

# MHCC CYBER SECURITY ADVISORY COUNCIL AGENDA

Date: May 20, 2022

Time: 10am

Facilitator: Dr Wayne Machuca

## Faculty Cyber Team

Item	Item	Owner
1.	Welcome Back – General Introductions a. Name, Organization, 1 interesting problem you are working on right now	Machuca
2.	State of the Program a. Introducing Dr. Kristin Lima, new Dean b. Returning to Campus c. New Labs d. NDG e. Outreach	Machuca+
3.	State of the BAS Degree a. Curriculum Review b. Discussion / Feedback c. Next Steps (Sperley/Lima)	Sperley
4.	Grants Update a. SCC Grant – Introducing Jenni Newby b. Certification Grant – McNeal c. S-STEM Scholarship Grant - Machuca	Various
5.	Discussion (encouraged throughout)	Open
6.	New Business – Good of the order – Next Meeting	Machuca
7.	Adjournment and Gratitude	Machuca

# ADDENDA

## Contact List:

Dr Wayne Machuca - [wayne.machuca@mhcc.edu](mailto:wayne.machuca@mhcc.edu)

Jeff Sperley - [jeff.sperley@mhcc.edu](mailto:jeff.sperley@mhcc.edu)

Katrinia McNeal - [katrinia.mcneal@mhcc.edu](mailto:katrinia.mcneal@mhcc.edu)

Pam Wiese - [pamela.wiese@mhcc.edu](mailto:pamela.wiese@mhcc.edu)

Dr. Kristin Lima, Dean - [kristin.lima@mhcc.edu](mailto:kristin.lima@mhcc.edu)

Darcey Huecker, Administrative Assistant - [darcey.huecker@mhcc.edu](mailto:darcey.huecker@mhcc.edu)

## Full Zoom Invitation

Dr. Wayne Machuca - MHCC is inviting you to a scheduled Zoom meeting.

Topic: MHCC AC May 2022 Advisory Committee Meeting

Time: May 20, 2022 10:00 AM Pacific Time (US and Canada)

Join Zoom Meeting

<https://mhcc.zoom.us/j/98986424470>

Meeting ID: 989 8642 4470

One tap mobile

+16699006833,,98986424470# US (San Jose)

+12532158782,,98986424470# US (Tacoma)

Dial by your location

+1 669 900 6833 US (San Jose)

+1 253 215 8782 US (Tacoma)

+1 346 248 7799 US (Houston)

+1 646 876 9923 US (New York)

+1 301 715 8592 US (Washington DC)

+1 312 626 6799 US (Chicago)

Meeting ID: 989 8642 4470

Find your local number: <https://mhcc.zoom.us/u/acGJxPZFQp>

## MHCC and Participating Industry Partners

CorVel Corporation	NW Natural Gas (OR)
Cybersecurity & Infrastructure Security Agency (US)	Port of Portland (OR)
NetSPI	Software Diligence

### Welcome & Introductions


The cyber team introduced ourselves. Dr. Wayne opened up introductions for all participants and asked them to describe (1) interesting problem they have recently encountered.

### State of the Program

- Dr. Kristin Lima was introduced to new Cybersecurity Advisory Council participants. We appreciate your input into our proposed Bachelor of Applied Science (BAS) in Cybersecurity.
- We are moving back to in-person courses as much as possible. Since we are computer and information system based, it allows us a little flexibility in our delivery of instruction using different modalities. Your feedback on what would be best for our students is important.
- Information Systems has moved from AC1271/1277 into AC2606/2610 and are also using AC2611 to assist us with face-to-face and hybrid courses.
- We are working on new labs for students utilizing NDG servers recently purchased. Right now these systems are internal only, and we are in the process of configuring courses and doing some beta testing to address any concerns. Cyber faculty continue to work with IT staff to assist in the management of the NDG servers.
- The Gresham-Barlow School District (through the CAL Center) has been instrumental in purchasing an additional server to incorporate as part of this plan. We look forward to working with them to deliver an exceptional service to not only MHCC students, but CAL students as well.

