

A Cross-Sector Capabilities, Resources, and Needs Assessment:

Research to Support the Drafting of the Oregon Cybersecurity Center of Excellence Proposal

Executive Summary and Overview

Updated April 2018

Prepared by:

Center for Public Service
Mark O. Hatfield School of Government
Portland State University

Rebecca Jensen Craven, MPA
Project Manager
Center for Public Service

Jess Daly, MPP
Policy Analyst
Center for Public Service

Elizabeth Gray
Project Coordinator
Center for Public Service

A Cross-Sector Capabilities, Resources, and Needs Assessment: Research to Support the Drafting of the Oregon Cybersecurity Center of Excellence Proposal

Oregon's Senate Bill 90 (SB90), signed into law and effective as of July 1, 2017, requires the Oregon Office of the State Chief Information Officer (OSCIO) to draft a proposal for an Oregon Cybersecurity Center of Excellence (CCoE). SB90 specifies that the CCoE must include information sharing and incident response support functions, and liaise and participate in cybersecurity initiatives nationwide; the Center also bears responsibility for drafting both a Cybersecurity Strategy and Cyber Disruption Response Plan. The CCoE has also been identified as the body responsible for carrying out strategic initiatives on behalf of the Oregon Cybersecurity Advisory Council (OCAC). To assist with the process of drafting the proposal for this high-priority initiative that fulfills all these requirements, the OSCIO engaged Portland State University's Center for Public Service (CPS) to conduct comprehensive research on the state of cybersecurity in Oregon and initiatives in other states that can serve as templates for the CCoE to follow. More specifically, CPS conducted the following research activities:



















































































































































- A policy analysis of cybersecurity efforts in other states;
- An online survey of Oregon organizations regarding their cybersecurity policies, processes, staffing, and needs;
- Cross-sector focus groups with cybersecurity professionals throughout Oregon;
- Catalogs of current funding opportunities for potential CCoE activities; and
- An inventory cybersecurity resources that currently exist in Oregon.

COMPARATIVE POLICY ANALYSIS

The comparative policy analysis shows that cybersecurity best practices exist in several other states that can inform Oregon's approach to a CCoE. This portion of the report utilized a public health framework to consider the cybersecurity activities of 11 states (California, Colorado, Florida, Illinois, Maryland, Michigan, New Jersey, New York, Texas, Virginia, and Washington) in terms of their prevention, monitoring, response and recovery activities, as well as leadership structures. Each of these categories is composed of several key indicators; state programs are evaluated by whether they have implemented, partially implemented, or not implemented/passed each indicator of a category. The performance of each of these states in each of these categories is summarized in Figure 1 below.

EXECUTIVE SUMMARY AND OVERVIEW

Figure 1: Comparative Programs Evaluation Matrix

 Implemented  Planned or partially implemented  Not implemented or not passed yet	1. LEADERSHIP				2. PREVENTION			3. ACTIVE MONITORING			4. RESPONSE AND RECOVERY		
	Competent Authority & Resources	Central Hub	Strategic Planning	Multi-Sector Capacity Building	Cyber Hygiene	Immunity Measures	Education and Workforce Training	Early Detection	Real-Time Info Sharing & Threat Monitoring	Federal Collaboration	Coordinated Incident Response	Outbreak Containment	Cyber Laws
California													
Colorado													
Florida													
Illinois													
Maryland													
Michigan													
New Jersey													
New York													
Texas													
Virginia													
Washington													

* Adapted and updates from - Francesca Spidaleri, "State of the States on Cybersecurity" (Pell Center for International Relations and Public Policy, November 2015) and Oregon OSCIO analysis

The findings of this analysis suggest that Colorado, Maryland, Michigan, and Virginia provide the most relevant examples of activities that are consistent with the State of Oregon’s approach to cybersecurity under SB90. These four states have made significant investments in cybersecurity planning, research, coordination, execution, awareness, education, and public outreach. The allocation of resources to these activities has resulted in a cybersecurity initiatives and processes that most closely align with the understanding of cybersecurity as a public good.

