

## Cybersecurity Advisory Council Meeting Agenda

### I. Introductions (10 min)

- We have some new members on our committee, and not everyone has had the opportunity to meet one-another.

### II. COVID Update (10 min)

- What does our program look like?
- What has the impact been?
- When will we return to normal?
- Any other questions?

### III. General Program Update (20 min)

- NDG servers being installed
- S-STEM grant approved; scholarships are being processed; fall term start
- First time teaching AWS, growing pains

### IV. Mini Program Feedback Workshop (30 min)

- Independent review: 10 minutes
- Small-group review: 10 minutes
- Whole-group review: 20 minutes

### V. Bachelor of Applied Science Degree (20 min)

- Our plan to offer a BAS
- Current Timeline
- Action Item: Need Letter of Support

### VI. Adjournment



🏠 **Location:** Remote via Zoom  
📅 **Date:** 5/14/2021  
🕒 **Time:** 10:00AM

### MHCC and Participating Industry Partners

Center for Advanced Learning (K-12)	PacStar Communications / Curtiss-Wright Defense Solutions
Cybersecurity & Infrastructure Security Agency (US)	Palo Alto Networks
Legacy Health Systems	Port of Portland (OR)
Multnomah County (OR)	Uptycs
NetSPI	

### Meeting Notes for May 14, 2021

Wayne introduced new members to the Cybersecurity Advisory Council, and provided a brief opportunity for everyone to introduce themselves.

**COVID updates** – provided an update as to Mt. Hood Community College’s current operational status. All classes are being held virtually at this time. However, the college is developing a reopening process that will allow some classes back on campus when it is safe to do so. We have had some retention issues due to a move from face-to-face/hybrid to remote or fully online. However, we are also trying our best to accommodate students needs. A Reopening Plan will be submitted within the next month or so for Winter 2022 courses back on campus.

### General Program Update

Last year MHCC purchased an NDG subscription as well as physical equipment in the form of two server racks, three NDG servers and lots of Cisco hardware. Tobin Shields is working with NDG to get the equipment installed once it arrives. We hope to use this equipment can help support virtual labs with real equipment on-site in the near future.

Our S-STEM grant application was approved for scholarship applicants and will start fall term of 2021. As part of the grant, a new ISTM100 – Preparation for an Education in I.T. – has been created to support a sense of belonging and help improve student retention in our Cyber programs. Right now it appears four or five students are eligible for the scholarship which is exciting.

We first offered the ISTM171 – Intro. to Cloud and Virtualization Technologies course this term and have been utilizing Amazon Web Services (AWS) to assist in curriculum delivery. The AWS labs are good, but updated in the middle of the term which don't allow our instructors an opportunity to troubleshoot potential issues quickly enough before the new labs are assigned. More work is needed to address this potential issue in the future.

### **Mini Program Feedback Workshop**

For this task we asked the advisory council members to provide feedback on our course offerings specifically to address:

- Are you happy to see something being taught that you feel is especially important?
- Are there any classes/topics that you feel like are missing that don't appear in the degree?
- Are there any classes/topics that are currently being taught that you feel like are not valuable presently, or may not be valuable in the next five years?
- What is your thought on the overall scope-and-sequence?

Here is some of the feedback that we heard.

- Fundamentals of Project Management is critical (should be offered early on).
- Cloud (ISTM171) is super important. Cloud security course would be a critical addition.
- Zero trust and modern triple AAA schemes need to be incorporated.
- Supply chain management – SolarWinds breach is an important lessons learned activity.

- Endpoint Detection and Response (EDR) and Security Orchestration, Automation, and Response (SOAR) also should be introduced.
- Vulnerability management is a huge topic that definitely needs attention – possibly introduced in ISTM183C – Fundamentals of Cybersecurity and assessed in ISTM283A – Fundamentals of Disaster Recovery and Business Continuity.
- Re-evaluate web authorization and mobile app authorization. Possibly replace with a course in secure coding practices.

### **Bachelor of Applied Science Degree**

The Oregon Legislature (2019) approved Senate Bill 3 which became effective January 1, 2020. Senate Bill 3 “permits community colleges to offer applied baccalaureate degree programs under specific conditions and upon receiving approval from Higher Education Coordinating Commission.” As most of you know, MHCC became the first cybersecurity program at the community college level which was approved in 2012. We are now interested in applying for a new degree pathway, specifically a Bachelor of Applied Science (BAS) in Cybersecurity. Our timeline for submission to HECC is very soon. We are asking for your assistance with two things: (1) a letter of support for a proposed BAS and (2) your response to the following questions:

- Do you have anticipated demand for (named) job title that requires competencies such as (list them)? Provide a brief description of specific job duties for this (named job).
- If there is demand, how many positions do you currently have open?
- How many do you anticipate having open over the next 3 years?
- Is a bachelor’s degree a requirement or preference for this position?
- Do you have difficulty finding Bachelor’s degree level applicants for this position? (If yes- explain)
- Will the proposed program (provide description) assist you in finding qualified applicants to fill your position(s)?

To move expeditiously, we are asking for your feedback to be submitted to Tobin Shields ([tobin.shields@mhcc.edu](mailto:tobin.shields@mhcc.edu)) and Dr. Wayne Machuca ([wayne.machuca@mhcc.edu](mailto:wayne.machuca@mhcc.edu)) no later than Thursday, May 20, 2021.