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

December 2017

Updated March 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

Portland State
UNIVERSITY

Table of Contents

Acknowledgements

Several individuals and organizations provided invaluable assistance that contributed to the completion of this project. The project team wishes to thank:

- Portland State University's Center for Public Service Director, Phil Keisling, for his leadership and unwavering support of the research team.

- Portland State University's Center for Public Service faculty, including Assistant Director Dr. Masami Nishishiba, for her careful eye reviewing our drafts and documents; Dr. Marcus Ingle, for his advice and input throughout the duration of this project; and Dr. Kent Robinson, for his help in translating initial ideas into a statement of work that ultimately resulted in this report.

- Charlie Kawasaki, for connecting the Center for Public Service to the Oregon Cybersecurity Center of Excellence initiative and providing valuable insights and resources for our work.

- The Technology Association of Oregon and Redhawk Network Security, for providing us with the opportunity to recruit central Oregon survey respondents and focus group participants at the Bend Cybersecurity Education Summit.

- Cayuse Technologies, for graciously hosting of the eastern Oregon focus group in their beautiful Pendleton-area facility.

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 of 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. The findings of this analysis are that states vary widely in terms of the activities and initiatives they pursue to meet cybersecurity goals. Funding varies widely across states, as does the reporting of this funding. 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. 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. This data, once quantitatively analyzed, provided insights into trends across organizations regarding these topics. In general, organizations of all types and located in all parts of Oregon have a difficult time staffing cybersecurity positions and expect finding qualified applicants for these positions to become more difficult over the next 5 years. The most common concerns noted by respondents centered around the creation of a cyber-aware staff, including both those in technical and non-technical positions, and shifting the organizational culture to allow a role for cybersecurity. A majority also 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.

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. Respondents nearly unanimously agreed that developing Oregon’s workforce is the most important initiative that the CCoE could contribute to. 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 seem enthusiastic about addressing it. Overall, respondents indicated that resource availability and their organizations’ cultures constituted the biggest barriers to improving cybersecurity postures.

Recommendations for CCoE Programming and Leadership

These research efforts, when considered together, culminate in three broad recommendations for the direction of 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.

Funding and Resources

These recommendations should be considered in conjunction with the catalog of funding opportunities and Oregon cybersecurity resources included in Chapters 5 and 6. 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. 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. 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.

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 success is possible in Oregon.

Introduction and Research Approach

Introduction

As high-profile system breaches and data theft continue making headlines, cybersecurity has become an increasingly salient point of concern for individuals and organizations across the United States. The State of Oregon is no exception as the recent passage of Senate Bill 90 (SB90) shows. While much of the bill focuses on centralizing and unifying the cybersecurity technologies, policies, and procedures of the State of Oregon's executive agencies, the legislation also acknowledges the integrated nature of state cybersecurity concerns with partners and other entities beyond state government. This is most clearly shown in Section 4, which calls for the Oregon Office of the State Chief Information Officer (OSCIO) to draft a proposal leading to the creation of an Oregon Cybersecurity Center of Excellence (CCoE) by January 1, 2019. The CCoE will coordinate and communicate with other sectors, organizations, and initiatives within Oregon, across other states, and at the federal level. More specifically, the new CCoE is to serve six primary functions[1]:

1. Coordinating information sharing regarding cybersecurity risks and incidents;
2. Supporting cybersecurity incident responses and investigations;
3. Serving as an Information Sharing and Analysis Organization that officially liaises with the National Cybersecurity and Communications Integration Center (within the Department of Homeland Security in the federal government);
4. Participating in federal, multistate, and private sector organizations that are relevant to the mission and activities of the CCoE;
5. Receiving and disseminating cybersecurity threat information from a wide range of sources;
6. Drafting the Oregon Cybersecurity Strategy, as well as the Cyber Disruption Response Plan, each to be updated biennially.

These functions go beyond servicing state entities, and require that the proposed CCoE have the resources and abilities to impact cybersecurity for organizations of all sizes and sectors in every part of Oregon. As further elaborated by the OSCIO, the CCoE is intended to provide "...a state-civilian interface"[2] that allows for cross-sector

[1] Oregon. State Legislature. *Senate Bill 90- Establishing the Oregon Cybersecurity Center of Excellence.* 2017. https://olis.leg.state.or.us/liz/2017R1/Downloads/MeasureDocument/SB90/Enrolled . Section 4.

[2] Oregon Office of the State Chief Information Officer. Implementation of E.O. 16-13, "Unifying Cyber Security in Oregon" - Written Testimony for the Joint Legislative Committee on Information Management and Technology. December 12, 2016. Pg 10-15. https://olis.leg.state.or.us/liz/2017R1/Downloads/CommitteeMeetingDocument/96166.

involvement and participation by key beneficiary groups (defined a local governments, educational institutions at all levels, nonprofit organizations, small businesses, law enforcement, and critical infrastructure). The creation of this center therefore depends on the incorporation of the perspectives of multiple stakeholders into a single coordinated effort that positively impacts the cybersecurity postures of all.

Beyond ascribing these functions to the CCoE, SB90 also created a multi-sector Oregon Cybersecurity Advisory Council (OCAC) to serve as a cybersecurity advisory body to the OSCIO[3]. The OCAC has several key roles to play, including providing a statewide forum for discussing cybersecurity issues, recommending best practices, and encouraging cybersecurity workforce development. The advisory nature of the OCAC makes a close partnership between this body and the CCoE likely, and the implementation of OCAC objectives within the purview of the CCoE. Additionally, the OSCIO has tasked the OCAC with developing the key tenets of the CCoE proposal, further cementing the relationship between the two entities.

Given the scope of this initiative, the intended impacts on all Oregonians, and the ambitious timeline of January 1, 2019, the OSCIO engaged Portland State University's Center for Public Service (CPS) to conduct background research on cybersecurity initiatives in other states, gather data on the needs and resources of Oregon organizations, and more generally support the CCoE proposal deliberations and initial CCoE proposal drafting efforts by the OCAC. A statement of work created through a collaborative process between CPS, OSCIO, several OCAC members, and other interested stakeholders ultimately resulted in a consulting agreement with CPS to perform five primary research tasks:

- Conduct a comparative policy analysis of the cybersecurity efforts in other states that are similar in size and scope to the CCoE proposed by SB90;
- Administer an online survey of Oregon organizations regarding their cybersecurity policies, processes, staffing, and needs;
- Facilitate a series of cross-sector focus groups with cybersecurity professionals located throughout Oregon;
- Catalog current funding opportunities for potential CCoE activities from both public and private institutions; and
- Inventory cybersecurity resources that currently exist in Oregon.

[3] Oregon. State Legislature. *Senate Bill 90- Establishing the Oregon Cybersecurity Center of Excellence.* 2017. https://olis.leg.state.or.us/liz/2017R1/Downloads/MeasureDocument/SB90/Enrolled . Section 3.

INTRODUCTION AND RESEARCH APPROACH

The intent of the CPS research as reported in this document is to support the OCAC in their proposal drafting process by providing raw data and thorough analysis for making evidence-based policy decisions regarding the CCoE's initial formation. This research report synthesizes CPS's findings and related conclusions associated with each contractual task. These conclusions are accompanied by tangible recommendations for CCoE programming in light of the requirements of SB90. These recommendations are meant to contribute to further collaborative discussion on the direction a CCoE proposal should take to fulfill the obligations set forth by the legislature, to serve the needs of Oregonians as identified through analysis of robust data, and to follow the best practices embedded in the successes of other statewide initiatives to address cybersecurity. The report also includes specific next steps recommended for the CCoE proposal drafting process.

Research Approach

The research approach used in this report is consistent with the "public health approach" to cybersecurity that has previously been identified by the OSCIO as an applicable guiding framework for this statewide initiative[4]. This approach is a departure from more traditional defense-oriented cybersecurity perspectives that invoke images of warfare[5], armed conflict,[6] and protecting castle walls.[7] Such perspectives tend to result in policies that focus most heavily on securing access points (strengthening the walls) and effectively reacting to attacks[8]. A public health approach, by contrast, recognizes the importance of facilitating preventative action by the general public[9] in effecting cybersecurity strategies. The metaphorical underpinnings of this approach are rooted in the comparison of the interdependent systems created through networked technologies to environments or ecosystems[10,11], with their complex biological components that combine to produce positive system-wide effects. Viewing cybersecurity from this

[4] Oregon Office of the State Chief Information Officer. Implementation of E.O. 16-13, "Unifying Cyber Security in Oregon"

[5] Josephine Wolff, "Cybersecurity as Metaphor: Policy and Defense Implications of Computer Security Metaphors," Paper presented at the Conference on Communication, Informaiton, and Internet Policy,

[6] Nathan Sales, "Regulating Cyber-security," *Northwestern University Law Review* 107, no. 4 (2013):1521-1525.

[7] Christian Leuprecht, David Skillicorn, and Victoria Tait, "Beyond the Castle Model of cyber-risk and cyber-security," *Government Information Quarterly* 33, no. 2 (2016): 250-257.

[8] Ibid.

[9] Josephine Wolff, "Cybersecurity as Metaphor": 11-13.

[10] Wojciech Mazurczyk, Szymon Drobniak, and Sean Moore, "Toward a Systematic View on Cybersecurity Ecology," in *Combatting Cybercrime and Cyberterrorism*, ed. Babak Akhgar and Ben Brewster (Switzerland: Springer International, 2016), pg. 17-37.

[11] Kristen Osenga, "The Internet is Not a Super Highway: Using Metaphors to Communicate Information and Communications Policy," *Journal of Information Policy* 3 (2013): 30-54.

perspective likens it to traditional public goods[12,13] (clean air, for example) that are neither rivalrous nor excludable. These goods also tend to experience market failures as a result of reduced incentives for private investments[14] and generate negative externalities[15] when these failures occur. To approach cybersecurity from a public health perspective requires both an emphasis on increasing investments in cybersecurity using non-market incentive structures, and an emphasis on preventative measures that reduce the likelihood of "contracting" cybersecurity issues and prevent the spread of "disease" should this contraction occur[16]. This emphasis occurs alongside the more typical monitoring and response activities that find space in the traditional defense-oriented perspectives and approaches.

The application of the public health perspective to cybersecurity policy deliberations is most descriptively presented by Sedenberg and Mulligan[17], and Rowe, Halpern, and Lentz[18]. The latter's work is primarily instructive for those designing and implementing specific activities and programs to address cybersecurity issues. By contrast, Sedenberg and Mulligan describe the application of 12 public health principles for public cybersecurity that are instructive in terms of both content of policies, and the methods by which those policies are constructed[19]:

1. …address systemic design weaknesses and underlying behavioral causes through the preventative orientation to prevent adverse security outcomes.
2. …achieve community health in a way that respects the rights of the individuals in the community.
3. Public cybersecurity policies, programs, and priorities should be developed and evaluated through processes that ensure an opportunity for input from community members.

[12] Nathan Sales, "Regulating Cyber-security": 1527.

[13] Steven Weber, "Coercion in cybersecurity: What public health models reveal," *Journal of Cybersecurity* (2017): 1-11.

[14] Alfredo Garcia and Barry Horowitz, "The potential for underinvestment in internet security: implications for regulatory policy," *Journal of Regulatory Economics* 31, no. 1 (2007): 37-55.

[15] Bruce Kobayashi, "An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and Other Public Security Goods", *Supreme Court Economic Review* 14 (2006): 261-280.

[16] Jeff Rowe, Karl Levitt, and Mike Hogarth, "Towards the Realization of a Public Health System for Shared Secure Cyber-Space," *Proceedings of the 2013 New Security Paradigms Workshop* (2013): 11-18.

[17] Elaine Sedenberg and Deirdre Mulligan, "Public Health as a Model for Cybersecurity Information Sharing," *Berkeley Technology Law Journal* 30, no. 3: 1687-1739.

[18] Jeff Rowe, Michael Halpern, and Tony Lentz, "Is a Public Health Framework the Cure for Cyber Security?" *CrossTalk*, November/December 2012, 32.

[19] Elaine Sedenberg and Deirdre Mulligan, "Public Health as a Model for Cybersecurity Information Sharing": 1737-1738.

4. …advocate and work for the empowerment of disenfranchised community members…
5. …seek the information needed to implement effective policies and programs that protect healthy networks, systems, infrastructure, and use of Internet-based communication.
6. …provide communities and stakeholders with the information they have that is needed for decisions… and should obtain the community and stakeholder's consent for their implementation.
7. …act in a timely manner on the information they have within the resources and mandate given to them by the public.
8. …incorporate a variety of approaches that anticipate and respect diverse values, beliefs, and cultures in the community.
9. Public cybersecurity programs and policies should be implemented in a manner that most enhances the physical and social environment.
10. … protect the confidentiality of information that can bring harm to an individual or community if made public.
11. Public cybersecurity institutions should ensure the professional competence of their employees.
12. …engage in collaborations and affiliations in ways that build the public's trust and the institution's effectiveness.

These principles are explicitly referenced in the construction of the research tasks and methods of analysis employed by CPS. Specifically requesting the perspectives of the broader public using a variety of methods aligns with these principles, as does the emphasis on underlying behavioral drivers of cybersecurity inefficiencies. This is accomplished by asking respondents about habits, policies, and processes of organizations through surveying and focus group methods, rather than evaluating the implementation of specific technologies. The collaborative discussions encouraged by this approach also allow opportunities for meaningful engagement, as well as education on current issues and policy initiatives[20]. In addition, the criteria used to consider the programs implemented in other states in the comparative analysis place a high value on the aspects of cybersecurity highlighted in this specific approach that are not necessarily found in others: systemic prevention measures and collaborative multi-sector leadership.

[20] Peter Shane, "Cybersecurity Policy as if 'Ordinary Citizens' Mattered: The Case for Public Participation in Cyber Policy Making," *I/S: A Journal of Law and Policy for the Information* Society, 8, no. 2 (2012): 433-462.

INTRODUCTION AND RESEARCH APPROACH

By embracing the public health approach to cybersecurity, this report provides a comprehensive analysis that reflects the challenges and opportunities Oregon organizations face with the prevention and monitoring of cybersecurity risks, as well as responses to incidents, and comparable ways all three of these elements have been addressed elsewhere. The data generated using this framework recognizes the human component of cybersecurity, and the potential of the CCoE to positively impact both the social and technical aspects of effective public cybersecurity policy. The research also constitutes one arm of an outreach effort that can help legitimize policy outcomes from the CCoE proposal process.

CHAPTER 1: STATE CYBERSECURITY COMPARATIVE POLICY ANALYSIS

Chapter 1: State Cybersecurity Comparative Policy Analysis

> *"While community institutions may fall outside the traditional ambit of state cyber security policy, our interdependence and shared information systems render individual and isolated interventions insufficient to stem the tide of cyber security threats—we are more resilient when we stand together."*
>
> - Oregon Office of the State Chief Information Officer

The **Oregon Cybersecurity Center of Excellence (CCoE)** aims to create an integrated cybersecurity resource hub working to protect the cyber health of Oregon's digital ecosystems. The Oregon CCoE aims to emphasize a shared responsibility for cybersecurity[21] by embracing the evidence growing over the last decade that network-wide cyber health is a public good that is currently underdeveloped and underfunded. This comparative analysis of cybersecurity policies in other US states assesses the initiatives and activities that have brought success to cybersecurity efforts by considering these efforts through the public health lens.

The Oregon Office of the State Chief Information Officer has enlisted the Center for Public Service to apply a public health approach in comparing existing cybersecurity initiatives in other states with those resembling the planned responsibilities and statutory vision for the **Oregon CCoE**.[22] We identify innovative practices for comprehensive and interoperable cybersecurity emphasizing the public health methods geared toward creating a ***Competent Authority*** that can address the ***Prevention, Active Monitoring*, and *Response and Recovery of Cyber ecosystems***.[23,24,25] This evidence-based philosophy necessitates that individuals, organizations, and governments all share a responsibility in keeping our networks healthy. This involves

[21] Oregon. Office of the State Chief Information Officer. *Implementation of E.O. 16-13, "Unifying Cyber Security in Oregon" - Written Testimony for the Joint Legislative Committee on Information Management and Technology*. December 12, 2016. Pg 10-15. https://olis.leg.state.or.us/liz/2017R1/Downloads/CommitteeMeetingDocument/96166.

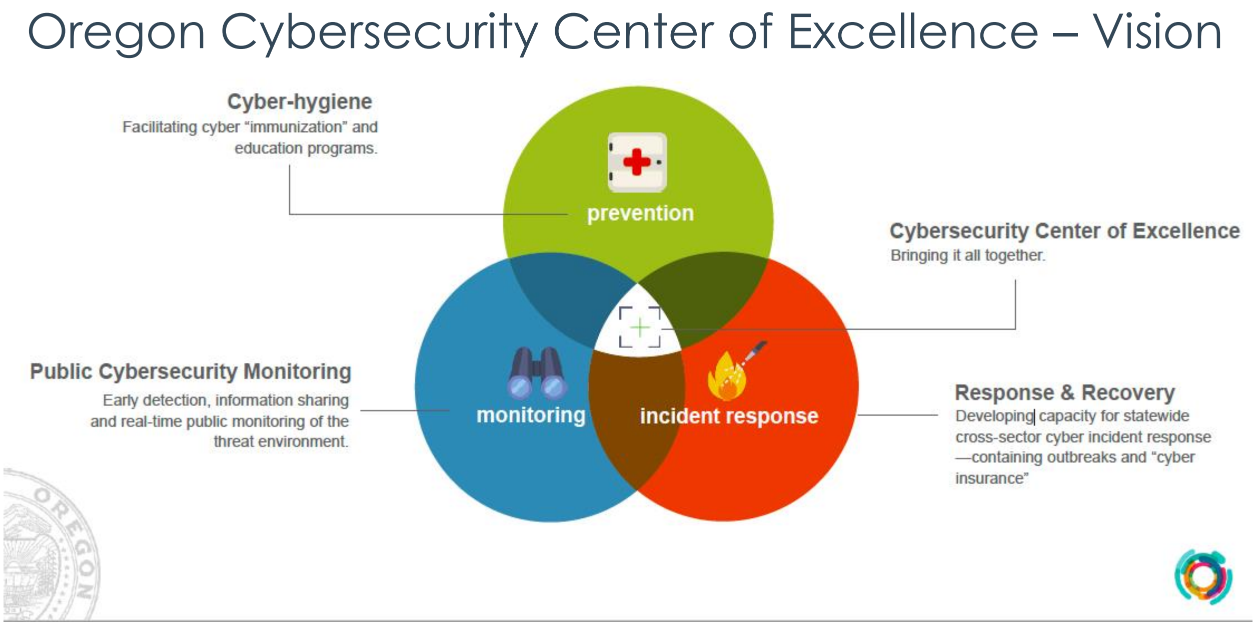
[22] Oregon. Office of the State Chief Information Officer. Implementation of E.O. 16-13, "Unifying Cyber Security in Oregon" - Written Testimony for the Joint Legislative Committee on Information Management and Technology. December 12, 2016. Pg 10-15. https://olis.leg.state.or.us/liz/2017R1/Downloads/CommitteeMeetingDocument/96166.

[23] Spidalieri, Francesca. "State of the States on Cybersecurity." The Pell Center. February 01, 2015. Accessed September 05, 2017. http://pellcenter.org/eight-states-lead-the-rest-in-cybersecurity/.

[24] Ibid, Mulligan and Schneider, 2011

[25] Ibid Sedenberg and Mulligan, 2015

keeping them free from infection and able to provide nimble and robust response, engaging in effective recovery, and astutely focusing on prevention and proper cyber hygiene.[26, 27] Compiling an Oregon specific evaluation framework allows our research to examine cyber health consistently with **Oregon's vision for the Cybersecurity Center for Excellence as an innovative entity embedded in the future-oriented cyber ecosystem of the Silicon Forest**. This vision for the Oregon CCoE is illustrated by the OSCIO in the graphic below.



Oregon Cybersecurity Center of Excellence – Vision

Cyber-hygiene
Facilitating cyber "immunization" and education programs.

Cybersecurity Center of Excellence
Bringing it all together.

Public Cybersecurity Monitoring
Early detection, information sharing and real-time public monitoring of the threat environment.

Response & Recovery
Developing capacity for statewide cross-sector cyber incident response —containing outbreaks and "cyber insurance"

From the Oregon Office of the State Chief Information Officer. Implementation of E.O. 16-13, "Unifying Cyber Security in Oregon"

This report's comparative policy analysis is meant to inform the CCoE Advisory Council's vision with a comparative analysis of other states' cybersecurity programs and initiatives that resemble the Oregon CCoE's mission to create cyber safe ecosystems.[28] Digital communities with low rates of infection and crime create collective economic impact

[26] Sedenberg, Elaine M., and Deirdre Mulligan. "Public Health as a Model for Cybersecurity Information Sharing." *Berkeley Technology Law Journal* 30, no. 2 (2015): 1737-9. Accessed September 05, 2017. doi:https://doi.org/10.15779/Z38PZ61.

[27] Hathaway, Melissa. "Cyber Readiness Index 1.0 | Belfer Center for Science and International Affairs." Harvard Kennedy School Belfer Center for Science and International Affairs. 2013. Accessed September 07, 2017. http://www.belfercenter.org/publication/cyber-readiness-index-10.

[28] Oregon. Office of the State Chief Information Officer. *Implementation of E.O. 16-13, "Unifying Cyber Security in Oregon" - Written Testimony for the Joint Legislative Committee on Information Management and Technology.* December 12, 2016. Pg 10-15. https://olis.leg.state.or.us/liz/2017R1/Downloads/CommitteeMeetingDocument/96166.

and shared value that is beneficial to everyone in the ecosystem; individuals, organizations, businesses, states, and federal networks. In other words, cybersecurity is a public good, allowing us to benefit from a virtual shared commons.[29]

COMPARATIVE ANALYSIS METHODS

Policy Analysis Methodological Framework & Comparators

Key Research Questions

- What efforts and initiatives exist in other states that are comparable in size and scope to the Cybersecurity Center of Excellence as described in SB 90?[30]
- What best practices regarding Centers of Excellence and cybersecurity initiatives have been recognized in academic and industry literature?
- What has contributed to the success or failure of cybersecurity initiatives in other states?

Framework

Compiling a Public Health Framework for Oregon's Unique Aims

The research questions are answered through a qualitative comparative policy analysis of similar initiatives in other states. We use a comprehensive literature review and apply an evaluative public health framework that holistically compares multiple states' efforts.[31] Viewing cybersecurity through the lens of a cohesive public health and safety framework, we combine literature and best practices from esteemed institutions to identify criteria by which we will evaluate existing cybersecurity initiatives against the backdrop of Oregon's unique needs**.**

The research questions are investigated by combining criterion to form an evaluation matrix (see Evaluation Matrix below). Criterion are compiled from the following guiding documents to identify innovative practices for comprehensive and interoperable

[29] Mulligan, Deirdre K., and Fred B. Schneider. "Doctrine for Cybersecurity." *Daedalus Journal of the American Academy of Arts and Sciences,* May 15, 2011, P.3, 9-12, 28-30. Accessed September 13, 2017. doi:10.1162/DAED_a_00116.

[30] Oregon. State Legislature. *Senate Bill 90- Establishing the Oregon Cybersecurity Center of Excellence.* 2017. https://olis.leg.state.or.us/liz/2017R1/Downloads/MeasureDocument/SB90/Introduced.

[31] Hathaway, Melissa. "Cyber Readiness Index 1.0 | Belfer Center for Science and International Affairs." Harvard Kennedy School Belfer Center for Science and International Affairs. 2013. Accessed September 07, 2017. http://www.belfercenter.org/publication/cyber-readiness-index-10.

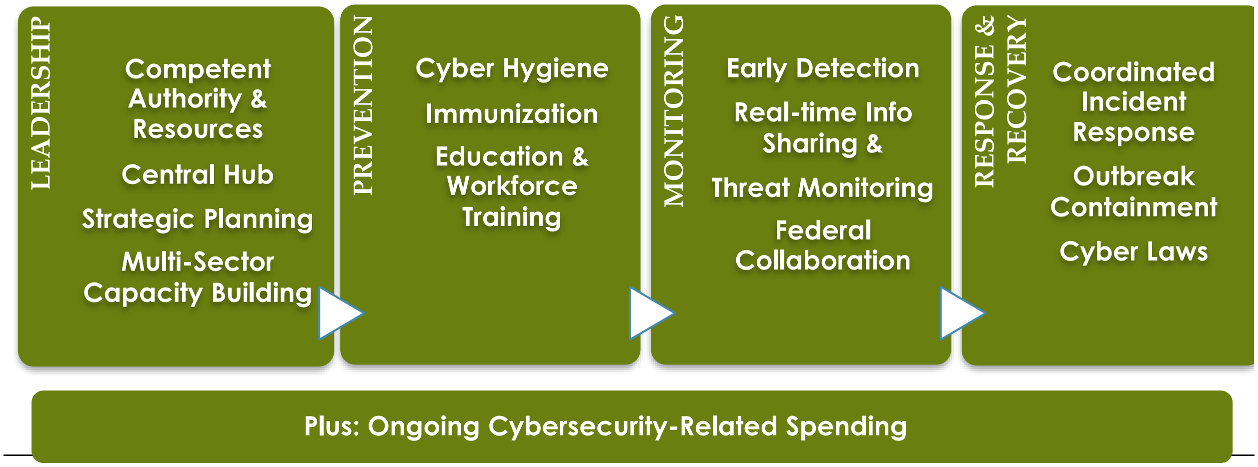
cybersecurity that **emphasize cybersecurity as a public good.** We isolate methods across the literature geared toward creating ***Competent Leadership*** that can facilitate and guide ***Prevention*****,** ***Active Monitoring*****, and** ***Response and Recovery of Cyber ecosystems***[32,33,34] as per the OSCIO's CCoE vision.

The Evaluation Matrix draws on these sources from the literature:

- Mulligan and Schneider's "Doctrine of Cybersecurity"[35]
- Sedenberg and Mulligan's "Public Health as a Model for Cybersecurity Information Sharing"[36]
- Hathaway's *Cyber Readiness Index 1.0 & 2.0*[37]
- Spidalieri's *State of States on Cybersecurity* report[38]
- Sales' "Regulating Cybersecurity"[39]

Evaluation Matrix

Promoting Healthy Cyber Ecosystems



LEADERSHIP

Competent Authority & Resources

Central Hub

Strategic Planning

Multi-Sector Capacity Building

PREVENTION

Cyber Hygiene

Immunization

Education & Workforce Training

MONITORING

Early Detection

Real-time Info Sharing &

Threat Monitoring

Federal Collaboration

RESPONSE & RECOVERY

Coordinated Incident Response

Outbreak Containment

Cyber Laws

Plus: Ongoing Cybersecurity-Related Spending

[32] Spidalieri, Francesca. "State of the States on Cybersecurity." The Pell Center. February 01, 2015. Accessed September 05, 2017. http://pellcenter.org/eight-states-lead-the-rest-in-cybersecurity/.

[33] Ibid, Mulligan and Schneider, 2011

[34] Ibid Sedenberg and Mulligan, 2015

[35] Ibid, Mulligan and Schneider, 2011

[36] Ibid, Sedenberg and Mulligan, 2015

[37] Melissa, Hathaway, and Potomac Institute for Policy Studies. *The Cyber Readiness Index 2.0: A Plan for Cyber Readiness Baseline and Index*. Publication. November 2013. http://www.potomacinstitute.org/images/CRIndex2.0.pdf

[38] Ibid. Spidalieri 2015.

[39] Sales, Nathan Alexander. "Regulating Cyber-security." *Northwestern University Law Review* 107, no. 4 (2013)

CHAPTER 1: STATE CYBERSECURITY COMPARATIVE POLICY ANALYSIS

The composite **evaluation matrix** consists of five categories of cybersecurity activities prevalent in the cybersecurity-from-a-public-health-perspective literature. These areas are **Leadership**, **Prevention**, **Monitoring**, **Response & Recovery** and **Cost**. Each category includes several sub-categories of activities that are recognized by the literature as essential to a cross-sectoral and state-wide cyber readiness plan to maintain healthy cyber ecosystems.

The comparative evaluation categories and sub-category activities encompass all of the statutory aims of the Oregon CCoE.[40] Eleven states were selected for the comparative analysis based on their identification in the literature as prioritizing cyber security as critical. Each has taken a proactive approach to creating innovative mechanisms and efforts that produce resiliency in the face of threats.[41] The Spidalieri baseline report is the source for 8 of our state cases. The Spidalieri study is largely based on the criteria of the *Cyber Readiness Index 1.0*. We have created a unique set of evaluative comparators that includes, but is not limited to some of those included in the Spidalieri analysis and the Cyber Readiness Index. Those studies heavily informed our research and provided an excellent baseline to identify states that employ exceptional cybersecurity practices. Our evaluative framework focuses on cybersecurity as a public good and goes beyond a threat readiness mindset by emphasizing the community-based public health literature. Three states were added to the states identified in the baseline Spidalieri research; these states (Colorado, Florida, and Illinois) were chosen because of recent national recognition for their innovative efforts. Our comparative analysis identifies key actions in each of the eleven states and categorizes them according to the five areas specified in the evaluation matrix as vital to promoting cyber health as a public good.

Our analysis found that each state has a different system and policy structure for handling cybersecurity. Some execute through the executive branch, others through the legislature. This makes cross-state comparisons difficult. We chose to focus on available cybersecurity strategic plans and government documents to piece together what the cybersecurity climate looks like in each state. **The goal of this research is to identify how each state addresses the goals that Oregon would like to pursue.** It is important to note that Oregon's population is smaller than each of our 11 comparative states. Each state may have pieces of an integrated strategy in place, there may be a

[40] Oregon. State Legislature. *Senate Bill 90- Establishing the Oregon Cybersecurity Center of Excellence.* 2017. https://olis.leg.state.or.us/liz/2017R1/Downloads/MeasureDocument/SB90/Introduced.

[41] Ibid. Spidalieri, p 4.

number of departments involved, some comparators included in our analysis may not be present in each state. This analysis attempts to clarify between stated strategic goals versus what actually gets funded and implemented, but this is not possible in all cases. The states examined are not expected to be "meeting" our public health criteria or applying any specific public health framework. **Our criteria and framework are intended to provide a scaffold by which Oregon can examine how to best utilize policy examples from other states to address cybersecurity as a public good. This analysis aims to figure out where other state's pieces might fit our puzzle.** *This research is not attempting to score other states based on our criteria.*

Evaluative Comparators

This section elaborates on the five evaluation categories that are used in our comparative analysis of the 11 selected states.

1. LEADERSHIP

Competent Authority & Resources, Central Hub, Strategic Planning, Multi-Sector Capacity Building

The Oregon CCoE aims to be a central cybersecurity hub and authority working across sectors to improve Cyber health and safety through prevention, monitoring, incident response and education and workforce capacity building.[42] The public health sector employs the Center for Disease Control to be the central authority and data collection hub for preventing, monitoring, and responding to public health crises. The CDC is relied upon to synchronize the diverse and highly de-centralized public health community on the appropriate measures of infection prevention, monitoring, response and recovery.[43] **The Oregon CCoE would ideally be akin to an equivalent state institution responsible for digital public health. The literature emphasizes the need for a state to have a highly competent central authority. This authority serves as the figure head for a central hub for cybersecurity with sufficient investment resources to design strategy, develop new capacity, and ensure effective and efficient implementation.** The authority should pursue the goals of sharing best practices, promoting cross sectoral, multi-state, and national cooperation, coordinating response to outbreaks, aligning public-facing educational resources about preventative

[42] Oregon. Office of the State Chief Information Officer. Implementation of E.O. 16-13, "Unifying Cyber Security in Oregon" - Written Testimony for the Joint Legislative Committee on Information Management and Technology. December 12, 2016. Pg 13-14. https://olis.leg.state.or.us/liz/2017R1/Downloads/CommitteeMeetingDocument/96166.

[43] Ibid. Mulligan and Schneider p 27-30

behaviors, and facilitating information sharing and monitoring of the health of the digital ecosystem. Strategy design should include workforce development, cybersecurity R&D, and academic/economic goal alignment.[44,45,46,47,48]

Contributions from the Stanford Social Innovation review and Harvard Business review provide the guiding principles and evaluation mechanisms of **shared value** and **collective impact** created by communities when there exists a **shared responsibility to improve systems and practices that hold potential to provide immense social and economic good**. **Multi-sectoral collaboration** is essential to this process in order to spur and sustain innovation and growth. **We include multi-sectoral collaboration as a comparator specifically because the literature emphasizes that in order to create shared value and collective impact, you must first build the capacity for multi-sectoral collaboration**. [49,50] Multi-Sector Capacity is defined for this purpose as actively involving state, federal, academic, health, business (not just cybersecurity or IT), and social sectors. Almost all states included state, federal, academic, and cybersecurity company involvement.

2. PREVENTION

Cyber Hygiene, Immunization, Education & Workforce Training

Key to addressing any public health crisis are preventative measures. Avoiding infection and spread of pathogens starts with basic hygiene tasks like handwashing, teeth brushing, staying home when sick, and prophylactics. In cybersecurity, preventative measures are just as important in avoiding the spread of infection among machines in a cyber community.[51] Effective Cybersecurity strategies emphasize and educate about **cyber hygiene and immunization. Cyber hygiene** includes public-facing cybersecurity resources, and policies aimed at requiring regular system threat monitoring, penetration

[44] Ibid. Spidalieri P 7.
[45] Ibid. Hathaway 2013, p 2
[46] ibid. Sales, p 1547-1551
[47] Ibid. Sedenberg and Mulligan, 2015 p 13-14
[48] Vez, Jean-Luc. "Recommendations for Public-Private Partnership against Cybercrime." World Economic Forum Cybercrime Project. January 2016. Accessed September 13, 2017. doi:http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf.
[49] Kramer, Mark R., and Michael E. Porter. "Creating Shared Value." Harvard Business Review. August 25, 2015. Accessed September 05, 2017. https://hbr.org/2011/01/the-big-idea-creating-shared-value.
[50] Kania, John, and Mark Kramer. "Collective Impact." Stanford Social Innovation Review. Winter 2011. Accessed September 05, 2017. https://ssir.org/articles/entry/collective_impact.
[51] Ibid. Sales. 2013. P 1539, 1541, 1561

testing, and updates for effective patching of vulnerabilities.[52] Employee training and public information campaigns promote safe browsing habits to increase defense against dangerous phishing attacks, email attachments, and nefarious sites.[53] **Immunity** in increased by bolstering the human firewall to protect individual machines and networks by creating a kind of **digital herd immunity** increasing the safety of the overall ecosystem.[54] **Immunity** is also increased by promoting the use of stronger passwords and authentication methods.[55,56] **Education and workforce training** programs both in cybersecurity specific academic-to-employment tracks and via public-facing media campaigns about Cyber Hygiene and Immunization are encouraged best practices.[57,58]

3. ACTIVE MONITORING

Early Detection, Real-time Info Sharing, Real-time Threat Monitoring, Federal Collaboration

The Center for Disease Control monitors our dispersed health care systems with a robust system of data sharing and reporting standards that increase our collective ability to monitor and respond to outbreaks of infectious diseases. Digital infections can be monitored in much the same way. Monitoring responsibilities are a key feature of a successfully integrated state resource hub like a CCoE.[59] Collaboration and coordination of information sharing across public and private sectors, multi-state, and national entities is paramount to maintain safe cyber communities. **Early Detection** of threats and infections, **real-time info sharing**, and **real-time threat monitoring** are essential to success.[60,61, 62] **National Collaboration** includes public-private partnerships, implementation of state-level best- and next-practice cybersecurity controls, and supporting coordinated incident response via cyber intelligence sharing. Coordination with the National Cybersecurity and Communications Integration Center (NCCIC), Multi-State Information Sharing and Analysis Center (MS-ISAC), regional Information Sharing

[52] Center for Internet Security Response To Commission On Cybersecurity. "CIS Response to NIST RFI for the Cybersecurity Framework: Input to the Commission on Enhancing National Cybersecurity." *National Institute for Standards and Technology*, 2016, P 2. Accessed September 14, 2017. https://www.nist.gov/sites/default/files/documents/2016/09/15/cis_rfi_response.pdf.

[53] Ibid Sedenberg and Mulligan, 2015 p 1696, 1704, 1736-38

[54] Ibid. Mulligan and Schneider, 2011 p 11-12

[55] Ibid. Sales. 2013 p 1512, 1517, 1535

[56] Ibid. Mulligan and Schneider, 2011, p 19

[57] Ibid. Spidalieri. 2015 p 8

[58] Ibid. Hathaway. 2013. P 4

[59] Ibid. Sales. 2015. P 1540-41

[60] Ibid. Spidalieri. 2015 p 8

[61] Ibid. Sales. 2015. P 1508-09, 1512, 1530, 1567

[62] Ibid. Sedenberg and Mulligan, 2013. P 1708, 1729, 1736

and Analysis Organizations (ISAOs), and sector specific counterparts are encouraged.[63,64] An ongoing culture of evaluating state specific cyber threat analysis & cybersecurity strategy planning, like a Cyber Disruption Plan or coordinated Incident Response plan, is also recommended.[65]

4. RESPONSE & RECOVERY

Coordinated Incident Response, Outbreak Containment, Cyber Laws

Coordinated Incident Response that facilitates rapid containment of outbreaks is becoming the centerpiece of state and national cyber preparedness. Security Operations Centers are employed by some, others coordinate with law enforcement and various Computer Emergency Response Teams (CERTs), National Guard, Homeland Security, and volunteer Cyber Corps. Consumer protections in the form of cyber health laws like data breach notifications, stronger personal information protection laws, criminalization of cyberattacks, more inclusive private sector coordination and cyber intelligence sharing, and products like cyber insurance, have also been recognized as productive tools for responding to and recovering from threats.[66,67, 68]

5. COSTS

Recent Cybersecurity Related Spending

The cost comparator is mostly anecdotal but included to provide a reference frame for the scope of differing state-reported cybersecurity costs. Many of the initiatives examined exist in their incipient stages. It was not possible to compare state-by-state cybersecurity costs due to the disparate departments and funding structures that are responsible for cybersecurity spending. Recent significant expenditures are noted for most states.

[63] Ibid. Spidalieri. 2015 p 6
[64] Ibid. Sedenberg and Mulligan 1698-99
[65] Ibid. Spidalieri. 2015 p 5-9
[66] Ibid. Mulligan and Schneider p 7-8
[67] Ibid. Sales. 2013. 1558-59
[68] Ibid Spidalieri. 2015 pg 7, 11

STATE ANALYSIS: CALIFORNIA

Leadership

Competent Authority & Resources, Central Hub, Strategic Planning

The California Department of Technology and the Office of Emergency Services (as a homeland security function) are responsible for the IT strategic plan, which includes some cybersecurity specific planning.[69] California is moving toward a more centralized entity for cybersecurity leadership through an executive order from 2015 that consolidated cybersecurity strategic efforts with the **California Cybersecurity Integration Center (Cal-CSIC**). The center will be responsible for cybersecurity strategic planning and aims to increase the state's cyber defenses against threats to the economy, critical infrastructure, or public and private networks. The first strategic plan from the Cal-CSIC is due in June 2018.

In September 2017, the legislature approved the creation and funding of the Cal-CSIC administered by the Office of Emergency Services in close coordination with the California Cybersecurity Task Force. Sixteen agencies are required to participate including the highway patrol, military services, Office of the Attorney General, Health and Human Services Agency, Utilities Emergency Association, university system, community colleges, FBI, U.S. Secret Service, and Coast Guard. The U.S. Department of Homeland Security is the sole funder of the endeavor at $1.8 million annually. The Cal-CSIS will be responsible for coordinating with these and other agencies and private sector partners to develop a comprehensive state-wide cybersecurity strategy, secure multi-sector information sharing online platform, cyber incident response team, and data privacy safeguards.[70]

Multi-Sector Capacity Building

The Cal-CSIC will work closely with the California Cybersecurity Task Force. The task force consists of 7 sub-committees (risk mitigation, information sharing, workforce development and education, economic development, emergency preparedness, legislation and funding, and digital forensics). The task force is a joint endeavor of the Office of Emergency Services and Department of Technology that began by executive

[69] California. Department of Technology. Director. *California Information Technology Strategic Plan 2016 Update.* By Carlos Ramos. 2016. Accessed November 14, 2017. https://cdt.ca.gov/wp-content/uploads/2017/03/CA-IT-Strategic_Plan_2016.pdf.

[70] California Legislative Information. 2017- 2018 Regular Session. *Bill Text - AB-1306 California Cybersecurity Integration Center.* September 15, 2017. Accessed November 14, 2017. http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB1306.

order in 2013 and focuses on education, information sharing, workforce development and economic growth.[71]

"All members of the Task Force work diligently to promote a culture of cybersecurity, cyber-hygiene, and best practices where all Californians can work, play, and explore freely and safely"[72]

California explicitly recognizes that 95% of critical infrastructure is owned and operated by private industry, requiring robust public-private partnerships to create a "community of information sharing and mutual aid." With the inclusion of public, private, academic, and economic development organizations the Cal-CSIC resembles a truly multisector effort.[73]

Prevention

Cyber Hygiene, Immunization, Education & Workforce Training

The California Information Security Office (CISO) works with agency officers to develop education and training of the state's workforce.[74] California requires that all state employees and contractors receive information security and data privacy training.[75] The Workforce and Development Sub-committee of the Cybersecurity Task Force publishes detailed cybersecurity workforce objectives and proposals in conjunction with academic institutions.[76]

The **CyberCalifornia** initiative works to generate public-private partnerships that relate to cybersecurity in business and commerce. CyberCalifornia manages the Innovation Hub (iHUB) and facilitates threat information sharing and research of cybersecurity in business, commerce, and the Internet of Things (IoT).[77,78] The California CIO has its own

[71] Spidalieri, Francesca. "State of the States on Cybersecurity." *Pell Center for International Relations and Public Policy*, November 2015, 9. http://pellcenter.org/eight-states-lead-the-rest-in-cybersecurity/.

[72] California. Governor's Office of Emergency Services. *Cybersecurity Task Force Task Force Subcommittees.* Accessed November 14, 2017. http://www.caloes.ca.gov/for-individuals-families/cybersecurity-task-force/task-force-subcommittees.

[73] California. Governor's Office of Emergency Services. *California Cybersecurity Integration Center.* Accessed November 14, 2017. http://www.caloes.ca.gov/cal-oes-divisions/law-enforcement/california-cybersecurity-integration-center.

[74] Ibid. Spidalieri. 2015. pg. 9

[75] "State Agency Annual Security and Privacy Training." California Department of Technology. Accessed November 14, 2017. https://cdt.ca.gov/do-all-employees-in-a-state-agency-need-to-take-annual-security-and-privacy-training/.

[76] California. *State of California Cybersecurity Task Force Workforce Development and Training Objectives.* June 2015. Accessed November 14, 2017. http://www.caloes.ca.gov/CybersecurityTaskForceSite/Documents/Workforce%20Objective%201%20Proposal%202015-06.pdf.

[77] State of California. *CyberCalifornia Initiative.* 2017. Accessed November 14, 2017. http://cybercalifornia.biz/.

[78] Ibid. Spidalieri, 2015, pg. 12

YouTube channel that includes cybersecurity PSA's for the general public as well as IT and state employee specific informational videos.[79]

The **California Mentors Program** connects young IT professionals with one-on-one senior IT leaders in an effort to address the IT shortage, facilitate knowledge transfer, and leadership and management skills.[80]

The California's academic institutions offer some of the most prominent IT and security education programs in the nation that are often coordinated with federal defense. (see below)[81,82]

ACADEMIC INSTITUTION	PROJECT
University of Southern California (USC)	Computer Systems Security (CCSS) DETER—Cyber Defense Technology Experimental Research project ($16 Mill DHS expansion)
Sacramento State College of Continuing Education and the College of Engineering and Computer Science	Information Security Leadership Academy Certificate Program targeted at state and local employees
UC Berkeley, Stanford University, San Jose State University	Team for Research in Ubiquitous Secure Technology (TRUST)
California State Polytechnic University, California State University Sacramento, Naval Postgraduate School	selective National Science Foundation CyberCorps Scholarship for Service
California State Polytechnic, California Military Department	California Cyber Training Complex, Central Coast Cyber Forensic Lab
UC Davis, Irvine, San Jose State University, National University, California State University, Sacramento, San Bernardino, Coastline Community College, Naval Postgraduate School, California State Polytechnic University Pomona	Designation as NSA/DHS Academic Centers of Excellence

[79] California Chief Information Office. "Protecting Your Computer." YouTube. March 22, 2017. Accessed November 14, 2017. https://www.youtube.com/watch?v=SDXpDIbpIZ4.

[80] State of California. California Mentor Program. Accessed November 14, 2017. http://www.camentorprogram.cdt.ca.gov/.

[81] Ibid. Spidalieri. 2015. Pg. 11-12

[82] U.S. National Security Agency and the Department of Homeland Security. *Current National CAE Designated Institutions.*https://www.iad.gov/nietp/reports/current_cae_designated_institutions.cfm.

Active monitoring

Early Detection, Real-time Info Sharing & Threat Monitoring, Federal Collaboration

California recently adopted a new information security policy AB-670 that requires at least 35 of the 77 state offices undergo an information security assessment each year. The state standards are a compiled from federal and state policies guided by the National Institute of Standards and Technology (NIST) Security and Privacy Controls.[83,84,85]

Implementation of AB-670 is overseen by the California Department of Technology, the Chief Information Security Officer and the Office of Emergency Services. The cost of the assessments, estimated at $10,000 to $40,000 each, are the responsibility of the agency being assessed. The development of the standards and updates to state protocols and the State Administrative Manual will cost $100,000- $150,000. The state estimates the cost to the Department of Technology to begin and fund the program are $2 Million the first year and $1.9 million per year for 12 full-time personnel plus additional "hundreds of thousands" in travel costs annually. These costs are weighed against the possibility of a single attack on critical infrastructure costing upwards of $1 Billion.[86] For many of these assessments the governor has proposed a one-time $14 million-dollar allotment to fund 58 positions, over 12 departments for FY 2017-2018.[87]

The California Information Security Office provides a security evaluation tool and requires state agencies to submit an IT security Plan of Action and Milestones (POAM) that are assessed quarterly. The Cal-CSIC plans to facilitate information sharing between local, state, and federal agencies, tribal governments, utilities, academic institutions, NGOs, and the U.S. Department of Homeland Security.[88]

[83] California Legislative Information. 2015- 2016 Regular Session. Bill Text - AB-670 Information Technology Security. October 6, 2015. https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201520160AB670.

[84] U.S. Department of Commerce. National Institute of Science and Technology. Joint Task Force Transformation Initiative. NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations Revision 4. Accessed November 14, 2017. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[85] California Department of Technology. CDT Services. Information Security Program Audit. By State Of California. Accessed November 14, 2017. https://cdt.ca.gov/services/information-security-program-audit/.

[86] California Legislative Information. 2015-2016 Regular Session. Assembly Analysis 9/08/15.Bill Analysis-AB-670 Information Technology Security. September 8, 2015. https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201520160AB670.

[87] California. Legislative Analyst's Office. Governor's Budget Proposal 2017-18. Governor's Proposal to Strengthen Information Security. February 28, 2017. http://www.lao.ca.gov/Publications/Report/3594 see entire Governor's Budget here: http://www.lao.ca.gov/Budget?yr=2017

[88] California. Department of Technology. Director. California Information Technology Strategic Plan 2016 Update. By Carlos Ramos. 2016. Accessed November 14, 2017.p 7. https://cdt.ca.gov/wp-content/uploads/2017/03/CA-IT-Strategic_Plan_2016.pdf.

