HB 2049 STAFF MEASURE SUMMARY

Joint Committee On Information Management and Technology

Prepared By: Sean McSpaden, Committee Coordinator
Meeting Dates: 2/1, 2/8, 2/15, 2/22

WHAT THE MEASURE DOES:

House Bill 2049 establishes the Oregon Cybersecurity Center of Excellence within Portland State University to supplement the cybersecurity related activities of the State Chief Information Officer and to coordinate, fund, and provide cybersecurity workforce development, education, awareness, and training for public, private, and nonprofit sector organizations, and cybersecurity-related goods and services to Oregon public bodies with a targeted focus on the unmet needs of regional and local government, special districts, Education Service Districts, K-12 school districts and libraries. The measure directs Portland State University, Oregon State University and University of Oregon to jointly operate the center by agreement and to provide administrative and staff support and facilities for center operations. Further, the measure transfers the existing Oregon Cybersecurity Advisory Council from the office of Enterprise Information Services to the center and modifies the composition and duties, powers and functions of the Council to serve as the Advisory Body for the center.

House Bill 2049 establishes an Oregon Cybersecurity Center of Excellence Operating Fund and continuously appropriates moneys in the fund to the center to carry out the functions and operations of the center. The measure establishes an Oregon Cybersecurity Workforce Development Fund and continuously appropriates moneys in the fund to the center to invest in cybersecurity workforce development programs. The measure establishes an Oregon Cybersecurity Grant Program Fund and continuously appropriates moneys in the fund to the center to provide cybersecurity-related goods and services to Oregon public bodies. Further, the measure establishes an Oregon Cybersecurity Public Awareness Fund and continuously appropriates moneys in the fund to the center to raise public awareness regarding cybersecurity threats and resources to be safer and more secure online.

House Bill 2049 becomes operative October 1, 2023, declares emergency, and is effective on passage.

ISSUES DISCUSSED:

- Various aspects of House Bill 2049.
- Attorney General Ellen Rosenblum and Oregon Department of Justice (DOJ) support for HB 2049.
- League of Oregon Cities, Association of Oregon Counties, Special Districts Association of Oregon, Lane Council of Governments, Coalition of Oregon School Administrators, Oregon School Boards Association, and Oregon Association of Education Service District's support for HB2049.
- Growing number of security and data breach incidents in Oregon: between 2015 and the beginning of 2023, approximately 820 security breaches were reported to the DOJ's Consumer Protection Section. Belief that passage of HB 2049 will help protect against and reduce the impact of these violations.
- Ransomware and other cyber-attacks are not always direct. Business disruptions can occur when an organization's service provider(s) are attacked. In some instances, public, private, and non-profit sector organizations rely on the same set of technology service providers and can experience independent business disruptions caused by attacks on common/shared service providers.
- The immediate and long lasting affects that ransomware attacks had on the City of Glendale and Tillamook County, respectively.
- City and Special District perspectives on ransomware attacks, cybersecurity vulnerabilities and challenges, and cybersecurity workforce gaps.

