



Tim Schaffer  
20th District

**Ohio Senate**  
Senate Building  
Room 137, First Floor  
Columbus, Ohio 43215  
(614) 466-8076  
sd20@ohiosenate.gov

**Committees and Special Appointments:**  
Agriculture & Natural Resources, Chair  
Armed Services, Veterans Affairs, and Public Safety  
Energy  
Ohio Expositions Commission  
Rules and Reference  
Transportation, Vice Chair  
Ways and Means

**Senate Financial Institutions, Insurance and Technology Committee**  
**Senate Bill 203 — Sponsor Testimony**  
**Tuesday, June 3, 2025**

Chairman Wilson, Vice Chairman Lang, Ranking Member Craig, and members of the Senate Financial Institutions, Insurance and Technology Committee, thank you for the opportunity to present sponsor testimony on Senate Bill 203.

This legislation was created with help from the State Auditor Keith Faber and will require all political subdivisions in Ohio, which are county, township, city and village governments as well as school, conservancy and park districts to adopt a cybersecurity program.

The bill also prohibits a political subdivision from paying a ransom unless there is a formal vote by its legislative body to pay or comply with the ransom.

The overall goal of this legislation is to prevent and mitigate cybersecurity incidents and protect taxpayer dollars by giving local political subdivision's the tools that they need to properly address these situations.

The most recent and high-profile example of the need for this legislation goes back to July of 2024 when the City of Columbus was hit with a ransomware attack. This incident led to critical city services becoming unavailable and inoperable for weeks and months following the incident as well as leaks of personal information of Columbus residents and employees.

While the City of Columbus did not pay the ransom, it did cost Columbus taxpayers over \$7 million in recovery costs from the cybersecurity incident. This includes up to:

- \$2.4 million for systems remediation and cyber threat monitoring.
- \$1.64 million for Experian identity theft protection
- \$1.95 million for legal counsel related to incident response
- \$1.3 million for long term cyber threat monitoring and legal counsel fees for related litigation

Another incident was one that had occurred in my district. The Granville Recreation District was a victim of a phishing scheme in 2023 and lost \$713,000. This occurred when a fraudulent account operated by a bad actor intercepted a transfer of funds between the Granville Recreation District and a construction contractor.

These cybersecurity incidents are just a couple of examples of the real threats facing our political subdivisions across Ohio and illustrate the need for a complete and robust cybersecurity plan to be in place.

Senate Bill 203 also requires political subdivisions to notify the Division of Homeland Security with the Department of Public Safety of a cybersecurity incident no later than seven days after the incident was discovered. The bill also requires that the Auditor of State's office be notified no later than 30 days after the incident occurs.

Additionally, there is an amendment that I am asking to be considered by the committee today. This amendment came at the request of State Auditor Keith Faber and his staff that clarifies that any record that identifies cybersecurity related software, hardware, goods, and services that are being used or considered for procurement by a political subdivision is not subject to disclosure under Ohio Public Records Law.

This change assures that this critical information cannot be accessed or requested by potential bad actors who are looking to target political subdivisions with a cybersecurity attack.

Thank you once again Chairman Wilson and members of the committee for the opportunity to present this legislation to you today. I will be glad to answer any questions at this time.