Oregon Cybersecurity Center of Excellence

Portland State University

Birol A. Yeşilada, Ph.D.

Professor & Director, Mark O. Hatfield Cybersecurity & Cyber Defense Policy Center

(National Center of Academic Excellence in Cybersecurity)

Oregon State University

Tom Weller, Ph.D.

Professor & Head, School of Electrical Engineering and Computer Science

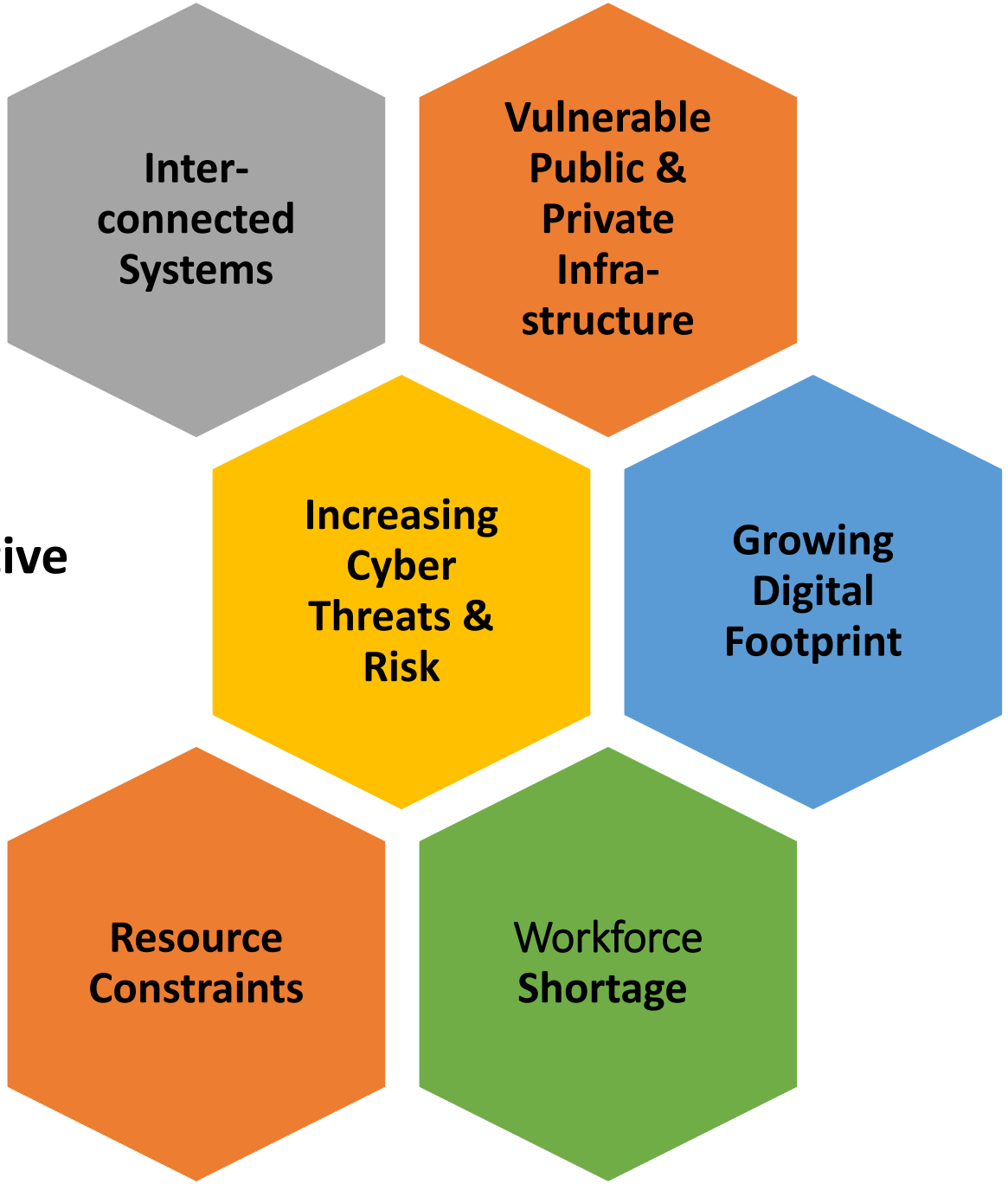
University of Oregon

Reza Rejaie, Ph.D.

Professor & Head, Department of Computer Science

Cybersecurity Problem

Calls for **Concerted**, **Coordinated** and **Collaborative** effort across public, private, and academic institutions!



Why Universities Host CCOE?

