Joint Legislative Committee on Information Management and Technology Planning for Interim Committee Work (Topics for discussion)

Topic: Cyber Incident Notification Requirement - all public bodies

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 reports to a central state entity for information sharing, analysis, coordination, and response.

The Oregon Department of Justice (DOJ) Data Breach Reporting Database reached 1419 data breach report entries on June 4, 2025. That is up from 822 on February 1, 2023 (an increase of 597 data breach reports in just 854 days) - an average of 1 new data breach report every 1.4 days.

Oregon DOJ Data Breach Reporting Database: https://justice.oregon.gov/consumer/databreach/

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, no requirement exists in Oregon for cyber incident notification or reporting by non-state agency public bodies to a central state entity. However, the trend of requiring public bodies to report cybersecurity incidents to a central state entity is growing, as states recognize the importance of centralized information collection, analysis, and sharing to combat cyber threats effectively.

States with Mandatory Cyber Incident Reporting Laws for Local Governments and Schools

1. **Georgia** - Utilities, state agencies, local entities, including school districts, must report all cyber incidents that render critical business systems unavailable.
   Reporting Timeline: For state agencies (within 1 hour of discovery). For local government entities - required to contact local emergency management agency within 1 hour of discovery. For Utilities, within 2 hours of notification to the U.S. government.
   - House Bill 156 (2021) https://www.legis.ga.gov/api/legislation/document/20212022/196159
   - GEMA: Report Util/Agcy Cybersecurity Incident | Georgia Emergency Management and Homeland Security Agency
2. **New Jersey** - As of 2023, public schools, government contractors, and state and local governments are required to report cybersecurity incidents within 72 hours of discovery.
   - https://pub.njleg.state.nj.us/Bills/2022/PL23/19_.PDF
3. **California** - California enacted Assembly Bill 2355 (2022). School districts are required to report cyberattacks that impact more than 500 students or personnel.
   - https://thejournal.com/articles/2022/10/06/new-california-law-requires-schools-to-report-all-cyber-incidents-impacting-500-pupils-or-staff.aspx
   - https://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=202120220AB2355

4. **Florida**: Florida enacted H.B. 7055 (2022). The measure mandates that political subdivisions, state agencies, and local governments report cybersecurity and ransomware incidents.
    - https://www.flhouse.gov/Sections/Documents/loaddoc.aspx?FileName=_h7055er.docx&DocumentType=Bill&BillNumber=7055&Session=2022
5. **Indiana**: In 2021, Indiana enacted legislation (HB 1169) mandating that all public agencies, including local governments and educational institutions, report cyber incidents to the Indiana Office of Technology. This initiative was driven by the state's need to gain a comprehensive understanding of cybersecurity threats across all levels of government.
    - https://legiscan.com/IN/text/HB1169/id/2361053
6. **Kansas:** In 2024, Kansas enacted a law (K.S.A. § 75-7244) requiring any public entity that has a significant cybersecurity incident to notify the Kansas information security office within 12 hours after discovery of such incident. Establishes timeframes for government contractors to notify the Kansas information security office in certain circumstances within prescribed timeframes.
    - https://www.kslegislature.gov/li_2024/b2023_24/statute/075_000_0000_chapter/075_072_0000_article/075_072_0044_section/075_072_0044_k/
7. **Maryland**: Maryland's SB 812, enacted in 2022, requires each unit of the Executive Branch and certain local entities to report specific cybersecurity incidents to the state's Security Operations Center. This law also established the Office of Security Management and the Maryland Cybersecurity Coordinating Council to oversee cybersecurity efforts and required the appointment of a Director of Local Cybersecurity to work in coordination with the Maryland Department of Emergency Management to provide technical assistance, coordinate resources, and improve cybersecurity preparedness for units of local government.
    - https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0812?ys=2022RS
    - https://mgaleg.maryland.gov/2022RS/Chapters_noln/CH_242_sb0812e.pdf
8. **Minnesota**: Effective December 1, 2024, Minnesota law (16E.36 in 2024) mandates that Public agencies – state agencies, local governments, public education entities, and government contractors – are required to report cybersecurity incidents —such as ransomware or network attacks—to the state. The reported information is anonymized and shared with appropriate organizations to bolster statewide cybersecurity support.
    - https://www.revisor.mn.gov/statutes/cite/16E.36

