MHCC CYBER SECURITY ADVISORY COUNCIL AGENDA

Date: November 19, 2022
Facilitator: Dr Wayne Machuca, MHCC

Faculty and Staff

Dr. Kristin Lima, Dean | Darcey Huecker, Admin | Jeff Sperley | Katrinia McNeal | Dr. Dustin Bessette | Pam Wiese | Dr. Wayne Machuca

Time	Item	Owner
Time	Welcome	KL
Time	Introductions – News from the Field?	KL
Time	Report from the Dean, updates on BAS progress • Introducing Dr. Dustin Bessette	KL/DB
Time	SCC Grant Stackable Credentials	WM
Time	S-STEM Grant – New Scholarships	WM
Time	BAS New Courses Question	??
Time	AAS/CIS/IT Degree Possible Modifications	JS
Time	Good of the Order	WM
Time	Plan for Next Meeting (~May 2023)	WM
Time	Adjournment	KL

MHCC and Participating Industry Partners

Archer Energy Solutions	PeaceHealth (OR)
Center for Advanced Learning	Port of Portland (OR)
Oregon State Legislature	Software Diligence
Palo Alto Networks	

Welcome & Introductions

After a brief welcome to the Cybersecurity Advisory Council participants, Dr. Lima introduced Dr. Dustin Bessette as our new Cybersecurity faculty hire. Dr. Bessette comes with prior experience at Portland State University and will be a valuable asset to our team. Other participants took a brief moment to introduce themselves as well.

Strengthening Community Colleges Grant – Stackable Credentials

Dr. Machuca introduced the concept of stackable credentials, and mentioned how it is a challenge. The challenge is while we are talking about cyber and cybertraining and credentialing (low, middle, high level) a lot of our thinking is based on our coursework here at MHCC. As we take these credentials and try to share them with sister colleges, there are courses that are similar across the state. Python, linux, MS office… most programs are the same types of training. Cert 1 – lower – what is the basic skills you need to get hired as... When you get into the mid range (second level), what are the skills you need to design, implement, modify… When you get into the high range (third level), what are the skills you need to participate as a … specialist? Are there legitimately hireable? Can you get hired without a degree but have basic certifications? Maybe you complete a few assignments in a particular topic, and you get a badge in… Are those important credentials for hiring?

Some feedback from the Cybersecurity Advisory Council indicated it's how students apply those skills. Internships, opportunities to practice those. In some cases, they haven't but you can show them these skills to show proficiency. Are you going to be successful for the role you looking at, or are you going to drown? Be able to adapt and respond to these bases. What's the process to go through the background to get you into these systems. You try and vet a lot of that before you go too far down that past.

Students need to have a strong foundation on critical analysis and critical thinking. End user support desk role – what do they understand is the problem? Determine what's going on, come up with a plan to implement these into the curriculum.

Some students have seen variations in hiring. Some are starting right out of high school. To be able to make a career pathway around that type of system. They can really easily see badges or minor certifications going towards help desk-type positions. Network tech, I don't know. Cyber, I really don't think so. We struggle with I want (5) classes, (10) weeks and I want to be hired.

Industry partners have been working on apprenticeship models. What is being described pairs very well with these. It's modular. The question is that doesn't align with a traditional approach to bring students in for the degree.

What we call entry-level cybersecurity is not truly entry-level. More often than not, they want to see systems infrastructure background, hardening systems, etc. Credential 1 might be A+ (help desk, IT-role). Credential 2 Cisco (Network Administrator, etc.). Credential 3 takes a look at Security+ (certification-focused). We could provide a peripheral knowledge to get them there. There are job roles that these could be tied to. That's what I'm hearing a lot. They want to hire people that have deep understanding of these systems. Some players don't care about the industry certs. Aligning our Mt. Hood cert with CompTIA certs – compared to those you just get these certs and run with them.

S-STEM Grant – New Scholarships

Last-year we created the Kawasaki-Berge cybersecurity certification fund. Our students have cited not being able to afford certifications. The least expensive one, it is $50. CompTIA range from $105-200. We wanted to be able to help them earn the certification to help make them more employable. Right now we currently have about $25,000. Recently we gave out (26) vouchers in total. This term we're offering it to students in our fall sections.

As part of an Ethical Hacking course last spring, the PenTest+ was issued as a final exam. 50% success rate on first attempt. What we're finding is once we removed the financial barrier, we need to get them through the anxiety and nervousness.

Have you considered pairing Sec+, Net+, A+ and others to reinforce that from a hiring manager's perspective you may be able to prove on multiple facets that you can accomplish these things. You're going to be way out of your comfort zone when you face an incident.

BAS New Courses

We have developed some ideas for a few other courses based on your feedback.

The conversations around this were absolutely explosive. I think I'm thinking what if we created a class in Identity and Access Management (IAM), cyber warfare, or a different more advanced certification?

The Cybersecurity Advisory Council mentioned IAM is being a part of some of their current roles. Integration with SAML and all the cloud-offerings that need to communicate.

The true entry-level security role tends to be the Security Operations Center (SOC) analysts. Watch for alerts. Know the anatomy of what the technologies that go into that. How to integrate all of the technology. I know that the the CompTIA Cybersecurity Architect (CySA) talks about that theoretically. At some point in a lab-based experience have a server, two workstations, and a SPLUNK system to analyze data. They need to know the anatomy of each part – how to get the data, and ask questions of the data. SPLUNK has significant amount of training as well.

AAS/CIS/IT Degree Possible Modifications

Three big realms. Python, python, python. Be enthusiastic. Can you demonstrate that you are interested in this conversation. In the discussions on proving (third part) – if you were to create a YouTube channel that shows your progress. Second one was when a CIO brought me aside and said have your folks make their own home network. Hardware is expensive, simulators or not. What did you do?

I've been doing a lot of research into cloud security. There is a massive investment headed in that direction. By the time your BAS program is up and running, I would recommend a substantial focus on cloud security. How that weaves through the coursework, or every one of the courses that you offer. Figure out a way that you can fire up a VPC and demonstrate skills in the cloud.

The initial intention of our degree is to do what everyone else is doing and a little bit more.

Possibly up to a server admin. Not necessarily desktop/IT support. Training on the most modern platforms – they can still get training in managing desktop operating systems. Office to Office 365. PCs are almost throw aways. I care about setting up my e-mail, mobile management, MFA.

We currently have three credits that's Microsoft Office. If I can crunch those down into Office 365 it opens up a spot for (2) or (3) other classes. Would you advise filling that spot with SPLUNK. Charlie – maybe not – if it's more technicians.

Interfacing with our own IT team at the CAL Center, I have a lot of need for our IT departments. They ask a lot of questions – as part of enterprise device management. How do you manage more of those enterprise management roles.

If these types tools are being powered out to third-party management systems, and more and more of this stuff gets sent out – do we need to have training in that kind of management? In (5) years who is going to have their own in-house e-mail system.

Functionality would be carry-over. The data loss concern, how am I managing it these. Don't invest in the idea that you have this thing – but what will you do with it. e-Discovery demand. How do my systems integrate to meet requirements to respond based on compliance and/or regulations. Bring in the right resources quickly, and how can you do this?

With a (2) year CIS degree, I am kind of going under the expectation that teaching the backend of productivity tools – probably not. However proficiency in various tools is important. Productivity tools in a class – Word, Excel, etc.

Good of the Order / Plan for the Next Meeting / Adjournment

We will have our most likely have our next advisory team meeting in May 2023. In the meantime we're definitely looking for new hires guest speakers who can present in our courses.

Figure out what should be added to the IT degree. Proposal – do we go to BA131 or do we go to CIS120L.