Response and recovery

Coordinated Incident Response, Outbreak Containment, Cyber Laws

In addition to the Cal-CSIC, in 2017 California established a cybersecurity Strategic Operations Center (SOC) for state systems that will support incident response and share threat intelligence with the Cal-CSIC.[89] To begin, the Cal-CSIC was co-located alongside the State Threat Assessment System in order to immediately integrate the California cyber intelligence community.[90] The SOC operations are being phased in over 2 years, phase one focuses on prevention and detection on the state network, phase 2 expands the SOC to cover assets owned or managed by the Department of Technology, phase 3 creates a pilot program with state partners, and phase 4 expands the pilot to other state entities.[91]

California requires state agency cyber incident reporting through the Office of Information Security (OIS) portal, the California Compliance and Security Incident Reporting System (Cal-CSIRS). Detailed instructions and resources are provided. The OIS coordinates with the Cal-CSIC, Highway Patrol, California Military Department, and Office of Health Information Integrity.[92] The Cal-CSIC is currently developing a centralized cyber incident response team.[93] The office also provides a list of resources connecting to the MS-ISAC, US CERT, SANS, and NIST.[94]

California has a data breach notification law where businesses and state agencies must report the breach of personal information.[95] The use of ransomware was recently criminalized by the state.[96] All state employees must complete mandatory cybersecurity training.[97] California's leadership has introduced Cyber Hygiene legislation at the federal level.[98]

[89] California Department of Technology. "CDT Launches State's First Security Operations Center." CDT TechBlog. 2017. http://techblog.ca.gov/2017/09/cdt-launches-soc/.

[90] California. Governor's Office of Emergency Services. *California Cybersecurity Integration Center.* Accessed November 14, 2017. http://www.caloes.ca.gov/cal-oes-divisions/law-enforcement/california-cybersecurity-integration-center.

[91] California Department of Technology. "CDT Launches State's First Security Operations Center." CDT TechBlog. 2017. http://techblog.ca.gov/2017/09/cdt-launches-soc/.

[92] California. Department of Technology. *CDT- Policy Resources.* Accessed November 14, 2017. https://cdt.ca.gov/security/policy/#Policy-Resources.

[93] California Legislative Information. 2017- 2018 Regular Session. *Bill Text - AB-1306 California Cybersecurity Integration Center*. September 15, 2017. http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB1306.

[94] California Department of Technology. CA Information Security Office. *Incident Management Program Resources.* August 18, 2016. https://cdt.ca.gov/wp-content/uploads/2017/03/Incident_Management_Program_Resources.pdf.

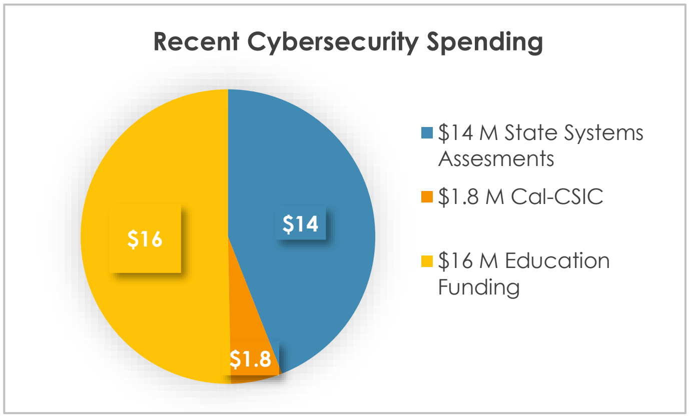
[95]California Department of Justice. Office of the Attorney General. *Data Security Breach Reporting.* Accessed November 14, 2017. https://oag.ca.gov/privacy/databreach/reporting.

[96] California Legislative Information. 2015- 2016 Regular Session. *Bill Text - SB-1137 Computer Crimes: Ransomware.* September 27, 2016. Accessed November 14, 2017. http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB1137.

[97] State Agency Annual Security and Privacy Training." California Department of Technology. Accessed November 14, 2017. https://cdt.ca.gov/do-all-employees-in-a-state-agency-need-to-take-annual-security-and-privacy-training/.

[98] Chalfant, Morgan. "Senators Introduce 'cyber Hygiene' Bill." The Hill. June 30, 2017. Accessed November 14, 2017. http://thehill.com/policy/cybersecurity/340160-senators-introduce-cyber-hygiene-bill.

Costs



RECENT CYBERSECURITY SPENDING $32.8 Million:

- $14M for state cybersecurity assessment staffing
- $1.8M DHS funds Cal-CSIC
- $16M DHS Education Partners

STATE ANALYSIS: COLORADO

Leadership

Competent Authority & Resources, Central Hub, Strategic Planning

Colorado's Cybersecurity authority is centralized under the Office of Information Technology (CoOIT) and the Chief Information Security Officer (CoCISO). The Chief Technology Officer is responsible for day-to-day access provisioning, network and end-point security monitoring, threat and vulnerability management, computer forensics, and incident response. In 2016 the state passed a comprehensive cybersecurity bill creating and appropriating funding for the Colorado Cybersecurity Council, Cybersecurity Cash Fund, a cyber operations center, education and workforce development plan, and research and development goals. Research and development goals including everything from working with local businesses and universities to certifying a Top Secret and Special Access Facility.[99]

The CoCISO is tasked with developing and implementing the larger IT strategic security plan titled **Secure Colorado** in partnership with the **Colorado Information Security Advisory Board**.[100] The National Governor's Association, National Association of State Chief Information Officers (NASCIO), and the Cybersecurity Leadership and Innovation Awards have all recognized the **Secure Colorado** plan as a landmark initiative in state-wide cybersecurity- particularly for states new to forming cybersecurity strategy.

> *"Secure Colorado was chosen as a model for the National Governor's Association policy academy to help states who are less mature in their cybersecurity programs to develop a sustainable cybersecurity strategy."*

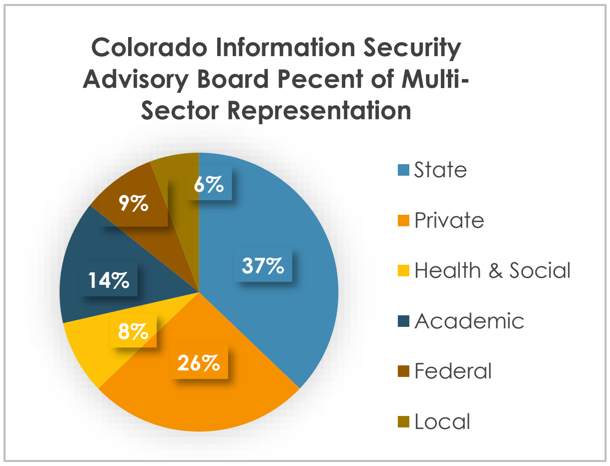
Secure Colorado's strategic priorities include the goals of protection, research and development, building partnerships, and compliance. These goals relate to 18 specific initiatives. Evaluation metrics quantifying the status of progress are applied yearly. The Secure Colorado Initiative is in its 3rd year, last year the program was approved to continue based on measurable evidence of security progress.

[99] Colorado. General Assembly. 2016 Regular Session. HB16-1453 Colorado Cybersecurity Initiative. 2016. https://leg.colorado.gov/sites/default/files/documents/2016a/bills/2016A_1453_signed.pdf.

[100] Colorado. Governor's Office of Information Security and Risk Management. *Secure Colorado Colorado's Strategy for Information Security and Risk Management Fiscal Years 2017-2019*. January 1, 2017. https://drive.google.com/file/d/0B0IQVOYmWcOoa2dadGQwZURUdVU/view.

Multi-Sector Capacity Building

The **Colorado Information Security Advisory Board** is responsible for evaluating and recommending improvements or other changes to the **Secure Colorado** plan. The Advisory Board consists of representatives from over **30 multi-sector entities** (State, Federal, Local, Academic, Health and Social, and private industry). The board provides ongoing evaluation, coordination, and capacity building within the project.[101] Secure Colorado objectives are also supported through the 2016 cybersecurity bill. The Cybersecurity Council is responsible for aligning the multiple objectives.



Colorado Information Security Advisory Board Pecent of Multi-Sector Representation

Prevention

Cyber Hygiene, Immunization, Education & Workforce Training

Secure Colorado conducts regular risk assessments and ranks each agency using a combination of risk Index evaluations, agency report cards, level of compliance, and systems hardening milestones to measure progress. The goal is decreasing each agency's risk index. Over the last two years, **the initiative has measured a very significant 48% risk reduction**. Colorado requires all state employees undergo cybersecurity awareness training and recently increased from annual to quarterly training, 95% of employees have completed the online training according to monthly reporting. This year, a new cyber hygiene community outreach program instructed its first 900 students in 6th-8th grades with internet safety presentations, the program is expected to grow. [102]

Colorado has recently embarked on a multi-sector, federal, and volunteer effort to begin the **National Cybersecurity Center (NCC)** that will coordinate response, training, education, and research for cybersecurity efforts in the state and nationally. The **NCC** is

[101] Ibid. Secure Colorado Colorado's Strategy for Information Security and Risk Management Fiscal Years 2017-2019. 2017. Pg 15.
[102] Ibid. Secure Colorado. 2017. Pg 11.

harnessing a combination of state, federal, and independent resources.[103] Colorado's goals for the program include designing, building, and operating tools, programs, and self-healing systems. Colorado is home to a robust cyber defense infrastructure and houses nine DHS/NSA certified Cyber Defense Centers of Excellence including: Colorado School of Mines, Colorado State University-Pueblo, Colorado Technical University, Pueblo Community College, Red Rocks Community College, Regis University, United States Air Force Academy, University of Colorado- Colorado Springs, and University of Denver.[104]

Active Monitoring

Early Detection, Real-time Info Sharing & Threat Monitoring, Federal Collaboration

Colorado reports that 98% of the state's systems are actively monitored using security tools in near-real time. All twenty Center for Internet Security (CIS) security controls are utilized.[105] Only a few years prior, before developing the Secure Colorado plan, the cybersecurity budget for the entire state was just $6,000. The first draft of Secure Colorado was simply working to implement the basic best practice of applying the first five critical CIS controls in 2014.[106] As mentioned, Colorado has dramatically reduced their risk index over these 3 years to *below* "low risk." It has been reported Colorado's risk score is below 11.[107] This is more secure than some banks with a score of 20 being a reasonable industry standard for financial institutions.[108,109,110]

Colorado is currently developing more robust identity management systems including two-way authentication methods as part of an effort to harden their network against

[103] Robinson, Helen. "NCC Seeks Volunteers, Donations." The Colorado Springs Business Journal, July 07, 2017. Accessed November 25, 2017. http://www.csbj.com/2017/07/07/ncc-seeks-volunteers-donations/. See also: https://www.nationalcybersecuritycenter.org/ncc-partners/

[104] U.S. National Security Agency and the Department of Homeland Security. *Current National CAE Designated Institutions.*https://www.iad.gov/nietp/reports/current_cae_designated_institutions.cfm

[105] Colorado. Office of Information Technology. *FY 2018 OIT Performance Plan.* July 2017. Pg 20-21. https://drive.google.com/file/d/0B_ZUv6gW8QZMTDlDNGxEMVBNblU/view.

[106] Colorado. Governor's Office of Information Technology. *FY15 Annual Report Transforming Colorado Government for Today and the Future. Pg 11.* 2016. Accessed November 25, 2017. https://drive.google.com/file/d/0B_ZUv6gW8QZMVlVGN0xzeXNJckk/view.

[107] Colorado. Office of Information Technology. *FY 2018 OIT Performance Plan.* July 2017. Pg 20-21. https://drive.google.com/file/d/0B_ZUv6gW8QZMTDlDNGxEMVBNblU/view.

[108] Ibid. *Secure Colorado. 2017. Pg 3,4, 11*

[109] Shueh, Jason. "For Funding, Colorado Cybersecurity Chief Says Strategy First." *StateScoop*, March 13, 2017. http://statescoop.com/for-funding-colorado-cybersecurity-chief-says-strategy-first.

[110] Colorado. Office of Information Technology. *FY16 Annual Report.* Accessed November 25, 2017. https://drive.google.com/open?id=0B_ZUv6gW8QZMcl9PcFVJb2ZtQzg.

unauthorized access and endpoint vulnerabilities. The state is an active participant in National Association of State Chief Information Officers (NASCIO) Privacy and Security Committee, MS-ISAC, and the SANS institute.

Response and recovery

Coordinated Incident Response, Outbreak Containment, Cyber Laws

The CoCIO reports that the average time it takes teams to respond to a cyber incident–from threat detection to containment and restoration of services–is less than 4 hours total.[111] Colorado strengthens incident response plans and multi-sector coordination by leading and participating in simulated cyber hazard and incident drills. These drills focus on investigation, containment, and response to cyber threats across Colorado's systems. The cyberwar games are conducted in partnership with the National Guard, academic, state, federal and local partners.[112] According to the National Cybersecurity Center's Interim director, the NCC Colorado Springs project will include a Rapid Response Center geared toward providing services to the 50,000 small-to-medium sized businesses[113] and individuals[114] in Colorado. This is in alignment with Secure Colorado's current biennium security goals that state Colorado aims to create and maintain a state-wide incident response and forensics team that can identify and isolate threats, recover systems, and potentially prosecute those responsible.[115]

[111] Ibid. Secure Colorado. 2017. Pg 11

[112] Ibid. Secure Colorado. 2017. Pg 3-4.

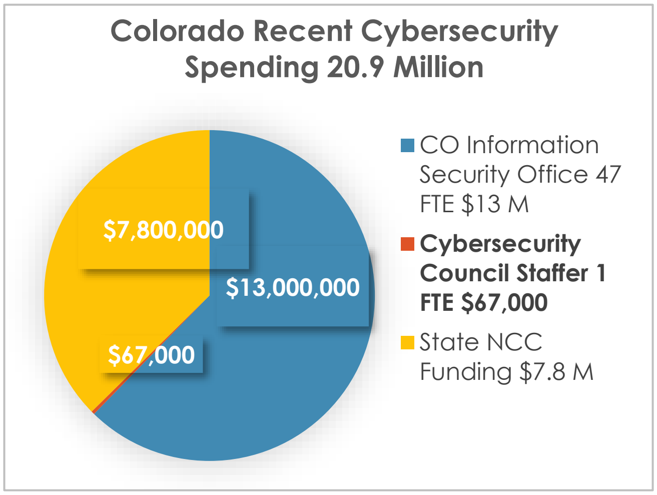
[113] Baillie, Amber. "National Cyber Center Takes Shape." The Colorado Springs Business Journal, October 31, 2016. Accessed November 25, 2017. https://www.csbj.com/2016/10/31/national-cyber-center-takes-shape/?v=402f03a963ba.

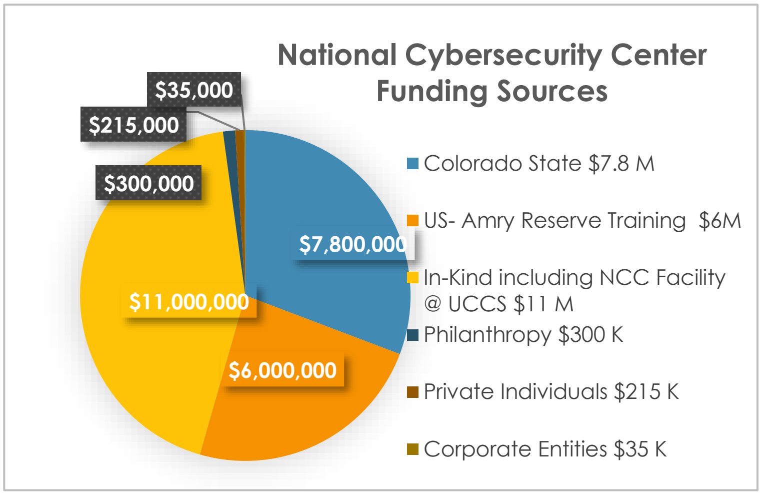
[114] Walker, Chris. "Colorado's National Cybersecurity Center Plans to Serve and Protect." Westword. September 25, 2017. Accessed November 25, 2017. http://www.westword.com/news/national-cybersecurity-center-in-colorado-springs-filled-a-growing-need-for-tech-protection-9269280.

[115] Ibid. Secure Colorado. 2017. Pg 9

Costs

Recent Cybersecurity Spending:[116]





[116] Colorado. Office of Information Technology. *FY 2018 OIT Performance Plan.* July 2017. https://drive.google.com/file/d/0B_ZUv6gW8QZMTDlDNGxEMVBNblU/view.

STATE ANALYSIS: FLORIDA

Leadership

Competent Authority & Resources, Central Hub, Strategic Planning

The **Florida Center for Cybersecurity (FC^2)** acts as the state clearinghouse of cybersecurity resources for business and industry, government, defense, and higher education. The **FC^2** was created by the state in 2014. **FC^2** is a coordinated effort of the twelve Florida State Universities housed under the authority of the University of South Florida. The program is a very substantial investment aimed at using cybersecurity as an economic engine.[117]

The **Agency of State Technology (AST)** is home to Florida's Chief Information Security Officer (CISO). This office was created the same year as the **FC^2** after being essentially abolished, leaving Florida without a state Chief Information Officer or CISO for two years. In 2014, **AST** funding was restored and the office was immediately tasked with creating a comprehensive IT security strategy. The **Statewide Strategic Information Technology Security Plan 2017** focuses on three strategies with 2-3 objectives each. The plan includes coordination with the **FC^2**. Now in the plan's third year, the office has achieved many objectives, some significant milestones are discussed below.[118]

The strategic IT plan–delivered in just 3 months–has seen success and was nominated for the 2016 NASCIO awards.[119] Despite disruptive events and gaps in leadership, Florida recently received the award for "largest state improvement" from the NASCIO.[120]

Multi-Sector Capacity Building

Multi-sector capacity building is mainly executed through the **FC^2's** research and development and workforce training coordination departments, and by serving as a

[117] State University System of Florida. Board of Governors. *Making Florida the Cyber State A Board of Governors Report Submitted to the Florida Legislature and Governor* .December 2013. http://www.usf.edu/pdfs/final-cybersecurity-report.pdf
See also: Florida Center for Cybersecurity FC^2 Homepage http://thefc2.org/about-us/index.aspx

[118] Florida. Agency for State Technology. Chief Information Security Office. *Statewide Strategic Information Technology Security Plan 2015-2018 (2017 Update).*February 2017. https://static1.squarespace.com/static/58bd820d86e6c0c5a7193736/t/590a41d2579fb34e49c6e0f0/1493844434713/2015-2018+IT+Security+Plan+2017.pdf.

[119] National Association of State Chief Information Officers. *Florida's Information Technology Security Plan.* 2016. https://www.nascio.org/portals/0/awards/nominations2016/2016/2016FL9-NASCIO%202016%20FL%20Cybersecurity%20AST%20Security%20FINAL.pdf.

[120] Florida. Agency for State Technology. Chief Information Security Office. *Statewide Strategic Information Technology Security Plan 2015-2018 (2017 Update).* February 2017. Pg 9. https://static1.squarespace.com/static/58bd820d86e6c0c5a7193736/t/590a41d2579fb34e49c6e0f0/1493844434713/2015-2018+IT+Security+Plan+2017.pdf.

cybersecurity resource for business and industry, government, defense, and higher education. The **FC^2's Collaborative Seed Award Program and Capacity Building Initiative** take a market-based approach to creating new cybersecurity technology and lab development, curriculum, and community outreach programs. Some funding comes from industry partners.[121]

A massive restructuring of the **Agency of State Technology (AST)** was passed by both houses the Florida legislature and vetoed by the governor in 2017. The bill would have severely gutted AST authority, centralized strategic planning, and created the Florida Cybersecurity Task Force made up of public and private representatives.[122] The AST has a tumultuous history since being completely defunded in 2005 reportedly over accountability, procurement, and spending issues, then again for two years in 2012.[123]

Prevention

Cyber Hygiene, Immunization, Education & Workforce Training

The State's goals for **FC^2** focus on aggressively investing in cybersecurity education, research, and workforce development. This is an effort to use cybersecurity expertise and commerce as a powerful economic driver for the state by attracting high paying cybersecurity jobs in financial, healthcare, utility, transportation, and defense to Florida. Recent investments in higher education totaling over $30 million in the first two years of the **FC^2**.[124] Florida has completed the first year of the *New Skills for a New Fight* initiative to provide free cybersecurity training to veterans.[125] The first year of the **FC^2** community outreach program exceeded the goal of 1,000 participants, reaching 1,642 Floridians through conferences and events.[126]

The IT strategic plan helped secured funding for cybersecurity training for 32 agencies' security personnel. The AST, as part of the IT strategic plan, created the **Cybrary**

[121] Florida. Center for Cybersecurity. 2017 Capacity Building Program. 2017. http://thefc2.org/documents/capacity_building_program_rfp.pdf.

[122] Florida. The Florida State Senate. House Bill 5301: State Agency Information Technology Reorganization. 2017. https://www.flsenate.gov/Session/Bill/2017/5301/ByVersion.

[123] Hanson, Wayne. "Update: Florida State Technology Office Loses Funding." Government Technology: State & Local Government News Articles. June 30, 2005. http://www.govtech.com/e-government/Update-Florida-State-Technology-Office-Loses.html.

[124] Florida State Senate. "Laws of Florida Ch.2013-40 (Senate Bill 1500-2013)." *Laws of Florida Ch.2013-40 (Senate Bill 1500-2013)*, 2013. laws.flrules.org/2013/40.

[125] Florida, University of South. "Education For Veterans." Florida Center for Cybersecurity. Accessed November 30, 2017. http://thefc2.org/education/forveterans.aspx.

[126] State University System of Florida. Board of Governors. *Strategic Progress Update July 2014 – April 2015*. April 30, 2015. http://www.system.usf.edu/board-of-trustees/health-sciences-and-research/research-docs/fc2-ubot-preso-4-30-2015.pdf.

resource center for state agency guidance complying with the new Florida Cybersecurity policy.

The Florida Department of Law Enforcement's Cybercrime Office runs a public outreach site **SecureFlorida.org** that provides basic cybersecurity information for small business, parents, kids, and the general public. The site also houses a community outreach resource **CSAFE (Cybersecurity Awareness for Everyone). CSAFE** representatives will come to your organization and give free presentations on cybersecurity over many topics ranging from online safety for children, parents, schools, small business human firewall employee training, and basic incident response planning.[127]

Active Monitoring

Early Detection, Real-time Info Sharing & Threat Monitoring, Federal Collaboration

The CISO is responsible for coordinating with law enforcement, the MS-ISAC, and others. The CISO is in the initial stages of coordinating with the **FC^2** to develop an Information Sharing and Analysis Organization (ISAO) within the state. The state recently purchased and installed a security information and event management (SIEM) platform and is working to improve their cyber incident reporting and information sharing processes.[128] Through **SecureFlorida.org** businesses can sign up for a cyber threat alert system (BusinessSafe) run by the state's law enforcement and DHS fusion center.[129]

The state has an extensive national defense network, eight of the twelve State Universities involved in **FC^2** are DHS/NSA National Centers for Academic Excellence certified institutions actively engaged in cyber security and cyber defense R&D.[130]

[127] Florida Department of Law Enforcement's Cybercrime Office. *Secure Florida.* Accessed November 30, 2017. http://www.securefla.org/, http://www.secureflorida.org/c_safe.

[128] Florida. Agency for State Technology. Chief Information Security Office. *Statewide Strategic Information Technology Security Plan 2015-2018 (2017 Update).*February 2017. Pg 4. https://static1.squarespace.com/static/58bd820d86e6c0c5a7193736/t/590a41d2579fb34e49c6e0f0/1493844434713/2015-2018+IT+Security+Plan+2017.pdf.

[129] Florida Department of Law Enforcement's Cybercrime Office. Secure Florida. Accessed November 30, 2017. http://businessafe.imarcsgroup.com/member/signup/

[130] U.S. National Security Agency and the Department of Homeland Security. National Centers of Academic Excellence. https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm.

Response and recovery

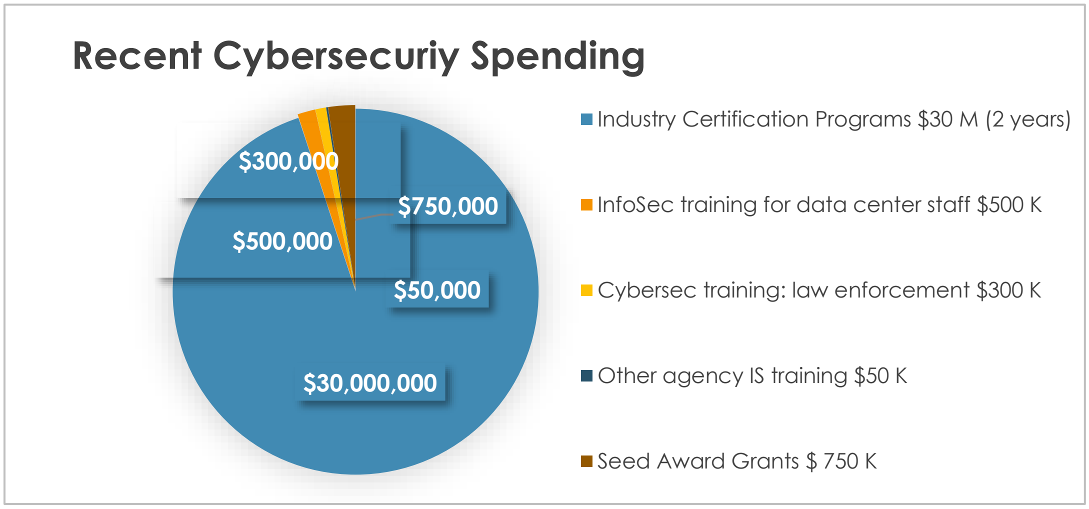
Coordinated Incident Response, Outbreak Containment, Cyber Laws

Currently, the **Florida Department of Law Enforcement's Computer Crime Center** is the principle cyber incident response authority. They operate a mobile cybercrime response team. The Strategic IT plan is in the drafting stages of the Cyber Disruption Plan, and is pursuing the goal of creating an enterprise incident response team.[131]

Florida has a data breach law, mandatory employee cybersecurity training programs, and mandatory risk assessments.[132] Florida has a spectrum of 14 cybercrime laws including criminal use of personally identifiable information, cyberstalking, credit card crimes, and communications fraud.[133]

Costs

Recent Cybersecurity Spending:



[131] Florida. Agency for State Technology. Chief Information Security Office. *Statewide Strategic Information Technology Security Plan 2015-2018 (2017 Update).* February 2017. https://static1.squarespace.com/static/58bd820d86e6c0c5a7193736/t/590a41d2579fb34e49c6e0f0/1493844434713/2015-2018+IT+Security+Plan+2017.pdf.

132 https://www.flsenate.gov/Laws/Statutes/2012/Chapter282/All ??? Florida. Florida State Senate. Chapter 282 - 2012 Florida Statutes. 2012. Accessed November 30, 2017. https://www.flsenate.gov/Laws/Statutes/2012/Chapter282/All.

[133] "Computer Laws." Secure Florida. Accessed November 30, 2017. http://secureflorida.org/legal/computer_laws/.

STATE ANALYSIS: ILLINOIS

Leadership

Competent Authority & Resources, Central Hub, Strategic Planning

The Illinois **Department of Innovation and Technology** was created by an executive order in 2016. The order consolidated 29 state agency IT security personnel and responsibilities under the Chief Information Officer and CISO at the **Department of Innovation and Technology (DoIT).** This effectively centralized 1,600 personnel and $258 million worth of personnel IT operating budget under a single agency and leadership.[134] Together, the **DoIT**, **CIO**, and **CISO** represent the central authority for cybersecurity matters in the state.[135] The first year of this consolidation, the **DoIT** was appropriated $900 million and began the initial infrastructure investment and retiring of old or redundant systems and replacing them with enterprise system components and applications. For FY 2018 $300 Million has been appropriated.[136]

The very first **Illinois Cybersecurity Strategy (ICS)** was published by the **DoIT** in spring of 2017. The cybersecurity strategy is designed to address existing vulnerabilities, increase cybersecurity training, social engineering awareness, build enterprise capacity, protect critical infrastructure, and align future actions including education and workforce development.[137] Included in the strategy is the goal of expanding Illinois' cybersecurity capacity to execute their "Smarter State" initiative that is harnessing cybersecurity, digital government and the Internet of Things (IoT) to streamline state and city services.[138]

Multi-Sector Capacity Building

To create the IT security plan, the **DoIT** collaborated with the National Governors Association (NGA), NASCIO, NIST and the Illinois Executive Committee for Cybersecurity.

[134] Illinois. Department of Innovation and Technology. Chief Information Officer. *Information Technology Transformation Update-Appendix D Budget by Agency Source.* December 31, 2016. https://www2.illinois.gov/sites/doit/Strategy/Transformation/Documents/DoIT_2016-Report-GA.pdf.

[135] Illinois. Office of the Governor. *Executive Order Consolidating Multiple Information Technology Functions Into a Single Department of Innovation and Technology.* January 25, 2016. https://www2.illinois.gov/Pages/government/execorders/2016_1.aspx.

[136] Illinois. Office of Budget and Management. *FY17 Final Appropriations and FY18 Enacted Appropriations.* August 8, 2017. https://www.illinois.gov/gov/budget/Documents/Budget Book/FY 2017 Budget Book/FY16 FY17 Enacted Approps Line Item Detail.xls.

[137] Illinois. Department of Innovation and Technology. *State of Illinois Cybersecurity Strategy 2017-2019.* Spring 2017. https://www2.illinois.gov/sites/doit/Strategy/Cybersecurity/Documents/CyberSecurity-Strategy-2017-2019.pdf.

[138] State of Illinois Sponsored White Paper. *Smarter and Future-Ready Illinois Continues to Execute on Its Digital Transformation Strategy: Update.* By Ruthbea Yesner Clarke. August 2017. https://www2.illinois.gov/sites/doit/Strategy/Documents/IDCWhitePaper-SmarterAndFuture-ReadyIllinois.pdf.

The plan includes forging relationships in academia and pursing public sector partnerships.

> *"Crucial strategic guidance was provided by the State of Illinois Executive Committee for Cybersecurity, which has helped ensure that cybersecurity is recognized not just as a business issue, but a matter of public safety concern…."*

Prevention

Cyber Hygiene, Immunization, Education & Workforce Training

Illinois now requires cybersecurity awareness training for all state employees.[139] The first 50,000 state employees were trained in 2016. The **DoIT** estimates this will save the state over $4.5 million on future cyberattack costs. The first state-wide agency assessment recommendations based on the NIST cybersecurity framework were completed in 2016, saving a reported $1 million on incident containment costs. The state also encrypted, secured, or destroyed over 5 billion records in order to secure personally identifiable information and consolidate over 200 file cabinets worth of paper records.[140] Illinois is home to eight colleges and universities certified as NSA/DHS Cyber Defense Designated Institutions. Illinois has partnered with the academic and private sector to design curricula in analytics, cybersecurity, and IoT. Partners include: GE, Rockwell Automation, Cisco, University of Illinois, MIT Sloan School of Management, Pearson

> *The Smarter State partnership between the DoIT and the University of Illinois will continue to leverage the skills of, and build skills for, the next-generation workforce.*[141]

[139] Illinois. Illinois General Assembly. *Mandatory Cybersecurity Training for State Employees-Full Text of Public Act 100-0040.* August 8, 2017. http://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=100-0040.

[140] Illinois. Department of Innovation and Technology. Chief Information Officer. *Information Technology Transformation Update.* December 31, 2016. Pg 4. https://www2.illinois.gov/sites/doit/Strategy/Transformation/Documents/DoIT_2016-Report-GA.pdf.

[141] State of Illinois Sponsored White Paper. *Smarter and Future-Ready Illinois Continues to Execute on Its Digital Transformation Strategy: Update.* By Ruthbea Yesner Clarke. August 2017. Pg 5-8 https://www2.illinois.gov/sites/doit/Strategy/Documents/IDCWhitePaper-SmarterAndFuture-ReadyIllinois.pdf.

Active Monitoring

Early Detection, Real-time Info Sharing & Threat Monitoring, Federal Collaboration

Illinois is moving toward formal cybersecurity governance, continuing to assess and enforce compliance with the recently implemented security requirements guided by the NIST cybersecurity framework. Technology infrastructure consolidation will result in wider use of more secure enterprise systems**.** The cyber security strategy includes establishing a Security Operations Center (SOC) and working to improve threat detection capabilities and incident reporting policies and procedures.

Response and recovery

Coordinated Incident Response, Outbreak Containment, Cyber Laws

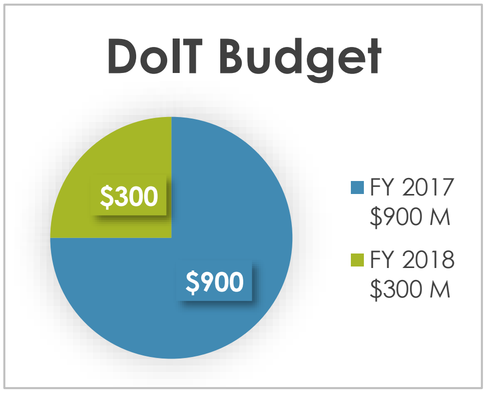
The DoIT cyber security strategy aims to further develop threat intelligence sharing capabilities and develop a Statewide Cyber Disruption Strategy alongside the Illinois Emergency Management Agency and the National Guard.142 Illinois updated its Personal Information Protection Act in 2016 to expand the definition of personally identifiable information and the requirements for notification of individuals.143

Costs

RECENT CYBERSECURITY SPENDING- Department of Innovation and Technology

The **DoIT** technology transformation was appropriated $900 million dollars the first year of the program FY 2017, $300 million was approved for FY 2018. The yearly required legislative report on the project is due December 31, 2017.[119,121]

NASCIO Recognized Illinois for outstanding achievement in the field of information technology for "The State of Illinois Data Center Server Consolidation and Virtualization Project."



[142] Illinois. Department of Innovation and Technology. *State of Illinois Cybersecurity Strategy 2017-2019*. Spring 2017. https://www2.illinois.gov/sites/doit/Strategy/Cybersecurity/Documents/CyberSecurity-Strategy-2017-2019.pdf.

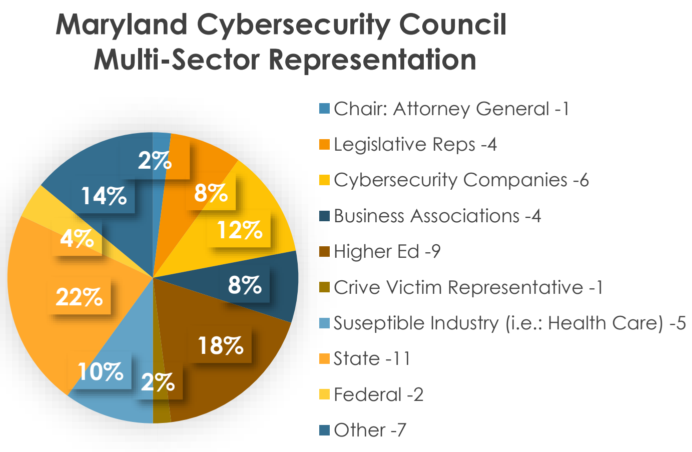
[143] Illinois. State Legislature. *Public Act 099-0503- HB 1260 Enrolled- Personal Information Protection Act- Update 2017*. http://www.ilga.gov/legislation/publicacts/99/PDF/099-0503.pdf.

STATE ANALYSIS: MARYLAND

Leadership

Competent Authority & Resources, Central Hub, Strategic Planning

Maryland has long led the states as a cybersecurity trailblazer on the national stage.[144] Maryland is home to an expansive defense infrastructure, the NSA, the first National Center for Cybersecurity Excellence, the Defense Information System Agency, and U.S. Cyber Command. However, recently Maryland has discovered room for improvement among state and local government cybersecurity policies and systems. In January of 2017, Maryland authorized the **Secretary of Information Technology** and CISO to create a **Director of Cybersecurity** position within the **Department of Information Technology (DoIT). The DoIT** will enact and enforce the **2017 Cybersecurity Program Policy (CPP).** The **CPP consists of 28 separate state cybersecurity policies** and replaces the State of Maryland Information Security Policy that previously served as the guiding cybersecurity document. Unlike the Information Security Policy, the **CPP** is specific to cybersecurity (not IT in general) and includes the delegation of authority to the **DoIT** to enact and enforce the requirements of the legislation. The previous plan was less comprehensive and less enforceable. [145,146] The **DoIT** is also undertaking a multi-year process to consolidate disparate state agency systems into a single enterprise system and central cybersecurity hub. The **DoIT** grew from 134 FTEs in 2016 to 252 by mid 2017, most are transferred from a home agency into the **DoIT**. A budget report on the initiatives of the cybersecurity projects is due early in 2018.[147]


Maryland Cybersecurity Council Multi-Sector Representation

[144] Spidalieri, Francesca. "State of the States on Cybersecurity." *Pell Center for International Relations and Public Policy*, November 2015, 9. http://pellcenter.org/eight-states-lead-the-rest-in-cybersecurity/.

[145] Maryland. Department of Information Technology. *Maryland Cybersecurity Program Policy. Pg 3,14* January 31, 2017. http://doit.maryland.gov/cybersecurity/Documents/cybersecurity-program-policy-v1.0%20(Updated%20with%20Sigs).pdf.

[146] Spidalieri, Francesca. "State of the States on Cybersecurity." *Pell Center for International Relations and Public Policy*, November 2015, 9. Pg. 15. http://pellcenter.org/eight-states-lead-the-rest-in-cybersecurity/.

[147] Maryland. Department of Information Technology. *Analysis of the FY 2018 Maryland Executive Budget, 2017.* 2017. Pg 8-10. http://mgaleg.maryland.gov/pubs/budgetfiscal/2018fy-budget-docs-operating-f50-department-of-information-technology.pdf.

Multi-Sector Capacity Building

The **Maryland Cybersecurity Council** (**MDCSC**) **is a truly multi-sector advisory entity**. The Council is chaired by the state's Attorney General and is comprised of **50 members**. The members form six subcommittees that guide the state's cybersecurity over 6 specific areas:

- Law, Policy and Legislation
- Cyber Operations and Incident Response
- Critical Infrastructure and Framework
- Education and Workforce Development
- Economic Development
- Public Awareness and Community Outreach

The council is staffed by the University of Maryland University College. Members are appointed by the Attorney General, President of the Senate, and Speaker of the House. The Council provides cybersecurity recommendations and reports to the General Assembly on the implementation progress of those recommendations. The council is also tasked with coordinating with the **DoIT, Maryland Military Department, and Maryland Emergency Management Agency** to create the **State of Maryland Cyber Disruption Plan** finalized in 2017**.**[148]

> *"The council's composition reflects a 'whole of community' approach to addressing cybersecurity issues"- MDCSC*

Prevention

Cyber Hygiene, Immunization, Education & Workforce Training

Maryland is home to the first NIST National Center for Cybersecurity Excellence and seventeen NSA/DHS certified Centers of Academic Excellence in Cyber Defense Education. However, Maryland does not have a centralized state community cyber outreach or cyber hygiene and prevention program. The **MDCSC** is currently curating a Cyber Resources and Best Practices Portal for critical infrastructure owner and operators.[149] The **DoIT** maintains a web page with links to basic cybersecurity resources

[148] Maryland. Maryland Cybersecurity Council. *Maryland Cybersecurity Council Activities Report.* July 1, 2017. Pg 3-4 http://www.umuc.edu/documents/upload/maryland-cybersecurity-council-biennial-report-2015-2017.pdf.
[149] Maryland. Maryland Cybersecurity Council. *Maryland Cybersecurity Council Activities Report.* July 1, 2017. Pg 13 http://www.umuc.edu/documents/upload/maryland-cybersecurity-council-biennial-report-2015-2017.pdf.

like StaySafeOnline.org, the MS-ISAC, and the US-CERT. The Maryland Department of Commerce partners with **CyberMaryland** and the **Cybersecurity Association of Maryland, Inc.** Both programs are run as public-private partnerships that focus on providing networking, partnership, and showcase opportunities for Maryland's business and industry, students, cybersecurity tech companies and professionals via conferences, contests, and events. The DoIT is currently devising a new-hire and yearly cyber security training for Maryland State Employees and Contractors.[150] The state reports that 90% of employees are participating in existing cybersecurity training.[151]

Active Monitoring

Early Detection, Real-time Info Sharing & Threat Monitoring, Federal Collaboration

The **DoIT** runs a 24/7 **Security Operations Center (SOC)** for enterprise systems and other state government clients. The Continuous Monitoring policy explicitly details the SOC responsibilities to detect, identify, and respond to cyber threats. The **SOC** uses the NIST Cybersecurity Framework, real-time (continuous) event and traffic monitoring, incident response, and training and awareness. The SOC, at current capacity must expand to pursue this mission, a Director of Security Operations and SOC manager will be appointed. A multi-function System Information and Event Management (SIEM) tool will be purchased. The SOC will operate on updated Incident Response Plan[152] and Security Assessment Policies.[153] These are among some of the 28 Cybersecurity Program Policies to be followed and enforced as part of the 2017 **CPP**.[154] Eighteen Agencies have undergone vulnerability assessments, penetration testing, or security audits. Three agencies participate in multi-agency security drills. The **MDCSC** has strongly recommended participation in regional Information Sharing and Analysis Centers, as

[150] Maryland. Department of Information Technology. *Maryland Auditing and Compliance Policy.* June 30, 2017. http://doit.maryland.gov/cybersecurity/Documents/Auditing-and-Compliance-v1.1.pdf.

[151] Maryland. Department of Commerce. *Analysis of the FY 2018 Maryland Executive Budget, 2017.* 2017. Pg. 3. http://mgaleg.maryland.gov/pubs/budgetfiscal/2018fy-budget-docs-operating-t00-department-of-commerce.pdf.

[152] Maryland. Department of Information Technology. *Maryland Cybersecurity Incident Response Policy.* January 31, 2017.http://doit.maryland.gov/cybersecurity/Documents/Maryland%20DOIT%20Incident%20Response%20Policy%20v1.0.pdf.

[153] Maryland. Department of Information Technology. *Security Assessment Policy.* January 31, 2017. http://doit.maryland.gov/cybersecurity/Documents/Maryland%20DOIT%20Security%20Assessment%20Policy%20v1.0.pdf.

[154] Maryland. Department of Information Technology. *Maryland Continuous Monitoring Policy.* January 31, 2017. http://doit.maryland.gov/cybersecurity/Documents/Maryland%20DOIT%20Continuous%20Monitoring%20Policy%20v1.0.pdf.

well as collaboration with a federal entity like the New Jersey NCCICC**,** or Arizona's InfraGaurd program that collaborates with multiple states and the FBI.[155]

Response and recovery

Coordinated Incident Response, Outbreak Containment, Cyber Laws

As noted, the **SOC** is responsible for incident response. Maryland has a Cyber Disruption Contingency Plan that was approved by the governor in April, 2017. The plan is considered "sensitive" and not available for public consumption.[156] A separate "Cybersecurity Plan" has been tasked to the Department of Homeland Security and will be created with input from the **DoIT** and **MDSCS,** the final document in due in 2018.[157] Maryland improved their Personal Information Protection Act to include the information stored by state agencies, a wider definition of illegal access, and a more succinctly defined notification requirement of 45 days to individual victims of compromised information. The definition of data and personal information was expanded to include biometric data, mental health and health insurance policy information. The **MDCSC** is currently investigating a Cybersecurity First Responders Reserve in coordination with the Maryland National Guard and Maryland defense force.[158]

[155] Maryland. Maryland Cybersecurity Council. *Maryland Cybersecurity Council Activities Report.* July 1, 2017. Pg 22 http://www.umuc.edu/documents/upload/maryland-cybersecurity-council-biennial-report-2015-2017.pdf.

[156] Maryland. Maryland Cybersecurity Council. *Maryland Cybersecurity Council Activities Report.* July 1, 2017. Pg 52 http://www.umuc.edu/documents/upload/maryland-cybersecurity-council-biennial-report-2015-2017.pdf.

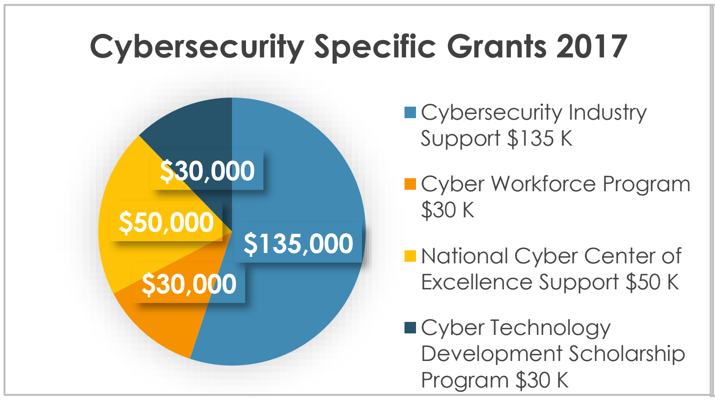
[157] Maryland, Executive Department. "Executive Order 01.01.2017.22 Maryland Cybersecurity." *Executive Order 01.01.2017.22 Maryland Cybersecurity*, 5 Oct. 2017. s3.documentcloud.org/documents/4067727/Hogan-Cyber-Order.pdf.

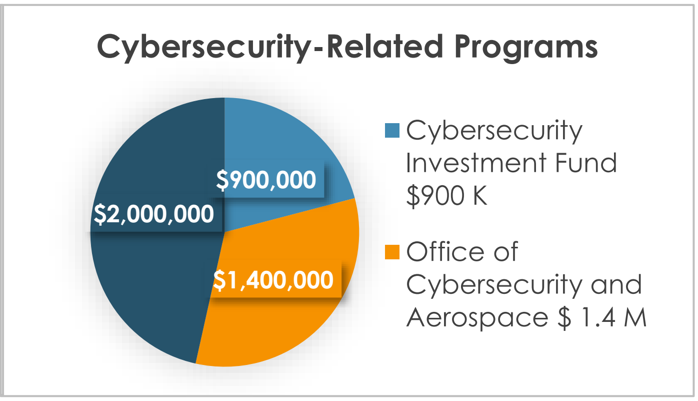
[158] Maryland. Maryland Cybersecurity Council. *Maryland Cybersecurity Council Activities Report.* July 1, 2017. Pg 10-12. http://www.umuc.edu/documents/upload/maryland-cybersecurity-council-biennial-report-2015-2017.pdf.

Costs

RECENT CYBERSECURITY SPENDING [159,160]

> *A comprehensive cybersecurity program is a direct contributor to the State's ability to meet its public safety and public service missions" –MDCSC*


Cybersecurity Specific Grants 2017


Cybersecurity-Related Programs

[159] Maryland. Department of Commerce. *Analysis of the FY 2018 Maryland Executive Budget, 2017.* 2017. http://mgaleg.maryland.gov/pubs/budgetfiscal/2018fy-budget-docs-operating-t00-department-of-commerce.pdf.

[160] Maryland. Office of the Governor. *Senate Bill 190- Budget Bill (Fiscal Year 2017.* 2017. Pg 157-160. http://mgaleg.maryland.gov/2016RS/chapters_noln/Ch_143_sb0190E.pdf.

STATE ANALYSIS: MICHIGAN

Leadership

Competent Authority & Resources, Central Hub, Strategic Planning

Michigan has an established cybersecurity culture. The state has pursued a cybersecurity strategic plan utilizing security controls, coordinating with MS-ISAC, academia, health care, and defense efforts since 2009.[161] The Department of Management and Budget and the Department of Information Technology, were fused in 2010 in order to increase government efficiency and centralize state data systems to create the **Department of Technology, Budget, and Management** (**DTBM).** The **DTBM,** whose department director is also the **Chief Information Officer,** are responsible for two strategic plans. Both plans are multi-agency, multi-sector collaborations. The **Michigan Cyber Initiative**[162] and the State of Michigan **Cyber Disruption and Response Plan** are the centerpieces of cybersecurity authority delegation and strategic planning in Michigan. The **Michigan Cyber Initiative** is a public-facing plan that integrates and leverages cybersecurity among business, academic, and civilian communities. The Michigan **Cyber Disruption and Response Plan**[163] is an effort undertaken by the **DTMB**, state CIO, Michigan State Police, and the National Guard to coordinate more effectively in response to cyber disruptions.

> *"The plan provides a framework that enables state emergency management and information technology to work seamlessly with public and private partners to rapidly respond to and minimize the impact of cyber disruption events in Michigan." - Michigan Cyber Disruption and Response Plan.*

> *"Businesses and citizens have the individual and collective responsibility to ensure the protection of their information technology systems." – Michigan Cyber Initiative*

[161] Michigan. Department of Information Technology. *Cyber Security Plan.* 2009. https://www.michigan.gov/documents/itstrategicplan/I_Cyber_Security_Web_234559_7.pdf.

