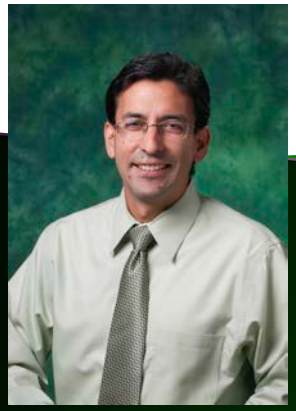
Pathway for Community College Students to an ABET-Accredited Degree in Cybersecurity

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
College of Engineering
UNT

- Mark Thompson
- Ram Dantu



Problem Motivation

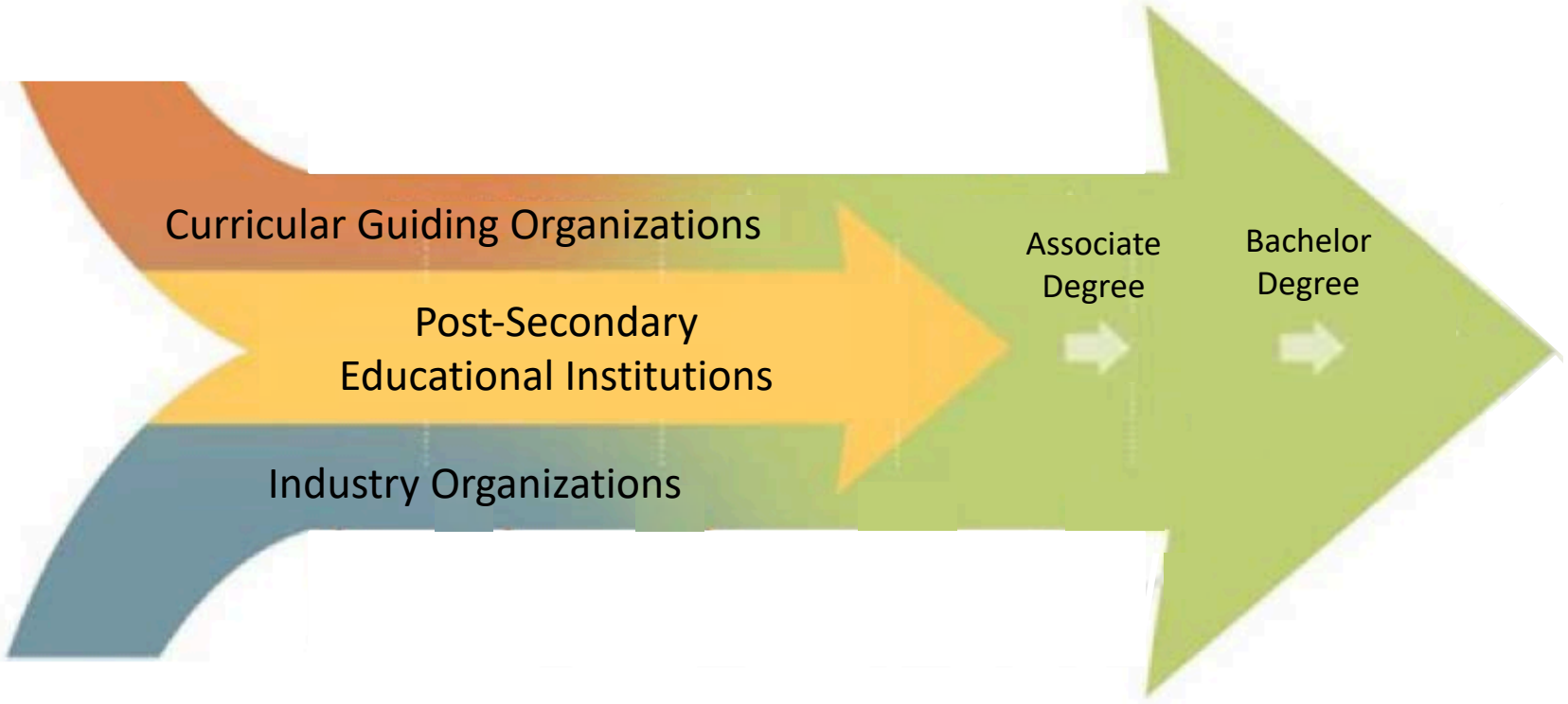
- Challenges in Cybersecurity
  - Cyber attacks are increasing in number and complexity
  - The good news is that companies are hiring…
    - But there exists a tremendous workforce shortfall in almost every position in cybersecurity
  - The problem is two-fold:
    1. We are not meeting the ever-growing demand
    2. We are not developing the right-kind of cybersecurity graduates that employers are looking for