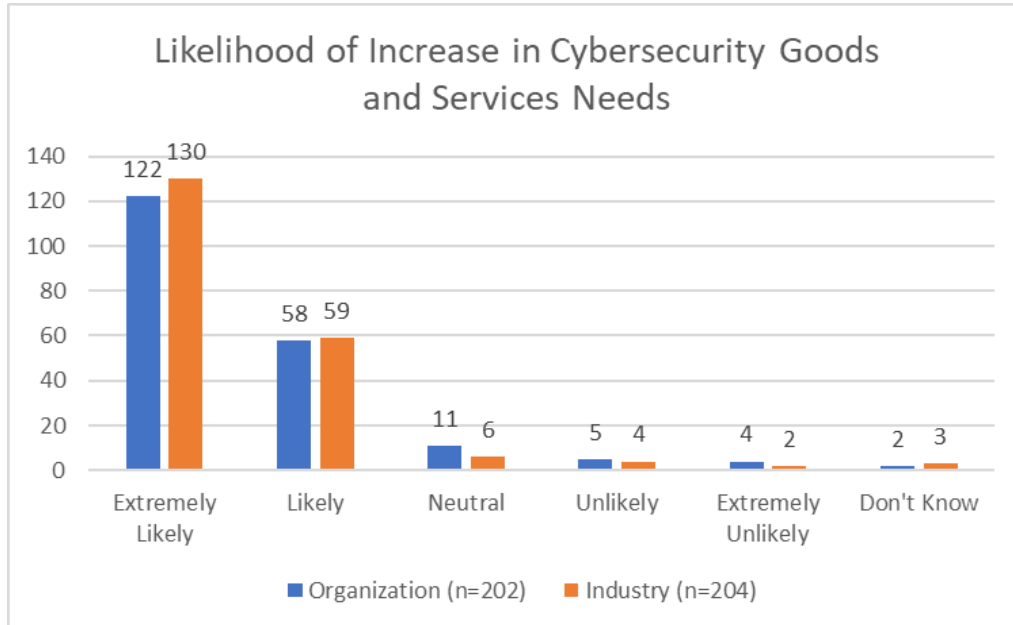
In general, we find that states vary widely in terms of the activities and initiatives they pursue to meet cybersecurity goals. Funding also varies widely across states, as does the reporting of this funding. Additionally, increasing transparency and accountability, as well as engaging in collaborative strategy planning processes, are identified as criteria for successful policy interventions in this field. Engaging a diverse group of multi-sector stakeholders can help ensure that initiatives are considering the needs of the state as a whole, and provide valuable perspectives that may be missed through government engagement exclusively with the cybersecurity field to address important cybersecurity issues and threats.

ONLINE SURVEY OF OREGON ORGANIZATIONS

The online survey of 205 respondents resulted in answers to 33 questions regarding the cybersecurity policies, practices, staffing, and concerns of Oregon organizations. A majority of respondents identified their organizations as government entities (55.2% - either local governments or other public entities); similarly, Government was the most common industry selected (35.1%). More than half of respondents represented organizations in the Portland Metro area (53.3%), and the vast majority of all organizations are headquartered in Oregon (88.7%). In terms of individual respondents, the most common job type was IT manager (31.9%), and more than half had received some kind of cybersecurity-specific training or education (56.2%).

The results of two key questions are highlighted below. Respondents were not required to answer all questions, so total responses may not always total 205. First, respondents overwhelmingly indicated that they expect the cybersecurity needs of both their organizations and their overall industry to increase in the next five years. Approximately 90% of respondents indicated that their organizations and industries are likely or very likely to require more cybersecurity goods and services during this time period.