[162] Michigan. Office of the Governor. *Michigan Cyber Initiative.* 2015. http://www.michigan.gov/documents/cybersecurity/Mich_Cyber_Initiative_11.13_2PM_web_474127_7.pdf.

[163] Michigan. Department of Technology, Management, and Budget. *State of Michigan Cyber Disruption Response Plan.* October 2015. https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf.

Multi-Sector Capacity Building

Multi-sector collaboration has become integrated practice in Michigan, it is built-in to both strategic plans. A culture of coordinated cybersecurity awareness and almost a decade of strategic planning places Michigan among the nation's most cyber prepared states. The **Michigan Economic Development Corporation (MEDC)** and the **Merit Network, Inc**. are also key facets of the multi-sector cybersecurity capacity in Michigan. The MEDC actively promotes Michigan as an ideal location for cybersecurity professionals and business.[164] The **MEDC** has the authority to leverage the Michigan Strategic Fund to promote economic growth and create jobs through a variety of means.[165,166] **Merit Network, Inc.** is a non-profit corporation co-owned by the 12 four-year universities in Michigan. The **Merit Network**, operational since 1966, manages the longest-running research and education network connecting the 12 research universities. This network is one of the pre-cursors to the modern internet that started with a National Science Foundation grant of $400,000 long ago.[167] **Merit** is also home to the **Michigan Cyber Range**, **Michigan Cyber Civilian Corps** (**MiC3**), and the **K-12 Michigan Statewide Educational Network (MISEN).**[168]

> *"A truly cyber-resilient ecosystem takes a holistic view of the environment and ensures it is working by strengthening existing partnerships and bringing all components of the ecosystem together to create a full Cyber Threat Alert Network." – Michigan Cyber Initiative*

Prevention

Cyber Hygiene, Immunization, Education & Workforce Training

Michigan runs an award winning public cybersecurity resource website (Michigan.gov/cybersecurity), holds cybersecurity conferences every two years, provides cybersecurity training for all state employees, and offers cyber toolkits for K-12 schools, individuals, and small businesses. The state employee cyber awareness training costs

[164] "Michigan Economic Development Corporation." Cybersecurity -Why Michigan - Michigan Business | MEDC. Accessed December 2017. https://www.michiganbusiness.org/why-michigan/cybersecurity-industry/.

[165] "Michigan Economic Development Corporation." About- MEDC Michigan Strategic Fund. Accessed December 2017. https://www.michiganbusiness.org/michigan-strategic-fund-msf/.

[166] Michigan. Office of the Governor. *Michigan Cyber Initiative.* 2015. Pg, 14-15 http://www.michigan.gov/documents/cybersecurity/Mich_Cyber_Initiative_11.13_2PM_web_474127_7.pdf.

[167] Merit Networks, Inc. *Merit History- Connecting Organizations, Building Communities.* Accessed December 2017. https://www.merit.edu/about-us/merits-history/.

[168] "Merit, Networks." Michigan Statewide Educational Network. Accessed December 16, 2017. https://www.merit.edu/misen/.

less than $200,000 and includes 18 lessons over a three-year period for every state employee. 50,000 employees have received the training. **At approximately 30 cents per lesson, the return on investment is estimated by the state to be more than 100 to 1.**

The state organizes town hall meetings with local school districts to more fully integrate cybersecurity programs into elementary and high schools state-wide. The state runs a traveling cybersecurity Breakfast Series and Cyber Awareness Luncheon Series in order to bring the Michigan Cyber Initiative and coordinated cybersecurity message to the entire state.[169] The Michigan Cyber Safety Initiative and OK2SAY programs are part of the state's K-12 education outreach curriculum that focus on online safety and awareness. Both programs are free to schools, nearly 2 million students through the K-12 system in Michigan have completed the curriculum.[170]

The Michigan Cyber Initiative focuses on education and public awareness aligned with the NIST's **National Initiative for Cybersecurity Education (NICE).** Courses and training are provided through the **Merit Network's** Michigan **Cyber Range**. The **Cyber Range** is a virtual training facility accessible from multiple universities on the network used for cybersecurity instruction, tabletop exercises, and coordinated threat drills. They also provide a variety of services including vulnerability testing, network security, high school cybersecurity competitions,[171] and other cybersecurity and technology programs.[172] The **Cyber Range** partners include a wide range of public, private, and defense entities. "Over $2 million was raised to establish the Cyber Range, with less than 20% coming from government sources."[173]

[169] Michigan. Office of the Governor. *Michigan Cyber Initiative.* 2015. Pg 8-10 http://www.michigan.gov/documents/cybersecurity/Mich_Cyber_Initiative_11.13_2PM_web_474127_7.pdf.

[170] Michigan. Office of the Attorney General. *2016 OK2SAY Annual Report.* 2016. https://www.michigan.gov/documents/ok2say/2016_OK2SAY_Annual_Report_Final__web_reduced_571284_7.pdf.

[171] Aderoju, Darlene. "Michigan Aims to Spur Economy through Student Cyber Competition."*State Scoop*, August 12, 2016. http://statescoop.com/michigan-aims-to-spur-economy-through-student-cyber-competition.

[172] Merit Network, Inc. Cybersecurity Services. Accessed December 15, 2017. https://www.merit.edu/services/cybersecurity-services/

[173] NASCIO 2013 Award Nominees. *Cyber Training 3.0: New Solutions Addressing Escalating Security Risks.* 2013. pg 7. http://www.michigan.gov/documents/dtmb/Cyber_Training_New_Solutions_Addressing_Escalating_Security_Risks_461703_7.pdf.

Active Monitoring

Early Detection, Real-time Info Sharing & Threat Monitoring, Federal Collaboration

The **Michigan Information Sharing and Analysis Center (MI-ISAC)** was established in 2006 and actively coordinates cyber threat intelligence sharing among all state and local governments and critical infrastructure. The **Michigan Intelligence Operations Center** (**MIOC**) is the 24/7 central fusion center for state, federal, and local law enforcement agencies and is run by the State Police. During a cyber event the **MIOC** coordinates with the **Michigan Cyber Command Center (MC3)** and the Chief Security Officer. **MIOC** also assists in ongoing investigations with the FBI and DHS.

Response and recovery

Coordinated Incident Response, Outbreak Containment, Cyber Laws

Michigan Cyber Command Center (MC3) coordinates emergency response, containment, forensic analysis and prosecution of cybersecurity events as the central command and control center during a cyber disruption. **MC3** is a group of military service personnel and civilian analysts, they have the authority to deploy cyber first responders.[174]

The **Michigan Cyber Civilian Corps** (**MiC3**) is a group of thoroughly vetted civilian volunteers. **MiC3** was authorized to deploy first responder teams in the event of a governor declared state of emergency situation. During the first three years, the MiC3 was never used, and in October of 2017 their mission was expanded to include selected deployment for cyberattacks, data breaches, and assistance to local government, non-profits, and businesses.[175]

All of the agencies mentioned in these two sections work together as the **Michigan Cyber Disruption Response Team** exercising the *Homeland Security Exercise and*

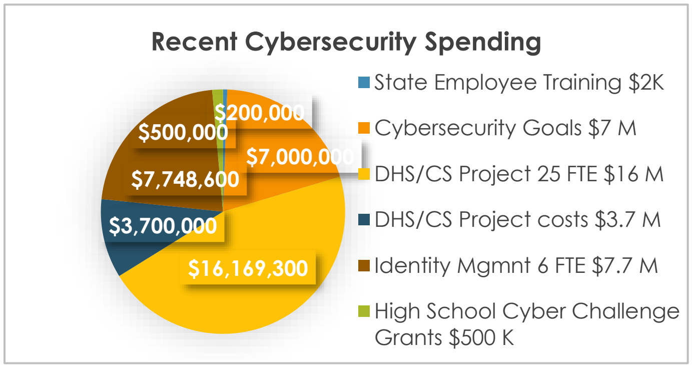
[174] Michigan. Department of Technology, Management, and Budget. *State of Michigan Cyber Disruption Response Plan.* October 2015. Pg.4,27-28 https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf.

[175] Michigan. Senate Fiscal Agency. *Cyber Civilian Corps Program- Bill Summary.* September 18, 2017. http://www.legislature.mi.gov/documents/2017-2018/billanalysis/Senate/pdf/2017-SFA-4508-F.pdf.

Evaluation Program framework that coordinates seminars, workshops, tabletop exercise, security drills, and full-scale multi-agency emergency simulations.[176]

Costs

RECENT CYBERSECURITY SPENDING [177,178,179,180]



[176] Michigan. Department of Technology, Management, and Budget. *State of Michigan Cyber Disruption Response Plan.* October 2015. Pg. 11-12 https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf.

[177] Michigan. Executive Budget Office. *State of Michigan FY 2018-2019 Executive Budget.* 2017. http://www.michigan.gov/documents/budget/FY18_Exec_Budget_550967_7.pdf.

[178] NASCIO 2013 Award Nominees. *Cyber Training 3.0: New Solutions Addressing Escalating Security Risks.* 2013. pg 7. http://www.michigan.gov/documents/dtmb/Cyber_Training_New_Solutions_Addressing_Escalating_Security_Risks_461703_7.pdf.

[179] Michigan State Legislature. 99th Legislature Regular Session Of 2017. *Public Acts of 2017 Approved by the Governor- Enrolled House Bill No. 4323.* July 14, 2017. Pg. 69, 71, 93, 98-99, 251. http://www.legislature.mi.gov/documents/2017-2018/publicact/pdf/2017-PA-0107.pdf.

[180] Michigan. 99th Legislature Regular Session Of 2017. *Public Acts of 2017 Approved by the Governor - Enrolled House Bill No. 4313.* July 14, 2017. Accessed December 15, 2017. Pg. 63-64. http://www.legislature.mi.gov/documents/2017-2018/publicact/pdf/2017-PA-0108.pdf.

STATE ANALYSIS: NEW JERSEY

Leadership

Competent Authority & Resources, Central Hub, Strategic Planning

New Jersey operates three primary cybersecurity entities. The New Jersey Office of Information Technology **(NJOIT)** creates the IT strategic plan (last published in 2014).[181] The office also provides policies and programs for cybersecurity framework, incident response protocols, and cybersecurity goals for state enterprise systems.[182] **NJOIT** houses the **Chief Technology Officer (CTO)** David Weinstein, the senior technology authority in the state. The NJOIT coordinates with the **New Jersey Office of Homeland Security and Preparedness (NJOHSP). NJOHSP** is home to the **Director of Cybersecurity**/**State Chief Information Security Officer (CISO**), Michael Geraghty. The **Director of Cybersecurity/CISO** is also the Director of the **New Jersey Cybersecurity Communications and Integration Cell (NJCCIC).**

Multi-Sector Capacity Building

Davis Weinstein, the state's **CTO** has been advocating for a more centralized approach to cybersecurity management. While New Jersey has many innovative and effective programs, there exist disparate systems, policies, aging legacy enterprise systems, and weak enforcement mechanisms that would benefit from a more unified cybersecurity culture. The **NJCCIC** is seen as a step in this direction. The state first started utilizing and consolidated enterprise systems back in the 80's and many of these systems are now outdated. The **CTO** created the **Chief Data Officer** position to begin working on the human element of connecting the 60,000 users and 70 departments' strategic IT goals that are heavily focused on security and risk management.[183]

Over the last two years, there have been cybersecurity bills introduced in New Jersey that would increase public-facing cybersecurity capability, awareness, and multi-sector capacity building efforts by creating the **NJ Cybersecurity Commission** at a cost of $50,000 per year. The commission would aim to capitalize on economic opportunities of cybersecurity workforce and education development, while strengthening a culture of

[181] New Jersey. Office of Information Technology. *IT Strategic Plan 2014-2016.* Accessed December 16, 2017. http://www.nj.gov/it/about/docs/OIT_2014_Strategic_Plan.pdf.

[182] New Jersey. Office of Information Technology. *IT Policies and Standards - Information Security Program.* 2017. http://www.state.nj.us/it/services/governance.shtml#policies.

[183] McCauley, Ryan. "Unified Cybersecurity Unit Is Necessary to Protect New Jersey Agencies from Threats." Government Technology: State & Local Government News Articles. May 24, 2017. http://www.govtech.com/security/Unified-Cybersecurity-Unit-Is-Necessary-to-Protect-New-Jersey-Agencies-From-Threats.html.

cyber hygiene within the state. Multi-sector membership would be mandated. The 13 members would include representatives from public, private, and academic sectors including finance, public safety, education, OIT, NJ Economic Development Authority, state police, and homeland security.[184]

Prevention

Cyber Hygiene, Immunization, Education & Workforce Training

The **NJCCIC** provides cybersecurity training and briefings online and in person. Topics include Sector-Specific Cybersecurity Risk and Best Practices, Ransomware Prevention Training Program, Intro to the Dark Web, History of Nation-State Hacking, and the Current State of Cybercrime.[185]

As part of Cybersecurity Awareness month, the **NJCCIC** started providing weekly webinars that focus on the themes including, cybersecurity culture at work, connected communities: staying protected while always connected, the Internet of Things (IoT) security, and cyber professional development. The state launched a two-factor authentication promotional campaign, #2FA4NJ, that included a live twitter chat on international #2FactorTuesday. The **NJCCIC** also provides weekly bulletins, cyber alerts, updated threat profiles and threat analysis, cyber blog, and resource catalogs for citizens and small businesses. The program includes webinars, cybersecurity training briefings, vulnerability assessment tools, exploit kit profiles, and more.[186]

If passed, **SB 808** would create and task the **NJ Cybersecurity Commission** to present recommendations for STEM education programs for all ages, elementary through university, in order to: *"improve the cybersecurity workforce pipeline…offer strategies to advance private sector cybersecurity economic development opportunities, including innovative technologies, research and development, start-up firms, and maximize public-private partnerships throughout the State…[and] offer suggestions for promoting awareness of cyber hygiene among the State's citizens, businesses, and government entities…"*[187]

[184] New Jersey. State of New Jersey 217th Legislature 2016 Session. *Senate Bill 808- An Act Creating the New Jersey Cybersecurity Commission.* 2016. ftp://www.njleg.state.nj.us/20162017/S1000/808_I1.HTM.

[185] "Training and Briefings." NJCCIC. Accessed December 17, 2017. https://www.cyber.nj.gov/cybersecurity-training/briefings/.

[186] "Resources- Citizens." NJCCIC. Accessed December 17, 2017. https://www.cyber.nj.gov/citizens/.

[187] New Jersey. State of New Jersey 217th Legislature 2016 Session. *Senate Bill 808- An Act Creating the New Jersey Cybersecurity Commission.* 2016. ftp://www.njleg.state.nj.us/20162017/S1000/808_I1.HTM.

Active MONITORING

Early Detection, Real-time Info Sharing & Threat Monitoring, Federal Collaboration

The NJCCIC is the state's Information Sharing and Analysis Organization created in response to Presidential Executive Order 13691.188 The NJCCIC is less than 2 years old and explains itself as "a one-stop-shop agency for cybersecurity information sharing, threat analysis and incident reporting."189 NJCCIC is located in the Regional Operations Intelligence Center that also houses the state's fusion and emergency operations centers that coordinate with national resources like the MS-ISAC, DHS, and the National Guard.

> *"The goal is to promote shared and real-time awareness of cyber threat for New Jersey's citizens, local governments, businesses, and critical infrastructure owners and operators. The NJCCIC bridges the information divide between local, state, federal, public, and private sector institutions to reduce New Jersey's cyber risk and respond to emergent incidents." - NJCCIC*

Response and recovery

Coordinated Incident Response, Outbreak Containment, Cyber Laws

Cyber incidents can be reported through the OIT, NJCCIC Cyber Liaison Offices, or the State Police Computer Crimes Unit (CCU). All data breaches are required to be reported to the state police before being disclosed to the customer. The CCU is equipped to respond to a number to cybercrimes. For cybersecurity specific events, large scale emergencies, and disasters, the National Guard Cyber Crimes Protection Team may be deployed. This is a joint venture between the New Jersey and New York National Guard.[190]

[188] Spidalieri, Francesca. "State of the States on Cybersecurity." *Pell Center for International Relations and Public Policy*, November 2015, 21. http://pellcenter.org/eight-states-lead-the-rest-in-cybersecurity/.

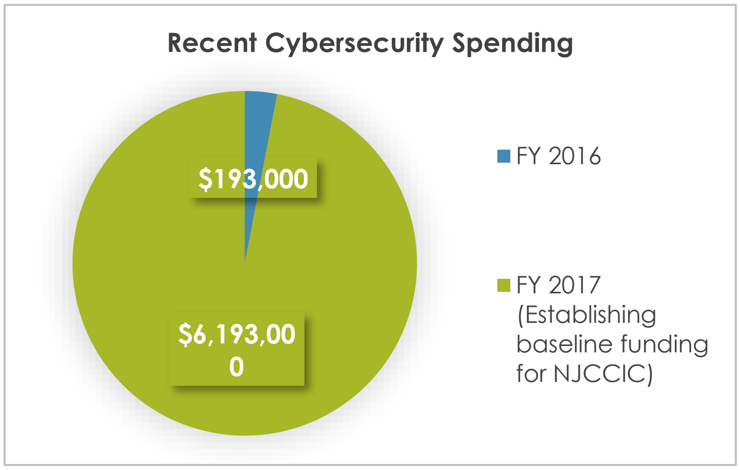
[189] New Jersey. NJCCIC. *Mission.* Accessed December 16, 2017. https://www.cyber.nj.gov/mission/.

[190] "Cyber Protection Team | NJ Army National Guard." NJ.gov. Accessed December 17, 2017. http://www.nj.gov/military/army/cyber-protection-team/.

Costs

RECENT CYBERSECURITY SPENDING

"The fiscal 2017 budget recommends a $6 million decrease for OIT...The fiscal year 2017 budget for the Office of Homeland Security and Preparedness (OHSP) totals $9.9 million, an increase of $6.0 million over the fiscal 2016 adjusted appropriation of $3.9 million. This increase is due to the consolidation of the State's investments in cybersecurity from the Office of Information Technology to the OHSP"[191]



[191] New Jersey. Office of the State Treasurer. *Citizens' Guide to the Annual Budget.* 2017. http://www.nj.gov/treasury/omb/publications/17citizensguide/citguide.pdf.

STATE ANALYSIS: NEW YORK

Leadership

Competent Authority & Resources, Central Hub, Strategic Planning

New York operates the **Enterprise Information Security Office (EISO)** within the Office of Information Technology Services **(NYITS)**. The **NYITS** is headed by the state **CIO. The EISO** and **CIO** are responsible for creating, revising, and enforcing the Information Technology Security Policy[192] and all other IT policies.[193] These policies are regularly updated (all in 2017) and exercised. The **EISO** works with all levels of government and the private sector to coordinate information security compliance and management, cyber incident response, monitoring and intelligence sharing, vulnerability and threat management, penetration testing, security policy and standards development, security awareness and training. Capacity for each of these areas varies.[194,195] The New York Department of Financial Services has recently launched a secure portal for mandatory reporting of cybersecurity incidents as part of a larger comprehensive cybersecurity bill that effects all financial institutions in the state.[196]

Multi-Sector Capacity Building

In 2013, the governor created the **Cybersecurity Advisory Board (CSAB)** a public-private entity to work with both state leadership and the NYITS. At its inception, the **CSAB, CIO, CISO** and **Chief Risk Officer**[197] created a pilot program to investigate how 5 state agencies were managing assets, risk, security policies, and awareness. As a result of that investigation, all state agencies are required to conduct risk assessments and cybersecurity awareness training.[198] Since its creation the **CSAB** has provided guidance

[192] New York. Office of Information Technology Services. *ITS Security Policies.* Accessed December 23, 2017. https://its.ny.gov/eiso/policies/security.

[193] New York. Office of Information Technology Services. *ITS Policies.* Accessed December 23, 2017. https://its.ny.gov/tables/technologypolicyindex.

[194] New York. Enterprise Information Security Office. *Welcome to the NYS Enterprise Information Security Office!* July 03, 2015. Accessed December 23, 2017. https://its.ny.gov/welcome-nys-enterprise-information-security-office.

[195] Spidalieri, Francesca. "State of the States on Cybersecurity." *Pell Center for International Relations and Public Policy*, November 2015, 24-26 http://pellcenter.org/eight-states-lead-the-rest-in-cybersecurity/.

[196] New York. Department of Financial Services. *DFS Cybersecurity Regulation.* August 2017. http://www.dfs.ny.gov/about/press/pr1708281.htm.

[197] Center for the Advancement of Public Integrity/Trustees of Columbia University. *New York State's Innovative New Program for Risk Management Bringing Leading Private Sector Practices to Government.* September 2016. https://www.law.columbia.edu/sites/default/files/microsites/public-integrity/326052761-nys-risk-management-program-capi-issue-brief-september-2016_0.pdf.

[198] Spidalieri, Francesca. "State of the States on Cybersecurity." *Pell Center for International Relations and Public Policy*, November 2015, 25. http://pellcenter.org/eight-states-lead-the-rest-in-cybersecurity/.

on other issues including, voting infrastructure security,[199] critical infrastructure, information sharing,[200] and financial services.[201] The **CSAB** is currently part of the governor's office. In both the 2017 and 2016 NY legislative sessions, a comprehensive cybersecurity initiative bill was introduced creating a **CSAB** permanently within the Division of Homeland Security and Emergency Services, a New York State **Cyber Security Partnership Program** for owners and operators of critical infrastructure, private sector business, academia, and private citizens, and a **New York State Cyber Security Sharing and Threat Prevention Program**. The bill is currently in committee.[202,203]

> *"…to enhance the security, protection and resilience of New York state's critical infrastructure, and private sector business interests, as well as the protection of the finances and individual liberties of every citizen, the state of new York must promote a cyber environment that encourages efficiency, innovation, and economic prosperity, and that can operate with safety, security, business confidentiality, privacy, and civil liberty."*- ***NY Assembly Bill A3448***

Prevention

Cyber Hygiene, Immunization, Education & Workforce Training

The ESIO provides some public-facing Cybersecurity awareness toolkits and resources for small business, private citizens, children, and local government.[204,205] The state, in partnership with academia and the private sector just held it's 20th annual Cybersecurity

[199] New York. Office of the Governor. Governor Cuomo Directs Cyber Security Advisory Board to Review Cyber Security of Voting Infrastructure Amidst Reports of Foreign Interference in 2016 Election. June 21, 2017. https://www.governor.ny.gov/news/governor-cuomo-directs-cyber-security-advisory-board-review-cyber-security-voting.

[200] New York. Office of the Governor. Governor Cuomo Announces Cyber Security Advisory Board. September 28, 2014. https://www.governor.ny.gov/news/governor-cuomo-announces-cyber-security-advisory-board.

[201] New York. Office of the Governor. Governor Cuomo Announces New Cyber Security Assessments for Banks. September 28, 2014. Accessed December 23, 2017. https://www.governor.ny.gov/news/governor-cuomo-announces-new-cyber-security-assessments-banks.

[202] New York. NY State Senate. NY State Assembly Bill A3448. November 08, 2017. https://www.nysenate.gov/legislation/bills/2017/A3448.

[203] New York. NY State Senate. Senate Bill S924- Cybersecurity Advisory Board. November 08, 2017. Accessed December 23, 2017. https://www.nysenate.gov/legislation/bills/2017/s924/amendment/original.

[204] "Awareness/Training/Events." New York State Office of Information Technology Services. November 27, 2017. Accessed December 23, 2017. https://its.ny.gov/awarenesstrainingevents.

[205] "Local Government." New York State Office of Information Technology Services. February 11, 2016. Accessed December 23, 2017. https://its.ny.gov/local-government.

Conference.[206] New York state agency employees must complete cybersecurity awareness training within 30 days of hire. Each agency must have an Information Security Officer. Annual risk assessments and an incident response plan are also requirements.[207] New York is the first state to create a **Chief Risk Officer** and state-wide risk management system. While not cybersecurity specific, the role does include cybersecurity as a main facet. In 2010, the state launched the MS-ISAC as part of the Center for Internet Security in coordination with DHS, and US-CERT.

Active Monitoring

Early Detection, Real-time Info Sharing & Threat Monitoring, Federal Collaboration

As mentioned, legislation was introduced in 2017 to create a state specific cyber intelligence sharing entity. All state and third-party systems must be scanned for vulnerabilities before installation and regularly thereafter. Penetration testing is required periodically. Security controls such as anti-virus, software integrity checkers, and web filtering are required for state systems where possible. Systems that are too old (not patchable or no longer supported) must be replaced. Intrusion detection monitoring systems are deployed strategically and must be configured to alert incident response teams.[208] The EISO provides cyber advisories about vulnerabilities and critical patches.

Response and recovery

Coordinated Incident Response, Outbreak Containment, Cyber Laws

The NY Office of Homeland Security and Emergency response is in the process of forming a new Cyber Incident Response Team that will focus on proactive protection of non-executive agencies, local governments, and public authorities.[209,210] Cyber incidents

[206] "NYS Celebrates 20th Annual Cyber Security Conference." New York State Office of Information Technology Services. June 08, 2017. Accessed December 23, 2017. https://its.ny.gov/press-release/nys-celebrates-20th-annual-cyber-security-conference.

[207] New York. Enterprise Information Security Office. *Information Security Policy.* Accessed December 17, 2017. https://its.ny.gov/sites/default/files/documents/nys-p03-002_information_security_0.pdf.

[208] New York. Office of Information Technology and Technology Services. *Information Security Policy.* 2017. https://its.ny.gov/sites/default/files/documents/nys-p03-002_information_security_0.pdf.

[209] New York. Division of the Budget. *Homeland Security and Emergency Services-Budget Highlights.* 2017. https://www.budget.ny.gov/pubs/executive/eBudget1718/agencyPresentations/appropData/HomelandSecurityandEmergencyServicesDivisionof.html.

[210] New York. Division of the Budget. *FY 2018 Executive Budget Briefing Book.* 2017. https://www.budget.ny.gov/pubs/executive/eBudget1718/fy1718littlebook/PublicSafety.pdf.

must be reported to the Cyber Command Center (housed in EISO). The **Cyber Command Center** responds to incidents in coordination with agency IR teams, first responders, and external entities such as MS-ISAC, FBI, NYS Intelligence Center, NYS Police, ISPs, and security solutions vendors. The standard operating procedures for incident response are the responsibility of the Cyber Command Center and must be tested via processes like tabletop exercises or cyber threat drills annually at minimum.[211] For cybersecurity specific events, large scale emergencies, and disasters the National Guard Cyber Crimes Protection Team may be deployed. This is a joint venture between the New Jersey and New York National Guard.[212]

Costs

Recent Cybersecurity Spending

In 2017 **$4.8 Million** was appropriated for cyber security, emergency preparedness, and emergency response training[213]

In the 2014-2015 budget cycle New York State spent **$15 million** in capital resources to fund initial planning and development costs for a new **College of Emergency Preparedness, Homeland Security and Cybersecurity.[214]**

[211] New York. Office of Information Technology Services. *Cyber Incident Response.* 2017. https://its.ny.gov/sites/default/files/documents/nys-s13-005_cyber_incident_response_0.pdf.

[212] "Cyber Protection Team | NJ Army National Guard." NJ.gov. Accessed December 17, 2017. http://www.nj.gov/military/army/cyber-protection-team/.

[213] New York. Division of the Budget. *FY 2018 Executive Budget | Agency Appropriations | Homeland Security and Emergency Services, Division of.* Accessed December 26, 2017. https://www.budget.ny.gov/pubs/executive/eBudget1718/agencyPresentations/appropData/HomelandSecurityandEmergencyServicesDivisionof.html.

[214] New York. Division of the Budget. *Additional Highlights from the 2014-15 State Budget Agreement.* Accessed December 26, 2017. https://www.budget.ny.gov/pubs/press/2014/pressRelease14_enactedBudHighlights2.html.

STATE ANALYSIS: TEXAS

Leadership

Competent Authority & Resources, Central Hub, Strategic Planning

The Texas **Department of Information Resources (DIR)** is large. It includes the Executive Director/Chief Information Officer, Chief Technology Officer, Statewide Data Coordinator, Chief Information Security Office, and Information Technology Services. The **DIR** also houses five other offices including Chief Operations Office, Chief Procurement Office, General Counsel, Public Affairs, and Chief Financial Office.[215] The **DIR** (as of 2015) was home to 196 full-time employees, and appropriations of $295,243,785.[216]

> *"The DIR not only provides various security services to state agencies and higher education institutions (which allows it to be a completely self-funded agency), but it also educates agencies about security threats and prevention strategies, negotiates favorable contracts for security services and tools, and has developed a standardized, statewide Cybersecurity Framework."* [217]

Strategic Planning and Reporting is accomplished through the State Strategic Plan, Department of Information Resources Agency Strategic Plan (ASP) and Technology Resources Planning, Information Resources Deployment Review, Corrective Action Plan, legislative planning, and biennial performance reports.[218]

Multi-Sector Capacity Building

The **Texas Cybersecurity, Education and Economic Development Council (TCEEDC)** was created to (1) Investigate and recommend strategies to improve cybersecurity infrastructure and partnerships between business, government, and higher education (2) Specific actions to accelerate the industry of cybersecurity within the state.

[215] Texas. Department of Information Resources. *Organization Chart.* Accessed December 22, 2017. http://dir.texas.gov/View-About-DIR/Pages/Content.aspx?id=16.

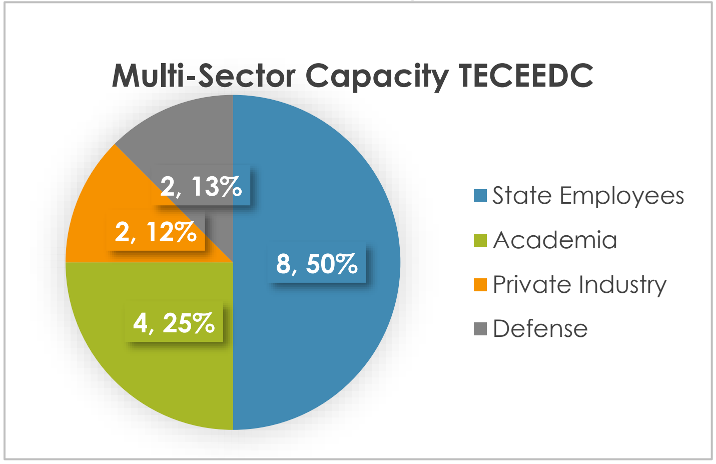
[216] Texas. Department of Information Technology. Salary Supplement Reporting. Accessed December 22, 2017. http://dir.texas.gov/View-About-DIR/Pages/Content.aspx?id=18.

[217] Spidalieri, Francesca. "State of the States on Cybersecurity." *Pell Center for International Relations and Public Policy*, November 2015. Pg 29. http://pellcenter.org/eight-states-lead-the-rest-in-cybersecurity/.

[218] Texas. Department of Information Resources. *Strategic Planning & Reporting.* Accessed December 22, 2017. http://dir.texas.gov/View-Resources/Pages/Content.aspx?id=20

The council has 16 members, and a "broad and open participation group defined as Council Partners." The Texas Legislature created the TCEEDC in 2011, and renewed it to operate through 2015.[219]

The **initial TCEEDC report** identified **10 key recommendations** including an overall statewide, community-centered approach to cybersecurity. The recommendations made by the council are appropriate for many states and include many recommendations similar to what other councils throughout the country have found.



> *"Texas must establish a statewide focus for its cyber environment. This focus would include Texas business and public leaders in collaborative efforts to identify and mitigate risks and threats to Texas citizens and to spur innovation in the cyber environment"*

13. Establishing a **Texas Coordinator of Cybersecurity** within the Office of the Governor
    Provides: strategic direction for forming public/private partnerships to secure state's infrastructures and promote the cybersecurity industry within the state.
14. Establishing **the Business Executives for Texas Security (BETS) partnership** to bring public and private sector leaders and cybersecurity practitioners together to form a framework for knowledge sharing and collaboration, making non-proprietary and industry-recognized best practices and solutions readily available for the collective improvement of cybersecurity across the state.
15. Establishing a "Cyber Star" program to foster improvement of cyber resiliency in both private and public infrastructures across the state and to **increase public trust by establishing a baseline for responsible cyber operations.**

[219] Texas. Texas Cybersecurity, Education, And Economic Development Council. Accessed December 22, 2017. http://dir.texas.gov/View-About-DIR/Pages/Content.aspx?id=23

16. Adopting the **Community Cyber Security Maturity Model (http://cias.utsa.edu/the-ccsmm.html)** as a statewide guide for developing a viable and sustainable cybersecurity program and fostering a culture of cybersecurity throughout the state.
17. Increasing the number of **cybersecurity practitioners** in Texas
18. Providing a consistent voice for industry regarding **cybersecurity policies** in order to facilitate communication between the state and industry.
19. Continuing **investment in higher education cybersecurity programs** in order to: attract students, spur research and development, and encourage institutions of higher education to become leaders in cybersecurity within their own communities.
20. Promoting **collaboration, innovation, and entrepreneurship** in cybersecurity to facilitate the commercialization of university research and development and encourage the development of new businesses with innovative products and services in cybersecurity.
21. Developing a comprehensive cybersecurity education pipeline through the BETS partnership to **introduce cybersecurity initiatives from K–PhD.**
22. Reviewing and sharpening the leadership role of the Texas Department of Information Resources (DIR) in establishing a **sustainable Cybersecurity Awareness Program for all Texans.**

> *"What the Council found missing is the framework necessary to collaboratively tie these cybersecurity strengths together. Texas is not alone in this regard. States throughout the nation are struggling to identify successful strategies for addressing cybersecurity concerns" - TCEEDC initial report*[220]

The Cyber Security Council is a cybersecurity specific version of the TCEEDC [221] The CyberTexas Foundation is a public-private partnership that emphasizes workforce

[220] Texas. Texas Cybersecurity, Education, And Economic Development Council. *Building a More Secure and Prosperous Texas.* December 2012. Pg 1-2, 27 http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Building%20a%20More%20Secure%20and%20Prosperous%20Texas.pdf.

[221] Texas. Department of Information Resources. *Texas Cybersecurity Council - Building a More Secure and Prosperous Texas.* December 15, 2016. http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Texas%20Cybersecurity%20Council%20Charter%202.0.pdf.

development, economic development, and preparedness including community awareness.[222]

*Note: Texas did not entirely meet our capacity building comparator according to the criteria presented in the public health framework simply because Texas does not go beyond the public-private and academic triad. However, Texas' cybersecurity collaboration efforts are robust and have received national recognition for many of their efforts.[223] The majority of publically available information is slightly outdated and may not reflect the current capacity.

Prevention

Cyber Hygiene, Immunization, Education & Workforce Training

As mentioned in the TCEEDC report, Texas is working toward a state-wide cyber awareness culture. To that end, the state is part of many forward-thinking initiatives. One of the most unique and immediately impactful programs is the **WeTeachCS program** (weteachcs.org). **WeTeachCS is an academic partnership run through the University of Texas that provides computer science certifications to K-12 teachers free of charge. Since 2015, the program has provided over 2,000 K-12 teachers in Texas with a certificate in computer science**.[224]

The Indiana-Texas Civic Hackathon Challenge is a hacking competition organized by the two states' IT departments. Participants are tasked with creating the best application using open data, code, and technology.[225] San Antonio received the FBI director's Community Leadership Award after becoming the 2nd city to certify a CyberPatriot Center of Excellence program emphasizing K-12 cybersecurity education and having the most CyberPatriot teams at the National Youth Cyber Defense Competition.[226, 227]

The Texas CISO Council is a volunteer body that helps to support stronger security practices throughout the state. They have recently provided a common public-facing

[222] "CyberTexas Foundation." CyberTexas Foundation. Accessed December 22, 2017. https://www.cybertexas.org/.
[223] "CyberTexas Foundation to Be Awarded FBI Director's 2015 Community Leadership Award." FBI. April 01, 2016. Accessed December 22, 2017. https://www.fbi.gov/contact-us/field-offices/sanantonio/news/press-releases/cybertexas-foundation-to-be-awarded-fbi-directors-2015-community-leadership-award.
[224] WeTeach_CS. Accessed December 22, 2017. https://www.weteachcs.org/.
[225] "Groundbreaking Indiana-Texas Civic Hackathon Challenge Declares Grand Champion." Indy Chamber. March 27, 2015. http://indychamber.com/news/indy-chamber-news/groundbreaking-indiana-texas-civic-hackathon-challenge-declares-grand-champion/.
[226] "CyberTexas Foundation to Be Awarded FBI Director's 2015 Community Leadership Award." FBI. April 01, 2016. Accessed December 22, 2017. https://www.fbi.gov/contact-us/field-offices/sanantonio/news/press-releases/cybertexas-foundation-to-be-awarded-fbi-directors-2015-community-leadership-award.
[227] United States. CyberPatriot. *AFA CyberPatriot Website*. Accessed December 22, 2017. http://www.uscyberpatriot.org/.

guide for institutions looking for basic guidance for how to create an information security program.[228]

Active monltoring

Early Detection, Real-time Info Sharing & Threat Monitoring, Federal Collaboration

The Texas DIR develops the security policies and strategic planning for the state and runs the **Network Security Operations Center**. DIR also runs the enterprise security program, provides vulnerability assessments, runs a 24/7 security alert system, and provides cybersecurity training, conferences, briefings, and forums to promote security awareness.[229]

The **Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management (SPECTRIM)** Incident Management Portal is a cybersecurity tool that centralizes risk assessment, emergency and non-emergency incident reporting management, incident response planning, and coordination with the **Network Security Operations Center**.[230]

Response and recovery

Coordinated Incident Response, Outbreak Containment, Cyber Laws

The DIR serves as the Internet Service Provider for 150 of Texas' state agencies. It operates a 24/7 incident response phone line, Security Operations Center, as well as the online SPECTRIM portal.[231]

The **Network Security Operations Center** was established in 2005 and provides, 24/7 network monitoring and mitigation, penetration testing, cyber threat recon, and also

[228] Texas. CISO Council. *Texasciso.* Accessed December 22, 2017. http://www.texascisocouncil.org/resources.

[229] Texas. Department of Information Resources. *DIR Agency Strategic Plan*. 2016. Pg. 4-5http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/DIR%20Agency%20Strategic%20Plan%202017-2021.pdf.

[230] Texas. Department of Information Resources. *The SPECTRIM Portal -Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management.* Accessed December 22, 2017. http://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=136.

[231] Texas. Department of Information Resources. *The SPECTRIM Portal -Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management.* Accessed December 22, 2017. http://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=136.

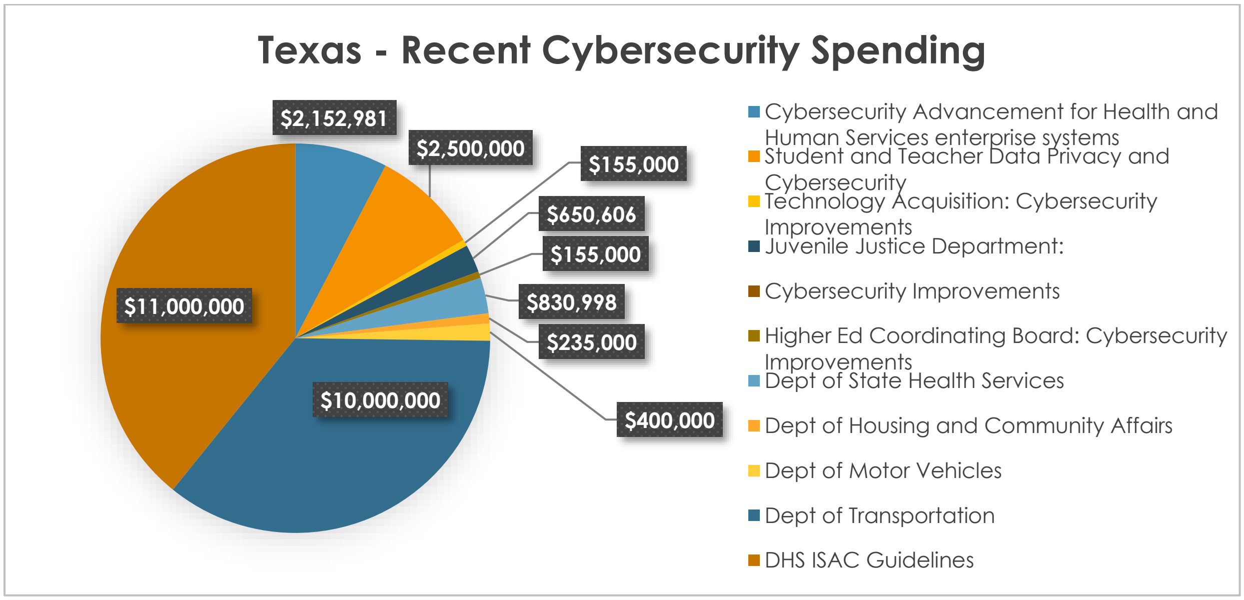
serves as the cyber intelligence sharing hub. They serve state agencies, higher education institutions and other public-sector customers.[232, 233]

Texas has a range of cyber legislation. They have criminalized cybercrime, require state agency security plans and reporting, bolstered personal information confidentiality, agency tech contracting, procurement, and monitoring of major information resources projects.[234]

Costs

RECENT CYBERSECURITY SPENDING[235]

Texas transparently track of where cybersecurity resources are allocated throughout the state, including over 22 million dollars in state funds from FY 2018-2019. Texas was recently awarded an 11-million-dollar contract from DHS to develop standards and guidelines for Information Sharing and Analysis Centers (ISACs) nation-wide.[236]



[232] Texas. Department of Information Resources. *2016 Threat Report Network Security Operations Center.* 2016. http://publishingext.dir.texas.gov/portal/internal/about-dir/information-security/ImageLibrary/2016%20NSOC%20Threat%20Report.pdf.

[233] Texas. Department of Information Resources. *DIR Basics Series-Cybersecurity.* 2016. http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/DIR Basics Series-Cybersecurity.pptx.

[234] Texas. Department of Information Resources. *Technology Legislation.* Accessed December 22, 2017. http://dir.texas.gov/View-Resources/Pages/Content.aspx?id=31.

[235] Texas. Eighty-fifth Legislature. *S.B. No. 1 General Appropriations Act.* 2017. http://www.legis.state.tx.us/tlodocs/85R/billtext/pdf/SB00001F.pdf#navpanes=0.

[236] Ibid., Spidalieri, Francesca. "State of the States on Cybersecurity."

TEXAS CYBERSECURITY APPROPRIATIONS	FY 2018	FY 2019
Health and Human Services: Cybersecurity Improvements	$2,152,981	$ 1,729,692
Student and Teacher Data Privacy and Cybersecurity	$ 2,500,000	$ 2,500,000
Technology Acquisition: Cybersecurity Improvements	$ 155,000	$ 70,000
Juvenile Justice Dept: Cybersecurity Improvements	$ 650,606	$ 65,000
Higher Ed Coordinating Board: Cybersecurity Improvements	$155,000	$70,000
Dept of State Health Services	$ 830,998	$ 830,998
Dept of Housing and Community Affairs	$ 235,000	$ 100,000
Dept of Motor Vehicles	$ 400,000	$ 0
Dept of Transportation	$10,000,000	Still Spending FY 2018 Funds
DHS ISAC guideline creation federal funding	$11,000,000 (FY2016)	

STATE ANALYSIS: VIRGINIA

Leadership

Competent Authority & Resources, Central Hub, Strategic Planning

The Commonwealth of Virginia's Chief Information Officer is the principal authority for cybersecurity as head of **the Virginia Information Technologies Agency (VITA)**. VITA provides cybersecurity, IT infrastructure services, IT governance, compliance and strategic planning.[237,238] The current Governor took Virginia's cybersecurity expertise to the national stage. The Governor partnered with the National Governor's Association (he was the chair of NGA at the time) to create the ***Meet the Threat*** website and initiative (https://ci.nga.org/cms/MeetTheThreat#) as a tool and resource library for states to utilize when strengthening their cybersecurity planning and culture. Virginia boasts one of the most integrated and collaborative cybersecurity industries in the country.[239]

Virginia embraces a community approach to cybersecurity integrating education to work pipeline, business, and government. Virginia is deeply rooted in the defense industry, housing over 650 cybersecurity companies, the National Science Foundation, National Cybersecurity & Communications Integration Center, and Army National Guard Readiness Center, Central Intelligence Agency, Department of Defense, and National Counterterrorism Center are among many national security organizations in the state. The state reports more than $44.6 billion in defense contracts, number one for DoD investment nation-wide.

> *"It is estimated, because of this new demand [for cloud services], that 70 percent of the world's internet traffic passes through Virginia largely due to the 60 data centers throughout the Commonwealth"* ***Virginia's Cyber Security Approach: Leadership through Diversity***

Multi-Sector Capacity Building

In 2015 the governor created the **Virginia Cybersecurity Commission (VCC)** and the **CyberVirginia** initiatives by executive order. **CyberViginia** is a public-facing cybersecurity resource for citizens, business, and government (http://cyberva.virginia.gov/). The **VCC** meets three times a year and submits an annual

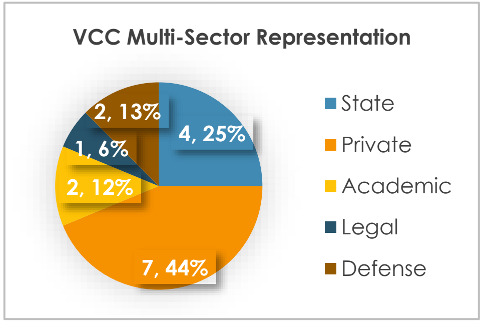
[237] Virginia. VITA. *About - VITA*. Accessed December 22, 2017. http://www.vita.virginia.gov/about/.

[238] Virginia. VITA. *IT Strategic Plan - 2017 Update - VITA*. Accessed December 22, 2017. https://www.vita.virginia.gov/it-governance/cov-strategic-plan-for-it/itsp---2017-update/.

[239] Spidalieri, Francesca. "State of the States on Cybersecurity." The Pell Center. February 01, 2015.Pg 32. Accessed September 05, 2017. http://pellcenter.org/eight-states-lead-the-rest-in-cybersecurity/.

report. The Commission's responsibilities include providing recommendations on the following 7 areas: [240]

1. Identify high risk cyber security issues facing VA
2. Securing Virginia's state networks, systems, and data, including interoperability, standardized plans and procedures, and evolving threats and best practices to prevent the unauthorized access, theft, alteration, and destruction of data
3. Provide suggestions for the addition of cyber security to Virginia's Emergency Management and Disaster Response capabilities, including testing cyber security incident response scenarios, recovery and restoration plans, and coordination with the federal government
4. Offer suggestions for promoting awareness of cyber hygiene among citizens, businesses and government
5. Present recommendations for cutting edge science, technology, engineering and math (STEM) educational and training programs for all ages, including K-12, community colleges, universities, in order to foster an improved cyber security workforce pipeline and create cyber security professionals with a wide range of expertise.
6. Offer strategies to advance private sector cyber security economic development opportunities, including innovative technologies, research and development, and start-up firms, and maximize public-private partnerships throughout the Commonwealth.
7. Provide suggestions for coordinating the review of and assessing opportunities for cyber security private sector growth as it relates to military facilities and defense activities in Virginia.



[240] Virginia. Office of the Governor. *Executive Order Number Thirty-Nine (2015) - Launching "Cyber Virginia" and The Virginia Cyber Security Commission.* 2015. https://governor.virginia.gov/media/3627/eo39-launching-cyber-virginia-and-the-virginia-cyber-security-commissionada.pdf.

