LAW

This Cybersecurity, Data Protection & Privacy Alert is intended to keep readers current on developments in the law and is not intended to be legal advice. If you have any questions, please contact Matthew H. Meade at 412.566.6983 or mmeade@eckertseamans.com, Xander Silva at 412.566.6069 or xsilva@eckertseamans.com, a member of our Cybersecurity, Data Protection & Privacy Practice Group, or any other attorney at Eckert Seamans with whom you have been working for further information and assistance.