Coordination & Information Exchange

Building Partnerships and Community

Synergizes Education, Innovation & Workforce Development

Many states are following a model of leveraging their universities

Network & Systems Security and Resiliency

Oregon State University

Systems Security & Privacy, Cyber Operations

Portland State

Public Policy & National Security

OREGON CYBERSECURITY CENTER of EXCELLENCE

Community Engagement, Workforce Development, Security Services & Cutting Edge Research

CCoE Purpose

- *(a) Awareness, education and training about cybersecurity and cybersecurity-related issues for public, private and nonprofit sectors;*
- *(b) Cybersecurity workforce development programs in coordination with:*
  - *(A) Public universities listed in ORS 352.002;*
  - *(B) Community colleges operated under ORS chapter 341; and*
  - *(C) Science, technology, engineering and mathematics and career and technical education programs;*
- *(c) Research about cybersecurity education and training methodologies;*
- *(d) Research and development of cybersecurity technologies, tools, policies and processes; and*
- *(e) Cybersecurity-related goods and services to Oregon public bodies, with priority given to local governments, regional governments, special districts, education service districts, school districts and libraries.*

Oregon CCoE Mission Areas (Complementing State CIO Efforts)

Oregon CCoE Strategy

- Partnerships, Collaboration, and Community Engagement!
  - Partnerships: Universities, Community Colleges, K-12, Libraries, TAO (Industry), City Governments, County Governments, Special Districts, State CIO, and Federal agencies (i.e., CISA, FBI)

- Understand the scope and magnitude of problems on the ground
  - Stakeholder Engagement & Pilot Assessments

- Align and re-orient existing capabilities and resources at OSU, PSU, UO, and partners to serve mission areas

- Reassess and re-align goals and strategies at the end of the biennium

Fastest Path to Impact for Stakeholders!

Oregon CCOE: First Biennium

Standing up the Center

- Developing a Joint Operating Agreement
- Hiring Personnel
- Drafting and Adopting a Charter
- Engaging the Advisory Council and the State CIO's Office

Workforce Development

Need robust **cybersecurity** programs statewide, from K-12 to graduate education, to meet the demand

- Identify, compile, and assess all cybersecurity related offerings and pathways across the State
- [K-12] Engage students (NW Cyber Camps) and teachers (curriculum development) in cybersecurity
- [College] Support development & offering of diverse Cybersecurity offerings at Associates, Bachelors & Masters level at multiple institutions
- [Non-degree] Support development of non-degree certificate programs for continuing education and upskilling
    - Establish a “cybersecurity certification testing” scholarship fund to support students at MHCC and other community colleges

Awareness & Training

Need for increased cybersecurity awareness in public and cybersecurity training for other professions

- [Workshops] Support development of cybersecurity workshops targeted to specific professions
- [Events] Cybersecurity focused events to build community and engage stakeholders
- [Web presence] Create a one-stop shop for cybersecurity career, education & training pathways, and employment opportunities

Foundations for Resilience Roadmap

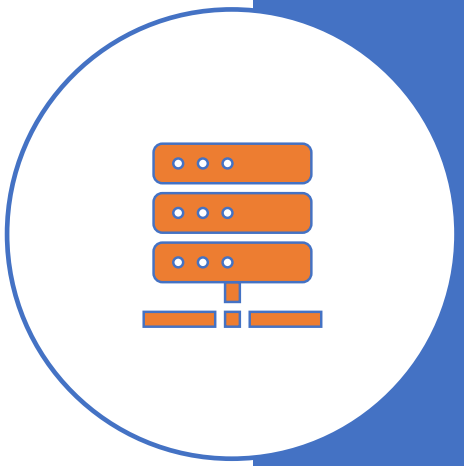
Understand current cybersecurity status across stakeholder entities for resilience roadmap

- Establish trust through engagement (listening sessions, etc)
- Gather information from stakeholders (surveys, infrastructure maps, etc)
- Conduct pilot assessments on selected stakeholders
- Develop scalable assessment model
- Prepare a preliminary resilience roadmap

Security Services

Provide security services for resource constrained public entities

- Compiling and sharing cybersecurity best practices
- Threat and risk information sharing and analysis
- Vulnerability scanning
- Network security monitoring
- Security assessment



Innovative and Engaged Scholarship

Bringing cutting-edge tools and practices to serve stakeholders

- Deploying scalable attack/anomaly detection between state cyber infrastructure and the Internet
- Developing new methods for detecting cybersecurity attacks against stakeholders
- Developing inter-disciplinary curriculum and innovative education methods

Federal & State Fund Management

Secure federal grants and manage state funds

- Catalyze and submit collaborative federal proposals
  - Research, education and workforce with community colleges, K12 and others
- Develop processes for fund disbursement
- Hire Fiscal Officer to manage state monies and federal grants

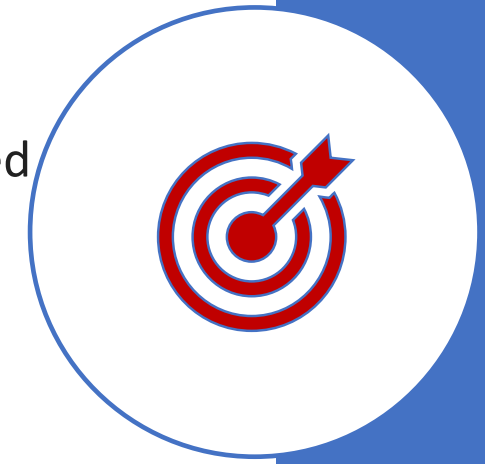
Expected Impact

Workforce Development, Awareness, Education, and Training

- Alignment and significant expansion of education and training programs across the State

Security Goods and Services

- Access to a growing set of cost-effective cybersecurity services for underserved stakeholders
- Clearinghouse for best practices and security information



Resilience Roadmap

- Preliminary resilience roadmap with a process for an informed resilience plan

Attract New Federal Funding

- Collaborative federal funding for research, education, and infrastructure


Q&A