The Impact of Ohio's New Cybersecurity Law on Townships

Ryan C. Spitzer, OTARMA General Counsel

The Ohio General Assembly recently passed House Bill 96, a bill establishing cybersecurity requirements for political subdivisions through the creation of Ohio Revised Code (R.C.) §9.64, which became effective September 30, 2025. The rationale behind this new law is to ensure that all government entities are protected from cybercriminals considering increased ransomware attacks against political subdivisions throughout the state.

Implications of R.C. §9.64

R.C. §9.64 requires all political subdivisions to adopt a cybersecurity program, outline reporting obligations related to cybersecurity and ransomware incidents, and requires approval of the board of trustees before the payment of any ransomware demand.

Cybersecurity Policy Demands

R.C. §9.64 requires each board of trustees to adopt a cybersecurity program that meets, at a minimum, the following requirements consistent with generally accepted best practices for cybersecurity, from entities such as the national institute of standards and technology cybersecurity framework, and the center for internet security cybersecurity best practices:

- A specifically designated individual to oversee the cybersecurity program;
- Identification of the township's critical functions and risks;
- Assessment of the potential impact of cybersecurity breaches;
- Implementation of threat detection mechanisms;
- Establishment of incident response procedures;
- A plan for recovery and continuity; and,
- Defined employee training requirements.

In addition to the cybersecurity program, R.C. §9.64 requires each board of trustees to adopt a resolution authorizing the payment of ransomware, before the payment occurs, which must include an explanation as to why the payment is in the best interest of the township.

Cybersecurity and Ransomware Incidents

R.C. §9.64(A)(1) defines "cybersecurity incidents" as:

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.

However, cybersecurity incidents do not include "mere threats of disruption as extortion; events perpetrated in good faith in response to a request by the system owner or operator; or lawfully authorized activity of a United States, state, local, tribal, or territorial government entity."

Similarly, R.C. §9.64(A)(3) defines a "ransomware incident" 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."

Reporting a Cybersecurity Incident

R.C. §9.64 requires townships to report cybersecurity and ransomware incidents to the Ohio Department of Public Safety within seven (7) days of the incident and the Auditor of State within 30 days of the incident. A township's reporting obligations related to cybersecurity and ransomware incidents began **September 30, 2025**.

The Auditor of State, ***for auditing purposes only***, has given townships until July 1, 2026, to adopt and implement a cybersecurity program.

Public Records and Open Meeting Exemption

Lastly, R.C. §9.64 excludes any documents, records, or reports related to cybersecurity programs or cybersecurity incident(s) from constituting public records under Ohio law. ■

About the Author

Mr. Spitzer is a partner at Isaac Wiles Burkholder & Miller, LLC, a Columbus, Ohio, law firm. His practice, the Labor and Employment and Public Law Practice Group, encompasses all areas of labor and employment law and litigation, with an emphasis on the complexities within public sector jurisdictions.