### Grants Update

- US Department of Labor (USDOL) Strengthening Community Colleges Training Grant. Purpose of the grant is to (1) build capacity of community colleges to collaborate with employers and public workforce systems; (2) meet local and



regional labor market demand for a skilled workforce. The Oregon Consortium grant is a \$5M award (4-year grant) through Jan. 31, 2025. MHCC and (8) other Oregon community colleges are participating in this grant. Our partners include the Higher Education Coordinating Commission (HECC), workforce investment boards, Oregon Workforce Talent and Development Board, and industry sector partners. Our focus is how we can accelerate learning pathways for Advanced Manufacturing and Cybersecurity sectors.

- One of the grant outcomes you can help us with is by becoming a strategic partner rather than an advisor partner. An **advisor partner** participates on industry advisory boards for Career Technical Education (CTE) programs only. A **strategic partner** is defined as employers who contribute resources such as expertise or equipment to strengthen career pathways, and participate in curriculum development, skill mapping, and validation – particularly for stackable credentials and badging components.
- The Cybersecurity Advisory Council members highly value internships (specifically our WE280CAD Co-op Internship). However it has been challenging to locate internships for our cyber students. Some of this is based on the nature of our programs (cybersecurity – no thank you, I would rather save money by not knowing my network isn't reliable; "You want to do some penetrating testing on my network!").

### **State of the BAS Degree**

There are many Bachelor of Science (BS) degrees in Cybersecurity programs across the country right now – at universities. We are looking to make our Bachelor of Applied Science in Cybersecurity program unique to help meet the needs of our industry partners and region constituents. We are seeking your input on the list of proposed courses to see what you think is relevant, what may be missing, and any other thoughts and ideas you may have. We are a practical application – our students have boots on the ground and are ready to rock and roll on day one, with some potential mentoring needs initially. There are several focus areas we are looking into for this program including *fundamentals; strategies; technical topics; management; languages and programming; competitions and intercollegiate; and projects.*

### **New Business | Good of the Order | Adjournment**

The list of proposed courses will be provided to the Cybersecurity Advisory Council participants for review. While the discussion at this point has been great, we seek your added input as we work on our proposal through the Oregon HECC.

# MHCC BAS Degree Courses Proposal

Courses are identified as first level (300- level) and second level (400- level) and are distinguished by course sequencing and not (necessarily) by year.

## Course

### Number Title and Description

#### x00 - Fundamentals

##### ISTM300 Issues in Cyber Security

This cyber survey class is designed to prepare students with either existing IS, IT, or Cyber Security AAS degree, or with equivalent IT industry experience, or returning student with advanced degree, to get foundational training on current cyber topics allowing successful entry into the Cyber Security BAS program.

#### x10 - Strategies

##### ISTM310 Cyber Defense Strategies (Blue Team)

This class establishes common defense strategy concepts and designs. Students will learn the basics of hardening an IT environment, implement monitoring and alerting tools across a network, and also conduct basic threat hunting activities. Students will develop a rudimentary Security Operations Center (SOC) as well as work with a Security Information and Event Management (SIEM) platform. Independent lab work is required.

##### ISTM315 Cyber Offense Strategies (Red Team)

This class will extend student's understanding of penetration testing concepts from previous courses and learn how to engage in a more complex set of attack types, tools, and processes. An emphasis will be placed on "Red Team" activities and learning how to attack an active and complex network with a wider attack surface.

#### x20 - Topics

##### ISTM320 Practical Digital Forensics

In this course students learn the fundamentals of digital forensics and incident response. They are introduced to digital forensic tools and techniques to analyze data collected from electronic devices (including computers, media, and other digital sources). They will become familiar with proper techniques and tools utilized for securing, handling and preserving digital and multimedia evidence. Students are also introduced to the incident response process.

##### ISTM321 Mobile Forensics

This course introduces students to the fundamentals of mobile forensics. Presented are techniques, tools, and procedures for conducting digital and network forensics of mobile devices. Topics include mobile forensics procedures, related legal issues, mobile platforms, bypassing locks, rooting/jailbreaking process, logical acquisition, physical acquisition, data recovery, analysis, and reporting.