- K-12 School/Education Service District perspectives on cybersecurity threats, challenges, and cyberattacks experienced by Oregon's public schools/education service districts.
- Regional and local government, Special District, and K-12 School/Education Service District perspectives on cybersecurity insurance, the accelerating threat from malware and ransomware, cost of recovery from and response to a cyberattack, and cybersecurity workforce challenges facing Oregon public bodies.
- Private Sector Technology firm perspectives on cybersecurity threats and challenges facing state and local governments and all those in the education sector.
- Increasing costs for and decreasing coverage included within cybersecurity insurance policies. Uncertainty in the cybersecurity insurance market.
- Options for future state government actions that could be taken to shore up the cybersecurity insurance marketplace.
- National studies identifying top cybersecurity barriers states must overcome - e.g. Legacy infrastructure and solutions to support emerging threats; Inadequate cybersecurity staffing and availability of cyberecurity professionals; decentralized IT and security infrastructure and operations; and increasing sophistication of threats.
- Need for immediate additional investments to help regional governments, local governments, special districts, schools, education service districts and libraries - IT modernization, cybersecurity, and workforce development and training.
- Shortage of cyber security professionals across the nation (over 700,000 unfilled cybersecurity jobs) and in Oregon (approximately 7500 unfilled cybersecurity jobs with 200+ new openings every month across all sectors). Efforts to continue to grow and diversify the cybersecurity workforce are essential starting in K-12 (e.g. NW Cyber Camp) and continuing through community college (e.g. Mount Hood Community College cybersecurity certification and degree programs) to higher education (e.g. Oregon State University's Oregon Research and Teaching Security Operations Center) and beyond and must involve diversifying the workforce by including more women and minorities.
- Threats from ransomware, information system vulnerability exploitation, and cyberattacks on industrial control systems and the supply chain are increasing and are increasingly sophisticated. Legacy infrastructure and solutions, cyber workforce shortages, and legacy mindsets on cybersecurity exacerbate these problems.
- Government agencies fight a losing battle to keep users, systems, and data secure if security is not designed in from the beginning and tested for during the software development process. Software developer education on secure coding practices and access to application security testing tools is necessary to protect data that is accessed through web applications that Oregon government organizations build or acquire, and use.
- Software supply chain risks are real and increasing. When software is acquired from a vendor, government agencies must be able to scrutinize the security processes that were used in the development of that software. Most government agencies don't have that capability on their own. They need help from public/private sector partners.
- Current imbalance between cyber attackers and cyber defenders. Defenders protecting legacy systems, using manual methods, and relying on scare cybersecurity staff, can't compete with cyber attackers with seemingly unlimited resources, using machine learning, artificial intelligence, and other automated methods of attack. Integrated, automated, and scalable solutions are needed in addition to increasing the supply of trained and certified cybersecurity professionals.
- Private technology firm certification, education, and training programs are available at reduced or no-cost to Oregon's public universities, community colleges, K-12 Schools, and state/local governments but are not universally accessed by Oregon's public bodies. Awareness and coordination of these and other programs like them is needed.
- Cybersecurity begins and ends with people. The foundation of Oregon's cybersecurity improvement efforts across all jurisdictions, must include an awareness and education program component.
- Whole of state cybersecurity planning and program development across the nation is increasing with varying efforts underway or in place in Arizona, Indiana, Maryland, Massachusetts, Michigan, New York, North

Carolina, North Dakota, New York, Pennsylvania, and Texas.

- Successful whole of state cybersecurity program development efforts involve: multiple levels of government - e.g. state government, tribal government, cities, counties, special districts, schools, etc.; coordinated governance, planning, implementation, and validation; and, combining resources to find better ways to share cybersecurity information, respond to incidents, address cyber workforce challenges, and standardize tool solution selection, deployment, and use where possible. Belief that the cybersecurity center of excellence and the diverse cybersecurity advisory council envisioned within House Bill 2049 will increase Oregon's chances for success.
- Need to better position Oregon to efficiently compete for and receive federal funding for cybersecurity. Belief that establishing the Cybersecurity Center of Excellence would help Oregon do that.
- Oregon is an interconnected digital community. The public, private, and non-profit sector organizations operating in Oregon are interconnected with each other. A risk to one is a risk to all.
- Need for collaboration on cybersecurity across all sectors. Cybersecurity as a team activity; the cybersecurity challenges that exist are too many and too complex for any single organization to solve on their own.
- Need to transfer cyber risk and responsibility from less capable parties (e.g. individual users, small public agencies) to more capable ones that have the staff, expertise, automated tool sets and services, and economies of scale needed to more effectively address these complicated challenges.
- Collaboration, information sharing, and partnerships are key across Oregon's public, private, and non-profit sectors.

EFFECT OF AMENDMENT:

No amendment.

BACKGROUND:

Ransomware and other cyberattacks threaten the nation’s critical infrastructure, economy and public health and safety. The threats from ransomware and other cyberattacks continue to worsen each day for public, private and nonprofit sector organizations operating in Oregon and across the nation. In the public sector - a whole of state approach involving coordinated cybersecurity planning, investment, and action across jurisdictions is required.

At the same time, Oregon and the nation face a shortage of qualified cybersecurity professionals to address these threats and vulnerabilities. According to cyberseek.org, an organization that provides detailed information on the cybersecurity job market across the nation, there are approximately 7,500 unfilled cyber jobs in Oregon across all sectors. In response, multiple cybersecurity workforce development and educational programs have been initiated within Oregon's public universities and community colleges over the past few years.

Oregon law (ORS 646A.600-646A.628) requires a business, state agency, or other "covered entity" to notify any Oregon consumer whose personal information, as defined, was subject to a breach of security. The law also requires that a sample copy of a breach notice sent to more than 250 Oregon consumers must also be provided to the Oregon Attorney General. The searchable database available on the Oregon Department of Justice Consumer Protection website indicates that 822 breach notices have been submitted from October 30, 2015 to January 20, 2023.

Oregon’s local and regional governments, education service districts, school districts and libraries have recently completed a variety of assessments that identify critical cybersecurity vulnerabilities and information technology modernization needs they cannot meet alone.