Oregon Cybersecurity Advisory Council

Workforce Development / EDU Update

November 2021

Testimony By

Charlie Kawasaki, CISSP

Vice-Chair, Oregon Cybersecurity Advisory Council
Board Member, Technology Association of Oregon
Executive Council, OSU EECS Industry Advisory Board
Advisory Board, Chair, ORTSOC
Advisory Board, Cybersecurity, Mt. Hood Community College
Advisory Board, 3GO Security
Consultant and Investor, DeepSurface Security
Consultant, PacStar (Curtiss-Wright)
Associate and EIR, Bulls Run Group
Venture Partner, Oregon Venture Fund
Founder, NW Cyber Camp

"I am excited to collaborate with public, private sector and educational efforts in Oregon to address the critical shortcomings in cybersecurity workforce development, preparedness and response.

Nearly every sector and citizen of our State urgently needs assistance, and I want to see Oregon become a testbed and leading example for the nation, for addressing these issues.

Please collaborate with my office to assist in the advancement of initiatives to make this a reality."

Senator Ron Wyden – September 17, 2021

Oregon Cyber Breaches

279 companies reported breaches since Jan 1, 2016

As of 2/24/19

https://justice.oregon.gov/consumer/DataBreach

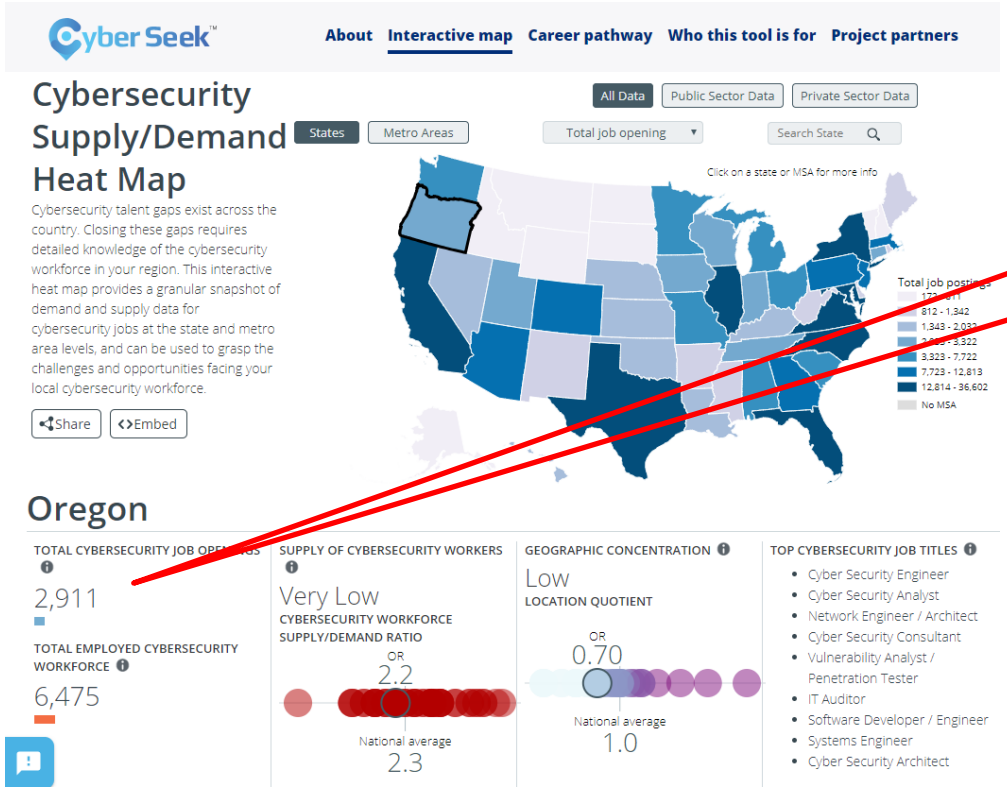
Oregon Cyber Breaches

New total: 610 companies reported breaches

As of 9/12/21

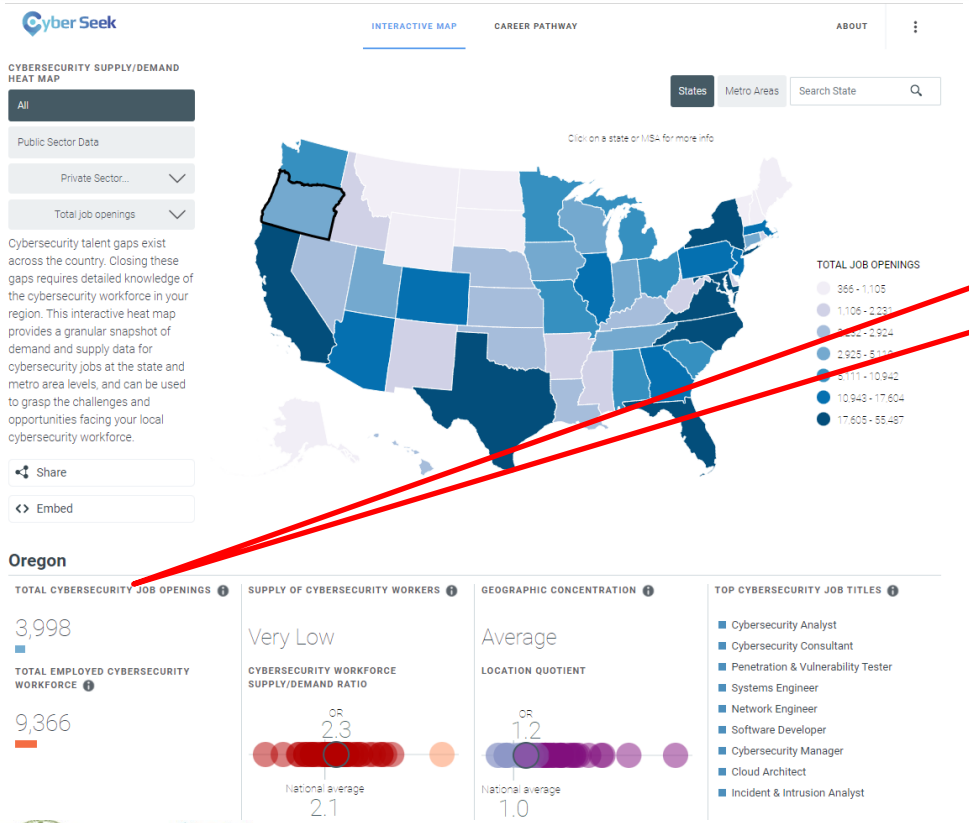
https://justice.oregon.gov/consumer/DataBreach

Snapshot Feb 24, 2019 http://cyberseek.org/heatmap.html



Oregon
2,911 unfilled positions

Snapshot Sept 12, 2021 http://cyberseek.org/heatmap.html

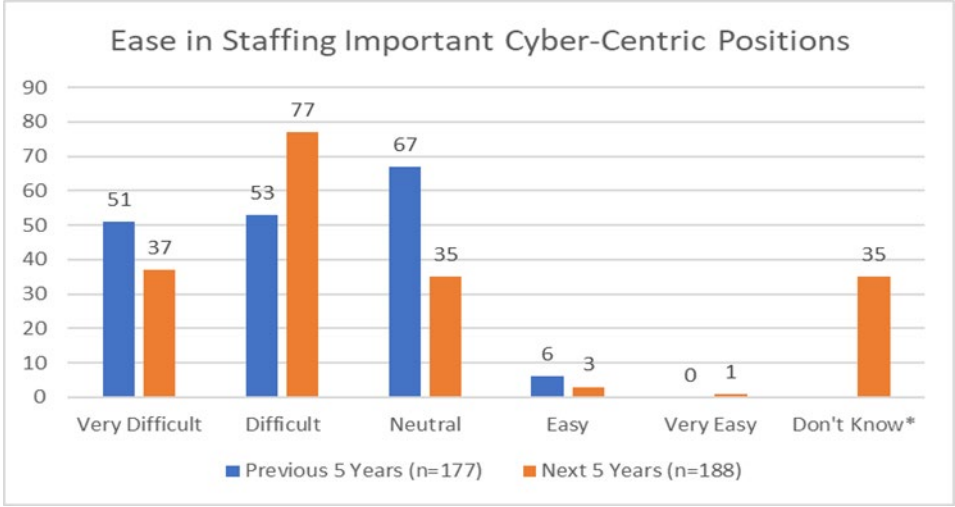


Oregon
3,998 unfilled positions

- **In 30 months since the last update 2,891 workers have joined the Oregon cybersecurity workforce.**
- **A 44% increase in the total workforce in under 3 years**
- **~100 new hires per month**
- *But the number of unfilled openings has gone up by 1087 – showing that the we are falling even further behind in meeting the need*

