Minutes for Cybersecurity Industry Advisory Board (CIAB)

November 13, 2020 at 10:00 A.M (Via Zoom)

Attended by: Dr. Frederick Adkins, Dr. Francisco Alarcon, Mr. Robert Buckingham, Mr. Kevin Dodds, Mr. Tom Dugas, Dr. Soundararajan Ezekiel, Dr. Waleed Farag, Mr. Dom Glavach, Mrs. Karen Pizarchik, Mr. Daniel Saylor, Mr. Nigel Wright, Dr. Xinwen Wu

Introduction of the IUP CIAB Members:

1. Dr. Francisco Alarcon: Chair of the IUP Department of Mathematical and Computer Sciences.
2. Dr. Rick Adkins: Assistant Chairperson for Computer Science Programs in the Mathematical and Computer Sciences Department.
3. Mr. Robert Buckingham: Senior Director Information Systems Presbyterian SeniorCare Network and Vice President InfraGard.
4. Mr. Kevin Dodds: CIO at S&T Bank. Numerous Security, compliance, and criminology backgrounds. Previous experience of NCIS.
5. Mr. Tom Dugas: Assistant Vice President and Chief Information Security Officer for Duquesne University. Network security awareness, cybersecurity awareness and strategy. Speaks and talks nationally on cybersecurity.
6. Dr. Soundararajan Ezekiel: Professor of Computer Science.
7. Dr. Waleed Farag: Director of the IUP Institute for Cybersecurity and Professor of Computer Science. Dr. Farag managed several active federally funded projects at IUP.
8. Mr. Dom Glavach: Chief Security Officer and Chief Strategist at Cyber SN: Technology SaaS. General defense of information and consulting firm leadership. Specializing with research in exploitation and vehicle security (offensive security).
9. Karan Pizarchik: Assistant Dean, IUP Kopchick College of Natural Sciences and Mathematics.
10. Mr. Nigel Wright: Technical Program Manager, Uber.
11. Dr. Xinwen Wu: Associate Professor of Computer Science.
12. Mr. Daniel Saylor: Secretary of the IUP Cybersecurity Club and student researcher.

Formal Welcome to the Advisory Board

Creation of the chair position of the board

1. The CIAB members decided to conduct the board chairperson election after the meeting via email.

Declaration the board main objectives

1. To advise and guide the Cybersecurity programs at IUP to ensure that graduates meet and exceed the expectation of various employers in the cybersecurity field.

Review of the Existing Cybersecurity Track

1. Definition of liberal study requirements
2. Mathematical requirements
3. Core Computer Science Courses
4. Core Cybersecurity Courses
5. Criminology Minor

Open Discussion

1. Question regarding criminology minor. Is this useful?
    - Dr. Farag: Intention is to remain unique to other cybersecurity programs but this requirement limit our ability to require more technically oriented courses because of the limit of 120 cr to graduate with a BS degree.
    - Dr. Alarcon : We did not collect specific data to measure how useful this particular mix to potential employers, but we believe it does help with students who take on a legal profession.
    - Mr. Glavach: Having the cybersecurity student exposed to Criminology courses is generally helpful.
    - Mr. Dugas also agrees that as an employer, a criminology tie is an good idea.
    - Mr. Dodds thinks that experience in criminal justice can be achieved after graduation via various trainings. There are numerous federal agencies that would find the minor appealing. Additionally, as a bank security officer, the amount of coordination with law enforcement is absolutely a plus.
2. Mr. Buckingham: Red Team/Blue Team environment is lacking in this curriculum.
    a. Seconded by Mr. Dugas.

b. Dr. Farag indicated that such experience is briefly covered in the Network Security course and our extracurricular activities such as the participation of our Cybersecurity Club in various Hackathons.
c. Mr. Saylor described the scope, importance, and utilization of cybersecurity club exercises in the IUP scope.

3. Question by Mr. Glavach: What are the goals of the cybersecurity curriculum at IUP?
    a. Dr. Farag described the importance of designing our curriculum to map to the CAE Knowledge Units Framework and share with board members the Program Education Outcomes.
4. Dr. Ezekiel: Raised the point that some criminology concepts can help prepare students to the digital forensics course.
    a. The panel were inclined that deeper technical knowledge should be pursued over a criminology minor.
    b. One suggested solution by Dr. Adkins is to reduce the number of required criminology course to three which will open the room for addition technical courses to be required.
5. Dr. Ezekiel raised a question about the current utilization of coding courses, and asked the panel to contemplate the need for numerous coding courses in a cybersecurity track, etc.
    a. Dr. Farag and Mr. Buckingham indicated that it is important that all students should have these backgrounds before tackling cybersecurity specific courses.
6. Dr. Alarcon noted that undecided pathway students are a large reason for the current program design. He proposes a *'Current Issues (trends, threats) in Cyber Security'* course.
7. Dr. Farag asked if the cybersecurity required courses are enough for a complete experience.
    a. It is noted that a criminology minor is narrowing the scope and lessening the amount of time available for a more in-depth cybersecurity experience.
8. Mr. Dugas asked if the coding courses are the only core course. He suggested that network security should become a core class for all Computer Science students and not

only Cybersecurity students and discussed the importance of mapping the curriculum to various standards.

a. Mapping security technology to NIST NCWF and other standards was also suggested by Mr. Dodds.

Future Planning

1. It is decided that the board will provide a written recommendation report within four to six weeks.
2. Chair election will be conducted by emails.
3. The panel discusses the next meeting date and decided it will be in late March or early April.

Meeting was adjourned at 11:10 AM

Respectfully submitted by Mr. Saylor and Dr. Farag