Figure 2: Growing Cybersecurity Needs

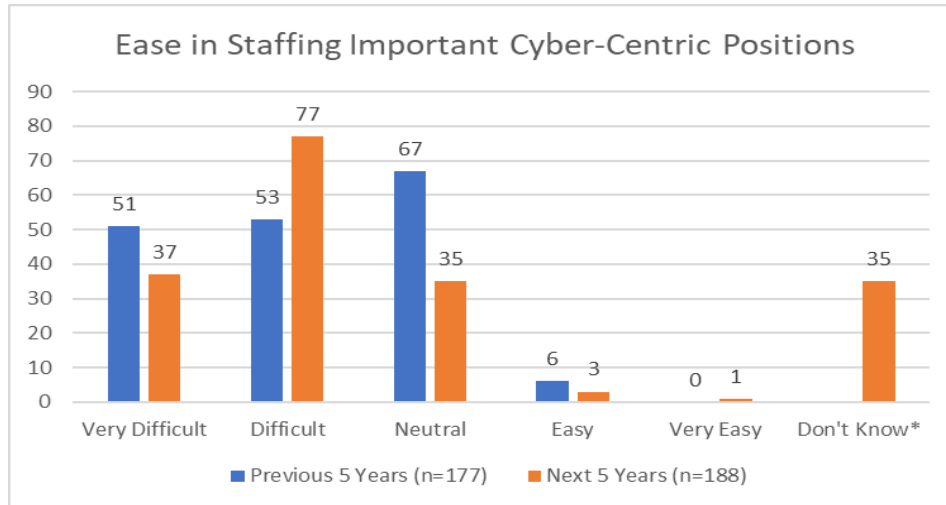


We also inquired about organizations' experiences with staffing cybersecurity positions. Respondents generally do not find cybersecurity staffing to be an easy task, with approximately 59% reporting that staffing these positions has either been difficult (53 of 177, or 30%) or very difficult (51 of 177, or 29%) over the past five years. However, the

EXECUTIVE SUMMARY AND OVERVIEW

most popular answer choice was “neutral”, with 67 of 177 respondents (or 38% of respondents) choosing this option. Expectations for the future are roughly the same, with 114 of 188 respondents (61%) believing that their organization will have a difficult or very difficult time with cybersecurity staffing. In general, the data from these questions show that respondents currently have difficulty staffing cybersecurity positions, and expect this difficulty to continue.

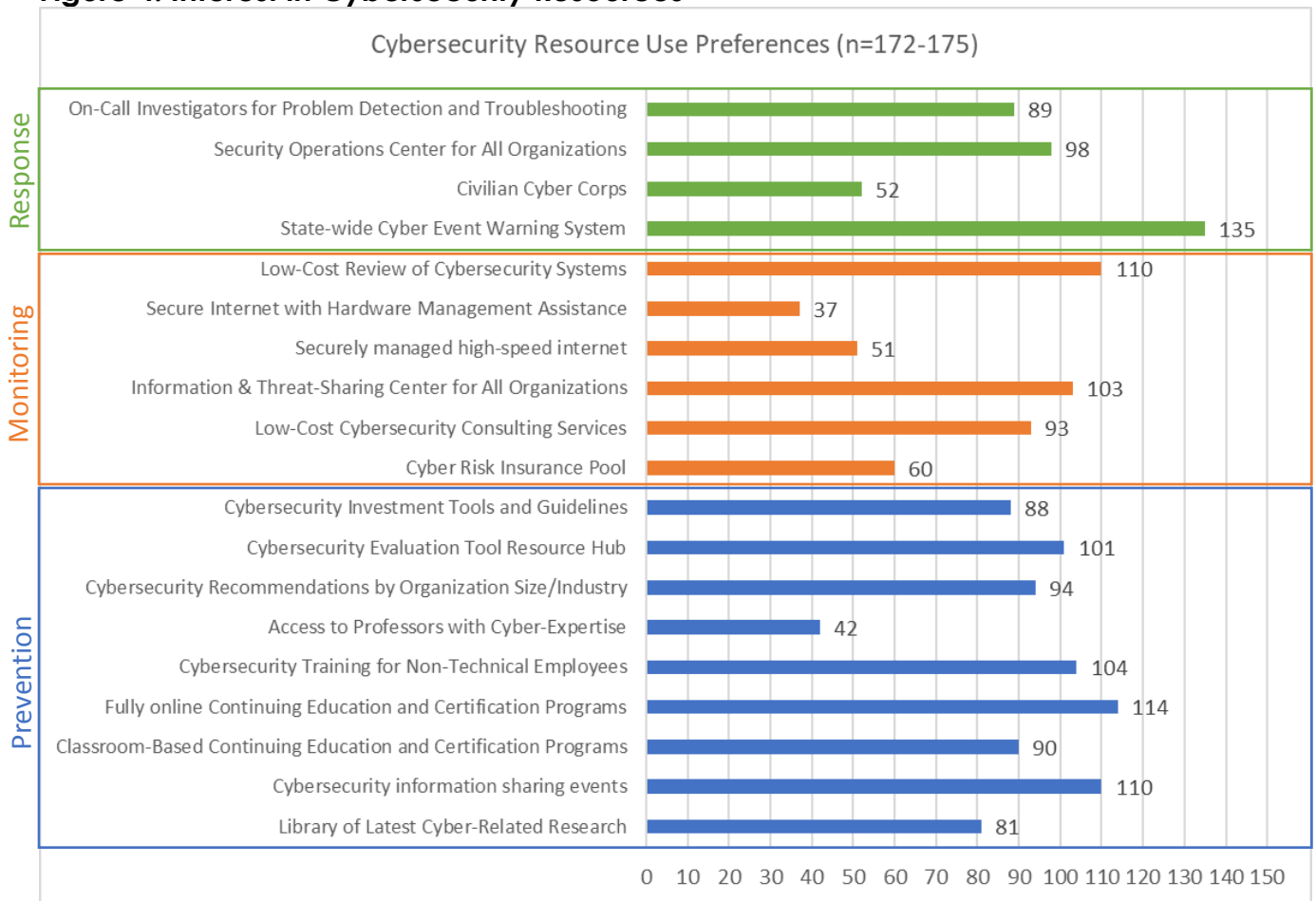
Figure 3: Difficulty Staffing Cybersecurity Positions