Survey: Difficulty in Staffing

"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"



ORTSOC

OREGON RESEARCH AND TEACHING SECURITY OPERATIONS CENTER

August 28, 2021

- "Teaching Hospital" to develop skilled workforce
  - National model for hands-on training
- Top-quality Security Operations Center to improve cyber security of "underserved", "resource constrained" organizations
- Research and Innovation to solve real-world problems
- Keystone of a World-Class Cybersecurity program
- Outreach for positive community impact

ORTSOC Academic Offerings

- Not just an internship: Curriculum Integration

- New undergraduate Computer Science Applied Track in Security Operations
  - Senior Year in Residence at ORTSOC
  - Real life, hands-on experience in a working SOC
  - Rotations in various operational areas
  - Mentorship from working professionals, guest lectures from experts

- New M.S. Track in Security Operations
  - Opportunity to specialize in operational areas
  - Exposure to Management/Leadership

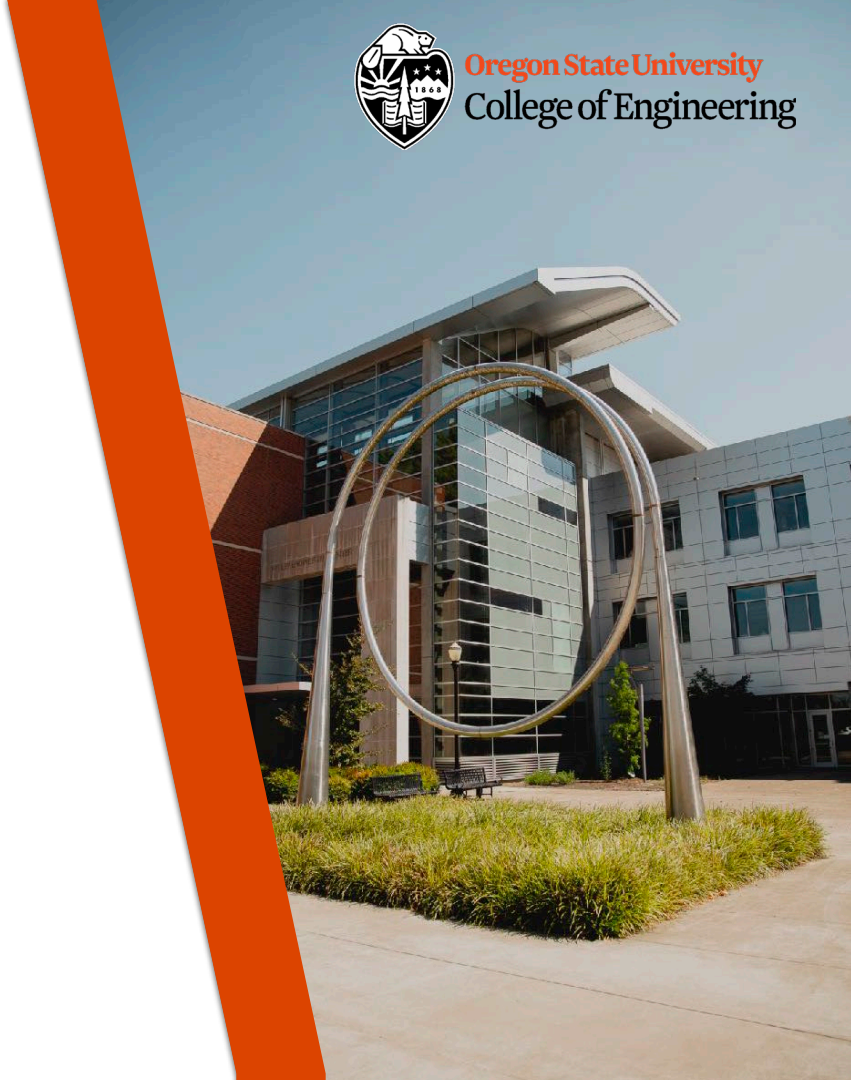
ORTSOC Consortium

- ORTSOC will be a consortium of Pacific NW Region "under-served", not-for-profit organizations, such as
  - K-12 School Districts and ESDs
  - Local Government and Special Districts
  - Tribal Government
  - Higher Education
    - ✓ Colleges
    - ✓ Community Colleges
  - Small Not-for-Profit Organizations