> *"This collaborative and cooperative model of shared security and resilience has only been developed and adopted by a few leading states; Virginia among the first."*[241]

Prevention

Cyber Hygiene, Immunization, Education & Workforce Training

Virginia is home to thirteen NSA/DHS Centers of Academic Excellence in Information Assurance and Cyber Defense. The Virginia Cyber Range is a cloud-based cybersecurity exercise arena, lab area, and course repository. The program is led by a committee representing 11 NSA/DHS certified Centers of Academic Excellence. Students from Virginia high schools, colleges, and universities can access the Cyber Range through an internet connection and conventional web browser at no cost. This means each local school does not have to bear the financial burden of building the infrastructure or teaching resources required for cybersecurity education and training.[242]

The MACH37 Cyber Accelerator is a market-centric cybersecurity incubator run by the non-profit government corporation the Center for Innovative Technology. The accelerator focuses on research, seed funding, product development, and commercialization.[243]

In addition to the CyberVirginia public resource guide, VITA also provides awareness toolkits for citizens, executives, and agencies.[244] The Virginia Cybersecurity Partnership is a 220-member public-private partnership whose goals include providing opportunities for skills enhancement, outreach and pipeline development, collaboration in cyber-related activities.[245] The Virginia Economic Development Partnership actively markets Virginia's cybersecurity industry as a pro-business and asset rich environment in order to attract more cybersecurity industry.[246] Virginia offers incentives including a number of grants, loans, investments, and business development tax credits for job creation,

[241] Virginia. CyberVa. *Virginia's Cyber Security Approach: Leadership through Diversity. Pg 4* . https://cyberva.virginia.gov/media/9245/virginiacybersecurity_printfinal-4.pdf.

[242] Virginia. *Virginia Cyber Range.* Accessed December 22, 2017. https://virginiacyberrange.org/about.

[243] Virginia. Virginia.gov. *MACH37 Cyber Accelerator.* Accessed December 22, 2017. https://www.virginia.gov/services/mach37-cyber-accelerator/.

[244] Virginia. VITA. *Citizen Awareness.* Accessed December 22, 2017. https://www.vita.virginia.gov/commonwealth-security/awareness-toolkit/citizen-awareness/.

[245] Virginia. CyberVA. *Virginia's Cyber Security Approach: Leadership through Diversity.*https://cyberva.virginia.gov/media/9245/virginiacybersecurity_printfinal-4.pdf.

[246] Virginia. Virginia Economic Development Partnership. *Unlock Virginia's Cybersecurity Advantage.* Accessed December 22, 2017. http://www.yesvirginia.org/cybersecurity.

research and development, research commercialization, worker retraining, and more.[247] Virginia also participates in the National Veterans Retraining Initiative.[248]

Virginia also has a Secretary of Technology office that oversees the Innovation and Entrepreneurship Investment Authority, Center for Innovative Technology (home of the MACH37 accelerator), and coordinates with VITA.[249]

Active Monitoring

Early Detection, Real-time Info Sharing & Threat Monitoring, Federal Collaboration

Virginia's Security Threat and Vulnerability Assessment Service within **VITA** provides cyber intelligence gathering using the **Commonwealth Security and Risk Management (CSRM)** as the go-between for coordination with state agencies, the FBI, and other law enforcement. They provide a monthly vulnerability scan, security advisories, and month information sharing meetings.

VITA provides centralized information security officer services for strategic planning and required annual updates. They provide IT security audit services, and security outreach and information sharing that works with the MS-ISAC, VA Fusion center,[250] FBI, and other security groups.[251]

Response and Recovery

Coordinated Incident Response, Outbreak Containment, Cyber Laws

All executive government agencies and higher education institutions are required to report information security events to VITA. [252] VITA offers security incident management through the CRSM and can deploy a team of first responders from the **Commonwealth**

[247] Virginia. CyberVa. *Virginia's Cyber Security Approach: Leadership through Diversity. Pg 22-33* . https://cyberva.virginia.gov/media/9245/virginiacybersecurity_printfinal-4.pdf.

[248] United States. Department of Homeland Security. National Initiative for Cybersecurity Careers and Studies. *Veterans: Launch a New Cybersecurity Career | National Initiative for Cybersecurity Careers and Studies.* Accessed December 22, 2017. https://niccs.us-cert.gov/training/veterans.

[249] Virginia. Secretary of Technology. *Technology.* Accessed December 22, 2017. https://technology.virginia.gov/.

[250] Virginia. Virginia Fusion Center. *Virginia Fusion Center.* Accessed December 22, 2017. http://www.vsp.state.va.us/FusionCenter/.

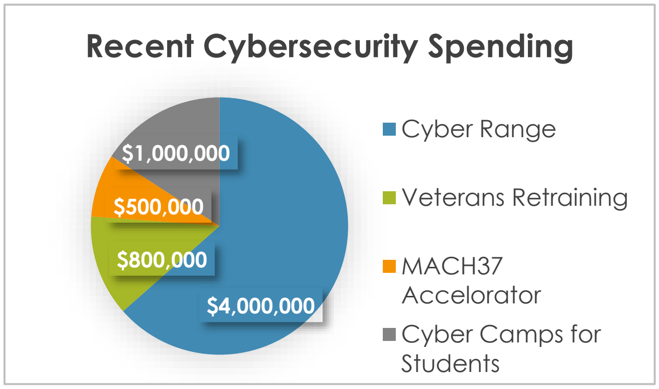
[251] Virginia. VITA. *Security Services Catalog.* Accessed December 22, 2017. https://www.vita.virginia.gov/services/service-catalog/security-services/.

[252] Virginia. VITA. *Incident Reporting.* Accessed December 22, 2017. https://www.vita.virginia.gov/commonwealth-security/incident-reporting/.

Security Incident Response Team (CSIRT).[253,254] Additionally, the Virginia State Police runs a High Tech Crimes Unit that can participate in investigations.[255]

Costs

Recent Cybersecurity Spending [256,257]



[253] Virginia. VITA. *Security Services Full Incident Management.* Accessed December 22, 2017. https://www.vita.virginia.gov/services/service-catalog/security-services/security-incident-management-full-service.html.
[254] Virginia. VITA. *Security Services.* Accessed December 22, 2017. https://www.vita.virginia.gov/services/service-catalog/security-services/security-threat-and-vulnerability-assessment-service.html.
[255] Virginia State Police – High Tech Crimes Unit. *Iacpcybercenter.org.* Accessed December 22, 2017. http://www.iacpcybercenter.org/labs/virginia-state-police-high-tech-crimes-unit-2/.
[256] "Gov. McAuliffe's Final Budget Focuses on Education, Medicaid." WTVR.com. December 18, 2017. Accessed December 22, 2017. http://wtvr.com/2017/12/18/gov-mcauliffes-final-budget-focuses-on-education-medicaid/.
[257] Virginia. VITA. *2016 Commonwealth of Virginia Information Security Report.* 2016. https://www.vita.virginia.gov/media/vitavirginiagov/commonwealth-security/pdf/2016COVSecurityAnnualReport.pdf.

STATE ANALYSIS: WASHINGTON

Leadership

Competent Authority & Resources, Central Hub, Strategic Planning

Washington has gone through a rapid transformation over the last two years. The state began strategic cybersecurity planning as an addition to the state's emergency management plan in 2015– the Washington Significant Cyber Incident Annex (WSCIA). Cybersecurity measures were largely defense based and the Emergency Management Division[258] In that same year the **Washington Office of Cybersecurity (WA-OCS)** was established as part of the Washington Technology Solutions department. The **WA-OCS** goes far beyond emergency management generating a much greater emphasis on public-facing cybersecurity with the **WA-OCS**. Washington's chart reflects the fact that reporting on the initial years of the WA-OCS does not include the Office of Cybersecurity.

The **WA-OCS** is led by the Chief Information Security Officer tending to the following priorities,

- Protecting individual privacy by securing personal information stored by state agencies.
- Securing the state's networks and digital infrastructure from attack.
- Engaging with regional and national public and private sector organizations to form deeper partnerships and build more unified response capabilities against cyber threats.
- Partnering with policy, budget and organizational leaders to ensure a modern and coordinated approach to cyber security.
- Ensuring the continuity of commerce for our state and our region in the event of a cyberattack on critical infrastructure. [259,260]

The **WA-OCS** is the primary entity responsible for cybersecurity strategic planning, technology, policy, private sector relationship building, public outreach, research and analysis, publication, and coordination between the different levels of government. The WA-OCS consists of six departments:

[258] Spidalieri, Francesca. "State of the States on Cybersecurity." The Pell Center. February 01, 2015. Pg 36-39 Accessed September 05, 2017. http://pellcenter.org/eight-states-lead-the-rest-in-cybersecurity/.

[259] Washington. Office of Cybersecurity. *Cybersecurity.wa.gov.* Accessed December 22, 2017. https://cybersecurity.wa.gov/.

[260] Washington. Office of Cybersecurity. *About Us*. Accessed December 22, 2017. http://soc.wa.gov/about-us.

- Computer Emergency Readiness Team **(WA-CERT)**
- Forensic Services **(WA-FS)**
- Information Security Program **(WA-SISP)**
- Information Sharing and Analysis Center **(WA-ISAC)**
- Security Operations Center **(WA-SOC)**
- Security Policy and Compliance **(WA-SPC)**

Multi-Sector Capacity Building

Multi-sector capacity building in Washington started with an emergency response plan and the Unified Cyber Coordination Group (UCG). The Cyber UCG is coordinated by the authority of the Homeland Security Advisor. The Group consists of representatives from state, federal, and local government, academia, critical infrastructure owners and operators, and private industry.261

`

Prevention

Cyber Hygiene, Immunization, Education & Workforce Training

The **WA-OCS** provides cybersecurity resources for awareness and training of the workplace, citizens, and parents. Technical guides benefit technology professionals and organizations through a resource consolidation of industry standard techniques and processes for creating your own security policy. [262, 263]

For the last three years, the state has run Hacktober. Hacktober is a cybersecurity game for all 65,000 state employees that raises awareness about cyber hygiene and cybersecurity practices.[264] The WA-OCS provides newsletters, scam alerts and security advisories linked to MS-ISAC, StaySafeOnline.org, and US-CERT.[265,266]

[261] Washington. Washington Military Department. *Washington State Significant Cyber Incident Annex To the Washington State Comprehensive Emergency Management Plan Annex D.*By Washington Military Department. March 2015. Pg. 7-8. https://mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf.

[262] Washington. Office of Cybersecurity. *Resources.* Accessed December 22, 2017. http://soc.wa.gov/resources.

[263] Washington. Office of Cybersecurity. *Information Security Program (WA-SISP).* Accessed December 22, 2017. http://soc.wa.gov/node/483.

[264] Washington. Office of Cybersecurity. *Hacktober.* Accessed December 22, 2017. http://soc.wa.gov/node/490.

[265] Washington. Office of Cybersecurity. *Cybersecurity Newsletters.* Accessed December 22, 2017. http://soc.wa.gov/resources/newsletters.

[266] Washington. Office of Cybersecurity. *Recent Scams.* Accessed December 22, 2017. http://soc.wa.gov/security-news/recent-scams.

Active Monitoring

Early Detection, Real-time Info Sharing & Threat Monitoring, Federal Collaboration

The **Washington-Security Operations Center** (**WA-SOC)** is responsible for real-time threat detection and monitoring, alerting and intelligence gathering[267]

Agencies are required to submit certification of compliance with security policy and standards each year. Agencies are required to provide cybersecurity training to all employees responsible for performing security procedures. Additionally, agencies must perform a Technology Security Policy and Standards Compliance Audit once every three years. [268]

Specific policies are available to help agencies comply with security planning and compliance. All employees must receive annual cybersecurity awareness training. Periodic security testing is required in the form of penetration testing, vulnerability assessments, and system code analysis.[269] The Washington state chief information officer has created an online library of more than 80 technology policies, procedures, and guides. [270]

WA-OCS also runs the **Washington Information Sharing and Analysis Center**, **WA-ISAC**.[271]

Response and recovery

Coordinated Incident Response, Outbreak Containment, Cyber Laws

WA-OCS operates the Washington Computer Emergency Readiness Team (**WA-CERT**). **WA-CERT** is responsible for incident validation and response, forensics, advisories, recovery. **WA-CERT** does security and risk assessments in the time between emergency

[267] Washington. Office of Cybersecurity. *Security Operations Center.* Accessed December 22, 2017. http://soc.wa.gov/node/481.
[268] Washington. Office of the Chief Information Officer. *Securing Information Technology Assets.* Accessed December 22, 2017. https://ocio.wa.gov/policy/securing-information-technology-assets.
[269] Washington. Office of the Chief Information Officer. *Securing Information Technology Assets.* Accessed December 22, 2017. https://ocio.wa.gov/policy/securing-information-technology-assets-standards.
[270] Washington. Office of the Chief Information Officer. *OCIO- Policies, Procedures and Guidelines.* Accessed December 22, 2017. https://ocio.wa.gov/policies.
[271] Washington. Office of Cybersecurity. *Information Sharing And Analysis Center (WA-ISAC).* Accessed December 22, 2017. http://soc.wa.gov/node/484.

response. [272] The state has clear security reporting communication procedures that each agency must follow.[273]

In September of 2017, the state entered into a federal partnership with DHS, MS-ISAC, and the Washington Elections Office to execute a 3-month long pilot program focusing on improved cybersecurity threat prevention, protection, response and recovery of election systems. This project surfaces in the wake of the 2016 election system breaches.[274] Washington partnered with DHS the year previous to start the Office of Privacy and Data Protection run by the state's **Chief Privacy Officer**. The office is responsible for training state agencies on privacy, and to serve the public through consumer outreach and education initiatives. [275]

Costs

Recent Cybersecurity Spending

FY 2017 $9,443,000 – consolidating technology services into the Office of Cyber Security.[276]

[272] Washington. Office of Cybersecurity. *Http://soc.wa.gov/node/478.* Accessed December 22, 2017. http://soc.wa.gov/node/478.

[273] Washington. Office of the State Chief Information Officer. *IT Security Incident Communication.* Accessed December 22, 2017. https://ocio.wa.gov/policy/it-security-incident-communication.

[274] Douglas, Theo. "Washington State Reveals Upcoming Federal Cybersecurity Pilot, After DHS Confirms Attempted Election Breaches." *Government Technology: State & Local Government News Articles*, September 25, 2017. http://www.govtech.com/security/Washington-State-Reveals-Upcoming-Federal-Cybersecurity-Pilot-After-DHS-Confirms-Attempted-Election-Breaches.html.

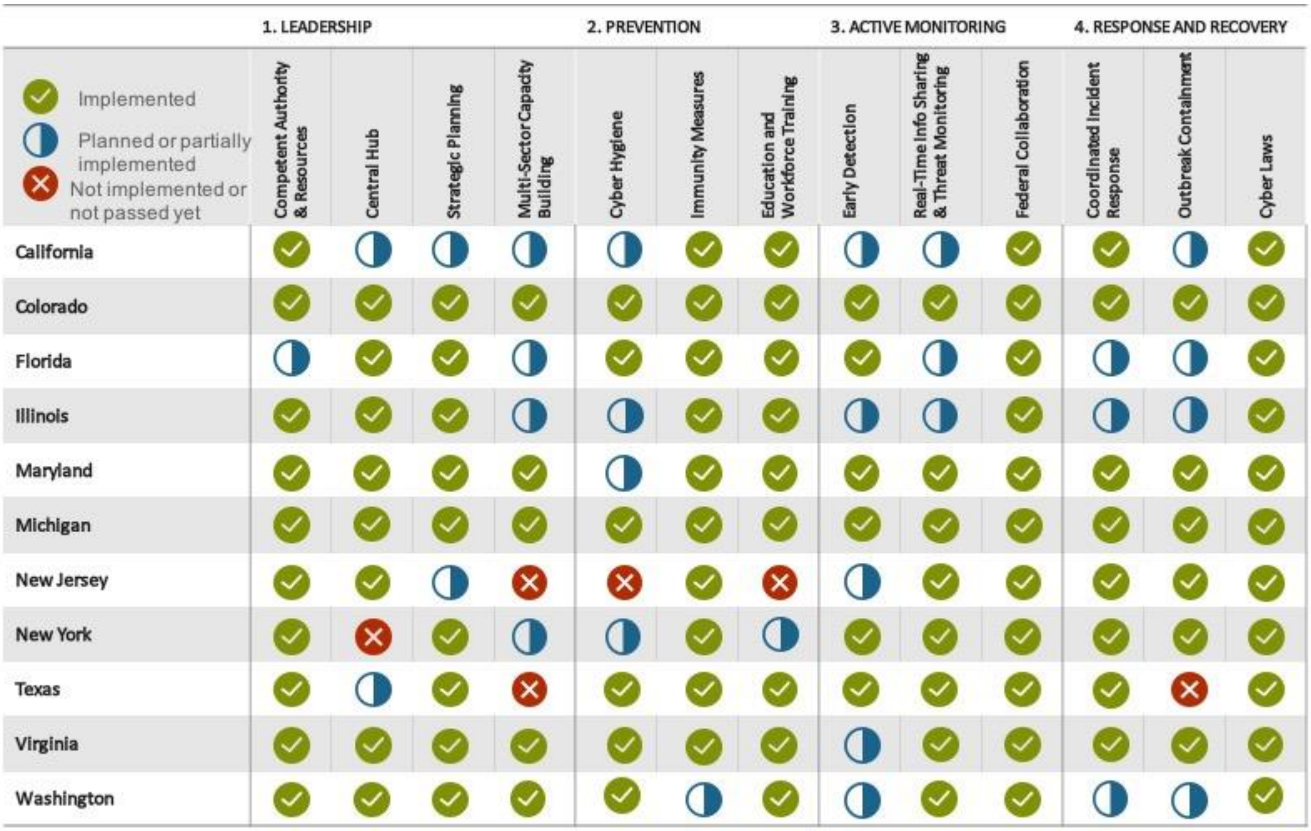
[275] "Washington State Announces Federal Cybersecurity Partnership, Office of Privacy and Data Protection." *Government Technology: State & Local Government News Articles*, January 6, 2016. http://www.govtech.com/security/Washington-State-Announces-Federal-Cybersecurity-Partnership-Office-of-Privacy-and-Data-Protection.html.

[276] Washington. Office of Financial Management. *Governors Supplemental Appropriations Bill.*2016. pg. 54 https://ofm.wa.gov/sites/default/files/public/budget/statebudget/18supp/bills/OperatingZ-0730.3.pdf.

CONCLUSIONS

Evaluation Matrix

State Cybersecurity Initiatives and Efforts in the Public Health Framework



	1. LEADERSHIP				2. PREVENTION			3. ACTIVE MONITORING			4. RESPONSE AND RECOVERY		
✓ Implemented ◐ Planned or partially implemented ✗ Not implemented or not passed yet	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 Spidalieri, "State of the States on Cybersecurity" (Pell Center for International Relations and Public Policy, November 2015) and Oregon OSCIO analysis

CHAPTER 1: STATE CYBERSECURITY COMPARATIVE POLICY ANALYSIS

General Conclusions

Colorado, Maryland, Michigan, and **Virginia** conduct cybersecurity in a manner that includes the most initiatives and processes identified by the cybersecurity-as-a-public-good literature and our resulting public health framework of evaluative comparators. These states have made significant investments in cybersecurity planning, research, coordination, execution, awareness, education, and public outreach.

Consideration must be paid to the fact that **CO, MI, MD,** and **VA** are home to some of our nation's most critical defense institutions and organizations. **Between the 4 states there exist no less than 43 colleges and universities designated as DHS/NSA Certified Academic Centers of Excellence in Cyber Defense.** The defense industry provides an ideal economic scaffolding to support strong school-to-work pipelines, access to federal funding, and a thriving cybersecurity industry.

1. Leadership

Competent Authority & Resources, Central Hub, Strategic Planning

Washington state's **Office of Cybersecurity** provides a simple and effective model for centralizing cybersecurity authoring, planning, and initiatives into a central hub and coordinating cybersecurity Prevention, Active Monitoring and Incident Response & Recovery. Michigan, Maryland, and Virginia adopt a similar structure. Colorado is working toward this structure as well.

While some states may not have a specific cybersecurity strategic plan, most states included in this analysis do have some type of comprehensive information security plan or policy and nearly all are working toward a more comprehensive and diverse approach. This is discussed further at the end of the report.

Multi-Sector Capacity Building

Our public health framework helped to identify the best practices a state would expect to find in a Cybersecurity Center of Excellence geared toward cybersecurity-as-a-public-good. A community approach to cybersecurity is growing in popularity among states. To embark on this process, a strong and diverse multi-sector advisory entity is essential to guiding cybersecurity policies aimed at providing for the public good. Simple public-private partnerships, while important, are falling behind the demand for a more holistic and community centered approach to cybersecurity and cyber health. Boards that include state, federal, and local government, academia, health, financial, business, industry, critical infrastructure owners and operators, and cybersecurity entities are affecting innovative change. Diverse guiding bodies are best fit to research and advise on solutions aimed at bolstering the cybersecurity posture of the state as a whole. This multi-sector advisory approach has been executed by states like Colorado, Michigan, Maryland, and California. This structure allows for a large advisory body that can delegate amongst themselves to provide a deeper focus when investigating specific cybersecurity policy areas via subcommittees. The structure provides for a more well-rounded and informed approach to cybersecurity than simple public-private partnerships.

2. Prevention

Cyber Hygiene, Immunization, Education & Workforce Training

Mandatory state employee cybersecurity training is becoming indispensable as the sophistication and proliferation of end-user attacks, and social engineering are rapidly becoming the most damaging and frequent class of cyber threats. These individual programs are relatively low-cost initiatives that can be accomplished almost immediately by a CCoE. Michigan's employee cyber awareness training costs less than $200,000 and includes 18 lessons over a three-year period for every state employee, 50,000 of which have received the training. At approximately 30 cents per lesson, **the return on investment is estimated by the state to be more than 100 to 1.**

The lack of cybersecurity professionals and rapidly growing demand place constraints on the ability of states to attract and maintain a qualified cybersecurity workforce, especially at public sector prices. The **school-to-work pipeline** is becoming more integral in staffing processes. Capitalizing on this fact and using cybersecurity as an economic driver by integrating academic and industry goals, and incentives are becoming popular ideas among leading states. This idea extends **beyond university programs and certifications to the K-12 system** in order to begin creating the next generation of cybersecurity professionals and increase cybersecurity awareness among communities. Michigan is the prime example in this area, Virginia also. Michigan has a K-12 cyber curriculum and each year the state gives $500,000 of $1,500 dollar individual grants to students participating in the High School Cyber Challenge. Virginia offers a variety of cybersecurity scholarships. Texas' WeTeachCS program and the CyberPatriot youth program are also standout initiatives.

3. Active Monitoring

Early Detection, Real-time Info Sharing & Threat Monitoring, Federal Collaboration

Eight states examined are monitoring all of their Enterprise systems in near-real time. Six states have early detection mechanisms. Some are requiring periodic risk assessments and penetration testing while building up to a real-time monitoring capacity. All states examined are collaborating with the federal government in some information sharing and incident reporting or response capacity. MS-ISAC, US-CERT, DHS, National Guard, StaySafeOnline.org, NetSmartKids.org and NIST coordination are some of the most common federal collaborations.

4. Response and recovery

Coordinated Incident Response, Outbreak Containment, Cyber Laws

All states examined are pursuing cyber laws and regulations beyond existing federal requirements. About half the states have a dedicated **Security Operations Center** coordinated with some kind of Computer Emergency Response Team. **Washington is an example of a state that recently consolidated all cybersecurity monitoring and response activities into the single Office of Cybersecurity**. Michigan, Maryland, Virginia, Washington, and Colorado are all working to have the complete set of in-house services that work in coordination with each other to combine active monitoring and incident response and recovery.

5. Costs

Recent Cybersecurity Spending

State cybersecurity expenditure patterns are very diverse. Transparency and accountability are important when large investments and appropriations are sought. Often, cybersecurity policy and spending originate in the executive branch by executive order. This means that congressional interference is possible if the legislature is not shown results or transparency. This can be particularly problematic because the results are hard to show in a sector whose purpose is primarily preventative. Gaining permanency from an executive order to a sustained center can be difficult for these reasons. Pointing again to the **Secure Colorado** initiative, the development of evaluation metrics as an activity of Colorado's initiative have been particularly helpful to the state CISO communicating progress and value to the legislature in order to justify continued funding. Florida had to experience this process and is still in the process of recovering and organizing cybersecurity capacity.

Discussion of Cybersecurity Strategy

While some states may not have a specific cybersecurity strategic plan, most states included in our sample do have some type of comprehensive information security plan or policy, and nearly all are working toward a more comprehensive and diverse approach. It is important to pay attention to why a state may or may not have a cybersecurity-specific strategic plan, and where they are in the consolidation process. Some states are starting from the ground up and must build a culture of cybersecurity. These states are concurrently beginning to centralize their state technology systems, organizational structures, and policies in order to become more secure. States like Colorado, Florida, and Illinois identified a pressing need for a cybersecurity strategy in a technology landscape that was already robust and flush with defense industry and academic resources, but lacking comprehensive coordination. These states are working to consolidate disparate state legacy and third-party systems into more centralized enterprise systems in an effort to save money and decrease risk of cyber incidents. Other states that were leading the way nationally, having already employed enterprise systems and information security policies, are working to re-evaluate and integrate community-centered cybersecurity, and not just IT security, more thoroughly among state agencies, multi-sector entities, and the general public. Many of the states on this side of the equation have been exemplary and very active on the national cybersecurity stage, while unfortunately not giving enough attention to state, local, and public cybersecurity. The defense industry has known for some time that investment in university programs is necessary to keep up with cybersecurity workforce demand. As we are facing a world-wide shortage of cybersecurity professionals, states are beginning to reach deeper into the K-12 systems, community colleges, university systems, and tapping civilian resources like volunteer cyber corps and the National Guard veterans retraining programs.

Oregon-Specific Conclusions

Many efforts exist that are comparable to what the Oregon CCoE intends to pursue, but very few states actually include every essential characteristic and activity of a public health approach to cybersecurity. **Bits and pieces from multiple states should be considered when compiling the proposal for the Oregon CCoE. The Secure Colorado model, as implemented from the beginning of the program, best fits Oregon's capacity and goals.** Colorado started with a $6,000 cybersecurity budget and no strategic plan. The first strategic plan included simply applying the first 5 CIS controls. Within 3 years, **98% of the state's systems are actively monitored** using security tools in near-real time. Colorado claims a better security rating than most banks, executes an exemplary incident response protocol, and requires mandatory employee cybersecurity training. Colorado also employs very specific **monitoring and evaluation of their efforts**, goals, and progress that provides accountability and legitimacy for the significant investments being provided by the state legislature**.**

Washington state's **Office of Cybersecurity** provides a simple and effective model for centralizing cybersecurity authoring, planning, and initiatives into a central hub and coordinating cybersecurity active monitoring and incident response.

However, there are specific initiatives from other states that could also lend well to Oregon's goals and can be undertaken almost immediately by a CCoE.

- Michigan's Civilian Cyber Corps
- Florida's *New Skills for a New Fight* veterans re-training program, the SecureFloria.org public-facing website
- Michigan's traveling cybersecurity breakfast and luncheon series' and K-12 town hall meetings
- California's Cyber Mentor program.
- Mandatory state employee cybersecurity training
- Michigan's employee cybersecurity training (100 to 1 ROI)
- Texas' WeTeachCS free computer science certification program for K-12 teachers
- CyberPatriot and NICE participation

Chapter 2: Oregon Cybersecurity Survey

A key aspect of embracing a public health approach to cybersecurity policy-making is necessarily engaging the public. Sedenberg & Mulligan[277] specifically call out the creation of opportunities for input from the community, with special emphasis on traditionally disenfranchised groups, as a key principle for creating public cybersecurity policies, programs, and priorities. As the drafting of the Oregon Cybersecurity Center of Excellence (CCoE) proposal both creates a policy-making body and is itself a policy-making exercise, it is appropriate to refrain from delegating cybersecurity policy to experts[278] and instead directly engage members of key beneficiary groups[279] to consider their perspectives. This also acknowledges that the lack of understanding and salience of emerging technologies make traditional proxies especially incapable of adequately representing the public's values, preferences, and beliefs[280]. In short, public participation in information and communication policy making is valuable and adds legitimacy to the outcomes[281].

To reflect the importance of diverse perspectives in the CCoE drafting development process, the CPS Oregon Cybersecurity Needs Assessment project uses two distinct methods to get public input on statewide cybersecurity initiatives: an online survey (discussed in this chapter), and focus groups (discussed in Chapter 3). The role of the survey in the broader research project is to reach representatives of a wide variety of Oregon organizations and efficiently and effectively assess the cybersecurity needs and concerns that are potentially addressable through the CCoE. The survey collects quantitative data using a single instrument to allow for comparisons across industries, geographies, and organization sizes. This allows for the identification of broader trends in Oregon, as well as differences based on geography and industry that may warrant more attention. Additionally, when paired with qualitative and comparative data in a

[277] Elaine M. Sedenberg & Deirdre K. Mulligan, "Public Health as a Model for Cybersecurity Information Sharing," *Berkeley Technology Law Journal* 30, no. 3 (2015): 1738.

[278] Peter Shane, "Cybersecurity Policy as if 'Ordinary Citizens' Mattered: The Case for Public Participation in Cyber Policy Making," *I/S: A Journal of Law and Policy for the Information* Society, 8, no. 2 (2012): 433-462.

[279] "Key beneficiary groups" are defined as local governments, educational institutions, nonprofit organizations, small businesses, law enforcement, and critical infrastructure.

[280] Albert Lin, "Technology Assessment 2.0: Revamping Our Approach to Emerging Technologies," *Brooklyn Law Review* 76, no. 4 (2011): 1309-1370.

[281] Kristen Osenga, "The Internet is Not a Super Highway: Using Metaphors to Communicate Information and Communications Policy," *Journal of Information Policy* 30, no. 3 (2013): 30-54.

mixed methods analysis approach[282], survey results contribute to a robust set of triangulated evidence to inform policy-making activities and provide legitimacy to outcomes. Because of this, the survey is intended to be used in conjunction with these other data sources to provide a comprehensive view of the current state of cybersecurity in Oregon as seen through the eyes of Oregon organizations.

SURVEY PURPOSE

The purpose of this survey is to quantitatively analyze the cybersecurity needs, resources, and concerns of organizations of all sizes, sectors, and types. Specifically, the survey systematically inventories current needs, capabilities, and resources of respondent organizations to allow for comparison, and assesses perceptions of cybersecurity-related trends at the level of both organizations and sectors. The research questions that the survey seeks to answer are:

- What are the needs, capabilities, and resources related to cybersecurity within the key beneficiary groups in Oregon?
- What expectations regarding service usage, advisory engagement, and overall cybersecurity salience can be expected from these groups going forward?

The first research question is addressed by the data gathered from Part 2 and Part 4 as described below, while the second is addressed by the questions contained in Part 3. Neither of these research questions, nor the questions in the survey itself, are specific to the Oregon CCoE as proposed in SB 90. This is to allow respondents to focus on their own cybersecurity needs and resources, and not require them to decipher a new piece of legislation with which they may not be familiar. Instead, the survey is intended to be a useful assessment of the state of cybersecurity across Oregon for all parties interested in addressing this issue, whether they are involved in this specific policy-making activity or not. However, the survey does provide a vehicle by which to raise awareness about SB90 and the CCoE proposal process. While not a part of the survey questions themselves, information about the CCoE and the ability to participate in a focus group to discuss possible CCoE activities were presented to respondents upon completion of the survey.

The survey also updates previous quantitative evaluations of Oregon's cybersecurity needs and concerns. The most relevant such evaluation, and therefore most heavily referenced, is the cybersecurity survey conducted by the Technology Association of

[282] John Creswell & Vicki Plano Clark, *Designing and Conducting Mixed Methods Research* (Thousand Oaks, CA: SAGE Publications, 2011).

Oregon (TAO)in 2013 and published in 2014[283]. The impetus of TAO's survey (proposing cybersecurity education initiatives in Oregon) is not as expansive as the current CCoE effort. However, its 19 questions serve as a template for this survey because of their validation by the technology industry through both the Technology Association of Oregon and the Oregon Engineering Technology Industry Council, and the ability to conduct trend analysis if necessary. Question text and response choices were updated to reflect the specific context of SB90 and its proscribed tasks for the CCoE, as well as the current cybersecurity environment. All question and response choice texts were reviewed and approved by Oregon Cybersecurity Advisory Council members and Oregon Office of the State Chief Information Officer staff at the September 27, 2017 Oregon Cybersecurity Advisory Council meeting.

SURVEY DISTRIBUTION AND RESPONDENTS

To recruit survey respondents, a landing page with a description of the project and survey, as well as a direct link to the survey interface, was set up on the pdx.edu/cps subdomain. The link to this landing page was then emailed to a wide variety of professional organizations, with a special emphasis on contacting organizations that count key beneficiary groups among their membership. Targeted groups included the League of Oregon Cities, the Association of Oregon Counties, Non-Profit Association of Oregon, Technology Association of Oregon, Oregon Association of Government IT Managers, Special Districts Association of Oregon, Oregon City/County Management Association, Nonprofit Technology Network, Oregon Health Information Management Association, Coordinated Care Organizations of Oregon, Oregon School Board Association, Oregon Library Association, Oregon Small Business Association, Oregon Association of Hospitals and Health Systems, Oregon State Sheriffs' Association, and Oregon Association Chiefs of Police; in all, leadership of at least 20 organizations were emailed by team members. The research team also distributed the landing page link and research description through both personal and Center for Public Service social media postings (LinkedIn, Facebook, Twitter, and various Slack channels). Several organizations posted, shared, or retweeted the survey link as well, including Portland Business Alliance, PDX Women in Tech, and the Oregon Library Association. Additionally, Oregon

[283] Technology Association of Oregon. *A Cyber-Studies Strategy for Oregon.* May 5, 2014. Accessed 16 June 2017. https://olis.leg.state.or.us/liz/2015R1/Downloads/CommitteeMeetingDocument/55023

Cybersecurity Advisory Council members distributed links through their organizational affiliations and social networks as well.

Despite this widespread effort and respondent recruitment that took place throughout the survey window, the research goal of 500 responses was not reached. In all, 205 substantive responses (those that answered any question beyond the respondent and organization descriptive questions in Part 1 as described below) were received. A recruitment strategy that so heavily relied on the willingness of third parties to share and distribute the landing page link amongst their membership undoubtedly contributed to the lower-than-expected response rate.

METHODS

The survey was administered in an online format using the Qualtrics survey platform. To collect data on cybersecurity issues across Oregon, the survey relies primarily closed multiple choice questions with responses in the form of modified Likert question structures[284]. Typical 5- or 7-choice responses have an added “don't know" response to account for generally low understanding and salience of cybersecurity issues and prevent the recording of insincerely held opinions and beliefs regarding organizational positions[285]. In cases where applied, this allows respondents that may be truly unfamiliar with the question topics posed to give an accurate response, while also allowing those that are familiar but genuinely neutral in opinion to provide a different, but also meaningful, response as well. A potential downside of including “don't' know" responses is the likelihood of “false negatives", or respondents that do not express an opinion despite actually having one[286]; these are addressed through the triangulation of survey data with focus group data. Several other multiple-choice questions are described as “select all that apply", which allows respondents to represent the breadth and depth of their connection to the topic instead of picking a single “best fit" or “most desirable" option. Open-ended questions are intentionally limited, and questions grouped into

[284] Rensis Likert, “A technique for the measurement of attitudes.” *Archives of Psychology*, 22, no. 140 (1932): 5-55.

[285] Philip Converse, "The Nature of Belief Systems in Mass Publics," in *Ideology and Discontent*, ed. David Apter, (New York: Free Press, 1964), 206-261

[286] Mikael Gilljam. & Donald Granberg, “Should We Take Don't Know for an Answer?” *Public Opinion Quarterly* 57, no. 3 (1993): 348-357.

categories for segmented display in order to counter the cognitive taxation of a long 34-question survey[287].

The analysis of survey questions is conducted using basic statistical depiction of responses for each question. Percentages and averages of responses are constructed where applicable. The organization and respondent characteristics are also calculated for each survey question and discussed here (the cross tabulations, or crosstabs, are available in a separate document entitled Appendix A). This type of descriptive analysis is appropriate when the research questions are exploratory in nature and do not call for hypothesis testing to assess causal claims[288].

Survey Questions

Four general categories of questions are included in the survey:

- Part 1: General Organization and Respondent Information

  These questions ask for basic descriptive facts about both the respondent and their organization, including *"How many total employees does your organization have?"* and *"How long have you been in your current position?"* Questions in this section are used to construct the crosstabs to investigate differences among characteristic groups' responses to the substantive cybersecurity questions in the rest of the survey.

- Part 2: Organization Cybersecurity Needs, Capabilities, and Resources

  These questions (20 total) form the most substantial portion of the survey and ask for information on the respondents' organizations' cybersecurity processes and practices. This includes items like *"How frequently are your organization's systems, technologies, and processes assessed for cybersecurity risks?", "In the next five years, how easy do you expect it to be for your organization to staff [cyber-related] positions?"*, and *"Does your organization participate in any cybersecurity information sharing arrangements with other organizations?"* This section contains a total of twenty questions presented to respondents over four pages.

[287] Mirta Galesic & Michael Bosnjak, "Effects of Questionnaire Length on Participation and Indicators of Response Quality in a Web Survey," *Public Opinion Quarterly* 73, no. 2 (2009): 349-360.

[288] David De Veus, *Surveys in Social Research* (Abingdon, UK: Routledge, 2013): 206-209.

- Part 3: Cybersecurity Resources for Your Organization

  Perhaps the most important for the CCoE development process, this section asks whether the respondents' organization would use any of several programs or services that either prevent cybersecurity issues, provide monitoring for cybersecurity issues, or respond when cybersecurity events occur. This section contains a total of three questions presented to respondents on a single page.

- Part 4: Final Summative Questions

  A final section allows respondents to describe their cybersecurity perspectives and pain points in response to the prompts: *"Right now, what are the biggest cybersecurity concerns for your organization?"* and *"Do you have any additional comments, concerns, or issues about cybersecurity in your organization that you wish to share?"* This section contains a total of two questions on a single page.

Parts 2, 3, and 4 are considered the "substantive" portions of the survey, as they ask questions that pertain to the cybersecurity subject matter. Therefore, to be included in the final survey data, respondents needed to answer at least one substantive question. Responses to each question are considered below, with special attention paid to any results that are either unexpected or that differ significantly by the characteristic groups from Part 1. There were no mandatory questions that required answers in order to continue in the survey, so response rates across questions can and do differ. A full accounting of each question by all characteristic groups is available in supplementary document Appendix A.

GENERAL ORGANIZATION AND RESPONDENT INFORMATION

Part 1 of the survey asked respondents to answer five questions about their organization, and three about themselves and their position within the organization. The responses to these questions are organized in the two tables below. To be included in the final survey data, respondents had to answer at least one question beyond those posed in Part 1.

Organization Characteristics

To assess the types of organizations represented by survey respondents, questions regarding the legal structure, industry, total number of employees, primary Oregon location, and headquarters location were asked. The table below summarizes these responses. Primary location had the lowest response rate in this category; locations have been grouped by county districts (as used by the Association of Oregon Counties) to aid in analysis. There was limited variation in responses to the headquarters location question, so this question was eliminated as a characteristic group.

ORGANIZATION CHARACTERISTICS	N	PERCENT
Legal Structure* [289] *(n=201)		
Local Government (Municipalities & Special Districts)	74	36.8
Other Public Entity (State and Federal Agencies)	37	18.4
Nonprofit	24	11.9
Private	63	31.3
Semi-Public or Public-Private Partnership	3	1.5
Association	0	0
Primary Industry*[290] *(n=202)		
Advanced Manufacturing (Non-IT)	8	4.0
AMTUC (Agriculture, Mining, Transportation, Utilities, Construction)	13	6.4
Education	20	9.9
Environment or Energy Technology	1	0.5
Financial, Banking, Insurance	15	7.4
Government (Federal, State, Local)	71	35.1
Healthcare and Medical	20	9.9
Hospitality/Food and Beverage	3	1.5
Information Technology (IT) or Telecommunications	32	15.8
Life Sciences	1	0.5
Media, Publishing and Entertainment	3	1.5
Professional Services (Non-IT)	8	4.0
Retail and Wholesale	7	3.5
Total Employees*[291] *(n=202)		
Less than 10	29	14.4
10 to 19	11	5.4
20 to 49	23	11.4

[289] For full crosstabs of this question, see Appendix A, p. 9

[290] For full crosstabs of this question, see Appendix A, p. 6

[291] For full crosstabs of this question, see Appendix A, p. 12

ORGANIZATION CHARACTERISTICS	N	PERCENT
50 to 99	22	10.9
100 to 499	47	23.3
500 to 999	19	9.4
1,000 or More Employees	51	25.2
Primary Oregon Location[292] (n=197)		
District 1 (Baker, Grant, Malheur, Umatilla, Union & Wallowa Counties)	10	5.1
District 2 (Crook, Deschutes, Harney, Jefferson, Klamath & Lake Counties)	22	11.2
District 3 (Gilliam, Hood River, Morrow, Sherman, Wasco & Wheeler Counties)	2	1.0
District 4 (Coos, Curry, Douglas, Jackson & Josephine Counties)	13	6.6
District 5 (Benton, Lane & Linn Counties)	14	7.1
District 6 (Marion, Polk & Yamhill Counties)	25	12.7
District 7 (Clatsop, Columbia, Lincoln & Tillamook Counties)	6	3.0
District 8 (Clackamas, Multnomah & Washington Counties)	105	53.3
Legal Structure (n=202)		
Yes, headquartered elsewhere in the US	21	10.2
Yes, headquartered elsewhere internationally	2	1.0
No	182	88.8

Individual Respondent Characteristics

To assess the cybersecurity experience and role of the respondents within their organizations, three questions regarding the respondent’s position type, tenure in that position, and cybersecurity education and training were posed. Position type and time in current position received the highest response rates of any question in the entire survey (n=205).

[292] For full crosstabs of this question, see Appendix A, p. 14

RESPONDENT CHARACTERISTICS	N	PERCENT
Position Type[293] (n=205)		
Senior Executive (CEO, President, Owner, Executive Director, Elected Official, etc.)	25	12.2
Executive – IT Function (CIO, CTO, VP or Equivalent)	29	14.2
Executive – Business Function (CFO, CMO, COO, VP or Equivalent)	11	5.4
Management – IT Function (Director, Manager, Team Leader, etc.)	65	31.7
Management – Business Function (Director, Manager, Team Leader, etc.)	20	9.8
Staff Level – IT Function	40	19.5
Staff Level – Business Function	10	4.9
IT Consultant	5	2.4
Business Consultant	0	0
Time in Current Position294 (n=205)		
Less than 1 Year	27	13.2
1 to 3 Years	54	26.3
3 to 5 Years	37	18.0
5 to 10 Years	40	19.5
10 to 15 Years	27	13.2
15 to 20 Years	10	4.9
20 Years or Longer	10	4.9
Cybersecurity-Specific Training or Education295 (n=201)		
Yes	113	56.2
No	88	43.8

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 is IT manager (31.9%), and more than half have received some kind of cybersecurity-specific training or education (56.2%).

[293] For full crosstabs of this question, see Appendix A, p. 19

[294] For full crosstabs of this question, see Appendix A, p. 22

[295] For full crosstabs of this question, see Appendix A, p. 24

A couple of limitations indicated by this data are worthy of note. First, while the response rate for government entities essentially reached the targeted number, the responses received from private and non-profit entities are much lower than expected. It is therefore difficult to attribute true generalizability to this data in terms of these groups. However, there is still value to considering the data presented from the perspective of Oregon as a whole given the wide variety of organizations that responded. The research team believes that this is the most comprehensive cross-sector cybersecurity evaluation attempt within Oregon at the time of publication. Second, the same caveat applies for many of the geographical areas of Oregon. Several counties are not represented in the data at all, and 2 of the 8 county districts have less than 10 total responses. These responses are therefore not likely generalizable to these populations as whole. However, relative confidence can be given to the Portland Metro area responses (District 8, n=105) because the high number of responses is in line with the original targeted response rate. These concerns make triangulation of this data with other data types and sources, such as the qualitative data attained through the focus groups, an essential part of the research process.

ORGANIZATIONS' CYBERSECURITY NEEDS, CAPABILITIES, AND RESOURCES

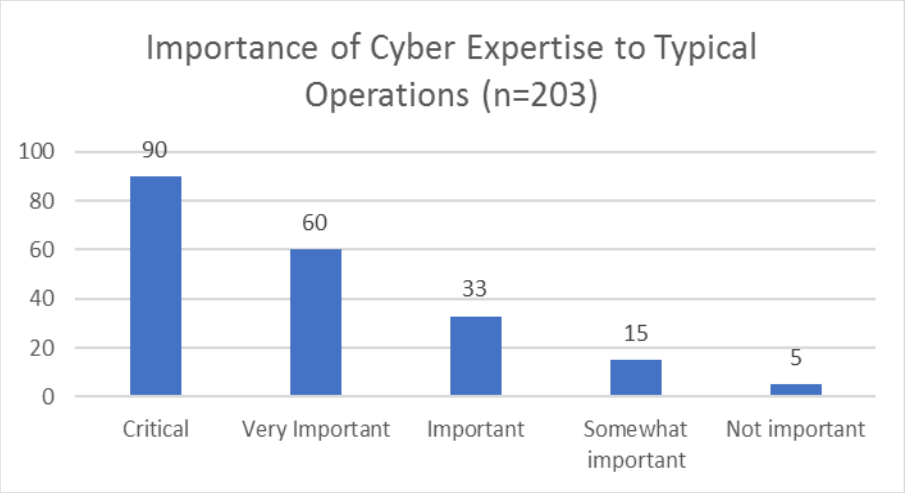
The substantive portion of the survey is discussed below. These questions assess various aspects of organizations' cybersecurity policies, staffing, and views of the future. By asking these questions consistently across geographies and industries, it becomes easier to see where meaningful differences in cybersecurity capabilities and needs may lie. The following sections discuss the data that resulted from groups of questions with similar themes; emphasis is placed on any deviations of characteristic groups (as determined by the organization and respondent characteristic questions in Part 1) from the overall average responses. A full set of crosstabs for each question's responses given by organization and respondent characteristics is available in Appendix A.

Current Role of Cybersecurity in the Organization

The first group of questions assesses the interaction of the organization as a whole with general cybersecurity principles and practices. While the focus is mainly on data compliance standards, risk assessment frequency, and the role of cybersecurity in typical organizational operations, questions about the perceived importance of cybersecurity to the future of both respondents' organizations and industries are also posed.

Importance of Cybersecurity to Organization's and Industry's Purpose

Respondents were asked to rate the importance of cyber expertise, including security, encryption, and data privacy knowledge and skills, to typical organization operations[296] using a five-category Likert response structure. Of the 203 responses received, nearly three-quarters said that cyber expertise is either critical (90, or approximately 44%) or very important (60, or approximately 30%). This response rate holds across all characteristic groups included in the data, including across industries, organization sizes, geographical areas, and respondent position types. In all, only 20 respondents rated cyber expertise as either somewhat important (15, or approximately 7%) or not important (5, or approximately 2%). This demonstrates that respondents believe cyber skills and abilities are necessary and needed in their organizations, regardless of the organization's purpose or primary industry.



