HB 4055 STAFF MEASURE SUMMARY

Joint Committee On Information Management and Technology

Prepared By:	Sean McSpaden, Committee Coordinator
Sub-Referral To:	Joint Committee On Ways and Means
Meeting Dates:	2/6

WHAT THE MEASURE DOES:

HB 4055 requires local governments, local service districts, and special government bodies to notify the State Chief Information Officer within 48 hours after discovering an information security or ransomware incident. The measure prescribes the information a public body is required to report and directs the State Chief Information Officer to establish a reporting system that allows a public body to submit a notification or report in a timely, secure and confidential manner. HB 4055 directs the State Chief Information Officer to establish and maintain a public webpage with clear instructions on what to report and how to submit reports. The measure further directs the State Chief Information Officer to provide a summary report annually to the Governor and Legislature for incidents reported during the preceding year. HB 4055 exempts the submitted incident reports from disclosure under Oregon's public records laws, while allowing the State Chief Information Officer to confidentially and securely share incident information with specific parties under certain circumstances.

Fiscal impact: *May have fiscal impact, but no statement yet issued.*

Revenue impact: *May have revenue impact, but no statement yet issued.*

Operative Date: July 1, 2026. Declares an emergency and takes effect immediately upon passage.

Detailed Summary

- Requires local governments, local service districts, and special government bodies to notify and submit a report to the State Chief Information Officer within 48 hours of an information security incident or ransomware incident.
- Defines covered incidents broadly, including substantial loss of confidentiality, integrity, or availability; operational disruption; compromised safety/resilience; and unauthorized access (including incidents caused by third-party providers).
- Prescribes the information that a public body is required to report including a description of response actions and specific steps taken or planned to prevent, mitigate, or recover from damage, unauthorized access, modification, deletion, or other system impairments.
- Directs the State Chief Information Officer to establish a reporting system that allows public bodies subject to the measure to submit a notification or report in a timely, secure and confidential manner. The incident notification and reporting system must be capable of:
  - Accepting reports, identifying and tracking trends, and producing analytical reports and incident summaries.
- Requires the State Chief Information Officer to establish and maintain a public webpage with instructions that, at minimum, describe how to report incidents, what types of incidents must be reported, and what information should be included in the notification or report submission.
- Requires the State Chief Information Officer to provide an annual report to the Governor and the Joint Legislative Committee on Information Management and Technology on the information security incidents and ransomware incidents reported for the preceding year. The report must, at minimum:
  - Summarize the number of notifications, incident types, and types of public bodies reporting, without including confidential security details

- Exempts incident reports from public disclosure under Oregon public records law, while allowing the State Chief Information Officer to share information with the Oregon Cybersecurity Center of Excellence, law enforcement, and other appropriate entities.
- Sets timing and implementation milestones. Authorizes the State Chief Information Officer to take pre-implementation actions to, among other requirements, ensure the incident notification and reporting system and webpage are established within 90 days after the bill's effective date.

ISSUES DISCUSSED:

EFFECT OF AMENDMENT:

No amendment.

BACKGROUND:

While all 50 states (including Oregon) have data breach notification laws requiring covered entities to inform individuals when their personal information or personal health information is compromised, these laws primarily focus on notifying affected individuals rather than mandating cybersecurity incident notifications reports to a central state government entity for real time information sharing, analysis, coordination, and response.

Oregon's executive branch state agencies are required to report information security incidents to the State Chief Information Officer per ORS 276A.300 and associated rules and policies. Oregon's state agencies, including the constitutional offices, the Attorney General, and the Judicial and Legislative Branches are also required to notify and report information security incidents to the Legislative Fiscal Office per ORS 276A.306.

Currently, there is no requirement in Oregon for cyber incident notification or reporting by local governments, local service districts, and special government bodies to a central state government entity. However, the trend of statutorily requiring public bodies to report cybersecurity incidents to a central state government entity is growing, as states across the nation recognize the importance of centralized information collection, analysis, and sharing to combat cyber threats effectively. To date, at least 15 states have enacted mandatory cyber incident reporting laws for local government and schools - California (2022), Florida (2022), Georgia (2021), Indiana (2021), Kansas (2024), Maryland (2024), Minnesota (2024), New Jersey (2023), New Mexico (2024), North Carolina (2021), North Dakota (2021), Texas (2023), Virginia (2023), Washington (2005), and West Virginia (2024).