9. **New Mexico:** In 2024, New Mexico enacted a law (NM Stat § 9-27A-3 (2024)) that, among other things, allowed the newly created cybersecurity office to establish a centralized cybersecurity and data breach reporting process for agencies and political subdivisions of the state.
    - https://law.justia.com/codes/new-mexico/chapter-9/article-27a/section-9-27a-3/#:~:text=A.,managed%20by%20the%20security%20officer.&text=(12)%20establish%20a%20centralized%20cybersecurity,political%20subdivisions%20of%20the%20state
10. **North Dakota**: In 2021, North Dakota enacted a law (CHAPTER 54-59.1) requiring political subdivisions—such as state agencies, counties, cities, school districts, special districts, and public libraries—to report cyber incidents to the state. This reporting enables the state to provide targeted cybersecurity support, including tools and training, to local entities.
    - https://ndlegis.gov/cencode/t54c59-1.pdf
11. **North Carolina**: North Carolina General Statute § 143B-1379 requires local government entities—including counties, cities, local school administrative units, and community colleges—to report cybersecurity incidents to the North Carolina Department of Information Technology within 24 hours of discovery. Additionally, North Carolina General Statute § 143-800 prohibits state agencies and local government entities from paying or communicating with threat actors in response to ransomware attacks, mandating consultation with the Department of Information Technology instead.
    - https://it.nc.gov/documents/files/cyber-incident-reporting-north-carolina-state-government/open
    - https://www.ncleg.gov/enactedlegislation/statutes/pdf/bysection/chapter_143/gs_143-800.pdf
12. **Texas**: As of September 1, 2023, Texas law (SB 271 - 2023) requires state agencies and local governments, including counties, cities, special districts, and schools, to report cybersecurity incidents to the Texas Department of Information Resources within 48 hours. To facilitate this, the state has launched an online portal for incident reporting.
    - SB 271 Security Incident Reporting - https://capitol.texas.gov/tlodocs/88R/billtext/pdf/SB00271F.pdf#navpanes=0
    - Incident reports will be submitted via the Archer Engage secure webform - https://dir.texas.gov/resource-library-item/local-government-incident-reporting-user-guide

13. **Virginia**: Virginia Code § 2.2-5514 mandates that all public bodies—including counties, cities, towns, school boards, and other entities supported by public funds—report certain cybersecurity incidents within 24 hours of discovery to the Virginia Fusion Intelligence Center, operated by the Virginia State Police. The Virginia Fusion Intelligence Center shares these reports with the Chief Information Officer at the Virginia Information Technologies Agency to enhance statewide cybersecurity coordination.
    - https://law.lis.virginia.gov/vacode/title2.2/chapter55.3/section2.2-5514/
    - https://www.reportcyber.virginia.gov/faqs/
14. **West Virginia:** In 2024, West Virginia enacted a cyber incident reporting law (W. Va. Code § 5A-6C-3) that applies to all state agencies within the executive branch, constitutional officers, all local government entities as defined by §7-1-1 or §8-1-2 of the West Virginia code, county boards of education as defined by §18-1-1 of the West Virginia code, the Judiciary, and the Legislature. Qualified cybersecurity incidents shall be reported to the Cybersecurity Office before any citizen notification, but no later than 10 days following a determination that the entity experienced a qualifying cybersecurity incident.

    Entities that must report: https://code.wvlegislature.gov/5A-6C-2/

    W. Va. Code § 5A-6C-3: https://code.wvlegislature.gov/pdf/5A-6C-3/#:~:text=Cyber%20Incident%20reporting%3B%20when%20required.
15. **Washington**: Under RCW 43.09.185, Washington state law requires local governments to immediately notify the State Auditor's Office in the event of a known or suspected loss of public resources, including those resulting from cybersecurity incidents. Agencies affected by cyberfraud must report details such as loss of funds, affected financial data, ransomware payments, and unauthorized access to information systems.

    https://app.leg.wa.gov/rcw/default.aspx?cite=43.09.185

Question: Is it time for Oregon to enact a cyber incident notification and reporting statute for all public bodies to facilitate better information collection and analysis, threat assessment, resource allocation, and coordinated information sharing and response to cybersecurity incidents that may affect all public bodies throughout the state?