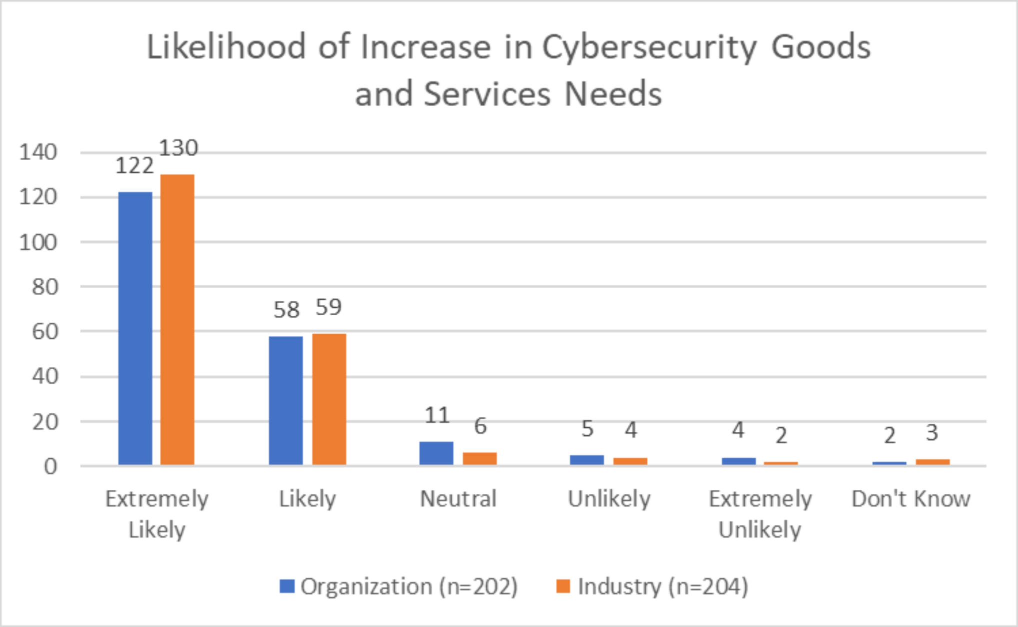
Respondents were also asked how likely an increase in cybersecurity goods and services would be in both their organization[297] and across their industry[298] in the next five years. These questions had very similar results, with approximately 90% of respondents indicating that both their organizations and industries were likely or very likely to experience increased cybersecurity needs. Of the small number of respondents that indicated that cybersecurity needs were either unlikely (5 for the respondents' organizations, 4 for respondents' industries) or extremely unlikely (4 for respondents'

[296] For full crosstabs of this question, see Appendix A, p. 26

[297] For full crosstabs of this question, see Appendix A, p. 29

[298] For full crosstabs of this question, see Appendix A, p. 31

organizations, 2 for respondents' industries) to increase, the majority were from respondents that identified their industry as local government. However, these responses make up less than 5% of the responses for each of these questions, and represent less than 8% of the total government group. Therefore, it appears that across all characteristic groups, most respondents think it likely that cybersecurity goods and services needs will increase for their organizations and industries in the next five years.



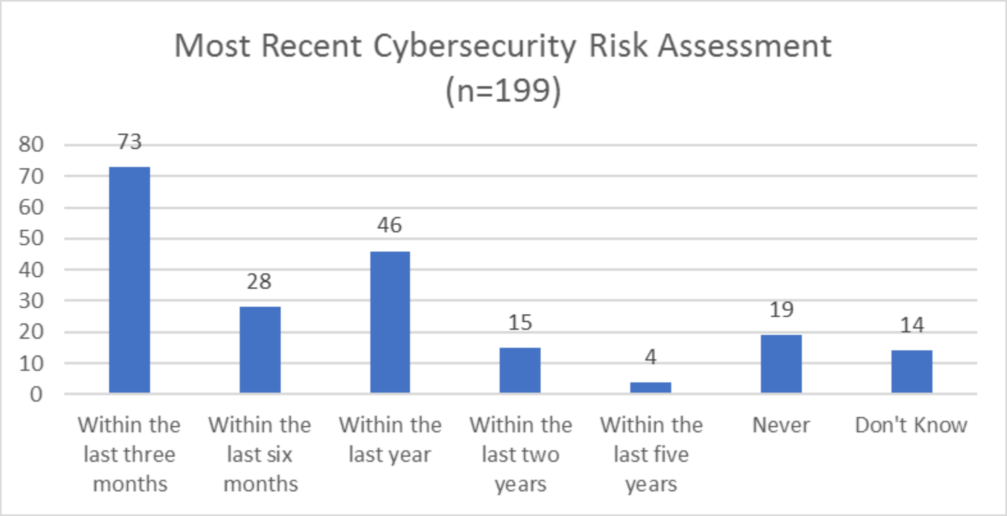
Organization's Risk Assessment Frequency

A key component of any organization's cybersecurity posture and strategy is the systemic assessment of risks. The frequency of these assessments can be indicative of an organization's cybersecurity posture overall. Respondents were first asked how recently their organization's systems, technologies, and processes were last assessed for cybersecurity risks[299]. A majority (147, or approximately 74%) of respondents indicated that their organization's most recent risk assessment was conducted within the last year; the most common response (73, or 37%) to this question was that systems had been assessed within the last three months.

A couple of specific characteristic groups' responses to this question are of interest. First, nearly half of the 16 respondents that either indicated that their organizations have

[299] For full crosstabs of this question, see Appendix A, p. 33

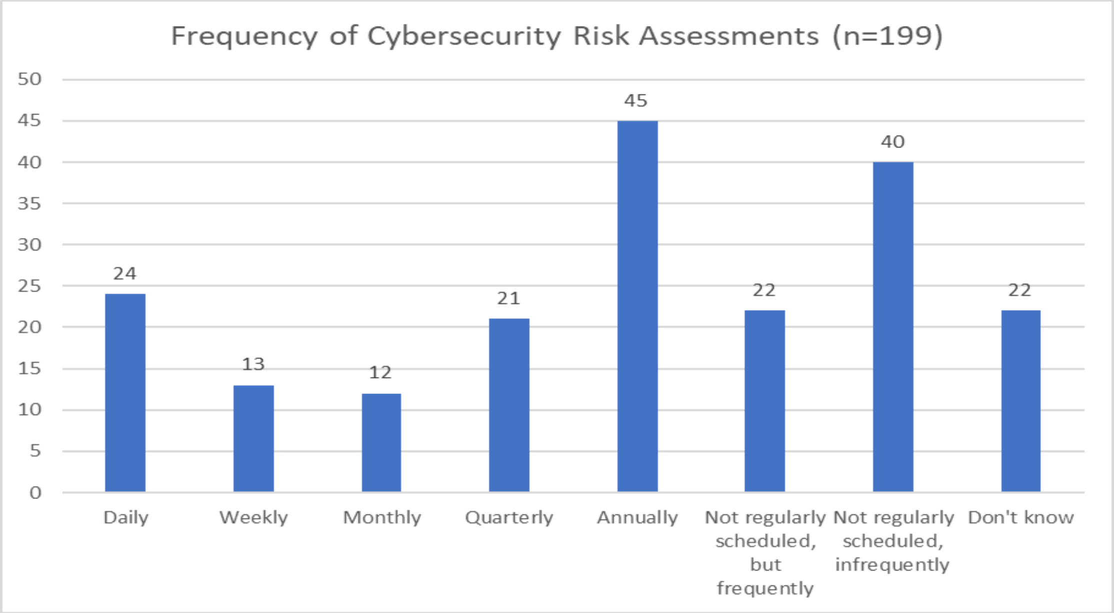
never conducted a risk assessment, or that they were unsure if their organizations conducted risk assessments, identified their organizations' legal structures as local government. This accounts for approximately 23% of the local government responses to this question. Second, respondents that indicated they had not received cybersecurity-specific training or education were more likely to indicate that their organization has never conducted risk assessments (14, or 16%, as compared to 5, or 5% of those with training or education), or that they were unsure if their organization conducts these assessments (11, or 13%, as compared to 3, or 3% of those with training or education). This means that nearly 30% of the organizations these respondents belong to may not be assessing their cybersecurity risks in a systematic way. These deviations from the average rates indicate that cybersecurity assessments are less likely to have recently occurred in local governments than in other settings, and those without cybersecurity training are less likely to work in organizations that have recently conducted cybersecurity risk assessments than those with relevant cyber training.



As a follow up to the last assessment question, respondents were also asked to indicate the overall frequency of their organizations' cybersecurity risk assessments[300]. Here, 70 respondents (or 35%) indicated that cybersecurity risk assessments are performed multiple times over the course of a year – either daily, weekly, monthly, or quarterly. These respondents were more likely to represent organizations with 100 or more employees, as 42% (47 respondents) of larger organizations assess cybersecurity risks

[300] For full crosstabs of this question, see Appendix A, p. 36

more frequently than once per year, while only 26% (22 respondents) of organizations with less than 100 employees report the same. The most common answer given is that cybersecurity risk assessments are conducted annually. Probably of most concern, however, is that approximately 20% of organizations infrequently perform risk assessments, and more than 10% of respondents were not aware of assessment frequency. This was a relatively frequent answer choice for governments (33, or 35% of government respondents) and organizations with less than 100 employees (36, or 43% of small organization respondents). Respondents with no cybersecurity-specific training or education were also more likely to choose one of these two responses (38, or 44%) than their trained counterparts (24, or 22%). Together, these questions show that a majority of organizations are conducting risk assessments on at least an annual basis, but that this is less likely for some specific organization types than others.

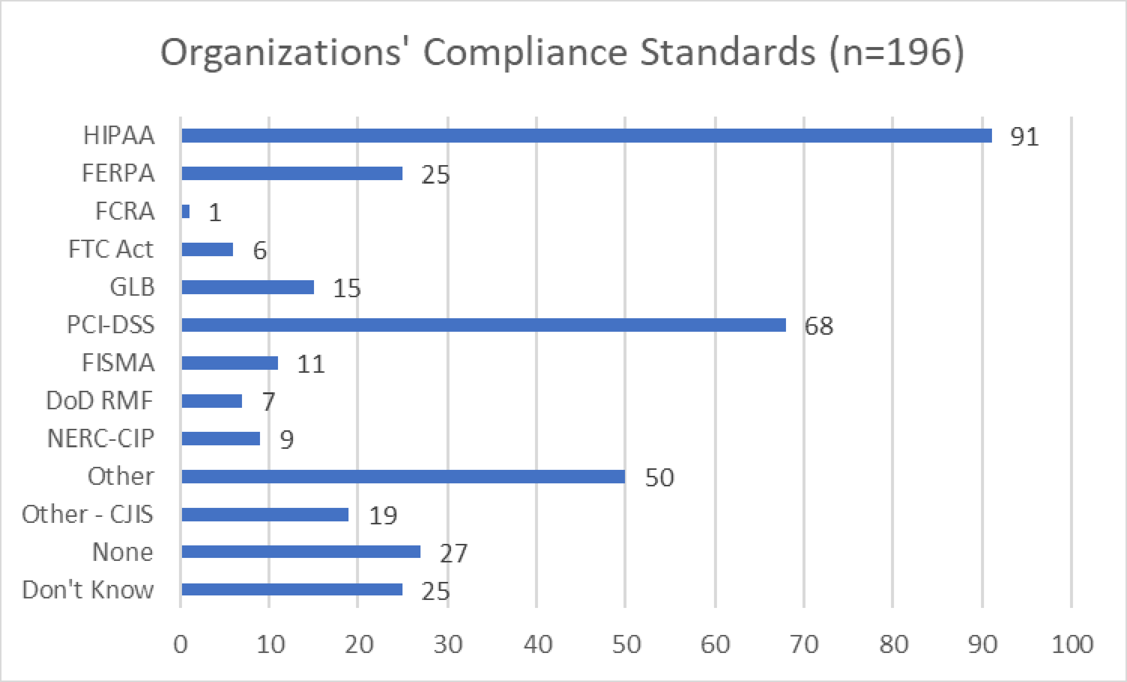


Federal/Industry Data Compliance Standards

Respondents were asked to indicate their organization's obligations to federal and industry data compliance standards[301]. Most respondents are subject to at least one standard, with the average respondent selecting 1.4 standards from the provided list. HIPAA and PCI-DSS were the most commonly chosen responses, with 46% (or 91 respondents) and 35% (or 68 respondents) respectively; FERPA was also indicated by

[301] For full crosstabs of this question, see Appendix A, p. 39

13% of respondents. Respondents could also select "other" and indicate additional compliance standards that were not explicit response choices; of the 50 that did so, the most commonly provided additional compliance standard was CJIS, or the Criminal Justice Information Services standards held by the FBI for (primarily public) organizations accessing and sharing law enforcement data and systems. 10% of respondents (19) indicated that their organizations are subject to CJIS standards. Approximately 13% of respondents (25) selected the "Don't Know" option in response to this question. This choice was more likely to be selected by respondents in senior executive positions (9 of 24, or 38% of these respondents) or those without cybersecurity-specific training and education (20 of 85, or 24% of these respondents). Most other characteristic groups provided "Don't Know" responses at or near the 13% average response rate.

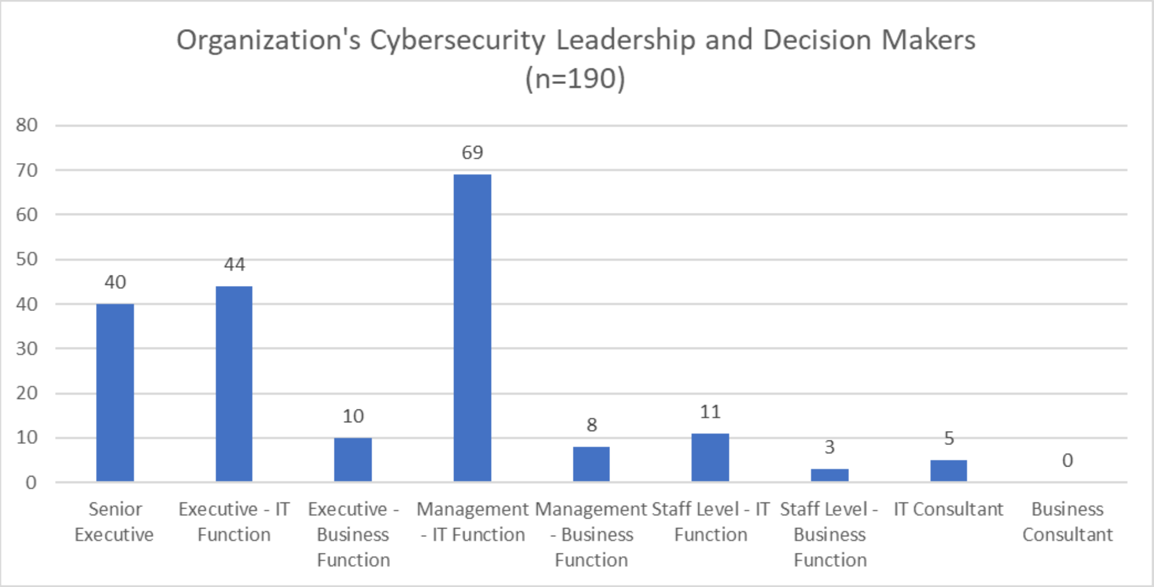


Organization Staff and Cybersecurity

The longest portion of the survey focused on organizations' cybersecurity leadership, staffing decisions, and roles for non-technical employees. 12 questions addressed these issues, and asked respondents to consider the overall state of Oregon's cybersecurity workforce given their organization's experiences.

Cybersecurity Leadership in Organization

When asked what position provides leadership for cybersecurity in their organizations, including approving spending, determining cybersecurity strategy, and any necessary oversight, the most common response (from 69, or 36% of, respondents) was that a management-level employee with IT responsibilities[302] provides this leadership[303]. This is also the most frequent response across characteristic groups with a few notable exceptions. First, respondents from organizations with less than 100 employees were more likely to indicate that the senior executive position[304] in their organization provides cybersecurity leadership (32%), while only 13% of organizations with 100 employees or more answered similarly. The most marked deviation from the average is among organizations with less than 10 employees, where 57% of respondents (or 16 out of 28) indicated that the senior executive oversees cybersecurity decision-making. Organizations with 100 or more employees were more likely to indicate that an IT executive[305] provides cybersecurity leadership (32% or 34 of 107 respondents), while only 11% of smaller organizations selected this answer choice (11%, or 9 of 82 respondents).



[302] The full text of the answer choice was: "Management – IT function (Director, Manager, Team Leader, etc.)".

[303] For full crosstabs of this question, see Appendix A, p. 42

[304] The full text of the answer choice was: "Senior Executive (CEO, President, Owner, Executive Director, Elected Official, City Manager, etc.)".

[305] The full text of the answer choice was: "Executive – IT Function (CIO, CTO, VP or equivalent)".

Another important data observation is that respondents were more likely to choose their own position level as providing cybersecurity leadership in their organizations. 64% of respondents that indicated their position is a senior executive also said that the same position provides cybersecurity leadership for their organization; 78% of IT executives said that their position type provides cybersecurity leadership; and 72% of management-level IT professionals said that cybersecurity leadership is an IT management task. There are many possible reasons for this correlation between stated position and perceptions of cybersecurity leadership, but at the very least it indicates that executive- and management-level respondents across organizations and industries feel that they themselves are responsible for cybersecurity strategies and oversight.

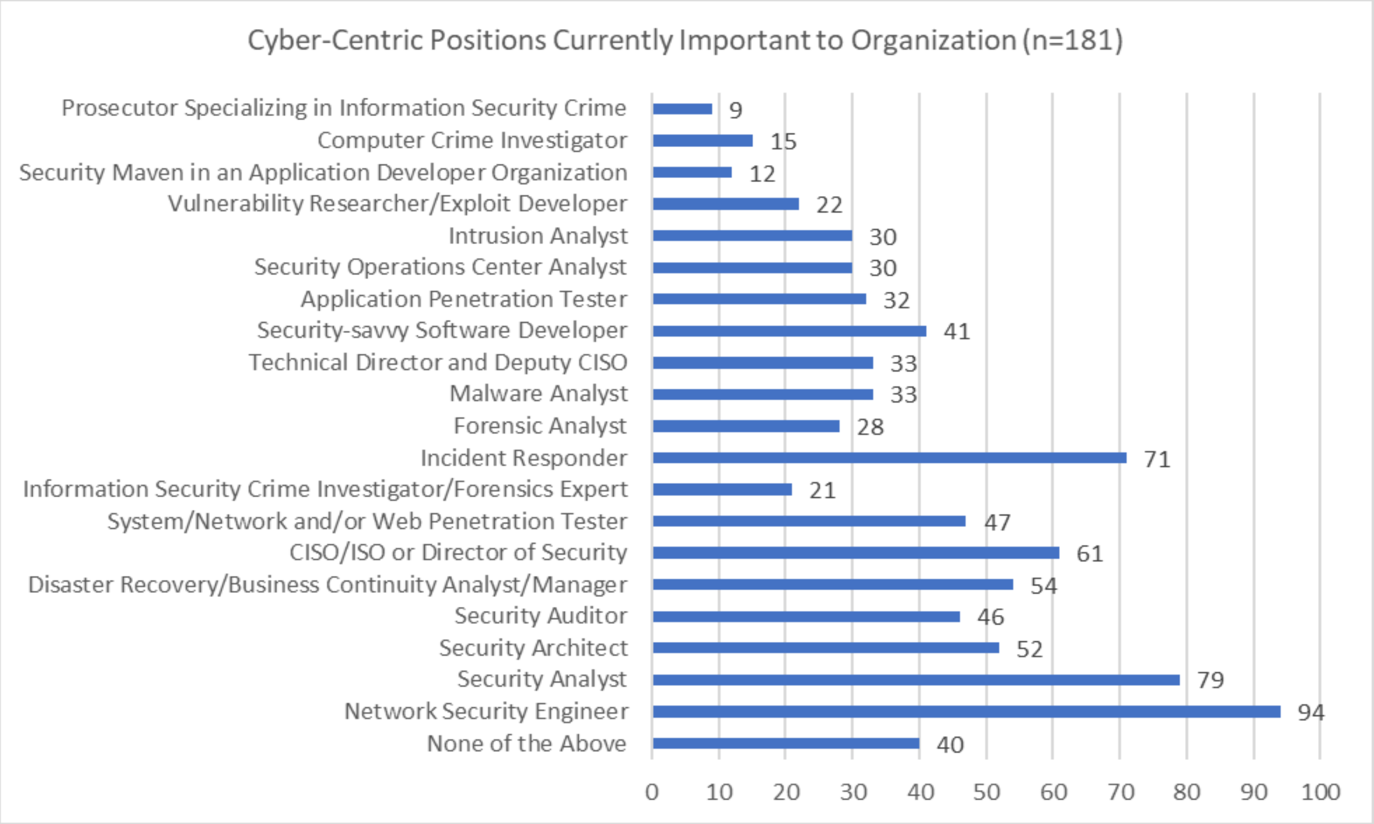
Staffing for Cybersecurity Positions and General Workforce Impressions

Several questions asked respondents to indicate how organizations currently staff for cybersecurity positions, including the types of positions that are important to organizations and the ease with which organizations have been able to fill these positions. First, respondents were asked to indicate which cyber-centric positions from a list of 20 are important to their organization[306]. Every position was selected by some respondents; only "Network Security Engineer" was chosen by more than half of respondents (94 of 181, or 52%). Most positions were chosen by a variety of respondents crossing all organizational and respondent characteristics, with the average respondent (excluding those that selected "None of the Above") choosing 4.2 positions as important to their organizations. A higher proportion of state and federal agencies indicated that positions were important than any other legal structure; nonprofit organizations were less likely to indicate that multiple position types are important. Additionally, across all position types, respondents that have cybersecurity-specific education or training were more likely to indicate that a cyber-centric position is important to their organization.

Despite the variety of positions selected by most respondents, 40 respondents (of 181, or 22%) selected "None of the Above". These organizations were more likely to be local governments or have less than 100 employees. Respondents choosing "None of the Above" were more likely to have a "business" position at any level, or not have any cybersecurity-specific education or training. In general, responses to this question

[306] For full crosstabs of this question, see Appendix A, p. 45

indicate that organizations of all types need to fill cybersecurity positions and that these needs are as diverse as the organizations themselves.

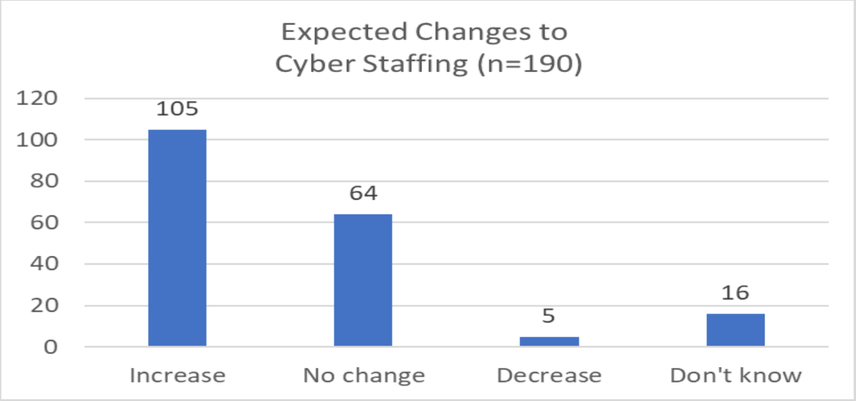


When organizations hire for these positions, the priority placed on industry certifications (including CISSP, CompTIA, SCP, and GIAC certifications) varies across all organization characteristics[307]. Overall, approximately 37% (or 68 of 186) of total respondents indicated that their organizations place a high or moderate priority on these certifications when hiring for cyber-centric positions, while 18% (or 34 of 186) of respondents said these certifications were not a priority. Organizations located in the Portland-Metro area (Multnomah, Washington, and Clackamas counties) are more likely to indicate that they prioritize these certifications than average, while governments and small organizations were more likely to indicate that these certifications are not a priority. 31 of 186 respondents (or approximately 17%) answered that they were unsure of the role that these certifications play in hiring decisions - the same number of

[307] For full crosstabs of this question, see Appendix A, p. 57

respondents that indicated these certifications receive a high priority. These respondents were more likely to be from public organizations that have less than 100 employees, and have business-oriented positions or have less than 5 years' tenure in their current position.

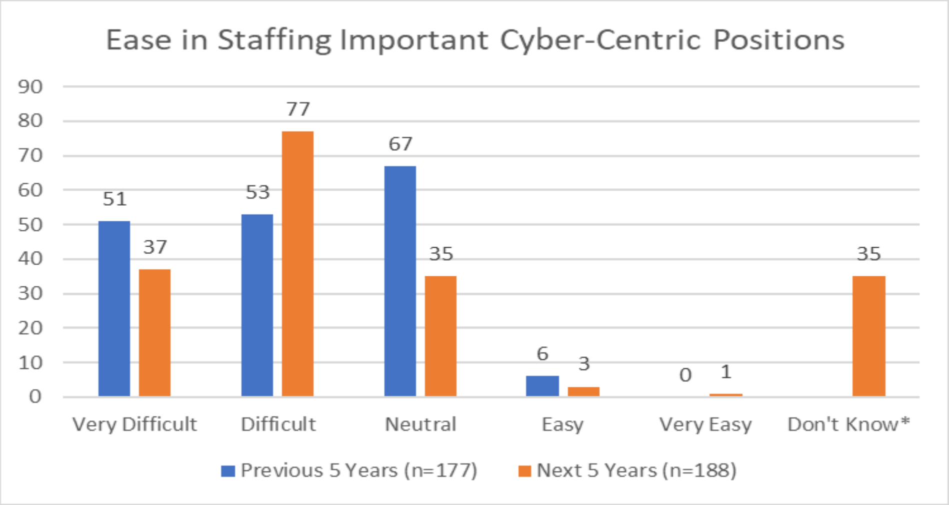
Organizations generally expect that they will require more experienced cybersecurity staff in the next five years[308]. 105 respondents (of 190, or 55%) expect their staffing levels for technical positions requiring cyber expertise or experience to increase, compared to 34% (or 64 of 190) that expect staffing levels to remain the same and only 5 respondents, representing approximately 3% of respondents, that expect a decrease. Organizations that expect increases to cyber staffing levels are mostly nonprofit and private organizations, with a higher percentage of respondents that selected information technology and telecommunications as their primary industry (approximately 87%) choosing this response than every other characteristic group with multiple respondents[309]. Three characteristic groups also differed from the average in terms of expecting staffing needs to remain the same. Governments indicated that they expected cyber staffing levels to remain the same over the next five years at a higher rate than average (53%). Senior executives also were more likely to indicate that they expected no change to cybersecurity staffing levels (13 of 25, or 52%), as were those that have been in their position between 15 and 20 years (8 of 10, or 80%). In general, however, the data indicates that Oregon organizations expect their staffing needs to at least remain at current levels, if not increase, in the next five years.



[308] For full crosstabs of this question, see Appendix A, p. 66

[309] Two subgroups, the Environment and Energy Technology industry group and the Life Sciences industry group, had higher response rates (100%), indicating that the sole respondent in these groups selected "Increase" in response to this question.

Respondents 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[310]. However, the most popular answer choice was "neutral", with 67 of 177 respondents (or 38% of respondents) choosing this option[311]. 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[312]. Government respondents deviated from the overall trend, with "Don't Know" being the most popular response for those who identified their organization's legal structure as local government (24 of 69, or 35%); those without cybersecurity education or training also selected "Don't Know" at a higher rate than those with training (31% of untrained respondents versus 9% of trained respondents). In general, the data from these questions show that respondents currently have difficulty staffing cybersecurity positions, and expect this difficulty to continue.



The final question in this section asked for the organization's perspective on the quantity and quality of cybersecurity talent in Oregon[313]. Here, 24% of respondents

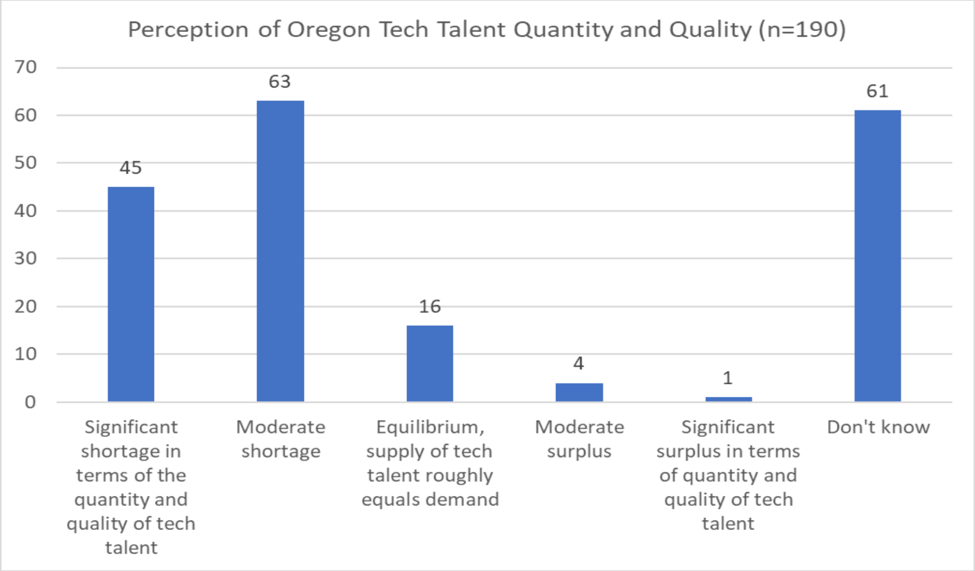
[310] For full crosstabs of this question, see Appendix A, p. 55

[311] An important methodological note for this question pair: due to an error when inputting survey questions and response choices, "Don't Know" was only available for respondents to select when considering staffing ease for the *next* five years, and not when considering the *previous* five years. While it is possible that those who selected "Neutral" may have selected "Don't Know" instead if it were available, it is impossible to know without resurveying with a full selection of answer choices. We assume, however, that a portion of the neutral choices (67 of 177, or approximately 38% of responses) in the question regarding the *previous* five years are from respondents whose perspectives would be more accurately captured by a "Don't Know" response.

[312] For full crosstabs of this question, see Appendix A, p. 63

[313] For full crosstabs of this question, see Appendix A, p. 60

indicated that they believe there is a significant shortage of qualified workers for important positions, while 33% believe there is at least a moderate shortage. 32% of respondents felt they could not assess the quantity and quality of talent in Oregon, and responded “Don’t Know”.



Private organizations, and those in the Information Technology or Telecommunications industry, were more likely to find Oregon’s technology talent lacking: approximately 62% of private organizations (38 of 61) and 77% of information technology respondents (23 of 30) indicated that there is a moderate to significant shortage from their perspective. Organizations with more than 100 employees were also more likely to choose one of these responses (69%, or 74 of 107, did so). Public organizations and organizations with less than 50 employees, as well as respondents that are senior executives or that do not have cybersecurity-specific training, were more likely to select the “Don’t Know” response than other subgroups. The results to this question show that, of those who feel qualified to provide an answer to the question, the dominant perception is that Oregon has a shortage of both the quantity and quality of cybersecurity talent.

Role of Cybersecurity in Organization's Non-Technical Positions

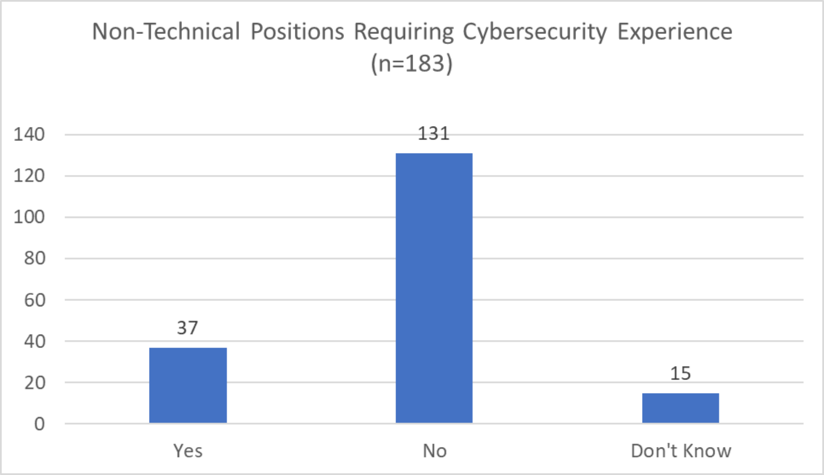
A majority of respondents indicated that non-technical positions in their organizations do not require cybersecurity experience[314]. Of the 37 respondents (20%) that indicated that at least some positions require cybersecurity experience, most identified their industry as either government (13 of 37, or 35%) or Information Technology and Telecommunications (10 of 37, or 27%), and have 100 or more employees (26 of 37, or 70%). Of 184 total respondents, 33% (61) expected that their organization would have more non-technical positions that required cyber expertise or experience within the next five years, while 47% (86) did not expect any changes in the quantity of types of positions[315]. Only the Information Technology and Telecommunications industry and organizations with 1,000 or more employees were more likely to indicate that they expect an increase versus expecting these staffing levels to remain the same. In general, then, while it seems that most organizations neither have nor expect to have non-technical positions that require cyber experience or expertise in their organizations, there is a substantial minority that may find it necessary to staff these types of positions in the future.

Respondents were also asked to indicate the minimum education or training level that would be required for non-technical positions that require cyber experience or expertise[316]; the most common response was that no cyber-specific education or training would be required (58 or 185, or 31% of respondents). This was the only response chosen by more than 20% of respondents, aside from the 25% of respondents that indicated that their organization did not have or expect to have these kinds of positions. The most common training or education response level chosen was technical or vendor training, with approximately 14% of respondents (or 25 of 185) selecting this option.

[314] For full crosstabs of this question, see Appendix A, p. 74

[315] For full crosstabs of this question, see Appendix A, p. 76

[316] For full crosstabs of this question, see Appendix A, p. 78

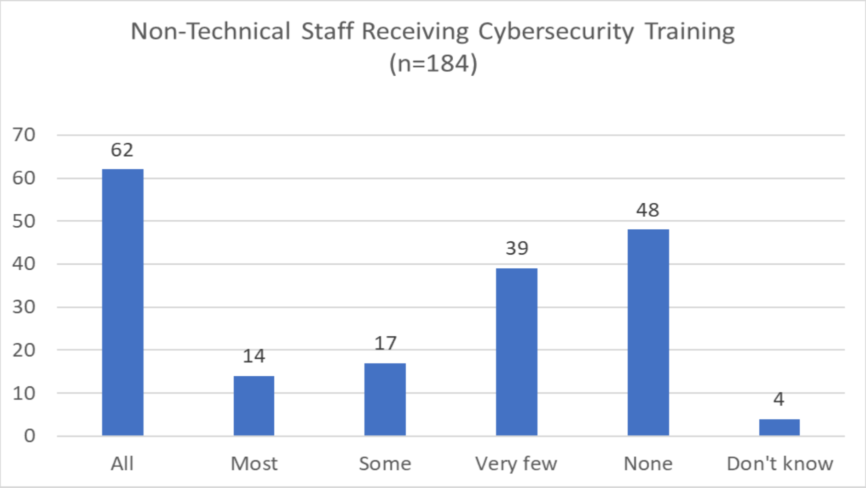


These results indicate that non-technical positions requiring cyber expertise or experience are not common in Oregon organizations, and that there is no majority opinion on the suitable level of education or training that should be required for these types of positions.

Training for Non-Technical Employees

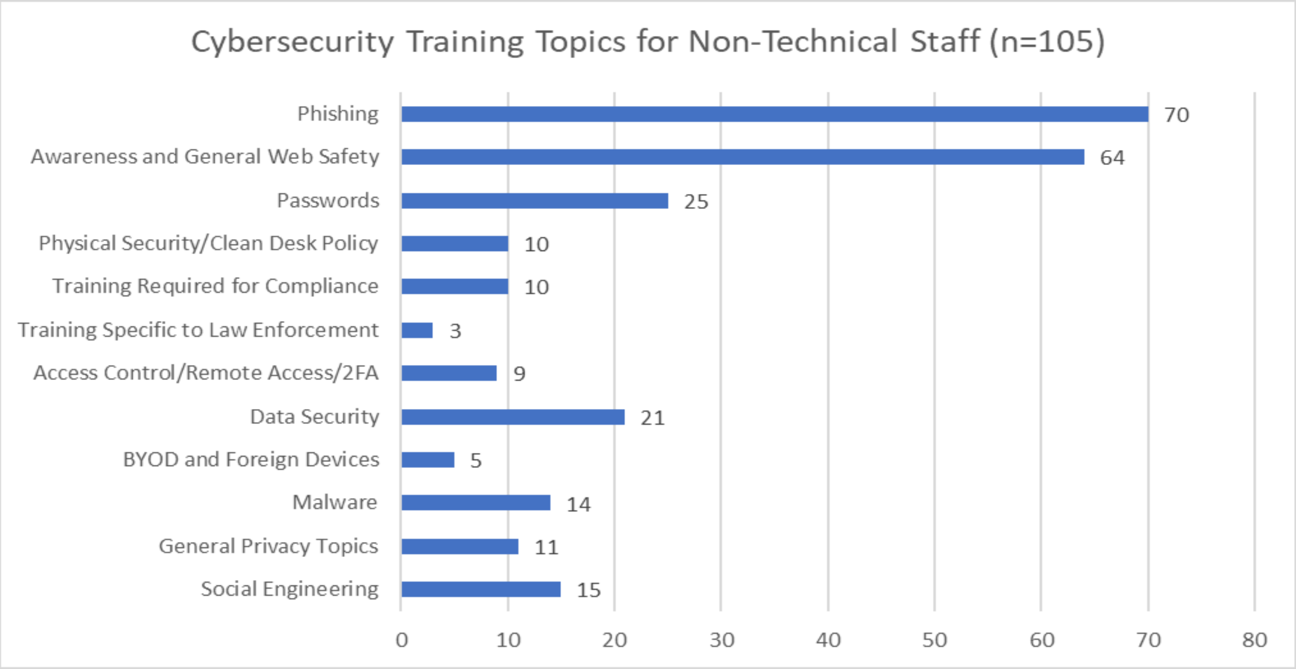
While approximately 34% of respondents reported that all of their organization’s non-technical staff receive cybersecurity training, 26% reported that none of these types of positions receive cybersecurity training, with another 21% noting that very few do[317]. Nonprofits were more likely to report that all or most non-technical staff receive training (17 of 30 respondents, or 57%, compared to the average of 41%), while government organizations were more likely to report that very few or none of their non-technical staff receive this training (44 of 69, or 64%, as compared to the average of 47%). Organizations with less than 10 employees deviated most strikingly from the averages, with only 14% reporting that all non-tech positions receive cybersecurity training, and 61% reporting that none of these positions receive training.

[317] For full crosstabs of this question, see Appendix A, p. 68



Most respondents that indicated that they provide training for non-technical employees also described the contents of this training in a follow-up question. These responses were coded and grouped to provide frequency statistics using a process similar to the analysis methods for focus groups described in the next chapter. The most commonly-mentioned training item was phishing (67% of respondents)[318]. This was followed by general awareness and web safety, a group that included generic phrases like “safe browsing“, “cybersecurity awareness“, and any social media references. Topics on password security were mentioned by 24% of respondents, and general data security and data sharing were also included in 20% of the responses. The average respondent listed approximately 2.4 distinct training topics when describing their cybersecurity training program.

[318] For full analysis of this question, see Appendix A, p. 70

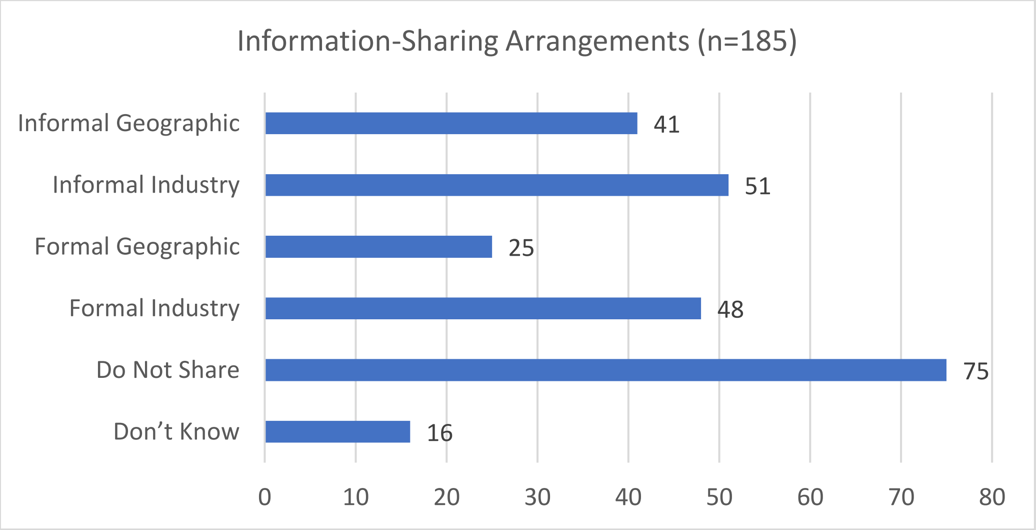


Social engineering, mentioned by 14% of respondents, is almost exclusively included in non-technical training programs for organizations with 100 or more employees (14 of 15 responses came from this characteristic group, or 93%). Most social engineering responses also came from respondents with cybersecurity-specific education or training (13 of 15, or 87%). While it was expected that training for compliance purposes would be more prevalent in healthcare and education, this seems to actually be a common theme across industries, with respondents in professional services, retail and wholesale, and government industries also mentioning this is a critical component of their non-technical cybersecurity training programs.

It is important to juxtapose the results of these questions with the 74% of organizations that indicated that cyber expertise is either critical or very important to typical operations, and the 89% of respondents that expect cybersecurity goods and services needs to grow for their organizations in the next five years. While these data points indicate that cybersecurity is important and its role in organizations is growing, training of staff has not necessarily kept up. Whether this is a result of prioritization, lack of resources, or both is a matter both brought up by focus group participants and addressed through qualitative data collection in the next chapter.

Organization Cybersecurity Information Sharing

When asked about information-sharing arrangements their organizations participate in, the most common response was that organizations have neither formal nor informal arrangements to share information (75 of 185, or 41%)[319]. This response was more prevalent for private sector organizations (32 of 60, or 53%) and organizations with less than 100 employees (44 of 80, or 55%). Organizations that do share information most commonly do so within their industry, with 28% of overall respondents indicating they participate in an informal industry information sharing arrangement, and 26% indicating they participate in a formal arrangement. Sharing cybersecurity information with others in the same geographical proximity seems to be relatively uncommon. In general, respondents in IT executive, IT management, and IT staff positions were more likely to report that their organizations participated in information sharing arrangements of all types.

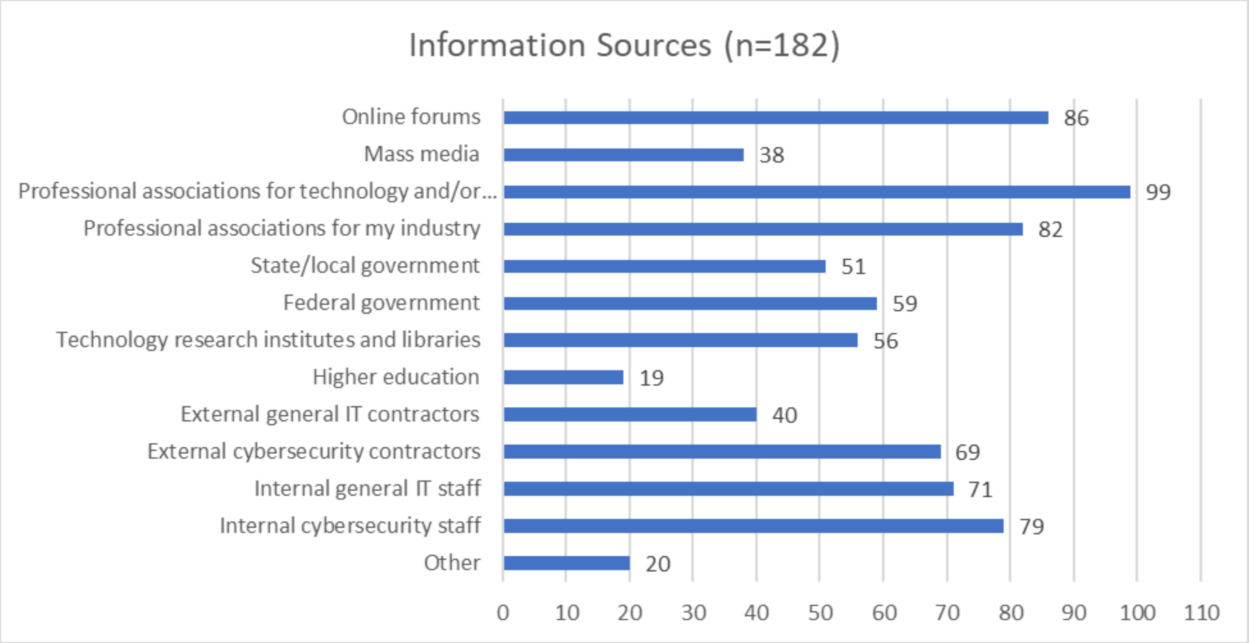


Organizations get cybersecurity information from sources beyond these information-sharing arrangements, too – these are more commonly information sources from which organizations consume information, but do not necessarily provide it reciprocally. The 182 respondents for this question indicated that they consult 3.8 different types of information sources on average[320]. The most common sources for cybersecurity information consumption are professional associations or organizations for

[319] For full crosstabs of this question, see Appendix A, p. 81

[320] For full crosstabs of this question, see Appendix A, p. 84

cybersecurity (54% of respondents), online forums (47%), and industry-specific professional associations or organizations (45%).

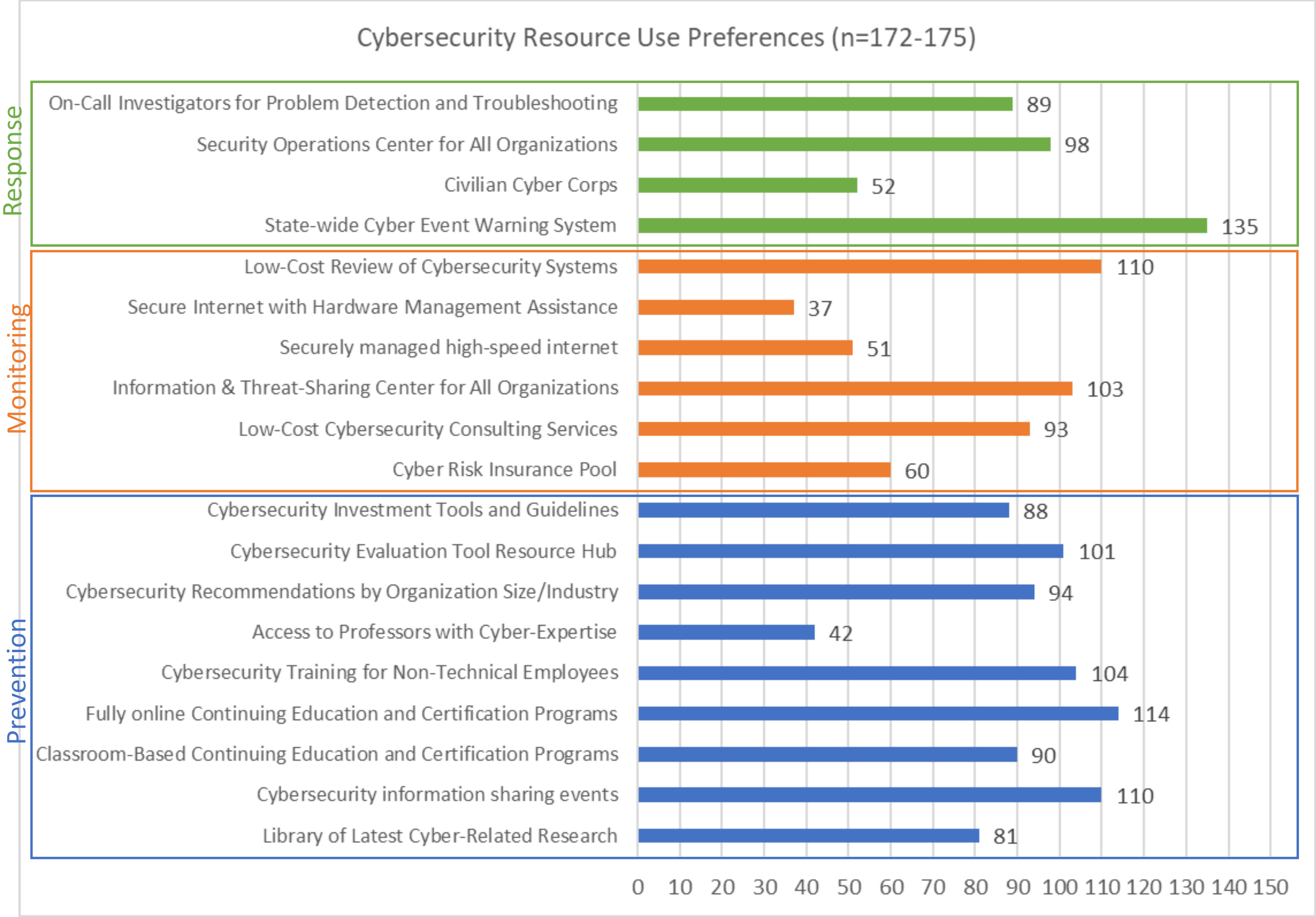


The biggest characteristic group differences for this question are in the responses that indicate that internal cybersecurity staff is a source of cybersecurity information. While 43% of overall respondents indicated they get information from internal cybersecurity staff, 55% of respondents in the Information Technology and Telecommunications industry consult internal cybersecurity staff, as do 57% of organizations with 100 or more employees, and 76% of organizations with 1,000 or more employees. This is most likely because large organizations and organizations in the IT industry have internal cybersecurity staff, while other organizations may not have the resources or perceive a need to hire internal staff of this type. The data also shows that larger organizations consult a wider variety of information sources as well: organizations with 1,000 or more employees indicated they use 5.6 information sources on average, while those with less than 10 employees only averaged about 2.4 sources. Whether this difference is a function of a shortage of time to consult these information sources, knowledge of available information sources, or industry preferences (though no similar differentiation was noted across industries) should be assessed in future survey work.