The most important survey questions for the Oregon Cybersecurity Center of Excellence development process are likely those from Part 3 regarding organizations’ interests in using particular prevention, monitoring, and response programs and services. The combined answers to these questions are shown in the figure below, with prevention resources represented in blue, monitoring resources represented in orange, and response resources represented in green. A majority of respondents indicated that they would be willing to use one or more hypothetical services provided to improve either the cybersecurity prevention, monitoring, or response to incidents by their organizations. By far, the most popular service choice was a state-wide cyber event warning system, with 135 respondents (or 78%) indicating that their organization would use this service; a majority of almost every characteristic group chose this option. Other choices that received support from a majority of respondents included fully online continuing education and certification programs (65%), cybersecurity information sharing events (63%), low-cost reviews of cybersecurity systems (63%), cybersecurity training for non-technical employees (59%), and an information and threat sharing center for all Oregon organizations (59%). The full results are shown in Figure 4 below.

EXECUTIVE SUMMARY AND OVERVIEW

Figure 4: Interest in Cybersecurity Resources



The data from the entire survey, once quantitatively analyzed, provided insights into trends across organizations regarding these topics. Overall, the most common concerns indicated by respondents centered around the creation of a cyber-aware staff, including both those in technical and non-technical positions. Respondents were also acutely concerned with shifting their organizations' cultures to allow a larger and more important role for cybersecurity. The survey results show a gap in access and/or availability of cybersecurity resources, and indicate that Oregon organizations are very interested in remedying this situation to stave off future cybersecurity issues.