- Consortium members are unable to find/afford commercial security services

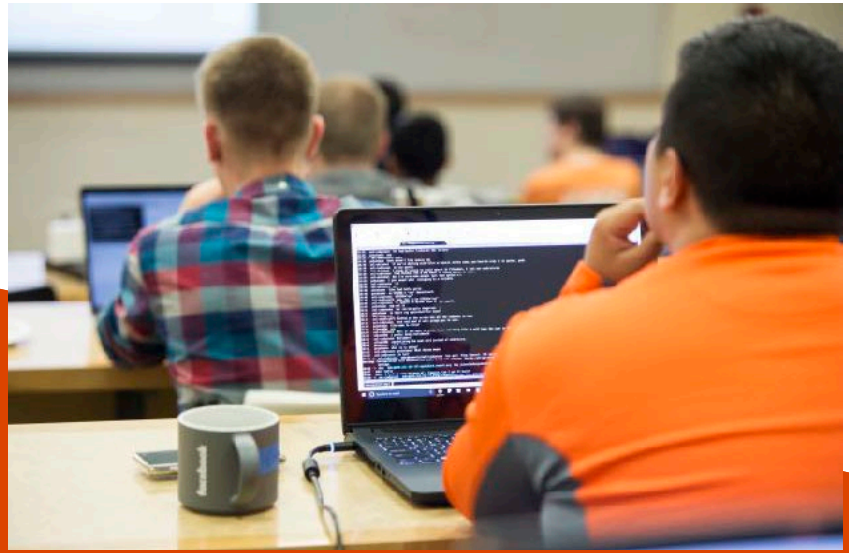
- ORTSOC will provide services to consortium members as a means of delivering real-world experience to our students

- Non-service memberships available for information sharing/collaboration with other regional organizations



Oregon State University
College of Engineering

Future Potential for Oregon



- The growth rate of ORTSOC, estimated at 250 students and 50 organizations served per year in 2031, could be significantly accelerated with additional financial support.
- The primary financial needs are for hiring additional cybersecurity professionals to provide oversight and mentorship, and providing student stipends
  - State funding of an additional $500k in 2022, $1m in 2023 & 2024 and $1.5m in 2025 and beyond would approximately triple the number of organizations served, and double student growth rate.
  - Further years of support would expand services offered and allow for advanced students to specialize in those areas.
- The ORTSOC core infrastructure and team is already funded by OSU and outside parties, so incremental funding directly impacts the rate of growth.

Thank you.

Rakesh Bobba, Ph.D.
Associate Professor
Electrical and Computer Engineering, OSU
Rakesh.bobba@oregonstate.edu
541-737-3333

Dave Nevin, CISSP
Assistant Professor of Practice, ORTSOC Director
OSU
Dave.nevin@oregonstate.edu
541-713-3549

Charlie Kawasaki, CISSP
Chair, ORTSOC Executive Committee
Software Diligence Services, LLC
ck@softwarediligence.com
503-906-1484

Mt Hood Community College Cybersecurity Department

Certification Fund Proposal

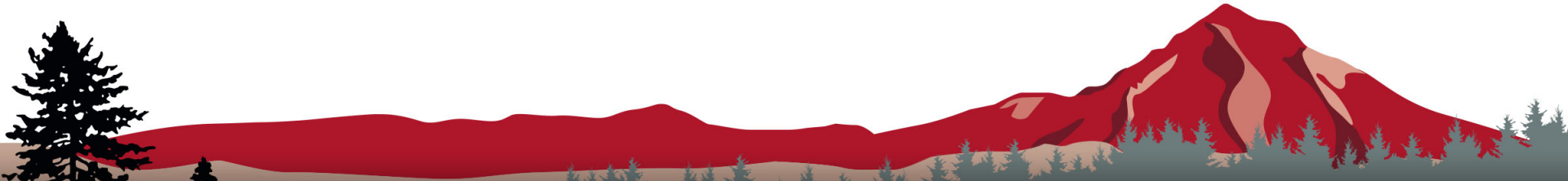
A Focus On Hands-On Education

We teach to the following credentials:

- CompTIA A+
- CompTIA Security+
- Cisco CCNA
- Cisco Cyber Ops
- AWS Cloud Practitioner
- Red Hat Certified Sysadmin

The mission of the MHCC Cybersecurity department is to offer ***relevant***, and ***applied*** education. That's why a number of our courses focus on training for industry certifications and modern practices and tools being used by professionals in industry.