CYBERSECURITY RESOURCES FOR ORGANIZATIONS

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. Each resource type received its own question with a list of possible programs and services from which respondents could select; each question received a different total number of responses (175 respondents answered the prevention resources question, 174 answered the monitoring resources question, and 172 answered the response resources question)[321]. 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. Respondents were also able to choose as many resources as they wanted from each list.

[321] For full crosstabs of these three questions, see Appendix A, p. 91 for prevention resources, p. 94 for monitoring resources, and p. 97 for response resources.



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. Notable exceptions are the Retail and Wholesale industry subgroup, with only two of five respondents, and the District 4 counties with only three of eight respondents, though with less than 10 respondents each these subgroups may not be truly representative. Other choices that received support from a majority of respondents include fully online continuing education and certification programs (114 of 175 respondents, or 65%), cybersecurity information sharing events (110 of 175 respondents, or 63%), low-cost reviews of cybersecurity systems (110 of 174 respondents, or 63%), cybersecurity training for non-technical employees (104 of 175 respondents, or 59%), and an information and threat sharing center for all Oregon organizations (103 of 174 respondents, or 59%). No major distinctions between characteristic groups exist for these options, as they seem to be equally supported across all descriptive categories for both organizations and individual respondents. On average, respondents chose a total of 4.7 prevention resources from the given options, 2.6 monitoring resources, and 2.2 response resources.

Respondents were also presented with a "My organization would not use these resources" option in the answer selections for each question. 13 respondents, or 7%, indicated they would not use any prevention resources; 18 respondents, or 10%, would not use any monitoring resources; and 15 respondents, or 9%, said they would not use any response resources. In all three questions, these responses were equally likely to come from local government or private organizations; organizations with less than 10 employees responded that they would not use these resources much more frequently than average (24% would not use prevention resources, 32% would not use monitoring resources, and 13% would not use response resources).

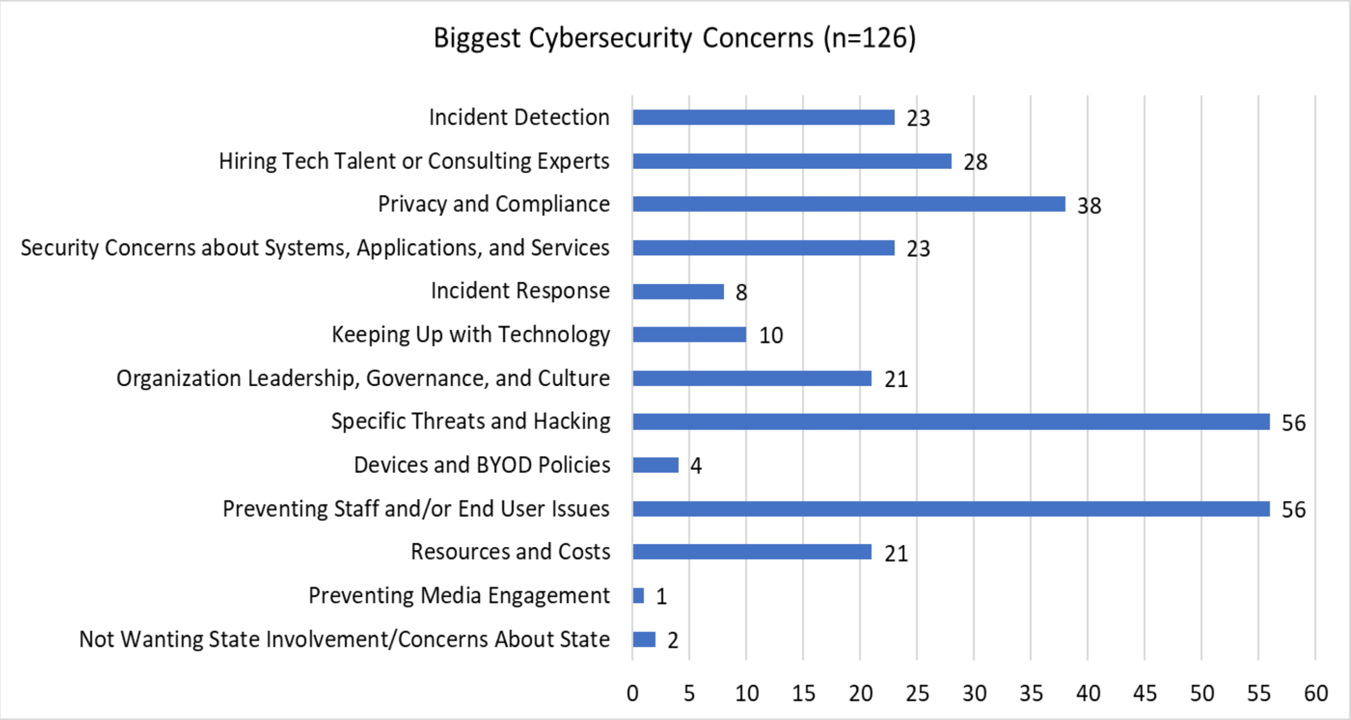
These results show that organizations of all sectors, sizes, and geographical locations perceive at least some of the included resources as being of use to their organizations. Additionally, the selection of resources across the three types of programs and services indicates that organizations are both interested in improving their cybersecurity postures, and also recognize the potential value in these specific types of offerings for their organizations.

FINAL SUMMATIVE QUESTIONS

The survey concluded with two open-ended questions that asked participants to name the biggest cybersecurity concerns for their organization right now, and for any additional comments, concerns, or issues about cybersecurity that they might want to share. The response rate for the second question was low (53 total answers were received, representing only 26% of the total respondents), some of which were simply a variation of "none" or "thank you" (12 of 53 answers, or 23%). Substantive answers received typically closely resembled those given by the respondent to the first question in this section. As a result, we did not code these responses beyond confirming these two facts.

126 respondents (approximately 62% of total respondents) provided answers to the question: "Right now, what are the biggest cybersecurity concerns for your

organization?"[322] Each discrete idea in these responses was given a descriptive code (meaning each response could result in multiple codes), and those codes were then grouped into overarching themes that accurately represent the whole code set. For example, the "Specific Threats and Hacking" theme includes the codes of ransomware, "nonstop threats", denial of service attacks, external hackers, general malware, phishing, and industrial espionage; each of these ideas is included in the theme, and this theme is included in 44% of responses received for this question. The average response invoked 2 of the identified themes below.



The most common themes in responses were the Specific Threats theme as described above, and Preventing Staff and/or End User Issues (mentioned by 56 of 126 respondents, or 44%). Codes grouped under this theme include preventing human errors, issues with internal actors, educating end users, controlling user access, preventing compromised accounts, and social engineering. These responses were equally likely to be given by all characteristic groups, though respondents from nonprofit organizations were slightly more likely to mention Preventing Staff and/or End User Issues than the average respondent (13 of 23 respondents, or approximately 57%). Privacy and Compliance was the third most common theme; this theme includes

[322] For full analysis of this question, see Appendix A, p. 99

responses that mentioned any sort of compliance with federal or industry standards. It also includes general privacy issues that may or may not be directly related to cybersecurity, such as concerns about "keeping information safe". Responses that mentioned issues with hiring and staffing cybersecurity-related positions were a fourth theme that was mentioned by 28 respondents (22%); this further echoes some of the earlier survey questions regarding ease of staffing and importance of cybersecurity talent to the respondents' organizations.

Based on these responses, the biggest concerns for Oregon organizations vary considerably. Both of the most common themes seem oriented toward perceived threats, however, with respondents considering both internal threats (in the Preventing Staff and/or End User Issues theme) and external threats (in the Specific Threats and Hacking theme) some of the biggest concerns they face today. The fact that these themes cut across all analyzed subgroups relatively equally shows that no particular organization size or type is perceived to be exempt from these concerns. The answers for this open-ended question also reflect many of the answers given in previous survey questions, showing that the identified issues or options that these questions are designed to analyze are important to potential Oregon Cybersecurity Center of Excellence participants and users as well.

DISCUSSION AND CONCLUSION

Data from this survey provides valuable insight into the cybersecurity needs and capabilities of Oregon organizations, and shows the extent to which organizations are looking for new cybersecurity resources. Overall, it is clear that survey respondents understand cybersecurity is an important part of organizations' operations today, and will become increasingly important in the future.

An important outcome of the survey analysis is the finding that there is significantly less variety among respondent organizations in terms of needs and resources than expected. Organizations of different industries, sizes, and in different locations had similar response rates to most questions, with a few notable exceptions among government organizations and small organizations. While it is difficult to generalize from the data because of the limitations noted in the analysis of response rates among specific organizational demographics and respondent characteristics, trends should be triangulated with the qualitative focus group data in the next chapter. Further surveying that attempts to rectify the small response sizes could lend additional credibility to the generalizability of these results.

A surprising outcome of the survey is the indication that most respondents' organizations are willing to utilize at least one potential resource or program that might be part of the CCoE. Additionally, there is fairly widespread agreement that respondents about several of these options, spanning the prevention, monitoring, and response resources that fit the full scope of the public health framework for cybersecurity policies. This shows that Oregon organizations of all kinds are looking for resources to help increase their cybersecurity capabilities, and that the kinds of resources that are of interest may not be as specific to industries or geographical locations as initially thought. The ability to serve diverse organizations through similar programs and activities should be encouraging to CCoE decision makers.

Finally, this data provides quantitative evidence that supports efforts to increase the Oregon cybersecurity workforce. Most organizations expect to increase their cybersecurity staffing, as well as their goods and services needs, over the course of the next five years. Embracing the opportunity to assist in the development of a workforce equipped to meet these needs for Oregon organizations is a potential opportunity for meaningful CCoE programming. This is further echoed by the indication that a majority of respondents' organizations are interested in cybersecurity training programs for both technical and non-technical positions. Further investigation regarding workforce development expectations through focus group data can help flesh out the exact needs and expectations that Oregon organizations may have for a statewide cybersecurity workforce development initiative undertaken by a CCoE.

Chapter 3: Cybersecurity Focus Groups

Consistent with a public health approach to cybersecurity policy making and implementation, "public cybersecurity programs and policies should incorporate a variety of approaches" and "ensure an opportunity for input from community members."[323] Accordingly, multiple methods of data collection are employed to ascertain Oregon organizations' perspectives on cybersecurity and a potential Oregon Cybersecurity Center of Excellence (CCoE). To complement the quantitative data collected through the online survey discussed in the previous chapter, qualitative data collected through eight focus groups conducted around Oregon is also analyzed. Focus groups are often used to fill in the quantitative and qualitative data gaps left by typical survey methodologies.[324] The role of the focus groups in the broader research project is to follow up on, and dive further into, the cybersecurity needs indicated in the survey[325], and to provide insight into the kinds of priorities that key beneficiary groups[326] throughout Oregon may agree upon for the CCoE's initial formation. This research also puts a narrative context into the data set, allowing representatives of key beneficiary groups to truly "speak for themselves" in a more authentic way than typically achievable through a survey with mostly closed-ended questions. The ability to consider this qualitative data along with the survey's quantitative data in a comprehensive analytical process is a vital aspect of this mixed methods approach to research[327].

FOCUS GROUP PURPOSE

The purpose of the focus groups is to qualitatively analyze the cybersecurity needs and concerns of organizations of all sizes, sectors, and types in Oregon; in this way, the groups directly correspond to the quantitative data collection efforts of the survey. However, an equally important purpose for these groups is the introduction of a potential policy intervention (in this case, the CCoE), and the ability to observe how

[323] Sedenberg, Elaine M., and Deirdre Mulligan. "Public Health as a Model for Cybersecurity Information Sharing." *Berkeley Technology Law Journal* 30, no. 2 (2015): 1687-1739, pg. 1737-1738. Accessed September 05, 2017. doi: https://doi.org/10.15779/Z38PZ61.

[324] Jenny Kitzinger, "The methodology of Focus Groups: the importance of interaction between research participants." *Sociology of Health & Illness* 16, no. 1 (1994): 103-121. Pg. 116.

[325] David Morgan,. *Focus Groups as Qualitative Research* (Thousand Oaks, CA: SAGE Publications Inc, 1997), chpt 3 pg. 11.

[326] "Key beneficiary groups" are defined as local governments, educational institutions, nonprofit organizations, small businesses, law enforcement, and critical infrastructure.

[327] Creswell, J. & Plano Clark, V. *Designing and Conducting Mixed Methods Research* (Thousand Oaks, CA: SAGE Publications Inc, 2011).

participants collectively and collaboratively respond to this intervention and its ability to address previously identified needs and issues[328]. This is uniquely achievable through focus groups, where the data is generated through interaction among the participants themselves[329][330], revealing insights that may not be accessible (to either participants or researchers) outside of this social context[331]. This allows the following research questions to be addressed through focus group data collection and analysis:

- How do members of [key beneficiary] groups understand and prioritize the tasks for the Cybersecurity Center of Excellence as stated in SB 90?
- How should these differing needs and priorities be balanced in a single Cybersecurity Center of Excellence that serves all groups?

Both research questions are primarily answered by the data gathered in the second half of the focus group protocol, which presents participants with basic information about the CCoE as outlined in SB90 and provides a set of guiding questions for participants to consider as they discuss possible directions a CCoE proposal could take. This allows for the participants to have a shared understanding offered by the facilitators from which to start their discussions; participants could ask clarifying and substantive questions of the facilitator[332] instead of reading and interpreting a piece of legislation that they may not be familiar with on their own. This information-sharing process also provided a vehicle to achieve a tertiary purpose of the primary data collection tasks: spreading awareness about SB90 and the CCoE proposal process and providing opportunities for informed public participation[333]. In this way, the focus groups meet the imperative to inform communities that features prominently in public health approach to cybersecurity.[334]

RECRUITMENT AND PARTICIPANTS

Eight one-hour focus groups were conducted between November 1 and November 14, 2017. Six groups were conducted as in-person sessions, and two were conducted using webinar technology that allowed participants to speak with and hear the facilitator and each other while visually seeing guiding questions on their computer screens. The six in-

[328] Morgan, chpt 3 pg 11-12.

[329] Ibid., chpt 2 pg 8.

[330] Kitzinger, pg. 103.

[331] Liamputtong, Pranee, *Focus Group Methodology: Principles and Practice* (London: SAGE Publications Ltd, 2011), chpt 2, pg 5.

[332] The same facilitator conducted all eight focus groups, in part to ensure that answers given to any questions from participants about the CCoE (and SB90 more generally) were consistent between groups.

[333] Peter Shane, "Cybersecurity as if 'Ordinary Citizens' Mattered: The Case for Public Participation in Cyber Policy Making," *I/S: A Journal of Law and Policy for the Information Society* 8, no.2 (2012):433-462

[334] Sedenberg and Mulligan, pg. 1736-1737.

person groups met in Portland (2 groups), Salem, Bend, Medford, and Pendleton. A coastal focus group was never scheduled due to lack of local responses.

Recruitment Process

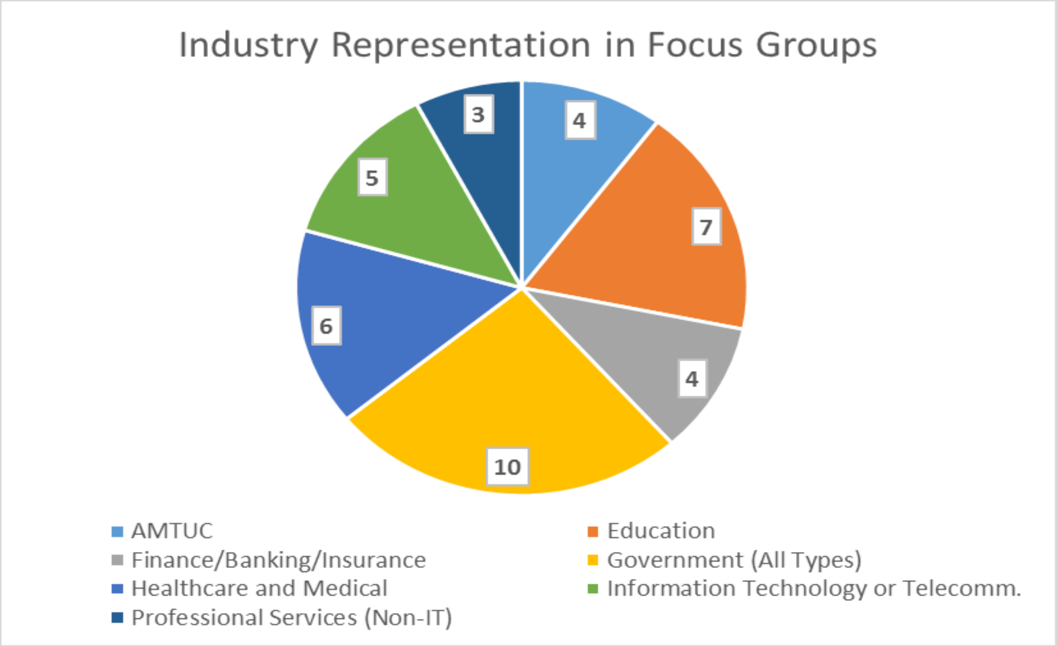
To recruit focus group participants, a landing page with a description of the project and focus groups, as well as a direct link to the Google form by which volunteers could submit their contact information to indicate their interest, was set up on the pdx.edu/cps subdomain. The link to this landing page was emailed to a wide variety of professional organizations, which a special emphasis on contacting organizations that count key beneficiary groups among their membership. Targeted groups included the League of Oregon Cities, the Association of Oregon Counties, Non-Profit Association of Oregon, Technology Association of Oregon, Oregon Association of Government IT Managers, Special Districts Association of Oregon, Oregon City/County Management Association, Nonprofit Technology Network, Oregon Health Information Management Association, Coordinated Care Organizations of Oregon, Oregon School Board Association, Oregon Library Association, Oregon Small Business Association, Oregon Association of Hospitals and Health Systems, Oregon State Sheriffs' Association, and Oregon Association Chiefs of Police. The research team also conducted direct outreach to select Chambers of Commerce and local governments near focus group locations. The research team also distributed the landing page link and research description through both personal and Center for Public Service social media accounts (LinkedIn, Facebook, Twitter, and various Slack channels); Oregon Cybersecurity Advisory Council members also distributed links through their organizational affiliations and social networks as well.

In addition, every online survey respondent was given the opportunity to sign up for a focus group at the end of their survey via a direct link to the Google form. Focus group sign-ups and survey responses were kept separate, and it was not possible to know whether survey respondents were focus group volunteers or vice versa. The only qualifications for participating in the focus groups were the participants be part of an organization that operates in the state of Oregon, and either use or have decision-making power over their organization’s information and technology systems and processes as part of their job duties. Overall, 59 individuals volunteered to participate in a focus group by completing the online form.

From the volunteers, focus group participants were selected for each session to maximize the number of different key beneficiary groups represented in each session and achieve the target of 5-7 participants per session. This selection process allowed researchers to verify that volunteers met the qualification requirements. Diversity across age, gender, race, and national origin was limited in this case by the small response group and demographics in the profession. Of the 59 individuals that initially volunteered, 46 signed up for a specific focus group, and 39 of the 46 attended a focus group session.

Description of Participants

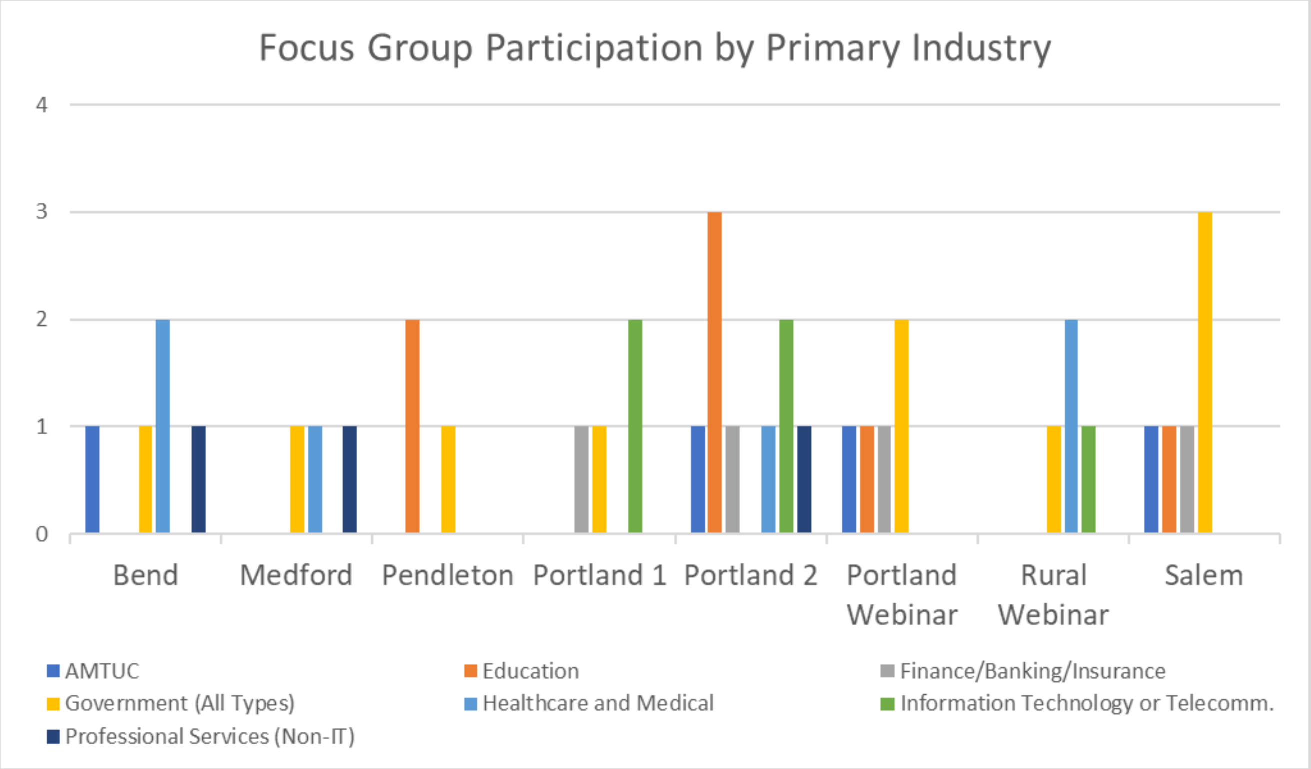
The 39 focus group participants represented 7 industry categories[335]: AMTUC (agriculture, mining, transportation, utilities, and construction), Education, Finance/Banking/Insurance, Government (federal, state, and local), Healthcare and Medical, Information Technology and Telecommunications, and Professional Services (Non-IT). Over 25% of participants were from government organizations, predominantly at the local and state levels; the smallest group is the Professional Services category, making up 7.7% of the total participants. A representative of an 8th industry group (Hospitality/Food and Beverage industry) signed up for a focus group but was unable to attend.



While 39 participants is slightly above the stated goal of 15 to 35 participants, more than the initially proposed 3-5 focus groups were required to accommodate this number of participants. Due to unforeseen cancellations, scheduling conflicts, weather-

[335] Participants were identified by the same list of 13 primary industries used in the online survey (see pg. 88 of this report).

related travel issues, and recruitment issues in areas outside of the Portland-Salem I5 corridor, four focus groups had less than the intended 5-7 participants: two focus groups had four participants (Portland 1 and Rural Webinar), and two focus groups had only 3 participants (Medford and Pendleton). While this was initially a cause for concern, there are in fact widely varying recommendations regarding focus group size, with indications in the literature that groups with as small as two participants to as many as twelve can produce valuable data.[336][337][338] The research team is therefore unconcerned with the inability to meet the targeted minimum of five participants for these focus group sessions. The size and represented industries in each focus group are represented in the graph below.



[336] Liamputtong, chpt. 4.

[337] Fern, chpt 7.

[338] Rosaline Barbour, *Doing Focus Groups*, (Thousand Oaks, CA: SAGE Publications Inc, 2007), chpt 5.

FOCUS GROUP PROTOCOL

Focus groups were facilitated with a semi-structured protocol in order to ensure consistency across groups, but also to allow for conversations to naturally develop among participants. This protocol was piloted in a session with key stakeholders and experts on August 25, 2017, following the 3rd Oregon Cybersecurity Policy Summit in Portland, Oregon. That session was transcribed and scrutinized by the research team, and several adjustments to the protocol were made based on the outcome of the pilot and feedback from participants.

To maintain the organization-level focus of the overall research project, questions primarily concerned participants' organizations and industries rather than their personal opinions, feelings, and perspectives. Participants were first asked to discuss their organizations' general approaches to cybersecurity. The purpose of these questions was two-fold: first, these questions allowed participants to become somewhat familiar with each other by discussing issues they are well versed in before being asked to collaboratively consider the Oregon CCoE. Second, these questions mirror some of the questions used in the online survey administered as part of this project (see previous chapter); this allows qualitative data collected from the focus groups to be used as a means of triangulation for the previously collected quantitative data[339]. This is especially true for survey respondent subgroups with smaller numbers of responses, including those geographically located in southern and eastern Oregon. Discussion in this portion of the focus groups generally lasted around 20-25 minutes, or about a third of the total allotted time for each group. Questions in this section included:

1. How would you describe your organization's general approach to cybersecurity?
2. Where do you go to learn about cybersecurity threats and trends?
3. What keeps your organization from making [cybersecurity] improvements?

Following this portion of the discussion, a handout was provided to each participant that introduced the CCoE proposed by SB90 and the general concept of a center of excellence. Included were "center of excellence" definitions from Frost et al[340] and Stricker[341], and brief summaries of the functions of the CCoE as identified in SB90 as

[339] Creswell, J. & Plano Clark, V. *Designing and Conducting Mixed Methods Research*.

[340] Tony Frost, Julian Birkinshaw, & Prescott Ensign, "Centers of excellence in multinational corporations," *Strategic Management Journal* 23, no. 11 (2002): 997-1018, pg. 1000.

[341] Jon Strickler, "Centers of Excellence Revisited," *Horizon Line Group*, April 1, 2014. Accessed August 14, 2017. http://agileelements.wordpress.com/2014/04/01/centers-of-excellence-revisisted/

shown in the table below. While SB90 includes six specific functions for the CCoE, following the pilot stakeholders recommended that four of the five functions attributed to the Oregon Cybersecurity Advisory Council in SB90 also be included in the handout for discussion by focus group participants, bringing the total number of functions presented to participants to 10. The location in SB90 of each item is footnoted for reference.

Coordinating information sharing regarding cybersecurity risks and incidents across all types of organizations.[342]	Drafting the State of Oregon Cybersecurity Strategy, as well as the Oregon Cyber Disruption Response Plan.[343]
Supporting cybersecurity incident responses and investigations.[344]	Providing a statewide forum for discussing cybersecurity issues.[345]
Severing as an Information Sharing and Analysis Organization that officially liaises with the National Cybersecurity and Communications Integration Center.[346]	Recommending best practices for cybersecurity to all types of organizations.[347]
Participating in federal, multi-state and private sector organizations that are relevant to the mission and activities of the CCoE.[348]	Promoting cybersecurity real-time situational awareness for all types of organizations.[349]
Receiving and disseminating cybersecurity threat information from a wide range of sources.[350]	Encouraging cybersecurity workforce development.[351]

Based on this information, participants were then asked to consider the Oregon CCoE from the perspective of the needs of their organization, as well as those of other participants in the group and Oregon as a whole. These experiential questions,[352] designed to extract similarities in participants' perspectives and gage agreement on

[342] SB90Enrolled, Section 4(1).

[343] SB90 Enrolled, Section 4(6).

[344] SB90 Enrolled, Section 4(2).

[345] SB90 Enrolled, Section 3(4)b.

[346] SB90 Enrolled, Section 4(3).

[347] SB90 Enrolled, Section 3(4)c.

[348] SB90 Enrolled, Section 4(4).

[349] SB90 Enrolled, Section 3(4)d.

[350] SB90 Enrolled, Section 4(5).

[351] SB90Enrolled, Section 3(4)e.

[352] Fern, chpt 1.

potential programs and activities for the Oregon CCoE, formed the bulk of the predetermined questions included in the protocol and were given the most discussion time (typically 35-40 minutes). The functions ascribed to the CCoE by SB90, and potential programs and activities that could fulfill these functions, were collaboratively considered by participants with an emphasis on collective prioritization and consensus-building. In this way, the focus group structure more closely aligns with a consensus conference model[353] than a traditional "group interview" model[354] . This collaborative discussion occurred through discussion of the following questions:

4. What benefits do you see in the Center of Excellence approach to cybersecurity?
5. Which of the [SB90] functions are most important to your organization?
6. What activities or programs can you think of that a Cybersecurity Center of Excellence could undertake to be most beneficial to an organization like yours?
7. Is there anything specific that is essential to the success of an Oregon Cybersecurity Center of Excellence?
8. Do you think your organization would use the services offered by an Oregon Cybersecurity Center of Excellence?

Questions in the second portion of the protocol were less likely to be asked verbatim by the facilitator, as conversations tended to transition between topics naturally and without the need for prompting with specific questions. However, by following a semi-structured protocol, the research team ensured that each focus group considered all questions at some point during the focus group session. Following the conclusion of the focus group, participants were reminded to take the online survey if they had not done so already, and asked to encourage anyone they knew that might have valuable input to participate in the research process as well.

DATA RECORDING AND ANALYSIS METHODS

Each focus group session was audio-recorded, and extensive field notes were taken by a notetaker (separate from the facilitator) in each session. Field notes were augmented by the note taker following each session by listening to the audio recording again and focusing on recording key points and ideas verbatim; the facilitator also constructed

[353] Shane, 447.

[354] Morgan..

field notes through recollection of key topics and by listening to each session again. Field notes were then compiled to form a robust data set for analysis[355].

Though transcription is the most common method of constructing data from focus groups for analysis, the research team did not create full transcripts of each focus group session. This decision was made for several reasons. First, the extent of transcription necessary for analysis depends on the level of analysis required to answer the research questions.[356] The research questions for this portion of the project are intended to explore general themes and patterns of interactions and collaboration; field notes that accurately capture these interactions, without necessarily including every spoken word, can fulfill this purpose.[357] Using field notes is also recommended when there is an abbreviated timeframe for analysis.[358] The research team only had approximately one month from the conclusion of the focus groups to complete and present the analysis, which certainly qualifies as an abbreviated timeframe. Finally, the extensive field notes created by researchers are considered transcription under some definitions within the wide variety that exist in the literature[359]. Thus, while verbatim transcripts of focus group sessions were not created in this research process, the data set created from augmented field notes is sufficient for the purposes of answering the previously discussed research questions and supported by the literature.

To process and analyze the data, four analysis groups were formed from the 8 focus groups:

- Portland Metro Area (2 in-person groups, 1 webinar): 18 participants total
- Salem (1 in-person group): 6 participants
- Bend (1 in-person group): 5 participants
- Rural Group (2 in-person groups - Medford and Pendleton, 1 webinar): 10 participants total

[355] Robert Yin, *Qualitative Research from Start to Finish* (New York: The Guilford Press, 2011). See especially chpt 7.

[356] J.W. Drisko, "Strengthening qualitative studies and reports: Standards to promote academic integrity," *Journal of Social Work Education* 33, no. 1 (1997): 185-197.

[357] Eleanor McLellan, Kathleen McQueen, & Judith Neidig, "Beyond the Qualitative Interview: Data Preparation and Transcription," *Field Methods* 15, no. 1 (2003): 63-84, pg. 67.

[358] Jane Bertrand, Judith Brown, & Victoria Ward, "Techniques for Analyzing Focus Group Data," *Evaluation Review* 16, no. 2 (1992): 198-209, pg. 202.

[359] Christina Davidson, "Transcription: Imperatives for Qualitative Research," *International Journal of Qualitative Methods* 8, no. 2 (2009): 36-52. A literature review of scholarship on data recording techniques in qualitative research that shows the wide and varying definitions of "transcription".

Portland and Salem were kept separate due to the high participation rate in Portland and prevalence in Salem of state agency representation. Bend was kept separate from other non-Portland Metro area locations because of the potential influencing effects of the Bend Cybersecurity Summit, which four of the five participants attended immediately before the group. No other participants save one Rural Webinar attendee were present at the Bend Cybersecurity Summit.

The analysis method used in this part of the research generally follows the recommendations put forth by Nili et al,[360] combining this framework with the more traditional qualitative analysis procedure of coding, categorization, and theme construction as described by Yin[361]. This process consisted first of open coding, in which a researcher assigns a code, or "a word or short phrase that symbolically assigns a summative, salient, essence-capturing, and/or evocative attribute,"[362] to the data; the research team focused on using participants' own words verbatim as these initial codes (a technique called "in vivo coding") where possible. The codes are then reassembled by grouping similar codes into categories; once categorized, themes are then identified that exist across the newly organized data set in an interpretive process[363]. To improve the reliability and validity of this qualitative data analysis method (which can be especially susceptible to researcher bias), an abbreviated version of an intercoder reliability process[364] was conducted by two researchers that included independent coding and collaboration on the development of categories and themes. The output of this qualitative analysis process is the creation of a list of themes that represent the most important and prevalent conceptual ideas in the dataset[365]. These themes are presented and explained in the context of the focus groups in this chapter, and inform the recommendations in the next chapter.

[360] Alireza Nili, Mary Tate, & David Johnstone, "A Framework and Approach for Analysis of Focus Group Data in Information Systems Research," *Communications of the Association for Information Systems*, vol. 40 (2017): 1-21.

[361] Yin, pg. 187-189.

[362] Johnny Saldana, *The Coding Manual for Qualitative Researchers*, (Los Angeles: SAGE Publications, 2013), pg. 3.

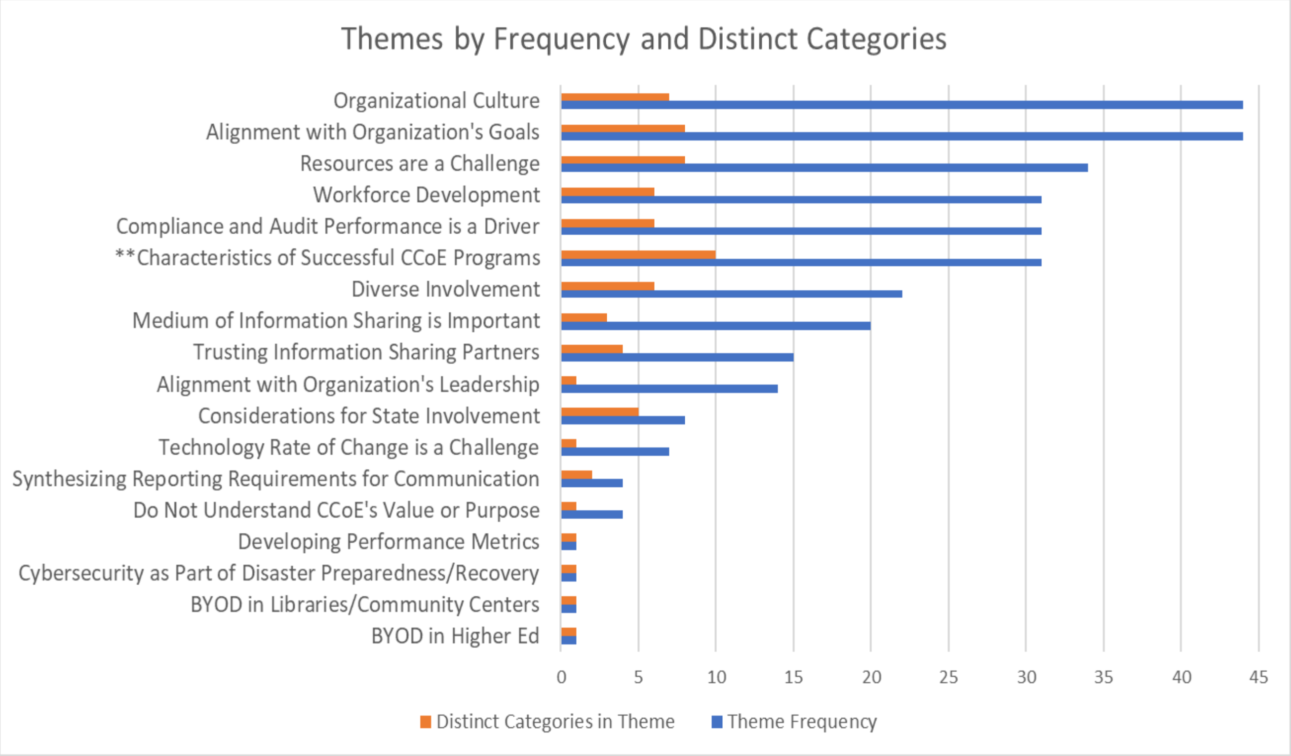
[363] Yin, chpt. 9.

[364] Karen Kurasaki, "Intercoder Reliability for Validating Conclusions Drawn from Open-Ended Interview Data," *Field Methods* 12, no. 3 (2000): 179-194.

[365] Saldana, pg. 14.

THEMES FROM FOCUS GROUPS

Through the coding, categorization, and the final identification of overarching themes as described above, the focus group data set contained more than 200 identifiable codes that were reorganized into 68 different categories that correspond to 18 distinct themes. While this number of themes is higher than the typical qualitative research project, there is no standardized number of codes, categories, or themes to identify and assign.[366] Additionally, the purpose of these focus groups exceeds the scope of typical qualitative research projects by including a collaborative component, and prioritizing diversity rather than homogeneity when selecting participants. The graph below shows the number of distinct categories in each theme, indicating the breadth and differences in ideas from all focus group sessions that make up that overarching theme. The "Characteristics of Successful CCoE Programs" theme is associated with the most distinct categories (10), while several categories did not fit well in broader themes, and thus became a single-category theme (see especially the bottom of the graph for these themes).



[366] Johnny Saldana, pg. 24.

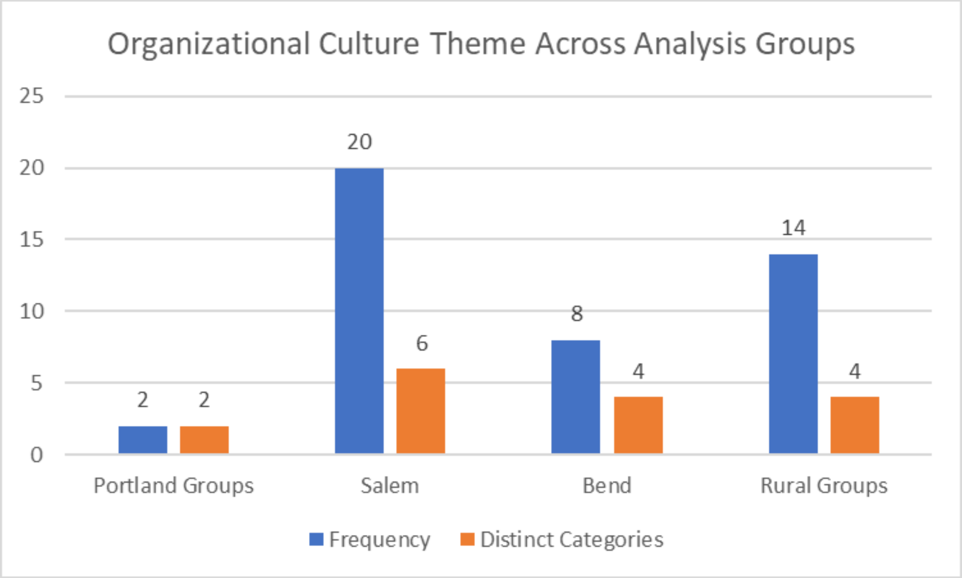
The graph also indicates the frequency of each theme across focus group sessions. These frequencies were determined by giving each category within the theme a score of high, medium, or low (corresponding to a frequency of 5, 3, or 1) for each analysis group. These scores are based on the number of codes in each category for that analysis group, the time spent on conversations relevant to that category, and the number of participants included in those conversations. Researchers involved in the coding process agreed on these frequency assignments as part of the intercoder reliability process.

Both the breadth and depth of these themes are of interpretive value. Those themes with low numbers of distinct categories but high frequency generally indicate greater consensus within those themes. For example, the Alignment with Organization's Leadership theme encompasses participants concerns regarding their organizations' executive-level leadership understanding, prioritizing, and providing resources for cybersecurity. These concerns were similar across all discussions, and therefore fit into a single category that ultimately became its own theme. These concerns also occurred relatively frequently, resulting in a higher frequency value for this theme than other one-category themes in the dataset. This indicates a greater degree of agreement among focus group participants regarding this theme than some other themes with more wide-ranging discussion that encompasses more categories. The Considerations for State Involvement theme illustrates this, as this theme has more distinct categories (5), but was also less frequently discussed over the course of the focus groups. It can be concluded that Alignment with Organization's Leadership has more cross-participant agreement than the Considerations for State Involvement theme.

The meanings, categories, and frequencies of each theme are presented and analyzed below. Key quotes from focus group participants that exemplify the meanings and categories of each theme are also included at the end of each theme's discussion.

Organizational Culture

Organizational Culture was one of the two most frequent themes in focus group sessions, with a frequency "score" of 44. This theme was discussed in all analysis groups, though it was a less frequent and less wide-ranging discussion in Portland-area sessions. The number of distinct categories and frequencies in each analysis group are shown in the graph below.



Seven total categories are represented within this theme. The *"human firewall"* category was initially an in vivo code from the focus group data set, meaning that this exact phrase was used by participants to describe an idea; interestingly, this phrase was used in different focus groups and by participants from different industries, showing that this phrase has meaning across a variety of geographical and industry contexts. This category encompasses ideas about organizations' staff and human resources serving as a metaphorical firewall or gatekeeper for the organizations' technologies, systems, and data. Participants also positively used this category, with most either describing their organization's human firewall as a point of pride, or talking about creating and supporting programs or systems that would allow their organization's end users to function in this capacity. This category overlapped with the *"culture of security"* category, which more generally indicates that conversations included participants' assessments of their organization's orientation toward security more broadly. This category was most often invoked as part of participants' responses to the first question of the focus group protocol. Those who felt their organization could improve cybersecurity tended to speak of the "culture of security" negatively, while those that felt their organizations have a positive security culture tended to talk more about the importance of maintaining that culture.

Cybersecurity was also considered relative to other organizational or cultural values in the themes of *"tradeoff between security and flexibility" and "tradeoff between security and other organization priorities."* Cybersecurity in organizations is seen as a zero-sum tradeoff with flexibility according to focus group participants; organizations weigh their preferences for flexibility directly against any cybersecurity programs, technologies, or other kinds of improvements. Participants also mentioned that many organizations consider cybersecurity in the same way that they consider priorities like equity, diversity, accessibility, and other values that are not necessarily related directly to the mission and purpose of the organization. These categories both attest to the importance of an organization's prioritization of cybersecurity within a broader set of values as determinative of cybersecurity posture.

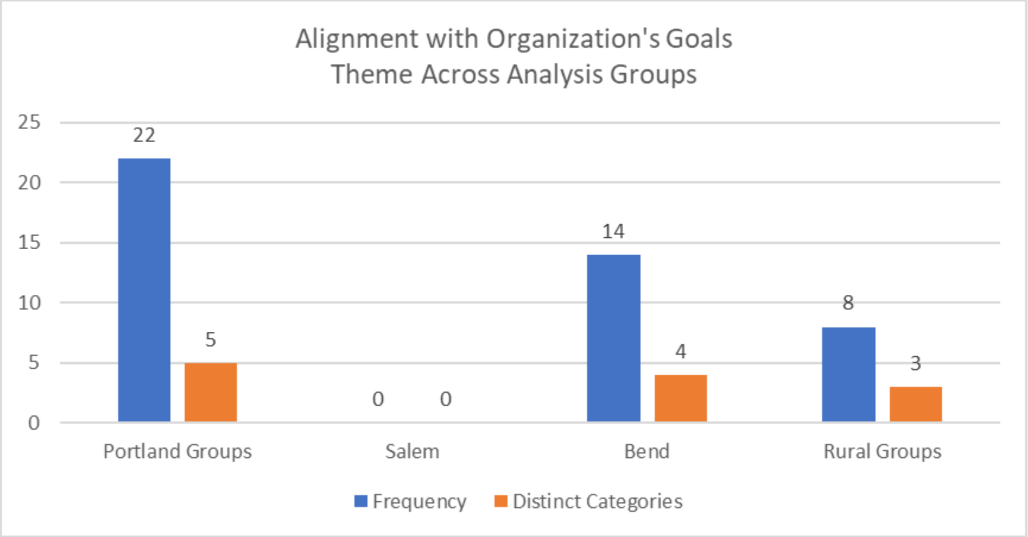
Other categories in this theme included: reactive posture for cybersecurity (or cybersecurity playing a limited role in organizational culture until a focusing event occurs), internal trust (meaning trust between organizations' end users and cybersecurity staff), and generational gap is a challenge. This final category was brought up by participants of different ages, genders, and from different industries; all commented that there were particular considerations regarding cybersecurity that needed to be made for older workers, and especially those nearing retirement. Two key quotes from participants sum up the key aspects of this theme nicely:

> *"The problem is the user." – Salem, Government industry participant*
>
> *"Everyone is on the security team, whether you think you are or not." – Portland, Government industry participant*

Alignment with Organization's Goals

Focus group participants were especially concerned with the alignment between their organizations' overall goals and cybersecurity. This theme was closely related to both the Organizational Culture theme discussed above and the Resources are a Challenge theme discussed next; as indicated by the data collected from focus group participants, these themes when taken together effectively encapsulate the majority of the negative, distressing, and problematic aspects of organizations' relationships to effective cybersecurity.

Categories in this theme included Awareness is a Challenge (participants expressed that their organizations' decision makers may not be aware of the role cybersecurity plays in achieving or derailing the organizations' goals), Partnering with Business (participants stated that requests for cybersecurity resources were more likely to be successful when partnering with existing business initiatives), and Making the Business Case (cybersecurity efforts that could be expressed and justified in typical business terminology found more success and received better reactions from decision makers and executives in participants' organizations).



The Salem focus group is the outlier in terms of this theme, and the only analysis group (and focus group session) that did not discuss cybersecurity alignment with goals. Though a definitive explanation for this difference is not possible without further study, one hypothesis for consideration is the high proportion of government participants in this group, and a potential for differences in goal alignment that is a result of industry characteristics. This may also account for some of the overlap between categories in this theme and categories in the Compliance and Audit Performance as Drivers theme, which did feature prominently in the Salem focus group session's discussion. Especially where compliance and audit performance are foundational parts of the organization's goals, the categorization of these concepts depends heavily on the way this idea is expressed in the focus group session. This overlap was observed and categorized under both themes in the Portland Groups analysis group and the Bend analysis group, but was not in the Salem analysis group, indicating a possible difference in language that could be further probed in follow-up research.