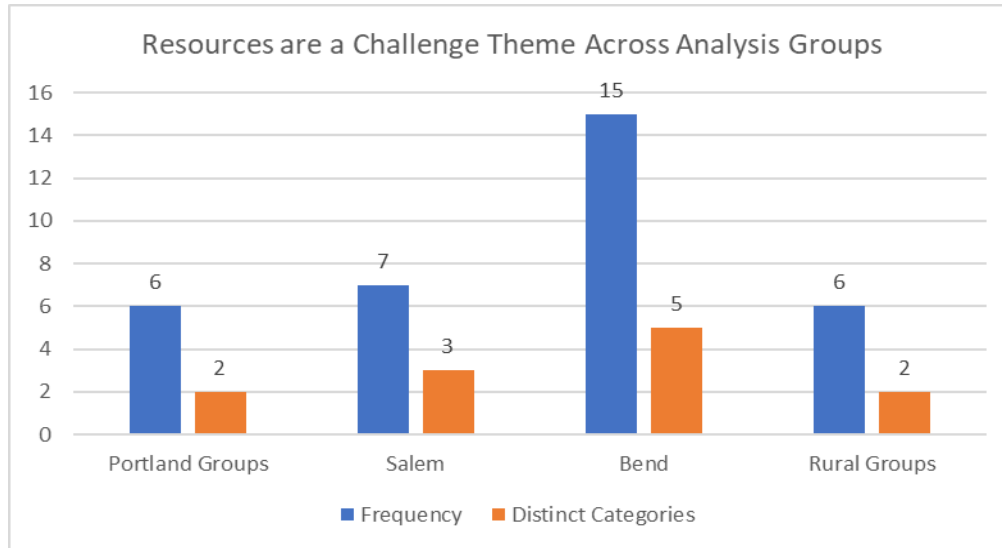
STATEWIDE FOCUS GROUPS

To complement the quantitative data collected by the survey, eight focus groups with a total of 39 participants were conducted across Oregon. The data from focus groups essentially triangulated the findings of the survey, especially those from characteristic groups (location, industry, etc.) with lower response rates. Overall, respondents indicated that resource availability and their organizations' cultures constituted the biggest

EXECUTIVE SUMMARY AND OVERVIEW

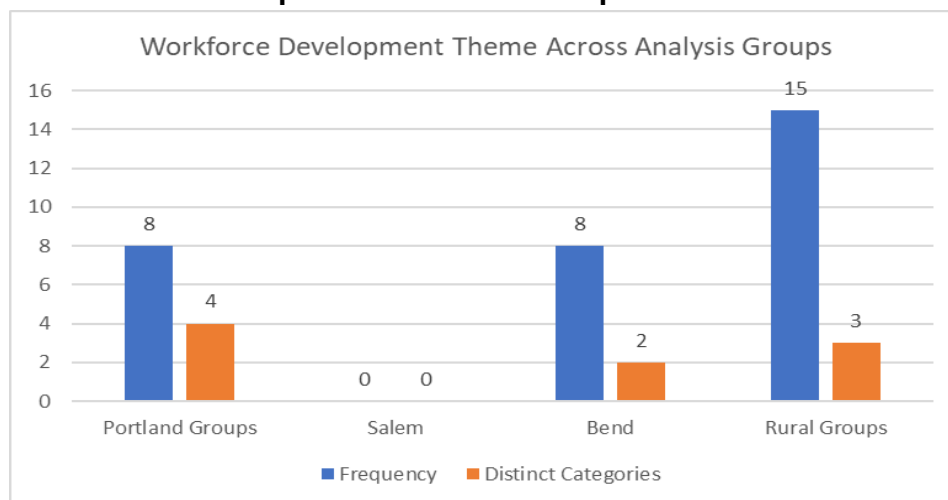
barriers to improving cybersecurity postures. The vast majority of participants identified organizational resources as the most pressing challenge for cybersecurity, with cost- and time-constraints, staffing, and executive support frequently mentioned as barriers. The prominence of this topic across all focus groups is shown in Figure 5 below.

Figure 5: Resource Challenges in Focus Group Sessions



Workforce development was widely agreed upon as an important initiative that the CCoE could contribute to; this finding was consistent across all industries and locations included in the focus groups, as shown in Figure 6 below. Participants from southern and eastern Oregon noted that they perceive that they experience more difficulties when trying to find qualified applicants and access continuing education opportunities and cybersecurity services than those in metropolitan areas. Portland participants were also aware of this disparity and seemed enthusiastic about addressing it.