We serve over 100 active students, with two degree programs and a professional certificate pathway.

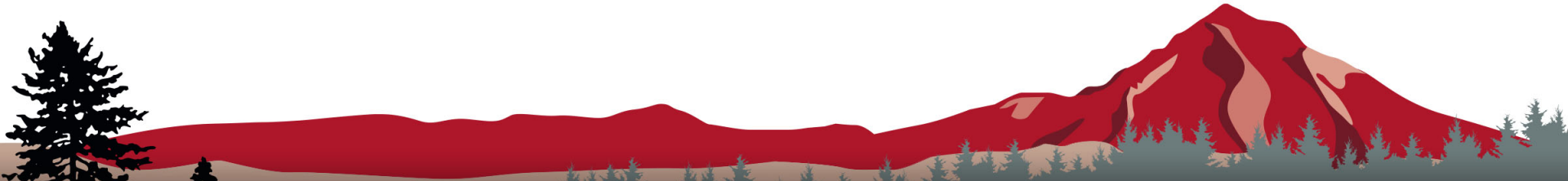


Serving a Diverse Community

The MHCC Cybersecurity program serves an incredibly diverse set of students, both in traditional DEI terms as well as others often less considered.

The average student age at MHCC is over the age of 30

- High population of students who are considered low-income
- Our program attracts a higher-than average number of veteran students
- Most of our low-income students are also traditionally underserved students (Black, Hispanic, Asian, etc.)



A Skills *demonstration* Gap

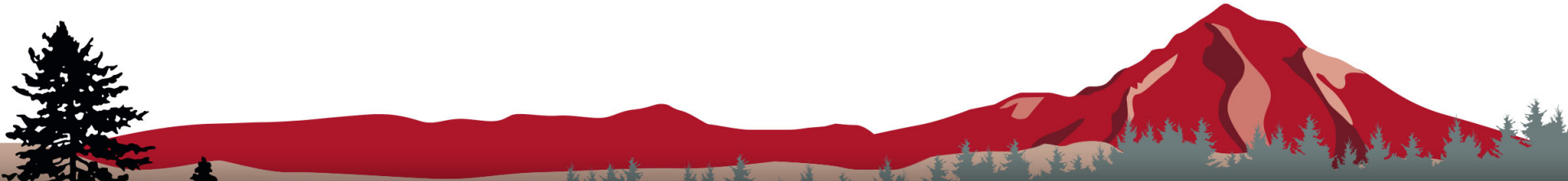
- Many industry partners are *willing* to hire AAS cyber graduates and rightfully so
  - ***Practical*** technical training
  - ***Immediate readiness*** for skills needed now using tools available now
  - ***Efficient*** – MHCC can source multiple graduates, streamlining hiring and training

But an Employability Catch-22 Emerges

Our industry partners tell us that students who obtain industry certifications can have a clear advantage in the job market—however, many of our students cannot afford to take these certification exams.

Students need the certifications to get a job, but they need a job to pay for the certifications.

Over 90% of our students cite the lack of funds for the reason why they do not take these exams.



Solution: Certification Fund

MHCC seeks donations to build a fund for student's certification exam vouchers.

With full funding, ideally, each student would receive two certifications per year.