Mismatch of Skills and Expectations

- A mismatch in the relevance of cybersecurity education programs and the needs of organizations
  - When hiring cybersecurity candidates, employers note a lack of understanding of fundamental concepts, practical experience, and essential soft skills
  - Graduates face steep barriers and require extensive on-the-job training before they're even able to begin work
- Employers not expect educational program to cover all specialized skills and sector-specific knowledge
  - But there should be a common baseline set of skills that meets employer workforce requirements

Post-Secondary Pathway

- Cybersecurity field is a vast, moving target requiring guidance and cooperation from all stakeholders



Industry Input

- Ensure students have a strong foundation in cybersecurity principles
  - Graduates need to be able to adapt throughout their careers against ever evolving cyber-threats and technologies
- Along with theory, students need practical training and hands-on experience to provide them with the tangible skills that employers expect
  - Program should have hands-on, applied learning methods
  - Internship offerings allow students to apply what they learned in a real-world environment
  - Integrate cybersecurity clubs and competitions to allow students to experience challenges modeled on real-world situations in a fast-paced adversarial environment
- Along with building technical proficiency, develop essential soft skills to improve student effectiveness and value for their employer

Standards and Accreditation

- Curricular guidance from CAE, NICE, ABET, and ACM
- Establish skill standards
  - Provide a set of core competencies, enable uniformity across institutions, and guidance in evolving and adapting to changes in the field
- Assess with certifications (where applicable)
  - Measurement of candidate's qualifications and credentials
- ABET accreditation guarantees a standardized, high quality, rigorous education in line with current research and taught by skilled and respected faculty
  - Competitive metric guaranteeing (at least) minimum set of skills and competencies expect from entry-level hires

Educational Institutions

- Community colleges prepare a wide range of cybersecurity professionals
  - Training of entry-level workers, maintenance of high level skills and knowledge, change jobs/positions, and *transfer to four-year programs*
  - Students need a clear understanding of goals and options for their program
    - Map pathways to student goals (select, maintain, progress)
- Relationship with local four-year institutions
  - Goal to have a seamless, transfer friendly degree pathway
    - Any leveling courses?
  - Establish clear pathway without adding barriers to completion

Cybersecurity Course Selection

- ABET math and science course requirements
- Since cybersecurity falls within the computer science domain, leverage existing core computer science courses to build foundational knowledge
  - Computer Programming I and II, Foundations of Computing, Systems Programming, Operating Systems, etc.
  - Most computer science programs already offer cybersecurity courses
- Critical need for highly technical cybersecurity skills rather than policy- or compliance-based focus
  - Includes secure system design, secure coding, penetration testing, tool development (offensive and defensive), etc.
- Interdisciplinary course options
  - BCIS, Criminal Justice, Information Science, etc.

Conclusion

- Students develop both hard and soft skills to ensure success
  - Provide strong foundation in cybersecurity principles as well as practical hands-on experience
  - Problem-solving forms the very foundation of effective cybersecurity work, especially in a fast-paced and changing field
  - Project-based experiential learning
- Companies and educational institutions build relationships with each other to communicate critical workforce needs and skill gaps to help align cybersecurity talent pipeline with the needs of industry
- Work with curricula guiding organizations and standards bodies to ensure current, relevant, and rigorous program