Ohio Revised Code

Section 9.64

Effective: September 30, 2025
Legislation: House Bill 96

(A) As used in this section:

(1) "Cybersecurity incident" means 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.

"Cybersecurity incident" does 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.

(2) "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.

(3) "Ransomware incident" means 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.

(B) A political subdivision experiencing a ransomware incident shall not pay or otherwise comply with a ransom demand unless the political subdivision's legislative authority formally approves the payment or compliance with the ransom demand in a resolution or ordinance that specifically states why the payment or compliance with the ransom demand is in the best interest of the political subdivision.

(C) The legislative authority of a political subdivision shall adopt a cybersecurity program that safeguards the political subdivision's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The program shall be consistent with generally accepted best practices for cybersecurity, such as the national institute of standards and technology cybersecurity framework, and the center for internet security cybersecurity best practices, and may include, but are not limited to, the following:

(1) Identify and address the critical functions and cybersecurity risks of the political subdivision.

(2) Identify the potential impacts of a cybersecurity breach.

(3) Specify mechanisms to detect potential threats and cybersecurity events.

(4) Specify procedures for the political subdivision to establish communication channels, analyze incidents, and take actions to contain cybersecurity incidents.

(5) Establish procedures for the repair of infrastructure impacted by a cybersecurity incident, and the maintenance of security after the incident.

(6) Establish cybersecurity training requirements for all employees of the political subdivision; the frequency, duration, and detail of which shall correspond to the duties of each employee. Annual

cybersecurity training provided by the state, and training provided for local governments by the Ohio persistent cyber initiative program of the Ohio cyber range institute, satisfy the requirements of this division.

(D) The legislative authority of a political subdivision, following each cybersecurity incident or ransomware incident, 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.

(E) Any records, documents, or reports related to the cybersecurity program and framework in division (C) of this section, and the reports of a cybersecurity incident or ransomware incident under division (D) of this section, are not public records under section 149.43 of the Revised Code.

(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 under section 149.433 of the Revised Code.