Scholarship Annual Funding Goals

Yearly Funding Goal	Outcomes
$6,250	25% of students are awarded two vouchers* ** *(GPA and needs-based)*
$12,500	50% of students are awarded two vouchers* *(GPA and needs-Based)*
$25,000	100% of students are awarded two vouchers though duration of their 2-year program*
$50,000	100% of students are awarded four vouchers through the duration of their 2-year program*

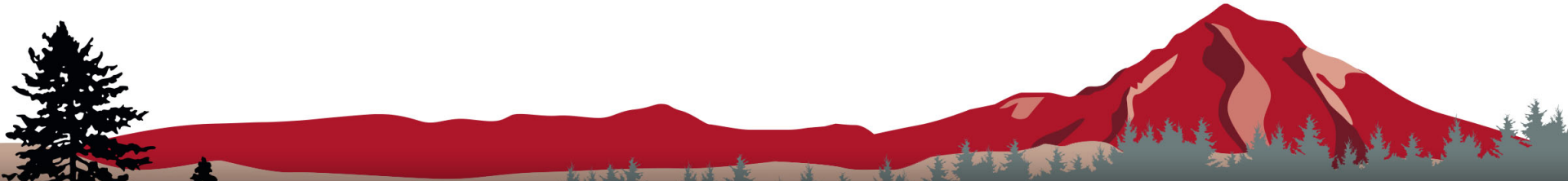
*Some exams are cheaper than others, which may allow a student to take more than two exams, while others might pursue a single more expensive exam

**Initial student uptake in this scholarship may need to ramp up, based on initial student hesitation and creating a culture of certification exam taking.

Future Potential for Oregon

This MHCC program could grow to 5-10 community colleges in Oregon, potentially serving several hundred students.

Assuming the program can be expanded to 500 students pursuing 2-year degrees, annual costs would be ~$250k. This would graduate 250 certified students per year, across Oregon community colleges.



Thank You!

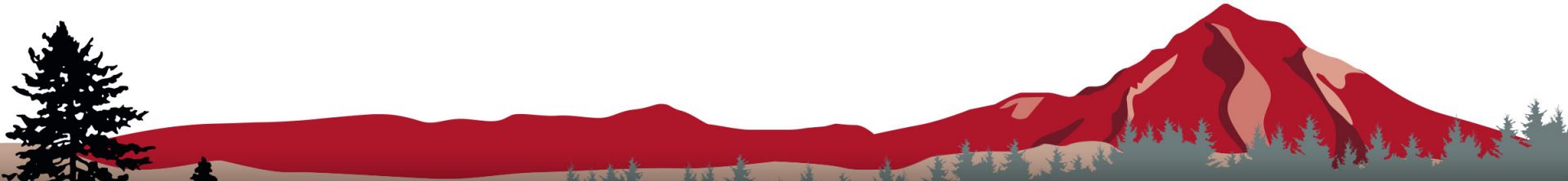
For questions about the program:

Charlie Kawasaki | ck@softwarediligence.com

Katrinia McNeal | Katrinia.McNeal@mhcc.edu

For questions about donating:

Al Sigala | Al.Sigala@mhcc.edu



2019 Sponsors

NW CYBER CAMP

NW Cyber Camp - Overview

- Web site: www.nwcyber.camp
- Founded and operating continuously since 2016
- Served hundreds of K-12 students, as a weeklong summer, day-camp
- Operating virtually since COVID
- Managed since 2019 by OSU and EnergySec
- Driven by volunteers, with a modest amount of industry financial support for direct expenses

NW Cyber Camps 2021-2022: Summer 2021

Purpose: "To **INSPIRE STUDENTS** Towards Careers in Cybersecurity

- One week educational camp for 9th to 12th grade students (novices)
- One week educational camp for 9th to 12th grade students (advanced)
- Dates: July 12 to July 16; Advanced Camp – July 19 to July 23
- Two locations simultaneously
  - Co-Ed, Online
  - Co-Ed, In-person Oregon State University, Corvallis OR
- $250 student fee - scholarships available based on financial need (up to 25% of students)
  - **We are able to keep the fee at an accessible level due to the generous support from sponsors!**
- Student Registration deadline, June 15th, 2020. Accepted on first come first serve basis
- Students register here: www.nwcyber.camp
- Managed by EnergySec (www.energysec.org) an Oregon 501c(3) non-profit, and STEM Academy of Oregon State University (OSU)

NW Cyber Camps 2021-2022: Workshops

Purpose: "To **INSPIRE STUDENTS** Towards Careers in Cybersecurity"