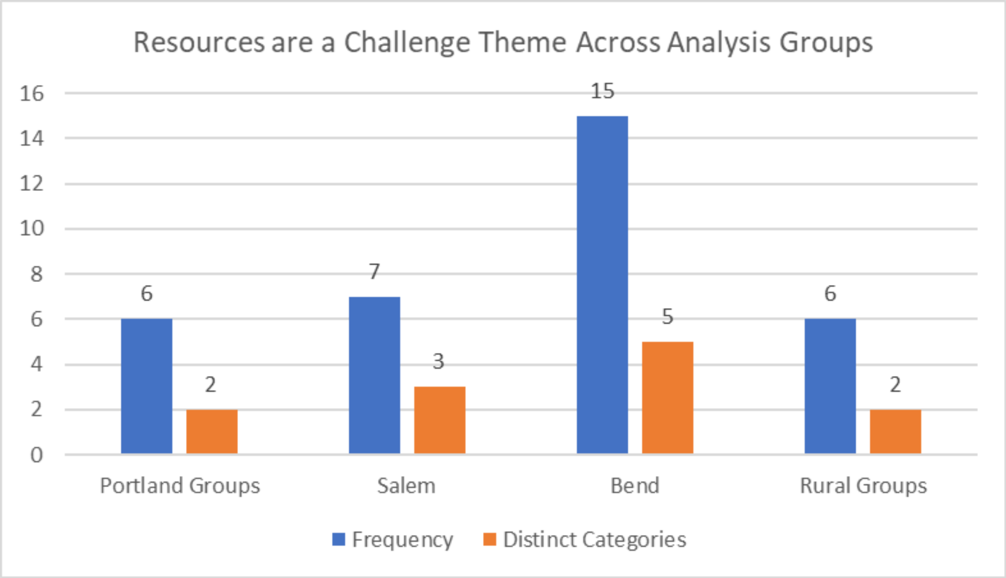
Key quotes from the data show the difficulty of aligning cybersecurity with organizational goals, but also indicate that participants are hopeful for the future in this regard:

> *"What makes cybersecurity unique is you see everything in the business. You're uniquely positioned to help the business." – Portland, Information Technology and Telecommunications industry*

> *"Not a lot of effort at every level, not everyone is working in the same direction." – Bend, Professional Services industry*
>
> *"[A barrier is] the basic understanding and knowledge of how cyber events can hurt an organization." – Rural Groups, Government industry*

Resources are a Challenge

The vast majority of participants identified resources as a challenge for cybersecurity in their organizations, which accounts for this theme being a frequent part of conversations in all analysis groups. However, this theme was especially prevalent in the Bend focus group, which saw both the greatest diversity in resource topics covered, as well the highest frequency of discussion around resource challenges relative to other topics.

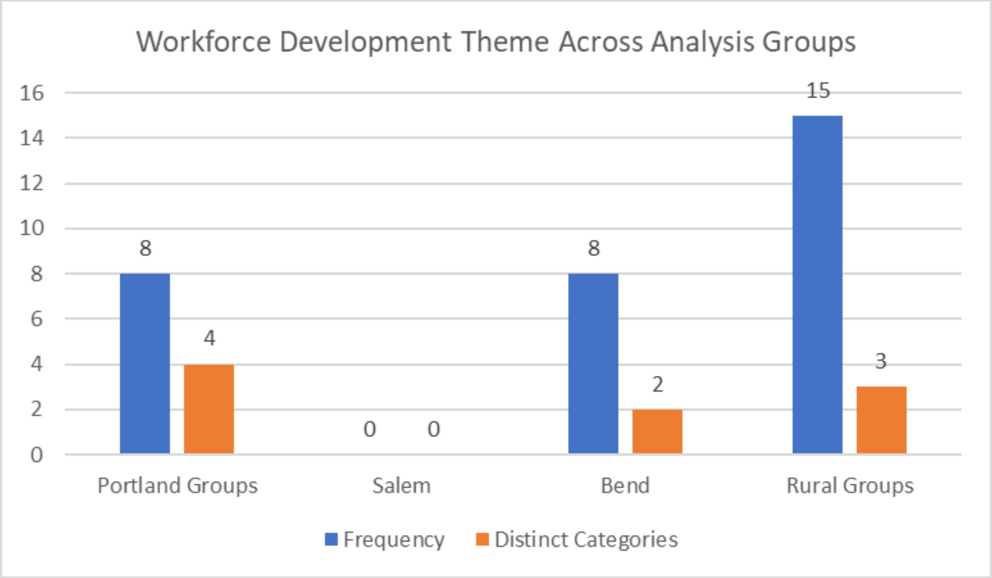


This theme includes the broad category of "resource challenges," to which non-specific lamentations by participants regarding the availability of resources for addressing cybersecurity were attributed. There are other more specific categories in this theme, including: creating training programs is burdensome on cybersecurity staff, cybersecurity and data insurance is cost prohibitive, and difficulty finding appropriate vendors and programs. Several participants noted that specific types of organizations are especially resource challenged, whether those participants were actually part of those organizations or not; the categories "public-sector-specific pay level issue" and "smaller organizations need more help" show wide recognition among participants that small organizations and public organizations have more difficulty with resource issues than many others. Finally, the category "lack of local resources" was especially prominent in the Bend and Rural Groups analysis groups, as participants in both of these settings recognized that resource issues may be partially due to the difficulty of accessing resources (talent and expertise in particular) outside of the Portland-metro area. Three key quotes exemplify this theme in the focus group discussions:

> *"It's expensive to do this right." – Bend, Healthcare and Medical industry*
>
> *"A big barrier [to improving cybersecurity] is expertise." - Rural Groups, Education industry*
>
> *"It's hard to articulate [resource need] when you're making stuff go away behind the scenes." – Portland, Finance/Banking/Insurance industry*

Workforce Development

Workforce development as a theme featured pervasively in most conversations regarding potential CCoE activities and programs; Salem was the sole exception to this observation. Surprisingly, much of the conversation around workforce development focused on the importance of K-12 education programs and other methods to introduce school-aged children to the cybersecurity field. The category of "Cybersecurity in K-12 Education" was the most prevalent within this theme. Other important categories within this theme included curriculum development (for both K-12 and higher-ed programs, as well as incorporating cybersecurity principles into non-technical degree programs), "Workforce Pipeline" and "Incentivizing Talent to Stay in Oregon" (or finding ways to maximize the number of Oregon graduates transitioning in to cybersecurity jobs in Oregon), and "Barriers to Becoming Cybersecurity Instructors" (the perception of some participants that teaching credential requirements keep cybersecurity experts from being able to educate in formal settings).



Another category that was particularly important in the Rural Groups analysis group was the “Incentivize Talent to Non-Metro Areas” category. Here, participants expressed concern that it is difficult to attract cybersecurity talent of any experience level to areas of Oregon outside of the Portland-metro area. This was usually paired with suggestions or requests for resources that could create or sustain such incentives.

It is important to note that Workforce Development was included in the facilitator-provided handout on CCoE functions that the facilitator in each group distributed to all participants as part of the focus group protocol, and this may contribute to this theme’s prevalence in focus group discussion. While workforce development was a theme of early conversations in some focus groups, it became a more dominant part of conversations following the distribution of this handout. Unfortunately, the effects of the distribution of this handout on the presence of Workforce Development as a theme in focus group conversations cannot be fully established. Even with this potential caveat to the Workforce Development frequency findings, the breadth of the conversation and its perceived importance to participants can be gaged by three participant quotes:

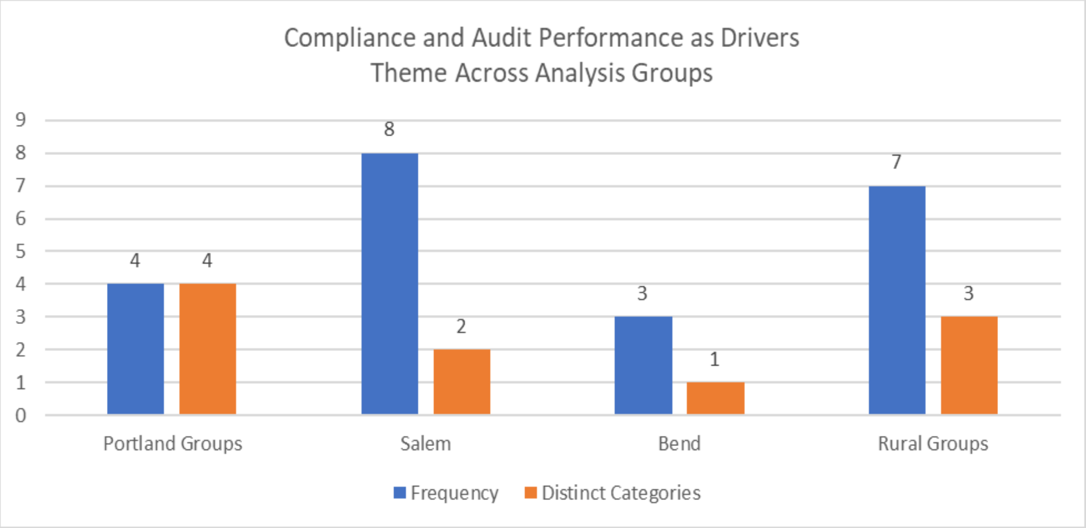
> *“If [the CCoE] only delivered workforce development, that would be an enormous leap forward.” – Portland, Information Technology and Telecommunications industry*

> *“If [the CCoE] can incentivize those people not to leave the state, business will come here to get that talent.” – Bend, Healthcare and Medical industry*

> *"The other piece is people that are already in the field, helping them continue their learning and growth." – Rural Groups, Government industry*

Compliance and Audit Performance as Drivers

Across all analysis groups, participants indicated that their organizations predominantly make investments and improvements to cybersecurity technologies, systems, and processes in response to either industry or legal requirements and standards, or in response to audit performance or experiencing a cybersecurity incident. Categories in this theme include: compliance as a cybersecurity driver; audit performance as a cybersecurity driver; and security event as a driver.



A Healthcare and Medical industry participant also indicated that the standards themselves pose a challenge to cybersecurity implementation; this sentiment seemed to be unique to the healthcare industry and was only mentioned in a single focus group session. Additionally, several Education industry participants brought up privacy as a related driver of cybersecurity action that is not quite synonymous with cybersecurity itself, leading to the category of "Privacy as Related by Separate." Based on the overall body of focus group data, these categories seem to be somewhat isolated to these specific industries.

Three key quotes from focus group participants embody the broader issues represented by this theme:

> *"We have to pay for people to show our weak points so that we can show our upper management that we need to remediate." – Bend, Healthcare and Medical industry*
>
> *"Without audits, the city would not have invested [in cybersecurity upgrades]." – Rural Groups, Local Government*
>
> *"[Cybersecurity is a] really difficult cost to justify outside of 'we have to do that.'" – Portland, AMTUC industry*

Characteristics of Successful CCoE Programs

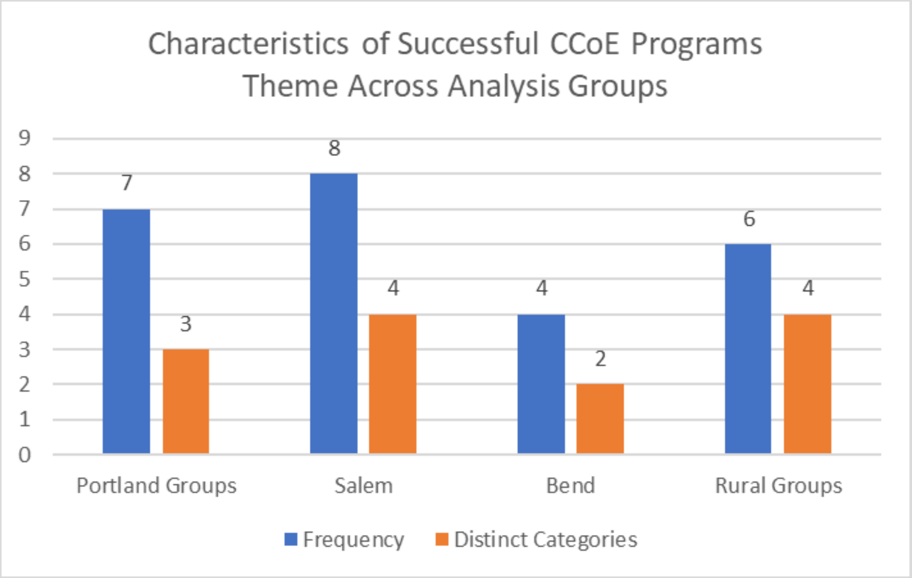
The "Characteristics of Successful CCoE Programs" theme differs from others because of its direct relationship to a question in the focus group protocol. Participants were asked to respond to the prompt: "Is there anything specific that is essential to the success of an Oregon Cybersecurity Center of Excellence?" Many of the responses to this question related to other topics that came up in course of each focus group conversations; those topics have been categorized and applied to themes elsewhere. This theme incorporates the remaining key characteristics for success that arose from the conversations.

The following categories, each of which encompasses a characteristic of a successful CCoE according to participants, are associated with this theme:

- *Actionable Programs:* Participants stressed that any CCoE activities needed to involve taking a tangible action rather than just providing information.
- *Addressing Resource Challenges through State Buying Power:* Participants that indicated their organizations had limited resources for cybersecurity investments were especially interested in the possibility of state-wide IT goods and services agreements.
- *Clear and Transparent Leadership of CCoE: Knowing* who is making decisions for the CCoE (as well as how and why) was brought up by several participants in response to the prompt.
- *Entertaining Initiatives:* Two participants specifically mentioned that CCoE activities should include an entertainment factor, such as humorous instructive videos or collaborations with artists for inforgraphics.
- *Executive Engagement with CCoE:* Many participants said that the success of the CCoE depends on its ability to effectively engage executive-level leadership in organizations.

- *Narrow Initial Focus to Show Success:* Included in this category were codes regarding "proof of concept" and "initial victories", with a caution that CCoE success depends on following through on initial plans and initiatives.
- *Need for Bipartisan Support at All Levels:* Concerns about the CCoE becoming too political an endeavor were mentioned by a couple of focus group participants, as was the need for widespread support across all political persuasions to ensure ongoing funding.
- *Vendor/Technology Agnostic:* Participants were concerned that the CCoE would either become a sales pitch and/or tool, or that dependencies on specific technologies would lead to premature obsolescence; ensuring vendor/technology agnosticism was the participant-provided method to prevent this and ensure CCoE success.

The diversity of the categories in this theme indicates the breadth of conversations that took place in response to the facilitator's question, which also likely accounts for the frequency levels of this theme in each analysis group. The prevalence of this theme is not necessarily indicative of consensus among participants regarding the categories and ideas that are included within this theme.

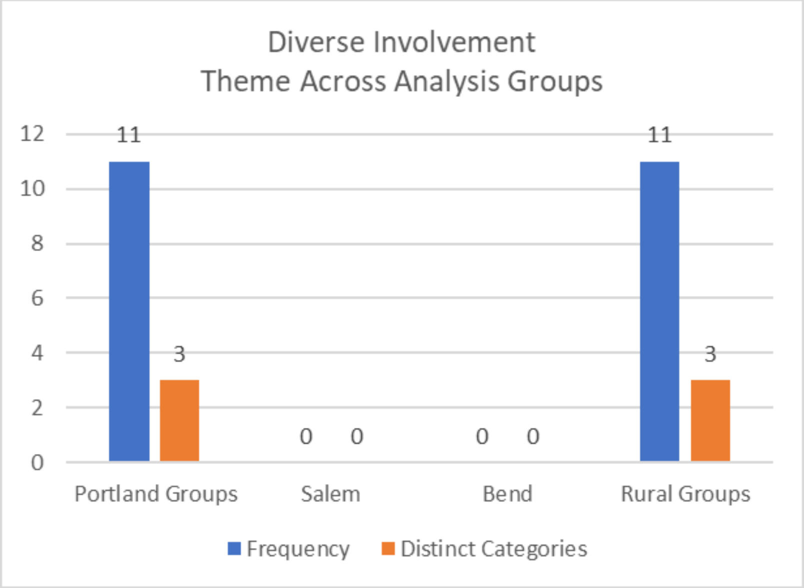


A key participant quote that exemplifies the sentiments of this theme as expressed in the focus groups comes from a Finance/Banking/Insurance industry participant in the Salem:

> *"…if I'm going to be involved – [I won't be] if it's a meeting, vote on this measure, elect this person. I want to come, contribute to something that will help other people, and bring something back to my business that is moving us all forward."*

Diverse Involvement

The Diverse Involvement theme captures participants' statements regarding the need for statewide cybersecurity initiatives to take a broad and inclusive approach. Diversity in this theme primarily refers to organization size, industry, and location. The Smaller Organizations Benefit the Most category includes observations made by participants from both small and large organizations that those with limited resources and staff stand to benefit the most from a statewide cybersecurity initiative. The Geographic Diversity and Access Limitations Outside I-5 Corridor categories indicate that participants were especially concerned that activities either take place in, or otherwise reach, areas outside of Portland and Salem. Participants also noted that a statewide cybersecurity initiative needs multi-industry events, programs, and activities; this sentiment broadly makes up the Need for Sector Diversity category in this theme.



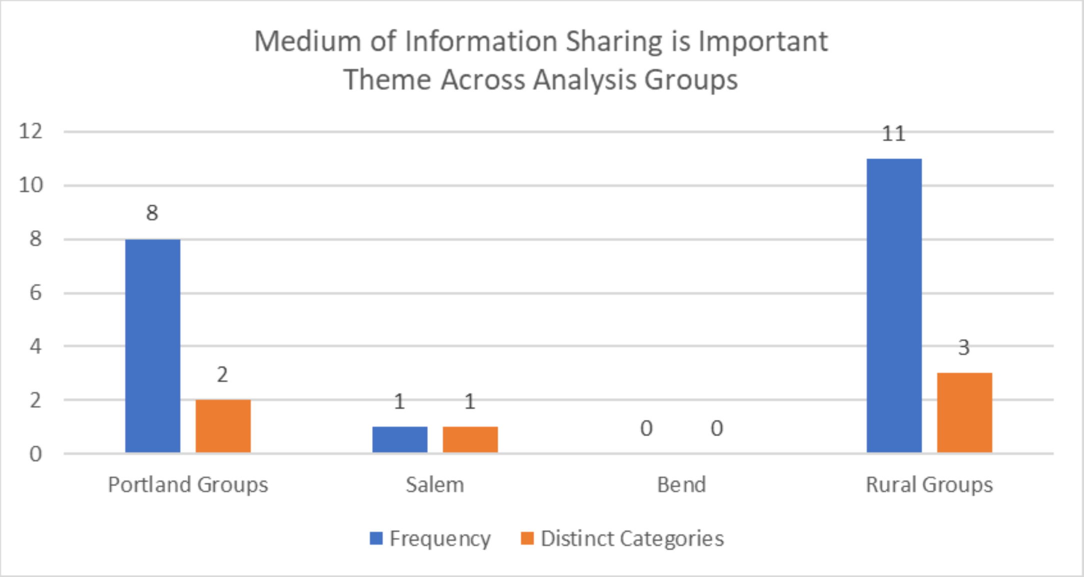
Of greatest interest to the research team is the geographical location of this theme. It is surprising that the biggest population center in Oregon was also equally as vocal about providing services outside of the Portland-Metro area. This shows a level of self-awareness about the kinds of opportunities that the CCoE might be able to provide, as well as a willingness of those who may not directly benefit from those opportunities to support them in the interest of serving the broader public. Further probing of this sentiment may be value for decision makers as planning for the CCoE moves forward.

Some reflections from focus group participants on the kinds of diversity that might be beneficial for the CCoE, as well as cybersecurity in Oregon more broadly:

> *"Small businesses are really where the impact is." – Portland, Financial/Banking/Insurance industry*
>
> *"Has to be outside the population centers." – Portland, Information Technology and Telecommunications industry*
>
> *"It seems like everything is in Portland or Salem. We need something that's more centrally located." – Rural Groups, Government industry*
>
> *"From our perspective, having a good broad group… making sure there are people from different sectors, not just State and education. All levels, state, local, public, private, educational, etc. Different expertise, too." – Rural Groups, Government industry*

Medium of Information Sharing is Important

A variety of participants expressed concern that any statewide initiatives focus not just on the content of the information being shared, but the method by which that information is shared. However, the concerns were markedly different in regard to the role of creating websites and online forums for information sharing. Three categories make up this theme. First, participants of all three analysis groups that discussed topics related to this theme agreed that Face-to-Face Sharing is Important. One of the Portland-based groups was so enthusiastic about multi-sector meet-ups to discuss cybersecurity that a majority of the participants stayed after the scheduled conclusion of the group to continue the discussion and exchange business cards amongst themselves. Rural groups were also enthusiastic about any and all opportunities to meet in person with other cybersecurity professionals regardless of the context; several participants mentioned how grateful they were that researchers were willing to travel to talk to them, and asked about any similar upcoming events. Related to this first category is an important second: Information Sharing Through Conversations and Conferences. There was widespread interest among participants in educational and information-sharing events that cover content that is applicable across industries; Portland participants noted that events that did not involve sales pitches from vendors are especially of interest to them. These two categories together make up the bulk of the Medium of Information Sharing is Important theme.



The third category that had less agreement across analysis groups is Online Information Sharing is Done Already. Portland participants generally noted that online information sources are already sufficient for their needs and they were not interested in “another website”; as one participant stated, there are “lots of places for information already… most of us are geeks, we know how to internet.” Rural Group participants, in contrast, were keen on increasing the availability of online content from trustworthy sources. In particular, the ability to access information remotely without needing to access a population center was an expressed need and/or desire. It seems, then, that the utility of creating online information resources for cybersecurity in Oregon is higher for those in locations outside of the I5 corridor, but significantly lower for those in the Portland-metro area.

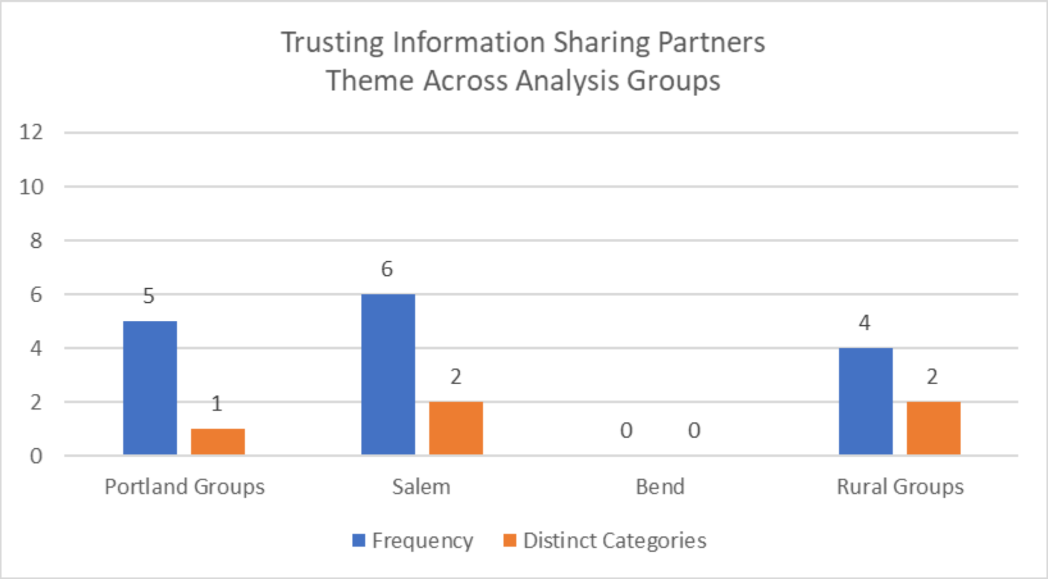
Participants’ thoughts on this theme are best summarized by the following statements:

> *“I’d like to see more of a peer meetup. Those types of lessons, it would take me a year to write it up on LinkedIn and people would get bored. IN a peer services group, those things could have a lot of value.” – Portland, Healthcare and Medical industry*

> *"It would be nice if there were more [events] in Bend, Central Oregon… like a yearly kind of thing, or twice a year." – Rural Groups, Healthcare and Medical industry*
>
> *"Having a centralized point of information would be huge. I have to go out and scour and see how to mitigate these threats. If it weren't for the internet there would be no way to know. I was really excited to hear [other participants] talking about a centralized portal." – Rural Groups, Government industry*

Trusting Information Sharing Partners

The Trusting Information Sharing Partners theme reflects a concern that often came up in conjunction with the Medium of Information Sharing is Important theme discussed previously and the Considerations for State Involvement theme discussed later in this chpater. Before participating in any statewide initiative that involves sharing information or experiences, participants in most analysis groups expressed a need for assurances of the trustworthiness of those with whom they'd be expected to share. Many expressed a desire for formalized arrangements to ensure a certain level of care with potentially sensitive disclosures before taking part. These concerns were categorized as Trust through Formal Arrangements. A related category, Legitimacy of Information Sharers/Sources, reflects a complementary need for some attestation to the knowledge and expertise of those involved in information sharing arrangements; one participant from the Rural Groups analysis group suggested an application process monitored by experts on the Cybersecurity Advisory Council to ensure that participants have relevant experience and/or credentials.



Focus group participants were also concerned that state involvement would necessitate state action in any sort of information sharing arrangement. One participant expressed trepidation about asking for or sharing information if it could lead to punitive action against them. However, with formalized confidentiality processes and procedures, that participant expressed confidence that a CCoE could facilitate effective information sharing that they would be comfortable participating in. A final category that only received mention in the Rural Groups was Information Sharing Among Legacy Systems Operators. These participants expressed a desire to have information sharing facilitated among verified operators and maintainers of legacy systems that may require specialized expertise, and indicated that it can be difficult to find trustworthy information on these kinds of systems.

Several participants' own words provide greater insight into this theme:

> *"One of the things that makes ISAC work is the confidentiality." – Salem, Education industry*

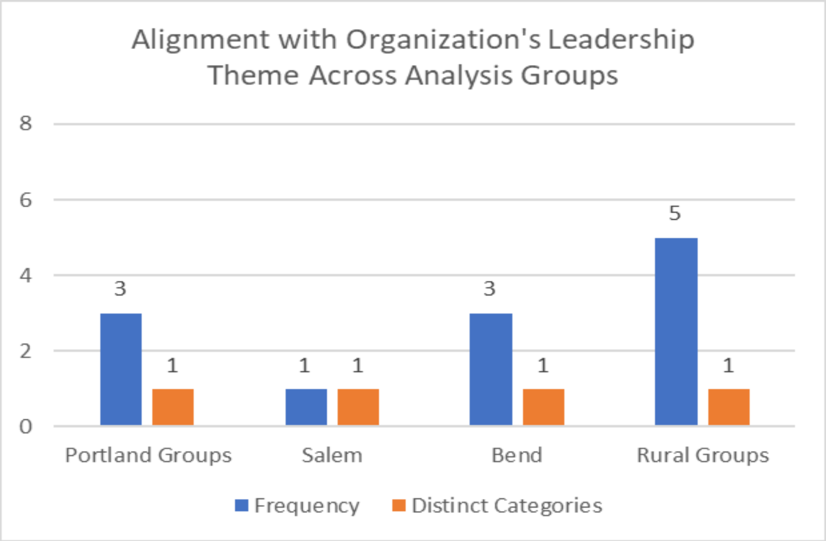
> *"I don't think this center should be open to the public. I think you should have to apply. That gets rid of the junk, spamming, trivial fighting… it can be hard to get relevant information." – Rural Groups, Government industry*

> *"[Any website] needs to be a credentialed site." – Rural Groups, Healthcare and Medical industry*

> *"Stance needs to be partnering, not punitive. If it becomes too 'state-y', that would be a deterrent." – Salem, Government industry*

Alignment with Organizational Leadership

Alignment with Organizational Leadership represents a theme with a single category but a fair amount of agreement among participants; this theme therefore plays a substantial role in the data of three of the four analysis groups, and a lesser role in the Salem focus group session. This theme also shows the importance of considering both the number of categories and frequency of the theme's occurrence in the data, as only looking at the breadth of categories contained in this theme would make it seem deceptively unimportant.



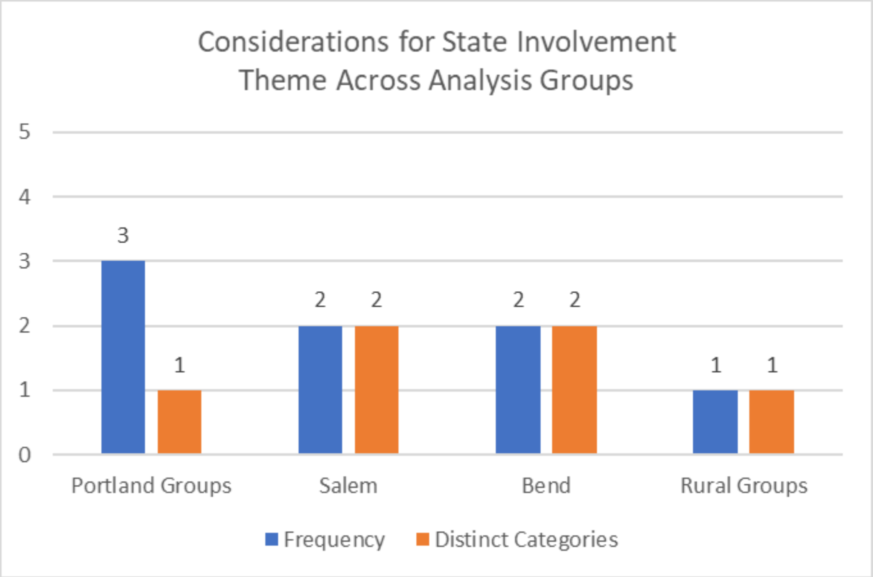
This theme contains all mentions of conflict or indifference between executive-level leadership and cybersecurity needs, staff, and initiatives. Several participants did report that their organization's leadership was supportive or even proactive regarding cybersecurity; there was no discernable pattern in terms of industries or geographies in which these participants work. However, the majority of participants indicated that executive-level leadership is an ongoing pain point for cybersecurity staff in their organizations. Most did not attribute this to any malicious intent on the part of executives, instead pointing to either a lack of knowledge and understanding, or a prioritization of other business goals and initiatives over cybersecurity. Many also reported that cybersecurity, and often IT in general, is not represented by a position at the executive level, unlike other administrative or supporting operational units (finance, human resources, etc.).

These concerns are best reflected in these examples from participants:

> *"Until [upper management/executives] see someone get their finger stuck in the light socket, they don't understand." – Bend, Healthcare and Medical industry*
>
> *"[I] need a way to reach the decision makers so they understand how important [cybersecurity] is." – Bend, Government industry*
>
> *"If you want security to move forward, you need a voice at the big table to share the resources required… if you want good cybersecurity, have to start from the board down." – Rural Groups, Healthcare and Medical industry*
>
> *"You can't talk to C-level as security, but as business leaders." – Portland, Finance/Banking/Insurance industry*

Considerations for State Involvement

Potential ramifications of the role of state government in a CCoE were of particular concern for several participants across all analysis groups, though this particular theme was not very frequently discussed overall. These concerns were both positive and negative, with some participants skeptical of the ability of state government to contribute positively to a broad cybersecurity effort like the CCoE, and others firmly in favor of state involvement.



Those participants that were concerned about state involvement made statements that were best organized into categories of Concerns about State Acting Efficiently and Removing Cybersecurity from Political Context. The code “red tape” was identified as part of the first category, while politicization and elections were mentioned in the latter. Other participants thought the state could lend credibility to a broad CCoE effort, leading to categories of State Can Require Compliance and State Can Consolidate Information in a Trusted Way. These participants essentially invoked the unique ability of the state to act as a convener for information sources, and the ability of the state to potentially create an environment that mandates cybersecurity efforts, as valuable contributions to this effort. Finally, a participant noted that state involvement would require decision makers to consider effective ways to Reconcile Conflict Between Public Initiatives and Private Industry (a fifth category in this theme), though this was discussed only as something to consider, and not necessarily a positive or negative aspect of state involvement.

Quotes that exhibit the breadth of the categories in the general theme of Considerations for State Involvement are:

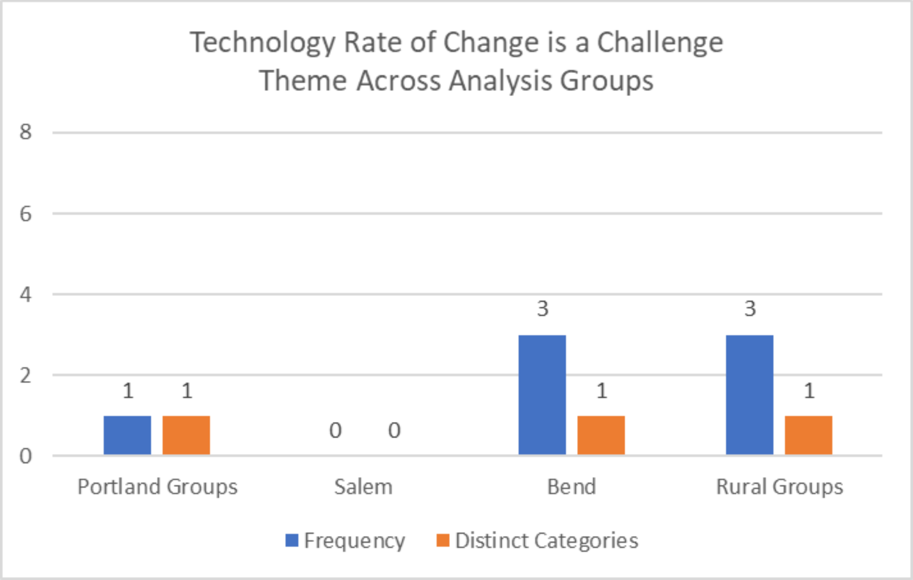
> *“I don’t want to be negative, but if it’s state employees doing this, no. It’ll be too much red tape.” – Portland, Education industry*

> *“The problem I see: the business sector is going to complain, you’re taking away from my profit. Anytime government tries to give something to the citizens, business complains.” – Salem, Government industry*

> *"It'd be good if the health of the state was involved, if it were mandated that a certain level of [cybersecurity] was part of organizations." – Bend, Government industry*

Technology Rate of Change is a Challenge

Several participants indicated that the rate of change in the information technology industry, and more specifically the cybersecurity industry, makes it difficult for their organizations to keep technologies, systems, and processes up-to-date. This theme was often mentioned concurrently with the Resources are a Challenge theme, as those who felt they lacked sufficient resources often indicated that this lead to an inability to research and remain sufficiently informed. This theme was discussed most in Bend and the Rural Groups, but was also mentioned in Portland Groups to a lesser extent.



Two key quotes from participants that capture the essence of this theme include:

> *"In this business, if you don't stay up for 6 months, you're irrelevant." – Rural Groups, Government industry*

> *"It's hard with how fast cybersecurity is booming to have local resources." – Rural Groups, Government industry*

Low-Frequency Themes

The remaining themes are considered low-frequency themes, in that they had both a low number of distinct categories and were infrequently discussed by groups. Often these categories and themes were only mentioned by a single participant in a single focus group, but did not completely fit in any of the other themes already discussed. Each is briefly considered below.

Synthesizing Reporting Requirements for Communication

Three participants were enthusiastic about a potential synthesis of information and reporting requirements for organizations that are subject to multiple standards and regulations. One Salem participant told a story about a situation arising in a previous work situation in which leadership and staff couldn't decipher the correct course of action; this was followed by the suggestion that "a guide that simplifies your obligations for your sector and place… including crossover between HIPAA and FERPA" would be a useful tool. A Rural Group participant mentioned that they simply do not have time to monitor the changing laws and regulations, and that communicating any changes would be a desired activity for a CCoE to undertake.

Do Not Understand CCoE's Value or Purpose

Two participants specifically raised questions about the CCoE's purpose, saying they were both unsure of what the goals and objectives of the CCoE would be, and that they didn't understand why a state-level CCoE was desirable (as compared to a local- or federal-level CCoE). Questions were also raised about how a CCoE would differ from a Fusion center, or other such programs that participants had experience with at primarily the federal level. As one participant stated, "I've been tracking SB90 for a while, there's been no explanation from the State Chief Information Officer of what exactly the entity is supposed to do." The clear implication of this theme is that goals and objectives of the CCoE need to be clearly defined and communicated through a collaborative process.

Cybersecurity as Part of Disaster Preparedness/Recovery

One participant in the Rural Groups mentioned concerns about cybersecurity and the resilience of critical infrastructure in the face of either natural or man-made disasters; another participant mentioned that the IT department is involved in drills and disaster simulations. This was the only brief conversation in the entire focus group dataset in which focus group participants considered cybersecurity from an emergency management point of view.

Developing Performance Metrics

A Salem focus group participant from the Education industry expressed interest in the development of "metrics that give you an idea for how your organization is doing overall… if there's additional stuff specific to Oregon, that would be great." Other participants in that same group mentioned that auditing organizations and compliance requirements essentially provide this service; the discussion of metrics for gaging cybersecurity performance never arose in other focus groups.

BYOD in Higher Ed and BYOD in Libraries/Community Centers

Two focus group participants wanted to discuss bring-your-own-device (or BYOD) policies, but the issues they described were more specific to their particular industries and didn't gain much traction with the rest of the focus group participants in their sessions. This is one particular instance where there seem to be marked differences between industries, and even within industries when considering the unique needs of institutions of higher education (with residential, educational, and medical components). While this topic was clearly of importance to the focus group participants that brought it up, it remained a low-frequency theme with limited discussion overall.

SPECIFIC IDEAS FOR CCOE PROGRAMS AND POLICIES FROM FOCUS GROUP PARTICIPANTS

Beyond the codes, categories, and themes identified in the analysis process, the research team also compiled the long list of ideas for programs and activities brainstormed by focus group participants. This brainstorming happened as a direct result of the prompt: "What activities or programs can you think of that a Cybersecurity Center of Excellence could undertake to be most beneficial to an organization like yours?" In total, participants across all focus groups generated 52 unique ideas (5 suggestions were received twice in different focus groups; these are denoted with an asterisk) for ways that the CCoE could positively impact their organizations. Due to the brevity of the focus group sessions, these ideas are not fully developed into actionable plans, but they do provide some insight into the kinds of activities, programs, and services that participants think would benefit their organizations given the broad parameters of the CCoE's functions outlined in SB90. These suggestions are grouped into eight categories in the table below:

Non-Technical Employees and End User Training – Employee training with testing and validation of completion* – General cybersecurity education for middle/executive management – Sector-specific cybersecurity education for C-level executives – Ready-made educational materials and programs for non-IT employee training – Mandatory cyber hygiene training for employees in non-technical positions – Cybersecurity content for vulnerable end-user populations	***Best Practices and Resource Documentation*** – Easy-to-follow cybersecurity templates – Standardized metrics for cybersecurity performance measurement – Guide to incident reporting and response obligations – Checklist of cybersecurity tools based on organization type – Central information-sharing hub – Central best practices hub* – Oregon-specific information library – Unified cybersecurity requirements at the state level
Cybersecurity Services – Weekly/monthly external security checks – Tools for PEN testing (by users) – Free PEN tests (by CCoE) – National-Guard-type cybersecurity service program (1 weekend per month) – Attorney General/legal 'hotline' for advice regarding mandatory reporting and notification requirements – Cybersecurity social engineering exercises – Forensic teams for incident response – Cybersecurity SWAT team or deployable incident response team – Subscription-based cybersecurity services and strategy consulting	***Events and Inter-Personal Collaboration*** – Mentoring program (pairing large organizations with smaller organizations) – Informal peer exchange events ('every two weeks over beers') – Learning webinars on specific topics – Yearly or twice-yearly conference for Oregon CS professionals – In-person events focused on specific cybersecurity issues – Best practices sharing through roundtables – Online forum for issue solutions – Connecting legacy system operators for information sharing
Procurement and Purchasing Assistance – State-based pricing for vendor contracts – Approved product list – Collective procurement for small organizations – Co-op/partnership pricing on goods and services	***K-12 Education*** – Cybersecurity in K-12 curriculum* – Cyber hygiene in K-12 curriculum – Afterschool cybersecurity clubs (similar to robotics teams)
Awareness – General cybersecurity outreach – PR/public service announcements regarding major cybersecurity events and imminent threats – Cybersecurity alerts on social media – Recognizing CCoE-participating organizations publicly – Reward/incentive program for cybersecurity performance – Cybersecurity as part of disaster response and recovery simulations	***Workforce Development*** – Cybersecurity as mandatory part of CS and IT degree programs* – Post-degree or post-certification workforce training and internships – Create access to cybersecurity professionals without teaching credentials in classrooms at all levels* – Online/virtual classrooms for students and current workforce – Mandatory cyber hygiene training for all Oregon higher-education students (regardless of degree type)

	– Bring national trainings and certification programs to Oregon – Scholarships for CyberCorps program – Credentialing program for Oregon cybersecurity practitioners

This list shows that focus group participants were generally enthusiastic about the possibility of a statewide initiative that could tackle some (or all) of these activities. Additionally, participants saw these activities as fulfilling the broad functions outlined for the CCoE in SB90. Together, this indicates that there are myriad ways to create a CCoE that adds value to Oregon's cybersecurity landscape and that, given a chance, participants in collaborative discussions like these focus groups can generate lists of innovative and wide-ranging programming that CCoE decision makers can consider.

DISCUSSION AND CONCLUSIONS

The focus group data provides an interesting look in the perspectives of IT and cybersecurity professionals in all sizes and types of Oregon organizations, located throughout the state. While all of this data is valuable to consider as the CCoE proposal process moves forward, there were several key aspects of these focus group discussions that warrant consideration for future interactions through these types of collaborative processes.

First, conversations around themes of organizational culture, goals, leadership, and resources are often intertwined. The coding of these ideas and concepts was a difficult analytical task, as participants often responded to prompts (and each other) with thoughts that covered all of these categories to some extent. The data indicates that many participants equate issues with one of these themes with all of them; a resource problem is also an organizational culture and leadership problem, and vice versa. Participants should not be expected to make distinctions between these concepts in the short timeframe of a focus group or brainstorming session. However, these themes also dominated the focus groups, so internal aspects of organizations can be expected to come to forefront of any public discussion regarding cybersecurity needs.

Additionally, the expected differences between industries and geographies were for the most part not observed in the data. There are generally similar concerns for organizations across all focus groups, with a few exceptions as noted in the analysis above. Even more surprising, participants were able to anticipate and appreciate the concerns that might be different between them. This is especially true of Portland sessions, with participants who were cognizant of the needs of organizations located outside of the Portland-metro area and seemingly anxious to help create a CCoE that might serve those needs. Decision makers seeking to create a CCoE that serves all Oregonians can rest assured that focus group participants are aware of the difficulties in this goal, yet remain interested in pursuing the greater good.

While it was not necessarily surprising that workforce development was a frequent theme in the focus group discussions, it was surprising that many respondents focused on K-12 education in the context of workforce development. K-12 education was also a point of emphasis in the brainstorming of possible CCoE activities and tasks. Finding ways to embrace K-12 educators and students in cybersecurity initiatives is a high priority for focus group respondents, and should be considered in the initial CCoE proposal design.

Finally, researchers met and interacted with a lot of engaged and motivated individuals in the process of scheduling and conducting focus groups. Many participants asked to be informed of research outcomes and future opportunities to contribute to the CCoE process. Maintaining and effectively harnessing this enthusiasm as the proposal is drafted and finalized can organically generate buy-in and legitimacy for the end result. Overall, Oregonians are ready and willing to contribute to a successful CCoE proposal process.

Chapter 4: Recommendations for Oregon's CCoE

The process of creating a proposal for a multi-sector Cybersecurity Center of Excellence (CCoE) for Oregon as outlined in SB90 is a daunting task. Drafting this proposal requires gathering input from multiple stakeholder groups and communities, analysis of the needs and resources of key beneficiary groups, and an understanding of what has and has not worked in the past for other entities undertaking similar initiatives. The preceding three chapters have preliminarily addressed each of these aspects by conducting document and literature reviews, surveying representatives of Oregon organizations, and holding focus groups of cybersecurity practitioners throughout Oregon. The data from each of these efforts has been presented and analyzed in those respective chapters; these analyses are now considered together to formulate concrete recommendations for the structure, initiatives, and programming for the Oregon CCoE. In total, three specific recommendations for the structure and activities of the CCoE are presented below: the inclusion of workforce development initiatives, the creation or curation of cyber hygiene materials and/or training services, and the expansion of leadership to include multi-sector representation. Some additional observations that warrant further consideration due to their importance in one, but not all, research activities are also included.

RECOMMENDATION: WORKFORCE DEVELOPMENT INITIATIVES

Workforce development consistently rises to the top of the potential programs and initiatives that might be offered by an Oregon CCoE. Survey data indicates that there is broad consensus across industries that cybersecurity staffing needs will increase over the next five years, and that staffing these positions will become more difficult; a majority of respondents also indicated that there is a moderate-to-significant shortage in the Oregon workforce for these types of positions. Focus groups confirmed this perspective, and nearly every session focused a substantial portion of its CCoE activities brainstorming discussion on workforce initiatives. This interest in these kinds of activities for the CCoE is mirrored by the support expressed for continuing education and certification programs (both online and in-person) in the survey data, as more than 50% of respondents expressed that their organizations would use these kinds of services if they were offered. Additionally, support for workforce development activities was not limited to higher education or continuing education; most focus groups spent a considerable amount of time talking about K-12 education possibilities in this context.

Both the quantitative and qualitative data collected from Oregonians through the preceding research efforts support the development of workforce initiatives at all levels.

Other states have also chosen to spend their limited cybersecurity resources to emphasize workforce development. Nearly every state examined in the comparative policy analysis engages in some program or activity designed to increase the quantity and quality of its cybersecurity workforce. These programs vary from the California Mentors program that focuses on nurturing young IT professionals in one-on-one mentoring relationships, to New York's newly created College of Emergency Preparedness, Homeland Security and Cybersecurity (hosted by SUNY-Albany), to Texas' WeTeachCS program that provides training for K-12 educations to receive computer science teaching certifications. Michigan's nurturing of young cybersecurity talent through the provision of scholarships to participate in the High School Cyber Challenge is an especially strong program that directly reaches young students and encourages them to enter the cybersecurity field. Retraining initiatives, particularly for veterans, are also included in many states' approaches to cybersecurity: Florida recently piloted a veterans retraining program that it is considering continuing, while Virginia is an active participant in the National Veterans retraining initiative. In short, many program templates have found success in other states, any of which could be used in Oregon to begin to meet this widely recognized need.

The consensus between these three pieces of analysis is clear: workforce development is a priority, and is a key factor in successful cybersecurity initiatives. An initial focus on K-12 initiatives in Oregon could later expand to all levels of education and professional development. As one focus group participant emphatically said, "If [the CCoE] only delivered workforce development, that would be an enormous leap forward."

RECOMMENDATION: CYBER HYGIENE TRAINING

Cyber hygiene programs, and general cybersecurity training for non-technical employees of Oregon organizations, are both a priority and concern for Oregon survey respondents and focus group participants. These efforts emphasize "healthy" practices and habits when using information technology and communications systems; survey respondents that provide this kind of training to non-technical employees most commonly indicated that phishing and general web safety topics are covered. However, nearly 50% of respondents indicated that either very few or none of their employees receive this type of training. This result is further confirmed by focus group data, in which many participants lamented the inability of their organizations to prioritize or provide resources for this type of training despite the desire of the technical staff to provide it. Participants in multiple focus group sessions talked excitedly about the possibility of creating a "human firewall" if increased numbers of non-technical employees could receive and absorb training on basic cyber hygiene topics. Several also noted the need for this type of training to begin before employees enter the workforce, and were generally supportive of including cyber hygiene content in K-12 settings.

Leading states included in the comparative analysis include cyber hygiene courses and training among their programming and initiatives. Most provide these types of training materials for government employees. Some states (Colorado, Illinois, New York) go one-step further and make such training mandatory for those in non-technical public sector positions; California extends this requirement to contractors as well. Some states have also taken the step of creating and providing materials and programming for audiences beyond state employees: the Florida Department of Law Enforcement's Cybercrime Office runs a public-facing website with hygiene information for the public, Michigan makes toolkits for small businesses and individuals available, and New Jersey conducts informative weekly webinars on cyber hygiene topics. States have also brought cyber hygiene programming to K-12 institutions: Colorado has a cyber-hygiene outreach program for 6th- to 8th-graders, while Michigan provides curriculum materials for schools to use that focus on online safety and awareness. The prevalence of these types of initiatives shows that other states have identified the provision of cyber hygiene training and informational materials as a priority with a high potential return on investment.