Figure 6: Workforce Development in Focus Group Sessions



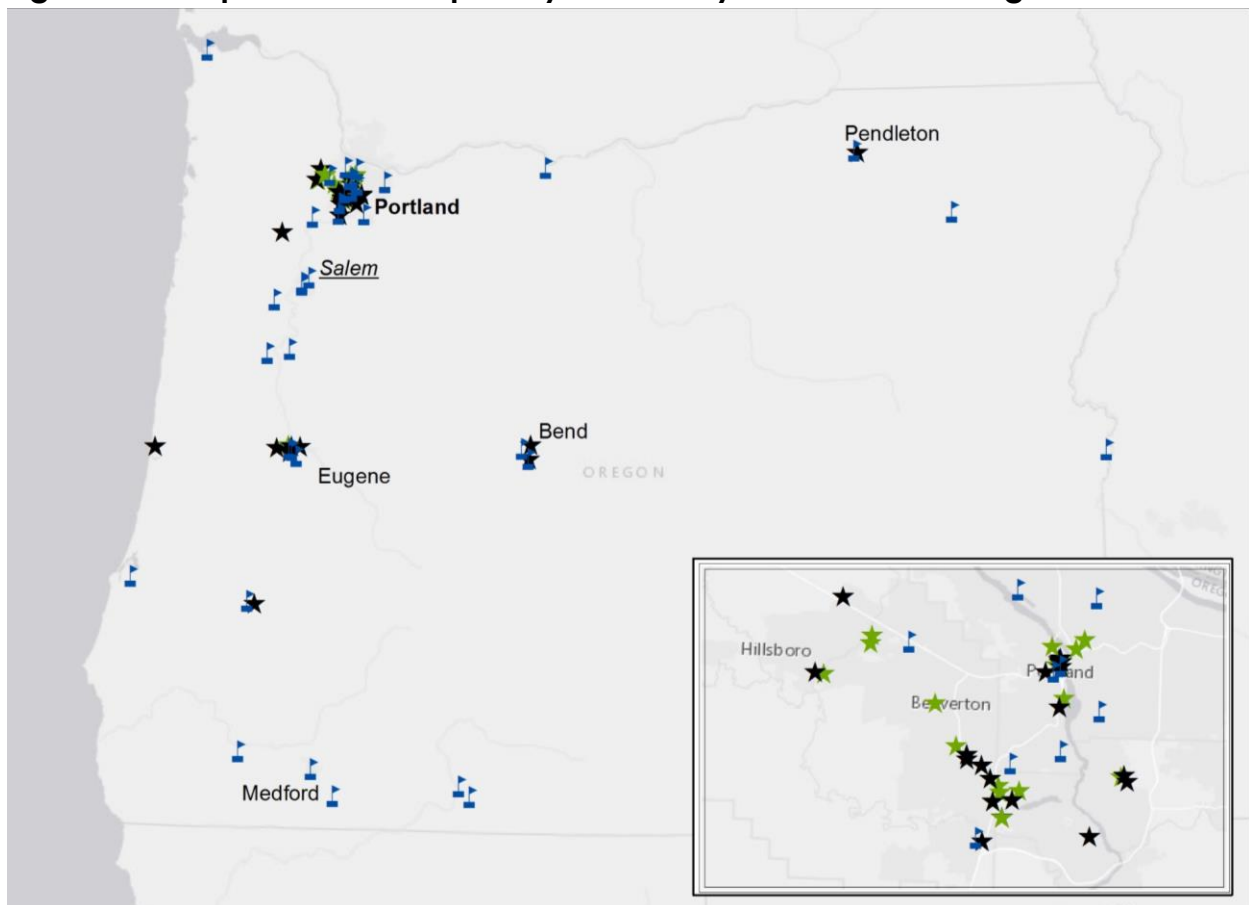
EXECUTIVE SUMMARY AND OVERVIEW

Surprisingly, much of the conversation in each focus group on this subject focused on the importance of K-12 education programs and other methods to introduce school-aged children to the cybersecurity field. This shows that participants take a broad view of workforce development and are interesting in supporting activities that foster cybersecurity expertise at all levels and ages. Beyond these programs, participants also generated a diverse list of 52 unique activities that an Oregon CCoE could potentially support (see pages 147-148 of the full report for the full list).

