THOMPSON HINE

Privacy & Cybersecurity Update

July 2025

Ohio Enacts Law Regulating Ransomware Payments and Cybersecurity

The Ohio Legislature included provisions in a recently enacted operating appropriations bill (Ohio House Bill 96) that regulate how and when state agencies can make ransomware payments, including a new requirement related to consultation with and approval from legislative officials. The bill also sets forth new cybersecurity standards and cyber-related event reporting requirements for state agencies. It is important that Ohio state agencies subject to the provisions update their incident response plans to include a process for engaging with legislative officials, among other areas, and update their information security policies.

Key Terms: Cybersecurity Incident and Ransomware Incident

The new Ohio law defines a "cybersecurity incident" and a "ransomware incident" differently. The former is defined as 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 to deliver goods or services
- The unauthorized access to an entity's information system or network, or nonpublic information contained therein, that is facilitated through or is caused by a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider, or a supply chain compromise

However, the term does not include a "mere threat" of a cyber disruption as extortion, any event perpetrated in good faith in response to a request by the system owner or operator, or lawfully authorized activity of certain federal, state, or local governments. In contrast to Ohio's data breach notification law, the new ransomware requirement is not limited to whether sensitive personally identifiable information has been impacted.

In addition, the new law 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."

New Ransomware Payment Regulations

Ohio's new ransomware payment requirements are straightforward. Specifically, they prohibit a "political subdivision" from paying a or otherwise complying with a ransom demand in connection with a ransomware incident – unless its applicable "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."

Importantly, the new Ohio law does not currently cover private-sector entities, and only applies to a "political subdivision," which 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." Interestingly, this definition

does not expressly include the terms "school districts" or "transit authorities," which are specifically enumerated in the definitions of "political subdivision" found in other portions of the Ohio Revised Code.

Updating Incident Response Plans

The entities subject to Ohio's new ransomware payment requirements should immediately update their incident response plans (IRPs). In particular, while a state agency's IRP should already include key external stakeholders, such as outside counsel, cyber insurance carriers, and digital forensic consultants, they now need to include points of contact within the agency's corresponding legislative branch who can efficiently and effectively draft and seek to enact a resolution or ordinance formally approving the payment or compliance with the ransom demand. This could potentially be a single member of the legislature, a special committee, or the entire legislative branch of the political subdivision, and will likely vary depending on logistical issues and political relationships.

In addition, it will be important for Ohio state agencies to undertake table-top exercises that include all key stakeholders, including those in the legislative branch, so they are prepared to address a ransomware incident in real time, including the potential need to enact formal legislation supporting the ransom payment decision. The IRP needs to account for frequent changes to the key stakeholders due to personnel changes resulting from elections or other factors.

New Reporting Requirements

The Ohio law includes new reporting requirements that apply to both a cybersecurity incident and a ransomware incident. Following either type of incident, covered entities must notify both of the following:

- The executive director of Ohio Homeland Security (OHS), a division of the Ohio Department of Public Safety, in a manner prescribed by OHS's executive director, as soon as possible but not later than seven days after the political subdivision discovers the incident
- The Ohio Auditor of State (AOS), in a manner prescribed by the AOS, as soon as possible but not later than 30 days after the political subdivision discovers the incident

The law also exempts certain records related to this reporting and cybersecurity programs in general (see next section) from Ohio's public record disclosure laws. A covered entity's IRP should also be updated to address these new reporting requirements.

New Cybersecurity Requirements

Under the new Ohio law, "[t]he legislative authority of a political subdivision" must formally adopt "a cybersecurity program that safeguards [its] data, information technology, and information technology resources to ensure availability, confidentiality, and integrity." The program must be consistent with generally accepted best practices for cybersecurity (e.g., NIST Cybersecurity Framework and Center for Internet Security Cybersecurity Best Practices). The program may include the following:

- Identify and address the critical functions and cybersecurity risks of the political subdivision
- Identify the potential impacts of a cybersecurity breach
- 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
- 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

According to guidance issued by CyberOhio, 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."

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Thora Knight, Ph.D.
212.908.3971
Thora.Knight@ThompsonHine.com

Kimberly Pack
312.998.4262
Kimberly.Pack@ThompsonHine.com
Certified Information Privacy Professional/United States (CIPP/US)
Certified Information Privacy Manager (CIPM)