HB 3228 -1 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:	3/21, 4/18

WHAT THE MEASURE DOES:

House Bill 3228 directs the Oregon Cybersecurity Advisory Council to study the use of cybersecurity insurance by Oregon public bodies and directs the advisory council to submit findings to the interim committees of the Legislative Assembly related to information management and technology no later than December 31, 2025. Further, House Bill 3228 establishes the Oregon Cybersecurity Resilience Fund and appropriates moneys in the fund to the Higher Education Coordinating Commission for distribution to the Oregon Cybersecurity Center of Excellence to assist public bodies with cybersecurity insurance requirements and cybersecurity incidents. The Act takes effect on its passage.

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

Detailed Summary:

- Directs the Oregon Cybersecurity Advisory Council to study the use of cybersecurity insurance for public bodies in Oregon.
- Directs the advisory council to submit findings, including recommendations for legislation, to the interim committees of the Legislative Assembly related to information management and technology no later than December 31, 2025.
- Directs the State Chief Information Officer and the Oregon Cybersecurity Center of Excellence to provide staff and support services to the advisory council necessary for the advisory council to complete the study and report.
- Establishes the Oregon Cybersecurity Resilience Fund and appropriates moneys in the fund to the Higher Education Coordinating Commission for distribution to the Oregon Cybersecurity Center of Excellence to assist public bodies with
  - Meeting cybersecurity insurance requirements, and
  - Preparing and planning for, mitigating, responding to and recovering from a cyberattack, information security incident or data breach.

Effective Date:

- Declares an emergency and is effective on passage.

ISSUES DISCUSSED:

- Support for the measure.
- Suggestions for modifications - expanding the scope of the measure to include artificial intelligence related considerations, threats and risks.
- Cyber warfare and ransomware attacks and the real and potential impacts on Oregon's critical infrastructure and public sector operations.
- High costs to recover from vs. lower costs to prepare for and mitigate impacts of cyber-attacks.
- Ever-increasing concerns about the impact of cyber-attacks on Oregon's county and city governments, school districts, ESDs, and community colleges. Many small and rural public bodies do not have dedicated IT staff to help guard against and prepare for a cyber-attack and have difficulty meeting minimum requirements for enhanced cyber insurance coverage.

- Reductions in federal cybersecurity assistance to state and local government and schools across the country.
- Role of the Oregon Cybersecurity Center of Excellence and importance of the proposed Oregon Cybersecurity Resilience Fund to Oregon's local governments and schools.

EFFECT OF AMENDMENT:

-1 The amendment modifies Section 1(1) of the measure. Instead of a broad study on the use of cybersecurity insurance by public bodies, the amendment directs the Oregon Cybersecurity Advisory Council to conduct assessments to identify and document cybersecurity vulnerabilities and recommend actions to address the reasons that public bodies are unable to meet cybersecurity insurance coverage requirements. The amendment also extends the date by which the advisory council must submit a report to the interim committees of the Legislative Assembly related to information management and technology from December 31, 2025, to no later than September 30, 2026.

The amendment modifies Section 2 of the measure, extending the date by which Section 1 of this 2025 Act would be repealed from January 2, 2026, to January 2, 2027.

The amendment modifies Section 3 of the measure, allowing monies in the Oregon Cybersecurity Resilience Fund to be used to assist public bodies with: assessing and documenting cybersecurity vulnerabilities and the specific cybersecurity insurance coverage requirements public bodies are unable to meet; and, cybersecurity training, in addition to the authorized purposes listed in the introduced version of the measure.

BACKGROUND:

During the 2023 Legislative Session, the Joint Legislative Committee on Information Management and Technology held an informational meeting focused on Cyber Insurance on May 17, 2023. At that meeting, representatives from the Oregon Department of Administrative Services Risk Management Program (on behalf of state government), CityCounty Insurance Services (on behalf of the League of Oregon Cities and Association of Oregon Counties), and the Special Districts Association of Oregon (on behalf of the Special Districts Insurance Services and Property and Casualty Coverage for Education Trust programs) expressed concerns that insurance policy options for public bodies in Oregon were becoming more limited, the requirements and premiums to obtain cyber insurance were continuing to increase, and the coverage limits available to recover from a cyberattack or data breach were continuing to decrease.

The sophistication, severity, and frequency of cyberattacks on public bodies across the nation, and here in Oregon, continue to increase and the use of artificial intelligence (AI) is accelerating the automation of those attacks. Ransomware-as-a-Service (RaaS), whereby criminals deploy predeveloped ransomware tools, is also expected to increase with the support of AI.

Although the cyber insurance market has stabilized, and insurance coverage options and limits have increased since 2023, many local governments, schools and special districts here in Oregon (especially small and rural public bodies with limited or no information technology staff and resources) struggle to meet basic cyber insurance coverage requirements. They are currently unable to obtain available cyber insurance coverage, or to plan or prepare for, mitigate, respond to, or recovery from a cyberattack or data breach without assistance from outside parties.