- Each 1-day workshop will take place on a Saturdays.
- Dates: TBD (In 2020/21 – Fall Workshop was October 10&17; Spring Workshop was April 24th and May 1st
- Workshop Overview
  - Introduction of basic cyber security concepts
  - Talks by local cybersecurity professional
  - Practice competition.
- Three locations simultaneously (Tentative: COVID protocols may require us to go fully online)
  - Mt. Hood Community College, Gresham, OR
  - Oregon Institute of Technology, Wilsonville, OR
  - Oregon State University, Corvallis OR
- $50 student fee - scholarships available based on financial need (up to 25% of students)
  - **We are able to keep the fee at an accessible level due to the generous support from sponsors!**
- Student Registration deadline: TBD. Accepted on first come first serve basis
- Registration information: www.nwcyber.camp
- Managed by EnergySec (www.energysec.org), an Oregon 501c(3) non-profit, and Oregon State University (OSU)

Future Potential for Oregon

- ***NW Cyber Camp needs funds for staff, teaching, curriculum development and student recruitment.***
- ***We believe there is enough demand for ~10 or more camps throughout the State of Oregon – serving as many as 300 students per year***
- ***However, NW Cyber Camp is in danger of discontinuing due to lack of sustaining financial support and tiring volunteers.***
- ***2018 budget models showed $180k/year could be sufficient to stabilize the program and grow it to 10 camps***

Program Organizers

Visit us on the web at:
www.nwcyber.camp

Twila Denham
EnergySec
503.850.0162
twila@energysec.org

Mary Parker
EnergySec
503.308.7963
Mary.parker@energysec.org

Rakesh Bobba, Prof
OSU
(217) 898-4921
Rakesh.Bobba@oregonstate.edu

Catherine Law
OSU
(541) 737-1822
catherine.law@oregonstate.edu

Awareness

Nearly all programs / stakeholders cite a need for awareness including for:

- Recruiting students into cyber educational tracks and careers
- Raising visibility at boards/governance
- Accelerating adoption of better defenses
- Building support for shared programs
- Promoting available resources/programs

Awareness: CyberOregon

CyberOregon.com

- Developed by OCAC, TAO
- Initially funded by with donations from cybersecurity companies
- Maintained by McKenzie Worldwide on a volunteer basis for the last few years
- Could easily be ramped up and expanded
- ~$160K per year for web site, conferences, social media

Portland State
Hatfield School of Government

Cybersecurity Community Development

NSA Grant Initiative 2021-8 option 3

Critical Infrastructure Coalition

(local & regional - multi-state project)

- *Professor Birol A. Yeşilada, P.I. Portland State University*
- *Professor Barbara Endicott-Popovsky, Co-P.I., University of Washington*
- *Professor Tuğrul Daim, Co-P.I., Portland State University*

Portland State University

NSA/DHS National Center Of Academic Excellence in Cybersecurity Research

Project Overview

Portland State
Hatfield School of Government

- This is a **2-year $2 million project** that focuses on the **Smart Grid** as one of the essential critical infrastructures which represents a complex network managed across federal, regional, and local level actors.
- The Federal Energy Regulatory Commission (FERC), augmented by the National Institute of Standards and Technology (NIST), identified six key priority functionalities of the **Smart Grid**:
  - (1) advanced metering infrastructure;
  - (2) demand response;
  - (3) electric vehicles;
  - (4) wide-area situational awareness;
  - (5) distributed energy resources and storage; and,
  - (6) distribution grid management.
- We will assess the system's strengths and weaknesses, with a special focus on local and country levels, to aid in bolstering cyber defense from physical infrastructure to human capacity through risk analysis of local and regional stakeholders' capabilities in cyber defense and the security of their connections to the SmartGrid.
- Local and county level vulnerabilities to cyber attacks represents ***America's Soft-underbelly***.
- Tabletop exercises will show how academic, government and industry partnerships can address these vulnerabilities and provide practical workforce training and education pathways with particular attention to the need for diversity and equity in cyberstudies.
- Our project will serve as a model to build and strengthen the NW Region's cybersecurity defense system through cooperation and collaborative problem-solving to provide mutual benefits in security, education, and multi-level (federal, state, and local) policy and technology alignment.

