



An Open University's Approach to Cybersecurity Education

Triple Threat Approach to Cybersecurity Learning and Workforce Development *Removing Barriers to Access*

Dr. Loyce Best Pailen, CISSP

Bruce deGrazia, JD, CISSP

*Dr. Valorie King**

Dr. Gregory Von Lehman



University of Maryland
University College

IT HAD TO BE UMUC | UMUC.EDU

**Not in attendance*

Title: Triple Threat Approach to Cybersecurity Learning and Workforce Development

- Three strategic approaches to support the development of cybersecurity professionals for the workforce.
 - Accessible,
 - Accelerated
 - Cybersecurity-aligned curriculum
- As THE Open University of the State of Maryland,
 - Meets educational needs of nontraditional students
 - Opens the door for diversity in students' academic and career backgrounds
 - Scales with customization, alignment and acceleration

Open Access Institutions

“What are open-access colleges?”

Open-access, nearly open-access, and nonselective institutions are defined as public four-year colleges and universities that admit at least 80% of applicants.”

Source: http://highereducation.org/pa_0210/index.shtml

Discussion

- Open Access to Cybersecurity Education
 - What does it mean?
 - How does it differ from traditional access?
 - Why does this choice matter?
 - Who does it benefit?
- Maintaining Open Access after Admission
 - Program Design
 - Curriculum Strategies

Open Access Begins with Admissions

- Who gets admitted?
- Who decides?
- What are the criteria for admission?
- How are these related to success in a cybersecurity career?

Typical Access Controls for Undergraduate Programs

- Ability to read / write (language of instruction)
- Earn High School Diploma
- Pass SAT or other standardized exam
- High School GPA
- Letters of Recommendation
- Community Service
- Extracurricular Activities
- Financial Wherewithal

Typical Access Controls for Graduate Programs

- Room in the Desired Program (# of seats per year)
- Earned Bachelors Degree (same field / closely related)
- Quality Metric for Previous Studies (e.g. Undergraduate GPA)
- Score on GRE or other standardized exam
- Statement of Academic Career Objectives and Evidence or Portfolio Showing Academic Potential
- Letters of Recommendation
- Financial Wherewithal

UMUC's Approach to "Access"

Graduate Cybersecurity

- Read / Write English
- Bachelors Degree (Official Transcript(s))
- Financial Wherewithal
 - Tuition & Fees
 - No textbook costs
 - Minimal additional direct costs
- Time

After Admissions ...

Access to Coursework in Cybersecurity

Where do Cybersecurity Courses Live?

- Computer and Information Sciences
- Computer Science
- Engineering
- Information Science
- Information Technology
- Management Information Systems
- Dedicated Programs in Cybersecurity

Program Approach #1: Bolt It On

- Add courses to major
 - Computer Security (3 credits)
 - Cryptography (3 credits)
 - Networking & Security (3 credits)
 - Incident Response & Disaster Recovery (3 credits)
 - Security Planning & Response (3 credits)
- Add content to elective or supplemental major courses
 - Cybersecurity and You (3)
 - Cybersecurity for the Social Sciences (3)
 - Cybersecurity for the Health Professions (3)

Program Approach #2: Build It In

- Dedicated Majors
 - Cybersecurity in IT
 - Cybersecurity in IT Management
 - Cybersecurity Policy
- Typical Length of Program
 - Undergraduate major = 30 to 36 focused credits
 - Graduate program = 36 focused credits

Removing Program Level Barriers

- Are Access controls really necessary?
 - What do you think about prerequisites
 - Question the "math" barrier
 - Question the "specialized" prerequisites barrier
 - Question the availability barrier (Sequencing, Scheduling)
 - Solution– add courses which are useful for majors AND non majors

Removing Program Level Barriers

- Accessible
 - Graduate school approach to enable career changers
 - Barriers removed by creating special courses
- Accelerated
 - 11-Week
 - Flexibility
 - Guided
- Aligned
 - Competency-based Foundation
 - ELM Project Based Learning

Project Based Learning

- ELM program
 - dispenses with mere acquisition of facts and terminology
- Replaced
 - with projects providing practical application for employment
- Knowledge
 - applied, not considered/learned in a vacuum

Student Population Considered

- Military and former military students
- Career changers
 - Offer them something they don't already have
- Professionals already in the field
 - students may know more about the details of the subject than professors

Closing Thoughts ...

- Practices and processes which control access to cybersecurity education should be examined to determine if they serve the needs of society.
- The structure of an academic program can facilitate or impede efforts to improve the availability of cybersecurity education.

Questions?