##### ISTM322 Critical Infrastructure

This class is an overview of the impact of cyber security critical infrastructure. Topics include attack targets, vulnerabilities, and actors. Various methodologies are appraised for mitigation of attacks and reduction of attack profiles. Lab work includes introduction to “ladder logic programming” and other Critical Infrastructure-based techniques. Prior programming experience in any modern language is recommended.

**ISTM323 Computer Architecture for CyberSec**

This course is an introduction to computer architecture, as it applies to cybersecurity professionals. Topics to be covered include: von Neumann architecture, pipelining, multithreading, storage, memory hierarchy, caching, cache analysis, operating systems, parallel systems, and emerging architectures.

**x30 - Management****ISTM330 Compliance**

This cyber management class explores the realm of cyber and legal compliance required for both business and government. Presented from the perspective of a layperson with no prior knowledge of concepts, topics in this class will include: the Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), personally identifiable information (PII) concepts, the Payment Card Industry (PCI), and various legal issues involving privacy directed toward how companies can effectively maintain a compliant stance.

**ISTM331 Risk Analysis**

This cyber management class takes an in-depth approach to understanding how to perform risk analysis and differentiate various kinds of risk affecting a particular organization. In this manner, all risks can be enumerated and then mitigated appropriately based on the technology and/or resources available to that organization.

**ISTM332 Project Management****x40 - Languages and Programming****ISTM340 Machine Learning and Artificial Intelligence I**

This course is the first of a 2-course sequence in machine learning (artificial intelligence). Topics to be covered include: terminology and scope of learning systems, mathematics of machine learning, classification of tasks, regression strategies, and evaluation of learning systems.

**ISTM440 Machine Learning and Artificial Intelligence II**

Topics to be covered include: regression analysis, unlabeled data, multilayer and convolutional neural networks, embedding machine learning models into web applications, and reinforcement learning.

**ISTM345 Assembly Language for Cyber Security**

This course is an introduction to assembly language programming, as it applies to CyberSecurity professionals. Topics to be covered include: C programming, assembly instruction set architectures (x86-64, IA32, and ARM), conditional and repetition structures, functions, and arrays in assembly.

**ISTM346 Secure Programming**

This course introduces the secure software development process, including designing secure applications, writing secure code that can withstand attacks, and security testing and auditing. It focuses on the security issues a developer faces, common security vulnerabilities and flaws, and security threats. The course explains security principles, strategies, coding techniques, and tools that can help make code resistant to attacks. Students will write and analyze code that demonstrates specific security development techniques.

**x80 - Competitions and Intercollegiate**

**ISTM380 Cyber Comp I**

This course is the first in a series of four total cyber competition courses offered for the AB in Cybersecurity program. This course will allow students to compete individually and in teams based on concepts / subject materials presented in Year 3.

**ISTM381 Cyber Comp II**

This course is the second in a series of four total cyber competition courses offered for the AB in Cybersecurity program. This course will allow students to compete individually and in teams based on concepts / subject materials presented in Year 3.

**ISTM480 Cyber Comp III**

This course is the third in a series of four total cyber competition courses offered for the AB in Cybersecurity program. This course will allow students to compete individually and in teams based on concepts / subject materials presented in Year 4.

**ISTM481 Cyber Comp IV**

This course is the last in a series of four total cyber competition courses offered for the AB in Cybersecurity program. This course will allow students to compete individually and in teams based on concepts / subject materials presented in Year 4.

### x90 - Projects

**ISTM490 Senior Project**

As a bridge from college to career, this capstone experience provides students with the opportunity to apply and expand on the knowledge and skills gained during their academic career. Students participate as teams in a virtual environment where they must defend a network with multiple devices while attempting to compromise the opposing team's network and devices. In this hands-on experience, they must rely on learned skills, industry best practices, and the teammates to be successful. Students also reflect and assess their own performance in this course.