OUR GOALS

Portland State
Hatfield School of Government

- Establish an academia-industry-government partnership in Oregon and the PNW.
  - By engaging NCAE-C leadership from five states working in coordination with their respective county and local end-users and private sector partners the goal is to build a coalition of academia, government, and industry partners to address these vulnerabilities in a sustainable long-term plan.
  - Address Workforce Homogeneity and the Significant Shortage of Cybersecurity Capacity.
  - Assess the Severe Vulnerabilities and Risks of Local and County Governments America's Soft-Underbelly and Address Corresponding Risks to FEMA, DHS, and CISA Regions.
  - Work with NSA, DHS, and FBI to Analyze National Security Risks with Local Implications to Meet New Challenges in Cyber Attacks from Both Foreign and Domestic Adversaries
  - Develop Evidence-Based Policy Recommendations for and a Technology Roadmap (TRM) to Improve Cybersecurity Whole of State System Strategy.
- **Recommendations will be presented to elected local, state, and federal officials, private sector partners, and federal agencies.**

Regional Steering Committee

Creates a common agenda, high-level framework and a shared measurement system for cybersecurity networks

- Portland State University
- OSU & UO
- Mt. Hood Community College
- Chemeketa Community College
- UColorado-Colorado Springs
- University of Idaho or ISU
- Industry Representatives
- WA, OR, CO, HI and ID CIO's

Backbone Organizations

Coordinates the larger initiative, convenes the partners and provides operations support.

Portland State University
Chemeketa Community College
2021-8 NW Lead

University of Washington
WA Partner (sub)
OSU & UO
UColorado-Colorado Springs
University of Idaho
University of Hawaii

- *Research*
- *Education*
- *Training*
- *Outreach*
- *Apprenticeship*
- *Consulting*

NW Regional Consortium of Community Development Networks

Community development members meet regularly to review data, discuss progress, and share information with and learn from the steering committee, backbone organizations, and working groups as needed. Through these discussions, the working groups can adjust strategies and create action plans to bring those strategies to life

Portland State
Hatfield School of Government

Multi-State Regional Critical Infrastructure: Energy Security and the Smart Grid (OR, WA, and ID)

To develop a mechanism for regional government and industry collaboration facilitated by the academic institutions' cybersecurity expertise, and the resulting program to provide an educational experience for NCAE-C students in the course of ensuring cybersecurity consultation and services to the region's critical infrastructure post-grant.

K12 Education Partnership with PSU

Economic & Workforce Development

Cross-Sector Partnerships in Cybersecurity

Network of cross-sector partners working collectively to address complex cybersecurity issues. Partners work on an array of activities involving representatives from multiple sectors. Such efforts range from events and one-time projects, to government-appointed commissions and ongoing programs, as well as alliances of organizations that together have a role in solving a problem and achieving a shared goal.

Public Sector

- Federal Agencies (NSA, DHS, DOE, DOD PNNL)
- National Guard/Military Reserves
- State Agencies (Depts. of Education, Energy, etc.)
- Local City/County Managers
- Utilities (BPA, Idaho Power, etc.)

Private Sector/Industry/Public

- OCAC
- PGE
- Palo Alto Networks
- T-Mobile

NGO/Civic Organizations

- EnergySec
- Link Oregon
- MESA
- ODE STEM Hubs

Establish Joint Center

- The State of Oregon can be the catalyst for growth and maintenance of academic-industry-public partnership for cybersecurity in Oregon:
  - Provide annual financial support to expand PSU's efforts beyond critical-infrastructure / smart grid.
  - Provide support for and long-term sustainability of cybersecurity community partnership.
- Leverage PSU's policy and coalition existing efforts, rather than duplicating.
- Start with PSU as legal entity, while standing up a Joint Center – which would include Oregon Higher Ed, K-12/ESD, Local Government, Special Districts, Critical Infrastructure and Private Sector.
  - ~7-8 FTE, and student researchers – with contributions from multiple schools and stakeholder entities
  - Budget of ~$1.5 million per year

Summary

Getting Started

We need to get started. Many organizations are at high risk now, and growing our workforce is a long lead-time project.

- Make initial funds available to under-protected local gov/districts, K-12 - to make progress on cyber & IT modernization now
- Foster and accelerate workforce development programs – long lead-time programs are well behind in meeting the needs
- Develop a shared awareness program – a shared resource that will benefit all programs
- Stand up a joint center, with participation from higher ed, K-12/ESD, local government, special districts, and private sector.
    - Conduct a thorough needs and gap assessment, with budgetary impacts
    - Begin development / foster additional programs to fill those gaps

Thank You!

Charlie Kawasaki, CISSP
ck@softwarediligence.com