An Oregon CCoE can meet the need identified by a variety of survey respondents and focus group participants by either creating or curating a collection of informative cyber hygiene materials that can provide basic cyber hygiene information to organizations of all sizes and sectors. Focus group respondents that work in cybersecurity described the difficulty they face in locating or creating suitable materials for their organizations' non-technical employees; while some mentioned that time to administer training sessions and materials is also difficult to find, this was a lesser concern than simply having credible information to present in compelling ways. Materials that cover the basics of cyber hygiene, as well as any Oregon-specific cybersecurity laws and requirements, were of great interest to Oregonians, and these types of initiatives fit well with the example set by other states.

RECOMMENDATION: MULTI-SECTOR ENGAGEMENT

Creating truly multi-sector engagement, in terms of both leadership and participation in programs and services, is a high priority for successful cybersecurity initiatives. This means both providing opportunities for interested cybersecurity representatives in all sectors, and across all industries, to participate in agenda setting and decision making, as well as providing opportunities for collaborative learning and education across sectors. These ideas both received widespread support in the focus groups conducted across Oregon as indicated by the prevalence of the Diverse Involvement theme. Anecdotally, participants also expressed ready interest in cross-industry events and sharing opportunities. Several noted that this is a particular type of sharing that is not facilitated by existing professional organizations (and especially ISACs), which tend to be fragmented by industry membership. Many participants also explicitly asked how they could become a part of the advisory and/or decision-making bodies for the CCoE; these participants spanned all represented industries in the focus groups. This, coupled with the volume of ideas generated in the brainstorming portion of the focus groups, shows that there is a potential for valuable leadership if the number of participants and the represented industries expands to become more inclusive of a truly multi-sector approach.

States that have embraced this approach, and can be looked to for practical implementation methods, include Colorado, Michigan, Maryland, and California. Maryland has the most diverse leadership entity, with 50 members spanning a variety of industries, including government, business, education, critical infrastructure, and cybersecurity more specifically. A key aspect of incorporating this many leaders is the creation of subcommittees with specific policy responsibilities; both Maryland and California provide templates for what these subcommittee structures might eventually look like. These bodies are equipped to serve in an advisory capacity that is inclusive of a variety of perspectives and viewpoints, arguably providing more context and insight into the cybersecurity needs of the state as a whole.

Creating opportunities for engagement across sectors seems vital to the success of an initiative that aims to reach as far and do as much as the Oregon CCoE. These opportunities need to be available for both potential leaders and those simply seeking services and resources. Following the lead of other successful initiatives, an expanded leadership structure and specific multi-sector events seem to be promising opportunities to foster this type of engagement.

OTHER NOTES FOR CONSIDERATION

Two final observations are important when considering the insights that the compiled data provides for CCoE structures and activities. First, centralization and unification of state cybersecurity activities often precedes the successful implementation of cybersecurity expanded cybersecurity initiatives in most of the studied states. This has the dual functions of increasing the transparency and accountability of actors representing state government, and also increases the legitimacy of state leadership in multi-sector cybersecurity initiatives. While not specifically related to the Oregon CCoE, consolidation of cybersecurity activities in Oregon government is included in other sections of SB90, showing at least some acknowledgement of the relationship between these two efforts. Ensuring that the implementations of other aspects of SB90 are moving forward concurrently with the CCoE proposal drafting process may ultimately make the proposal more successful with the legislature and a more legitimate and representative venture in the eyes of the Oregon public.

A second observation is the need for activities and programs that target executive-level leadership of organizations. Though not featured in any of the state analyses included in the first chapter, content geared toward educating C-level leadership was an especially vibrant topic in the focus group discussions. Cybersecurity professionals across industries, geographies, and regardless of organization size expressed difficulties in conveying the importance of cybersecurity to executives; attempts to involve executives in cybersecurity education and information sessions were often unsuccessful if originating from within the organization. Participants also requested both general cybersecurity education and sector-specific cybersecurity education programs for executives as part of the CCoE activities brainstorming sessions, with broad agreement among participants when these suggestions made. Incorporating programming specific to the highest levels of management for Oregon organizations should be another item considered in an initial agenda for the CCoE.

Chapter 5: Funding Opportunities and Challenges

An important part of new initiative is securing the financial means to put plans into action and make goals into realities. The funding catalog included in Appendix B aims to gather current funding opportunities for cybersecurity efforts that could be pursued to accomplish the mandates and goals of the Oregon Cybersecurity Advisory Council (OCAC) and the Oregon Cybersecurity Center of Excellence (CCoE)[367]. The catalog includes both private and government sources. "Private sources" in this case refers to private foundations, and not monetary or in-kind donations from private companies that may become a part of Council and CCoE programming through sponsorship or targeted donations. "Government sources" focuses on federal grants as opposed to federal contracting. In an effort to be inclusive, and because funder priorities may fluctuate, this report also references past federal grant funds awarded to Oregon entities when that information is available and relevant to these efforts. This information contributes to the overarching research goal of arriving at Oregon-specific recommendations from a variety of data collection and analysis approaches.

As the catalog demonstrates, the most fundable activities relate to workforce development. While cybersecurity specific funding is limited, a wealth of public and private STEM funding can also be relevant to cybersecurity efforts. Finally, both types of opportunities require attention to the type of entity seeking funding. Several federal opportunities specify universities as the awardee, and private funders generally require recipients be tax-exempt and, in some cases, to qualify for 501(c)(3) designation. Cultivating relationships in the public and foundation spheres can also contribute to the overall success of funding efforts by increasing the likelihood of appropriations from block grants, discretionary funds, and sponsorship of specific programs and initiatives.

METHODS

The search for funding sources was intended to be informed by reviewing funding sources for cybersecurity efforts in other states as part of the comparative policy analysis included earlier in this report. These states' cybersecurity activities were often nested in the overall information technology budget, or funded by one-off grants, appropriations or sponsorships, most of which are not included in the scope of the funding sources. Funding sources and grants that fit within the scope noted in the statement of work

[367] These 11 mandates and goals can be found in SB 90, Sections 3 and 4.

were still assessed, but with the understanding that funding from similar initiatives may not be found through these means. First, city, county, non-profit, foundation, and grant funding opportunities were assessed. This was followed by a search for funding opportunities through federal grant structures.

FOUNDATION OPPORTUNITIES

One efficient and effective tool for reviewing private foundation opportunities is the Foundation Directory Online (FDO), a subscription service of the Foundation Center that offers searchable information on more than 140,000 grant makers and 500,000+ recipients.[368] While the service charges $88-200/month depending on the plan chosen, access to the database is available free in over 400 locations nationwide through Funding Information Centers; as of this publication date, Multnomah County's Central Library (801 SW 10th Avenue, Portland) is the only entity in Oregon offering this free access.[369]

The research team used FDO to search for foundations that fund projects in Oregon and appeared to have either general interests or specific funding opportunities relevant to CCoE programming. The following information, where available, is noted for the funders located in this initial search:

- Funding Entity
- Funding Opportunity/Foundation Interests (depends on specificity of organization information)
- Connected SB 90 function
- Website/contacts
- Funding Range in $ and deadlines
- IRS/Nonprofit restrictions

Websites are not available for some foundations because, as the Foundation Center notes, approximately 90% of U.S. foundations do not maintain a website.[370]

[368] Foundation Center "Foundation Directory Online Professional." https://fconline.foundationcenter.org. Accessed December 20, 2017.

[369] Foundation Center. "Find Us." Accessed December 20, 2017. http://foundationcenter.org/ask-us/find-us.

[370] Foundation Center "Foundation Directory Online Professional". Accessed December 20, 2017. https://fconline.foundationcenter.org

CHAPTER 5: FUNDING OPPORTUNITIES AND CHALLENGES

FEDERAL FUNDING OPPORTUNITIES

The research team reviewed funding opportunities from several federal sources, including the following departments, institutes, and foundations:

- Department of Homeland Security (DHS)
- National Institute of Standards and Technology (NIST)
- Department of Defense (DOD)
- Department of Education (DOE)
- Department of Justice (DOJ)
- Department of Commerce (DOC)
- Department of Agriculture (USDA)
- National Science Foundation (NSF)

The primary source for federal grants opportunities is the government website Grants.gov. The team performed searches on this website using keywords including “cybersecurity,” “cyber,” and “information technology,” as well as several other variations of these terms. More general keyword searches on terms such as “training” and “workforce” were also used to sort through currently active, closed, and archived funding opportunities. Each federal organization’s website was also consulted for any notices and press releases regarding grant funding updates and forecasted proposals.

Information about past and current federal funding opportunities is organized in a similar manner as the private sources, with some modifications:

- Funding Entity
- Funding Opportunity and Description (brief summary of the grant terms and any key language)
- Open window (for current or recently open grants)
- SB 90 function
- Website/RFP address
- Funding range and specifications for proposers
- Proposer specifications (type of entity allowed to seek funding)

FINDINGS

The information contained in the funding catalog is the best available as of publication. Though funder priorities may change and new opportunities will appear, we hope that this information will be helpful in guiding future searches.

General Notes on Foundation Opportunities

The funding catalog provides an overview of 15 possible foundation funding opportunities that fit the stated functions of the OCAC and CCoE. The most fundable function appears to be workforce development, especially when this is broadly interpreted as education initiatives for all ages of Oregon students.

A primary consideration for securing future grant funding is the legal designation of the CCoE or other grant-seeking entity. As noted in the catalog, the majority of foundation funders explicitly require a 501(c)(3) designation from the IRS. Depending on the grant, some specify furthermore the type of entity, such as a library or school. Some funders may be more willing than others to fund start-up costs, though most in the catalog prefer a track record for the program requesting funding.

The funders in the catalog represent funding opportunities ranging from $1,000 up to $75,000, when funding ranges were published. Because of the time and effort involved in the preparation and submission of most foundation grants, the Council and any other involved parties may wish to engage with qualified and connected grant writing professionals at the appropriate stage. While the FDO is a useful resource that the Council may wish to utilize from time to time, a well-connected grant writer could provide additional insight. The council may wish to target those grant writers experienced with major local funders and also those experienced with fundraising for STEM and/or workforce development proposals.

General Notes on Federal Funding Opportunities

Through searching Grants.gov, it became clear that the National Science Foundation currently offers, and has offered in the past, most of the relevant opportunities for funding cybersecurity initiatives as described in SB 90. The catalog includes 9 NSF grants particularly pertinent to cybersecurity efforts that are statutorily ascribed to the CCoE and OCAC. Because the National Science Foundation provides more detail on the funding opportunities than Grants.gov, citations from the former are provided in the catalog. There are also three grants that fund economic development activities in rural areas that can be broadly construed to include cybersecurity workforce development or cybersecurity service provision in rural Oregon communities. Other opportunities included are a DHS grant that funds “target hardening” and cybersecurity training for nonprofit staff, a Centers for Disease Control grant for incident response assistance in emergency situations, and a Bureau of Education and Cultural Affairs (Department of State) grant for an international technology camp. While the latter entails efforts that may go beyond the initial priorities for the CCoE, it is included with the rest to give a picture of the potential diversity of federal funding opportunities in cybersecurity.

Current grants offer support for the following activities:

- Higher education technology infrastructure updates, paired with research opportunities for students
- K-12 STEM education
- Training and education for scientific and engineering workforce development
- Career pathways/technician education
- Broad economic development activities, including “technology-based economic development”
- Educational exchange programs for young women from the Middle East, featuring technology camps provided by U.S. entities

Past grants have funded these and activities and also:

- Direct support for university students studying cybersecurity
- Capacity building for cybersecurity education
- Security for cyber-physical systems
- Cybersecurity-specific education

Additional considerations for seeking federal grants include the diverse entities that may apply, and which of these entities might be best positioned to do so. Several grants are available to all NSF-qualified entities, a broad group that includes the following[371]:

- Universities and colleges
- Non-profit, non-academic institutions (such as museums, observatories, laboratories)
- For-profit organizations, especially when paired with universities and colleges
- State and local governments

[371] National Science Foundation “*NSF Proposal & Award Policies & Procedures Guide.* Accessed December 21, 2017, pp. 4-5. https://www.nsf.gov/pubs/policydocs/pappg17_1/nsf17_1.pdf.

- *In rare cases*: unaffiliated individuals, foreign organizations, or other federal agencies.

Some grants limit funding to the first two categories, or require a cross-sector partnership.

Of the various opportunities available for universities, the CyberCorps scholarships may be of particular interest to the council. One funding stream of CyberCorps (Scholarships for Service) provides direct support to university students in cybersecurity programs, which is followed by public service obligations; this funding is not yet available at any Oregon school. A Portland focus group participant specifically mentioned the program, and a desire that it be promoted more widely to facilitate interest in the cybersecurity field; a survey participant wrote that "…merit awards to keep kids here would be good, but public universities typically do not give out many of those." CyberCorps provides one tool for recruiting the future cybersecurity workforce the cybersecure and will hopefully be funded again after the most recent 2017 call for proposals.

Several Oregon institutions have found success through NSF funding. These successful grant applications are detailed in the funding catalog, with more information on these projects available through the linked abstracts. These funded programs include, but are not limited to:

- **Portland State University**: funding for development of Capture-the-Flag games for emerging security practitioners
- **Portland State University:** network infrastructure upgrades coupled with associated research opportunities for students underrepresented in STEM fields
- **Klamath Community College:** development of a rural virtual internship program for STEM fields
- **University of Oregon:** travel support for bringing out-of-town students to annual Oregon Security Day with cybersecurity speakers
- **Lewis and Clark College:** development of tools that automatically assess student learning in practical cybersecurity tasks

Conclusions and Suggestions

The information provided in the funding catalog in Appendix B captures a moment in time of funding opportunities. It is necessarily limited by two factors: the often-incomplete information readily available from private funders, and the fact that federal opportunities currently considered "open" will expire in 2018 (though two of the NSF grants have deadlines listed for 2019 and beyond).

The research team is encouraged by funder interests not only in cybersecurity but in the general areas of STEM and workforce development. With workforce development as a CCoE function held in high regard by survey and focus group participants, and a prominent line of programming in other states' cybersecurity initiatives considered in the comparative policy analysis, the OCAC and CCoE may be in a strategic position to operate as a disinterested broker in coordinating and advancing cybersecurity funding efforts in Oregon.

Chapter 6: Current Cybersecurity Efforts in Oregon

The geographical and network analysis categorizes and catalogs current cybersecurity efforts across the state of Oregon. This information supplements the survey and focus group responses with additional identification of organizations, programs, and initiatives throughout Oregon that either are, or can become, resources to a state-wide cybersecurity effort. Given the sensitive nature of many cybersecurity relationships and difficulties securing information other than what was publicly available, the ability to ascertain connections between entities was more difficult than expected. As a result, this section focuses primarily on cataloging and geographically analyzing cybersecurity education programs and private organizations that provide cybersecurity services.

METHODS

The intent of the researchers was to complete this task using a combination of document review and a series of targeted conversations. In both areas, serious challenges arose that hindered the ability to obtain the depth of information necessary to be able to accurately display and analyze connections between organizations. This is attributable to two primary issues:

- The understandable reluctance of private enterprises to share information regarding clients (based on non-disclosure agreements) and other business arrangements, and
- Difficulties finding organizations of all types (including education organizations, non-profits, private corporations, and government entities) willing to respond to researcher requests for information and insight into their relationships with others, either through documentation or brief conversations with researchers.

Two groups merit special recognition for their enthusiastic response to researcher inquiries and participation in interviews: the Cybersecurity Education and Research Team at Oregon State University, and a contingent of staff members at Cayuse Technologies (Pendleton, Oregon). Insights from these interviews are included in the conclusions section.

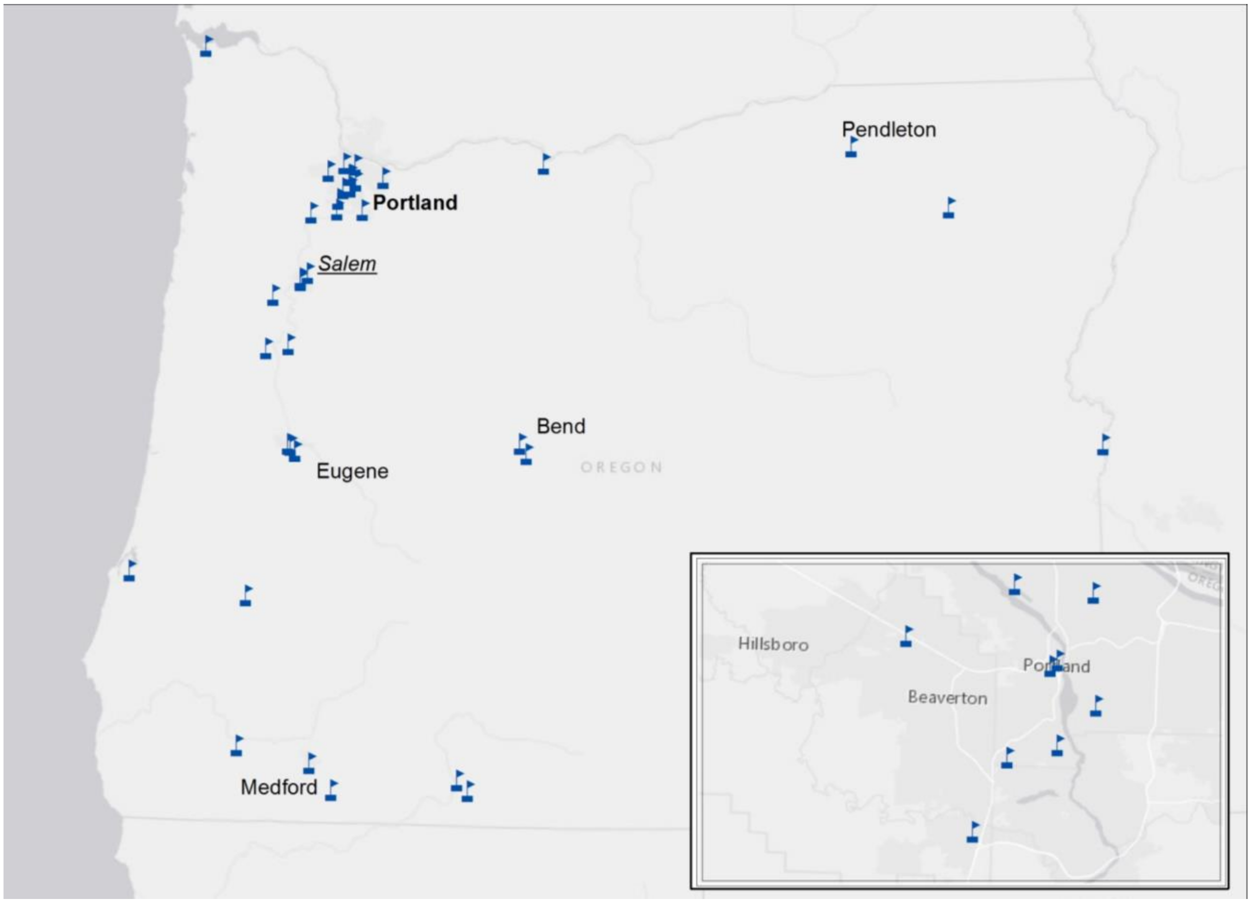
Considering the aforementioned challenges, the research team focused on mapping two primary categories of resources in Oregon: educational institutions and cybersecurity professional services. Below, these visualizations are displayed and assessed in juxtaposition with each other, considering overall concentrations of resources within the state. This allows for a greater understanding of areas of strength within the state, as well as particular institutions or regions that may be under-resourced or have untapped potential.

EDUCATION RESOURCES: MAPPING AND ANALYSIS

The first graphic depicts the availability of Computer Science and Computer Engineering education throughout the state, including institutions both public and private and with terminal degrees ranging from associates to doctoral.

All institutions offering training in either of those two fields are included; physical locations of for-profit training centers operated by New Horizons and ONLC that provide access to industry training and certification programs are also included.

OREGON CYBERSECURITY EDUCATION RESOURCES



Within this group of educational institutions, institutions can distinguish themselves through affiliations and recognitions. Three are analyzed in-depth below: MECOP (Multiple Engineering Cooperative Program), CyberWatch West, and the National Centers of Academic Excellence in Cyber Defense designation.

MECOP (Multiple Engineering Cooperative Program)[372]

The MECOP program is an Oregon education-business partnership offering paid internships to students from four participating universities (Oregon State University, Oregon Institute of Technology, Portland State University, and the University of Portland). MECOP targets students in 18 engineering-related areas of study, including fields traditionally associated with cybersecurity like computer engineering, computer science, and information systems.

MECOP provides a progressively involved structure for these students to incorporate professional development into their undergraduate studies through two paid internships. Over 140 public and private employers access pre-screened and motivated future engineers which they may "try out" for six months in an internship capacity. While there is no requirement to hire interns, over 90% of graduates continue to work in Oregon, and 70% with MECOP companies.[373] These statistics indicate that MECOP may be valuable resource in providing the kinds of incentives for cybersecurity talent to stay in Oregon that several focus group participants mentioned in workforce development discussions.

Publicly available MECOP information does not identify which participating employers match with students in cybersecurity-related fields, or the size of the cohorts employed by organizations in a given year. However, the longevity of this program indicates that it is considered valuable by both the educational institutions and the companies employing interns. While the program is currently limited to four universities, other educational institutions are eligible to join MECOP[374].

[372] MECOP (Multiple Engineering Cooperative Program). Accessed December 20, 2017. https://www.mecopinc.org/students, https://www.mecopinc.org/industry,

[373] MECOP. "Company Membership." Accessed December 20, 2017. https://www.mecopinc.org/industry.

[374] MECOP. "University Membership." Accessed December 20, 2017. https://www.mecopinc.org/universities

CHAPTER 6: CURRENT CYBERSECURITY EFFORTS IN OREGON

CyberWatch West

Several schools in Oregon participate in the regional CyberWatch West (CWW) network. Based out of Whatcom Community College in Bellingham, Washington, the center is funded through a National Science Foundation Advanced Technological Education Grant, with the stated mission to "increase the quantity and quality of the cybersecurity workforce throughout the western United States." The center was designed and funded to support fourteen Western states, though membership is open nationwide.[375] In service of that goal CWW offers resources, such as course materials and a mentoring program[376], primarily for instructors in higher education institutions. There are also resources available for students, including scholarship information and a variety of cybersecurity competitions.[377]

The process to join CWW is inclusive and simple: educational institutions, including high schools, apply through the education pathway, while businesses, nonprofits, and professional organizations can join as industry partners. Currently five Oregon institutions participate:

- Lewis & Clark College
- Linn-Benton Community College
- Mt. Hood Community College
- Oregon Institute of Technology
- Portland Community College

The review of educational institutions involved in this indicates the following accomplishments and interests from current Oregon CWW members:

[375] CyberWatchWest. "About Us." Accessed December 20, 2017. https://www.cyberwatchwest.org/index.php/about-us.

[376] CyberWatchWest. "About Faculty Development." Accessed December 20, 2017. https://www.cyberwatchwest.org/index.php/faculty-141.

[377] CyberWatchWest. "About Student Development." Accessed December 20, 2017. https://www.cyberwatchwest.org/index.php/students-138

Institution	Notable accomplishments and/or areas of interest in cybersecurity	More information
Lewis and Clark College	2 National Science Foundation grants related to cybersecurity	https://college.lclark.edu/live/news/30529-cybersecurity-education-tools
Linn-Benton Community College	Dual Partnership Program offers dual enrollment with OSU for computer science students; no further details on cybersecurity-specific programming available	https://www.linnbenton.edu/degree-partnership https://www.linnbenton.edu/current-students/student-support/instructional-departments/computer-systems/computer-science
Mt. Hood Community College	Home of Oregon Center for Cyber Security Provides cybersecurity services to small businesses around Oregon through network of Small Business Development Centers (SBDC)	https://www.mhcc.edu/OCCS/ https://bizcenter.org/cybersecurity/
Oregon Institute of Technology	Operates Cyber Defense Center (staffed by students in Information Technology degree program)	http://www.oit.edu/cyber-defense-center
Portland Community College	Offers a certificate in Cybersecurity Fundamentals	https://www.pcc.edu/about/events/cyber-security/ https://www.pcc.edu/programs/computer-info/cyber-security.html

CHAPTER 6: CURRENT CYBERSECURITY EFFORTS IN OREGON

National Centers of Academic Excellence in Cyber Defense

Two institutions in Oregon have been recognized through the National Centers of Academic Excellence in Cyber Defense program jointly sponsored by the National Security Agency (NSA) and Department of Homeland Security (DHS). The program offers three paths for two-year and four-year programs alike to receive national recognition for their program of cyber defense education[378]. Mt. Hood Community College has received the National Centers of Academic Excellence in Cyber Defense 2-Year Education (CAE-2Y) designation, while the University of Oregon has received the National Centers of Academic Excellence in Cyber Defense Research (CAE-R) designation; both are effective through 2019.

While these designations create opportunities for students to pay for their education through CyberCorps Scholarships for Service grants (discussed in the funding chapter), the designation does not guarantee any institution-specific funding.[379]

In addition to the current Centers at Mt. Hood Community College and the University of Oregon, our research identified at least three Oregon schools working on earning the designation and/or aligning with the pursuant curriculum requirements:

- Umpqua Community College[380]
- George Fox University[381]
- Oregon Institute of Technology[382]

Summary of Education Mapping Strengths and Gaps:

Initial analysis of the resources indicates some gaps in participation and resource availability. First, several schools with notable strengths in cybersecurity do not participate in CyberWatch West, including:

- George Fox University (linked above)
- Linfield College- offers Cyber Security and Digital Forensics certificate online[383]

[378] National Security Agency. "National Centers of Academic Excellence in Cyber Defense". https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/. Accessed December 21, 2017.

[379] CAE Community"What is a CAE?"https://www.caecommunity.org/about-us/what-cae. Accessed December 21, 2017.

[380] Umpqua Community College. "Cybersecurity: AAS". https://www.umpqua.edu/cybersecurity. Accessed December 22, 2017

[381] George Fox University. "Cyber Security Concentration". https://www.georgefox.edu/college-admissions/academics/major/cyber-security-concentration.html. Accessed December 22, 2017.

[382] Kawasaki, Charlie. "Cybersecurity in Oregon: Overview". https://cyberoregon.com/wp-content/uploads/2017/11/Cybersecurity-Education-Summit-Charlie-Kawasaki.pdf. Presented on November 3, 2017.

[383] Linfield College. "Cyber Security and Digital Forensics Certificate Program" http://www.linfield.edu/dce/certificates/cyber-security-and-digital-forensics-certificate.html

- University of Oregon – has been awarded several National Science Foundation grants and hosts the Center for CyberSecurity and Privacy and Oregon Security Day, as well as holding the Center of Excellence designation

Also, two of Oregon's 17 community colleges appear to not have any educational programs in computer science or computer engineering programming: Tillamook Bay Community College and Oregon Coast Community College. For this reason, these schools are not depicted on the map of educational institutions. However, this presents a clear opportunity to support the development of computer science and cybersecurity curricula at these institutions and bring new workforce development and training opportunities to the Oregon coast.

CYBERSECURITY IN THE PRIVATE SECTOR: MAPPING AND ANALYSIS

A second type of data review and visualization considers the cybersecurity services available in Oregon. Data compiled from a variety of sources were used for this analysis, including a list of respondents to State of Oregon RFPs for cybersecurity incident response services and the list of attendees at the 3rd Oregon Cybersecurity Policy Summit held on August 25, 2017. Organizations that did not appear to offer cybersecurity services, or no longer appeared to be in business, were removed from the dataset.

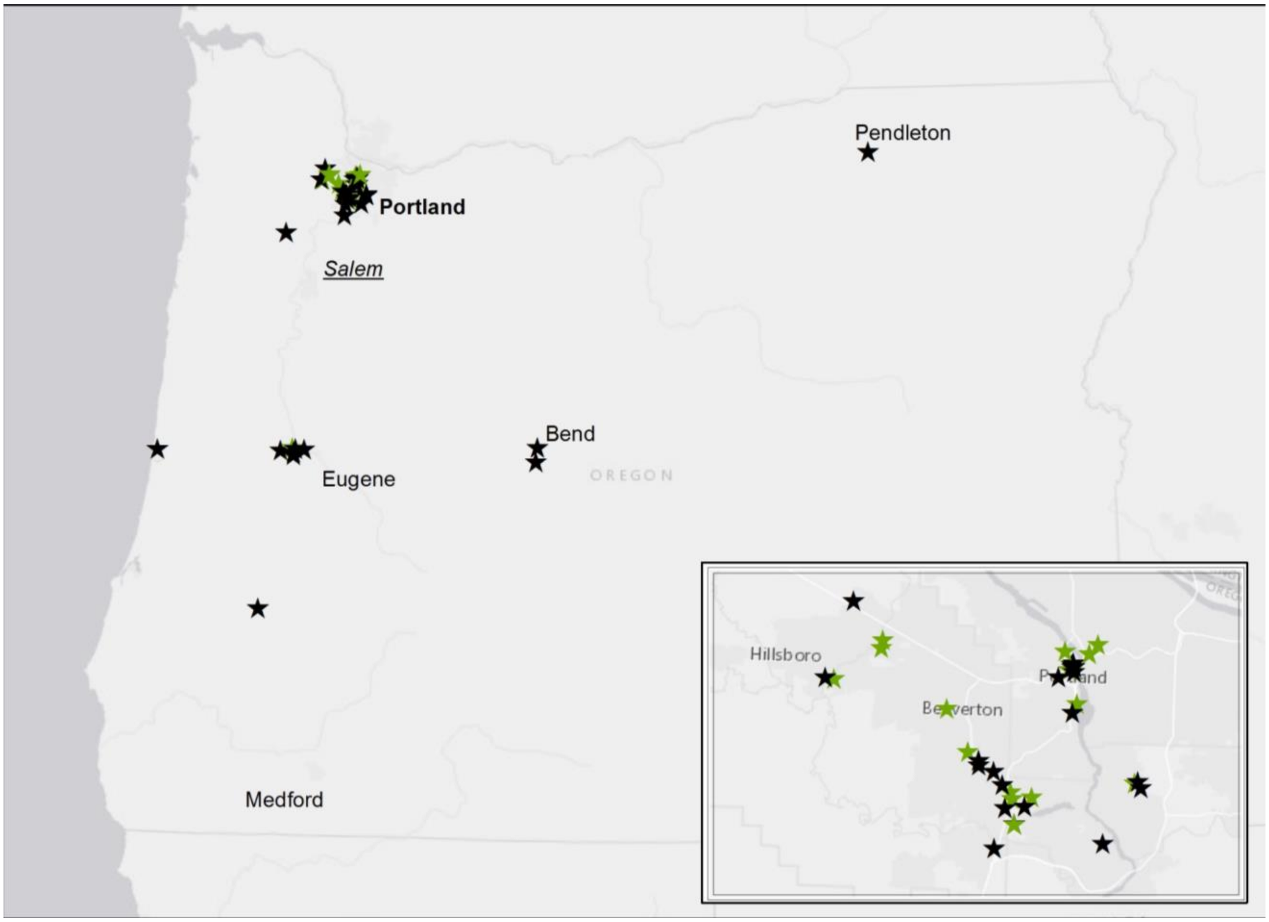
In the map on the next page, the location of an organization's headquarters are used to distinguish between three types of companies offering cybersecurity services:

- Companies headquartered in Oregon (36 companies) – represented by black stars
- Those headquartered elsewhere with an Oregon branch (19 companies) – represented by green stars
- External Business with No Oregon Branch but Established Oregon Presence (8 companies) – not included in map

As the map shows, the Portland-metro area has the highest concentration of cybersecurity companies by far. This is helped by the fact that most companies headquartered outside of Oregon appear to locate their Oregon branches in or around Portland. This is unsurprising given the status of Portland as Oregon's biggest city and population center, and only major metropolitan area. There are also small clusters of businesses located around Eugene and Bend, though they contain substantially less activity than the Portland cluster. Individual operations located in the Pendleton area, Roseburg area, and central Oregon coast round out the map.

It is important to note that this map is not necessarily an exhaustive list of every company offering any type of cybersecurity service within Oregon. However, to the best of the research team's abilities, every organization of a large enough size to potentially serve as a resource for the CCoE (as opposed to being a recipient of services from the CCoE) is included. Additionally, the map does not depict or differentiate between the clientele of these organizations; as mentioned above, obtaining this information was difficult for a multitude of reasons.

OREGON PRIVATE-SECTOR CYBERSECURITY ORGANIZATIONS



Future attempts to quantify and qualify the relationships between private cybersecurity service providers and other types of organizations should be intentionally designed with input from these important information sources to ensure that necessary data can be gathered. Perhaps with appropriate data controls and confidentiality procedures, as utilized in the anonymous online survey and confidential focus groups described in Chapters 2 and 3 respectively, would yield better returns on requests for information.

CONCLUSIONS

The Oregon Cybersecurity Landscape: Business, Education, and the Other Stakeholders

A review of the resulting maps yields several conclusions. First, 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 in the way of business activity. Several other community colleges operate in areas without any significant cybersecurity 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 the areas that provided their education.

Of course, a holistic understanding of the cybersecurity efforts must also consider resources not included on the maps in this report. Many organizations and institutions operate in communities do not have cybersecurity as a core or even periphery goal, but can serve as conveners for new initiatives or intermittent programming. Depending on the functions of an eventual CCoE, any or all of the following could be valuable partners:

- Public libraries and community centers with computer education and cyber hygiene programs
- Other Small Business Development Centers throughout the state
- School districts
- Chapters of industry organizations (for example: ISAC, ISSA)
- Certifying organizations (if local)

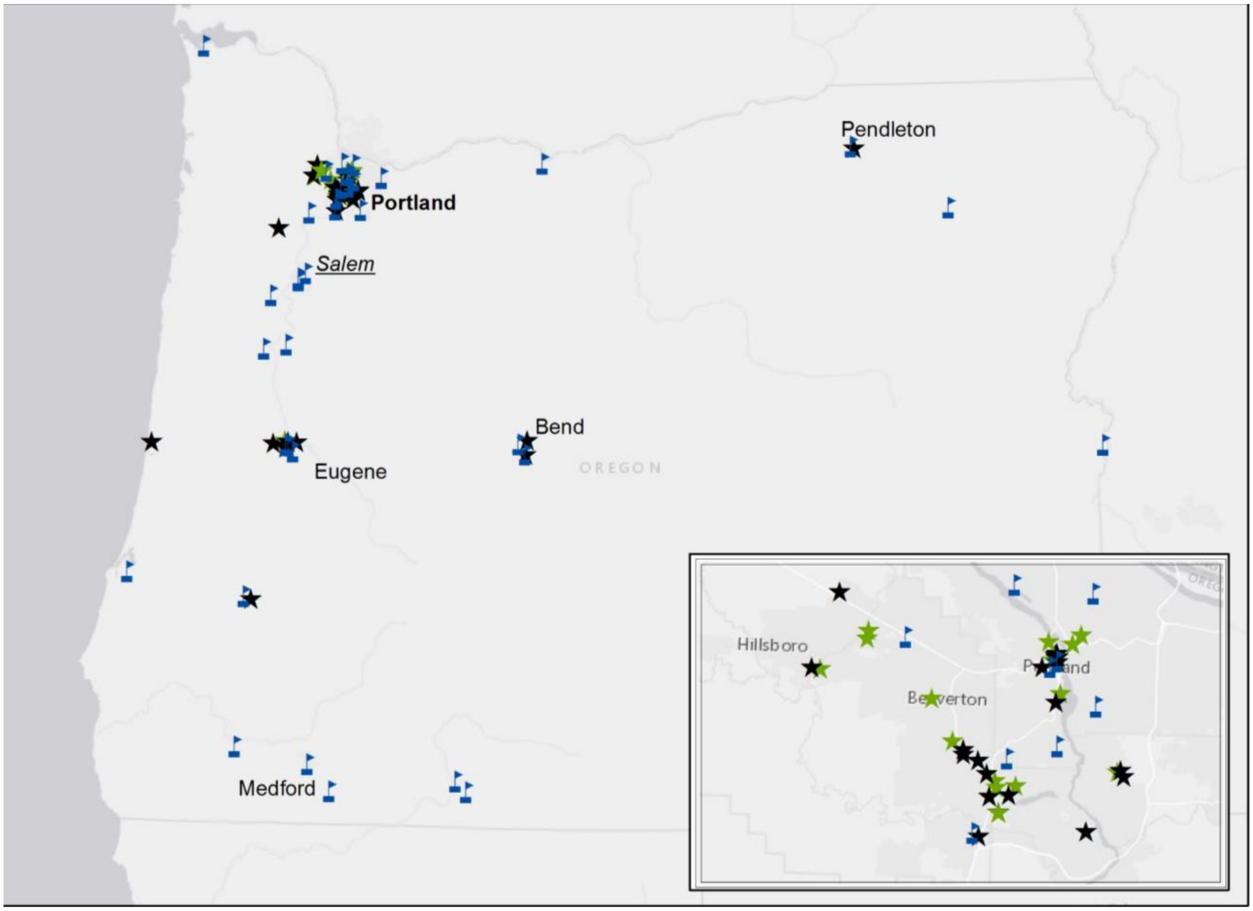
The Council and CCoE may also wish to consider the value of further interviews with cybersecurity resources, considering the insights gleaned in the short discussions the research team was able to conduct. For example, the discussion with OSU Cybersecurity faculty members raised the possibility of co-locating cybersecurity resources at already established OSU Extension Centers.[384] The discussion with representatives of Cayuse Technologies, the first Native-owned onshore delivery center, illuminated some of the challenges of attracting resources and investment to eastern Oregon in particular. A participant indicated that those looking for technology services or seeking employment in the field often do not think to consider the resources in the area before taking their business to more populous areas of Oregon like Portland.[385] The Cayuse representatives also indicated that even with the resources of the local community college, the scheduling of classes complicates attendance for those working during the day, and the location makes attendance in inclement weather difficult.

While two interviews on current networks and relationships is an extremely limited sample from which to discuss resource strengths and challenges, it does provide a perspective on the landscape that contributes to the attached visualizations. The information gleaned in this resource analysis process can be used in conjunction with the other research methods included in the project proposal to generate recommendations for the Oregon CCoE.

[384] Web-based Interview – OSU Cybersecurity Team – September 28, 2017
[385] Interview – Cayuse Technologies – November 8, 2017

CHAPTER 6: CURRENT CYBERSECURITY EFFORTS IN OREGON

COMPREHENSIVE MAP OF CYBERSECURITY RESOURCES IN OREGON



Chapter 7: Concluding Thoughts and Next Steps

This report has considered a variety of evidence that can help decision makers draft a proposal for the Oregon Cybersecurity Center of Excellence (CCoE). Both the raw data and analysis provided in the previous chapters are valuable sources of information that can support an evidence-based policy process that culminates in a successful CCoE proposal. However, even with this research as background, the scope of the CCoE's potential activities and influence, coupled with an aggressive timeline, make the proposal-drafting process challenging. Keeping the outcomes of the data collection and analysis efforts in mind, the research team therefore recommends several tangible "next steps" for decision makers engaged in this process. These next steps also align with the public health approach to cybersecurity that has served as a theoretical framework for this report, and the principles of public cybersecurity practice set forth by Sedenberg and Mulligan[386] more specifically.

NEXT STEP: DECIDE ON A LEGAL STRUCTURE

An essential early step in the proposal drafting process needs to be determining the legal structure of the CCoE. SB90 does not require a particular structure for the CCoE, which allows for some flexibility in terms of the kinds of legal structures that decision makers can consider. Potential structures include a government (state-level, executive) agency, nonprofit, public-private partnership, or a more cooperative- or consortium-style arrangement; a CCoE can also stand alone as an independent entity, or become a part of another government, nonprofit, or educational institution.

There are several reasons that this step is important to take early on in the drafting process. First, the legal structure has important implications for funding. Many grants have limitations on the types of organizations to which they can be awarded, and direct sponsorships and donations may be more forthcoming with some types of legal structures than others. The legal structure may also need to allow the CCoE to serve as a central clearinghouse of funding opportunities for participating organizations, though this depends on the mission, vision, and specific programming envisioned to fulfill the functions set out in SB90. Examples of this clearing house function include assisting

[386] Elaine Sedenberg and Deirdre Mulligan, "Public Health as a Model for Cybersecurity Information Sharing," *Berkeley Technology Law Journal* 30, no. 3 (2015): 1737-1738.

small businesses and nonprofits in their own grant applications for cybersecurity funding, or acting as a neutral convener for multi-institution educational grants for cybersecurity education.

The CCoE's legal structure is also important for clarifying its leadership and decision-making processes, as well as the extent to which both the State of Oregon and vendors are involved. Several members of key beneficiary groups expressed concern about the lack of a clearly identified CCoE mission or set of goals throughout the research process, as well as concerns regarding the transparency of the processes by which these are determined. Specific concerns about inefficiencies ("red tape") and politicization of cybersecurity initiatives through state involvement were mentioned mainly in the focus group data. Additionally, participants were unclear about the extent to which cybersecurity vendors might be involved in any state-wide initiatives. Suggestions for vendor agnosticism and clarification on the role of the Oregon Cybersecurity Advisory Council from focus group participants and survey respondents can be accommodated through intentional design that is clearly communicated. Identifying a legal structure can help potential participants in the CCoE understand its leadership and decision-making processes and the extent to which the State of Oregon is involved in them.

Finally, states that can serve as reference points for Oregon's CCoE have seen success with different types of legal structures. The use of other states' activities as inspiration or models for the CCoE can be better tailored once a legal structure is determined. The legal location and structuring of the CCoE within the Oregon Office of the State Chief Information Officer more closely follows the example of Colorado and its emphasis on securing state agencies. An official affiliation within an institution of higher education, as seen in the Florida Center for Cybersecurity's relationship with the University of South Florida, may shift leadership and reference points for programming in a different direction. Considering the types of activities that decision makers are interested in pursuing to meet the requirements set forth in SB90 is an important endeavor that requires an appropriate legal scaffolding for the scope and envisioned services to key beneficiaries.

Choosing a legal structure is a critical step in the proposal drafting process, as this communicates to key beneficiary groups the nature of the CCoE's leadership and programming orientation going forward. This decision should be made early in the process and with the utmost care for decision makers' desired role of the CCoE in statewide cybersecurity. The importance of this decision in the overall design process cannot be underscored enough.

NEXT STEP: ENGAGE FUNDING EXPERTS

Ensuring adequate funding is one of the most important aspects of a establishing and operating a successful CCoE. A variety of sources have been used by other states to fund cybersecurity initiatives, including state legislative appropriations, federal grants, sponsorship and donations from businesses, and contribution of resources in-kind. States like California and Texas receive a substantial portion of cybersecurity funding from federal sources (primarily the Department of Homeland Security) and legislative appropriations at the state level, while initiatives like Colorado's National Cybersecurity Center received large in-kind contributions of facilities, and specific programs like Florida's veterans retraining program (New Skills for a New Fight) were funded by private corporations. It is important to note that most states with large amounts of funding tend to receive that funding from federal sources, with much of this funding coming from successful grant applications.

To navigate the complex funding landscape for cybersecurity initiatives, CCoE decision makers should consult with grant-writing and funding experts throughout the proposal drafting process. This expertise can help target sources of funding and provide valuable insight on the types of grant applications that are likely to be successful in the current funding climate. As the funding catalog shows, there are many highly competitive grants that can be pursued to fund CCoE activities, most of which require complex applications with a variety of supporting documentation and proof of additional financial support from other sources. Additionally, this expertise can help inform the legal structure decision described above, as some legal structures may make the CCoE more attractive for grants than others. Individuals that have successful written grant applications for initiatives of the size and scope of the CCoE, and especially those well versed in cybersecurity grants, should be sought out for the unique expertise they can bring to the funding portion of the proposal.

NEXT STEP: BRING BENEFICIARIES INTO THE PROPOSAL PROCESS

A successful CCoE proposal rests on the ability of decision makers to effectively engage and consider the perspectives of the diverse key beneficiary groups that the CCoE aims to serve. It bears repeating that public health approaches to cybersecurity necessarily involve the public. No less than four of Sedenberg and Mulligan's 12 practices of public cybersecurity[387] involve seeking input or engaging in collaboration with the public;

[387] Elaine Sedenberg and Deirdre Mulligan, "Public Health as a Model for Cybersecurity Information Sharing," 1737-1738.

special emphasis is given to engaging those that are typically disenfranchised from such decision-making processes. Rowe et al also indicate that engaging a diverse audience through a variety of communications methods is vital to successful interventions[388]. Additionally, as Shane notes, "public participation can aid in agenda setting by clarifying the problems that need to be addressed and the priorities that ought to attach to them,"[389] especially with complex technology topics. Based on these arguments, actively seeking and considering public input on cybersecurity policies and initiatives from impacted communities is an important way to increase the success of a CCoE proposal.

Oregon survey respondents and focus group participants echo this sentiment. The need to engage a variety of stakeholders in decision-making processes and CCoE programs and initiatives was continually noted by participants throughout the focus groups, making "Diverse Involvement" one of the more prevalent themes to emerge in the data analysis process. This diversity especially includes making efforts to gather perspectives of those outside of the Portland-Salem I5 corridor, which participants recognized as a specific shortcoming of previous statewide initiatives. Respondents and participants from these areas also indicated widespread willingness to continue to be a part of dialogue and decision-making processes, and encouraged any report resulting from this research to emphasize this desire to be involved in any capacity moving forward. A key example from the comparative analysis of this type of effective outreach is Michigan's traveling Breakfast Series and Cyber Awareness Luncheon Series[390]. This series has provided opportunities for both outreach and dialogue on cybersecurity issues with communities across the state, including those that are located more remotely. Meeting face-to-face with members of communities outside of population centers should feature prominently in any plans for further information gathering by CCoE decision makers.

NEXT STEP: FOCUS ON WORKFORCE DEVELOPMENT

Workforce development can be a major contribution of the CCoE to Oregon's cybersecurity landscape, and as such deserves considerable focus in the initial CCoE programming and initiatives. This subject has featured prominently in every section of this report: myriad programs exist in other states that seek to increase workforce

[388] Brent Rowe, Michael Halpern, and Tony Lentz, "Is a Public Health Framework the Cure for Cyber Security?" *CrossTalk*, November/December 2012, 32.

[389389] Peter Shane, "Cybersecurity Policy as if 'Ordinary Citizens' Mattered: The Case for Public Participation in Cyber Policy Making," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012): 455.

[390] Michigan Office of the Governor, *Michigan Cyber Initiative*, 2015: pg. 8-10. http://www.michigan.gov/cybersecurity/Mich_Cyber_Initiative_11.13_2pm_web_474127_7.pdf

quantity and quality; survey respondents express great interest in increasing training opportunities; this theme is one of the top five identified through analysis of the focus group data; and many opportunities for grant funding from both public and private sources are for workforce development programs and initiatives. This is also one of the key substantive recommendations identified for the CCoE's initial structure and emphases. Taken together, this shows that creating and/or supporting programs that positively impact the cybersecurity workforce is an important part of the initial CCoE proposal development process, and warrants more immediate attention. Further specifics on workforce development needs and recommendations can be found in other sections of this report.

NEXT STEP: CONTINUE LEARNING FROM OTHER STATES

A final recommendation is simply to continue learning from other states. Make connections, have conversations, and get perspectives from those who have been a part of building cybersecurity initiatives from the ground-up in the states discussed in the comparative policy section of this report. If specific programs or initiatives are being considered for the proposal, seek out those who have been involved in similar initiatives elsewhere to learn from their experiences. States and advisory bodies were generally forthcoming with information for this project, and any decision makers can expect similar candor when seeking out these perspectives. The public Oregon Cybersecurity Advisory Council meetings can provide an excellent forum for decision makers and the interested public to ask questions and gather information from these resources; this is also a opportunity for identifying possibilities for multistate collaborations (a key function ascribed to the CCoE under SB90). Attendance at relevant professional meetings and trainings over the next year can also serve this information-gathering and learning purpose. Two examples of these kinds of events include the CyberUSA Conference in January 2018, and the National Initiative for Cybersecurity Education meeting in December 2018.

This list of basic next steps can be beneficial to the CCoE proposal drafting process, regardless of the contents of the proposal or the make-up of the decision-making body. There is considerable interest in this proposal within Oregon's cybersecurity industry that can be harnessed to create opportunities for meaningful engagement and deliberation. It is imperative that this effort results in a proposal that benefits all key beneficiary groups. By engaging a broad spectrum of actors and learning from the successes of others, decision makers can maximize the chances of its success.