FUNDING AND RESOURCES

Any CCoE should consider the funding opportunities and Oregon cybersecurity resources that already exist; these are detailed in Chapters 5 and 6 of the full report. A comprehensive map of college and university education programs, as well as cybersecurity businesses and organizations, are included in Figure 7.

Figure 7: Comprehensive Map of Cybersecurity Resources in Oregon



EXECUTIVE SUMMARY AND OVERVIEW

The cybersecurity resource maps show where colocation of educational programs and cybersecurity industry goods and services are limited; two 2-year education institutions that lack computer science and cybersecurity curricula are also identified. The majority of Oregon's cybersecurity companies, and a substantial portion of overall educational institutions, are located in the Portland-metro area. The Medford, Klamath Falls, and Salem areas have educational resources but less business activity. With the exception of possibilities for remote work and telecommuting, this poses a significant problem for students looking to attend educational programs and participate in the workforce concurrently. It also deters alumni from staying in areas that provided their education and are already underserved in terms of cybersecurity resources.

There is potential to quickly and effectively expand cybersecurity efforts in Oregon by capitalizing on existing infrastructure in communities that lack sufficient cybersecurity educational and professional opportunities and focusing on initiatives that are good candidates for external funding through existing grant programs. Funding opportunities are abundant for workforce development initiatives, and accessible through a variety of sources including foundations and various agencies and departments in the federal government.

RECOMMENDATIONS FOR CCOE PROGRAMMING AND LEADERSHIP

These research efforts, when considered together, culminate in three broad recommendations for the activities and programming for the CCoE proposal:

- **Workforce development initiatives:** Successful cybersecurity initiatives in other states most often include programs and activities designed to grow the cybersecurity workforce. There is also a perceived need and high level of support for these kinds of initiatives throughout Oregon.
- **Cyber hygiene training:** Training non-technical employees in the basics of safe cyber practices was a major pain point noted by cybersecurity practitioners in the survey and focus groups. Additionally, other states have experienced quantifiable benefits from offering materials and programs covering these topics to state employees, educational institutions, and (in some cases) the general public.
- **Multi-sector engagement:** There is a lot of interest in contributing to the decision-making process for the CCoE from Oregon cybersecurity professionals across all industries, and inclusive advisory and leadership structures is a common characteristic across leading cybersecurity initiatives in other states.

EXECUTIVE SUMMARY AND OVERVIEW

NEXT STEPS FOR DECISION MAKERS

The wealth of data included in this report, and the practicalities of undertaking such a broad and inclusive statewide initiative, lead to the following recommendations for decision makers' more immediate next steps:

- **Decide on a legal structure:** This decision will both help to determine the types of funding pursued for the CCoE, and communicate leadership, decision-making structures, and priorities to key beneficiary groups.
- **Engage funding experts:** Funding a massive statewide initiative requires experienced professionals to provide input on funding strategies and targeted and efficient grant applications.
- **Bring key beneficiary groups into the proposal process:** Opportunities for key beneficiary groups to positively contribute to deliberative processes are highly desired by these groups, and consistent with a public health approach to cybersecurity policy.
- **Focus on workforce development:** These initiatives can have a large immediate impact and be cost effective for an initiative with limited resources.
- **Continue learning from other states:** Efforts to learn from other states that have successful cybersecurity initiatives, or have implemented programs and policies of interest to the OSCIO and OCAC, can help determine specific proposal design elements. These include start-up costs, necessary positions and job duties, and effective leadership structures. Leveraging this valuable experience and taking lessons learned from those with prior experience should play an important role in the CCoE proposal drafting process.

The timeline for the CCoE development process may be aggressive, but the evidence collected and analyzed through this report shows that there are many opportunities to make a positive impact on cybersecurity for all Oregonians. Targeting high-priority needs of key beneficiary groups has been successful in other states, and by utilizing existing resources and strategically engaging funding sources, the same level of success is possible in Oregon.