Futuristic Cybersecurity Education and Workforce Development Initiatives

A Proposal by Amos Olagunju, IT Professor

St Cloud State University, St Cloud, MN

0. Foreword

The survival of the current and future cybersecurity workforce will depend on effective strategies for the recruitment, retention, and continuous educational training of diverse students in high schools, two and four-year academic institutions. This proposal provides justifications and advocates initiatives for continuous successful recruitment, retention and training of diverse students for sustaining cybersecurity workforce.

1. Recruitment

Four-year academic institutions should form partnerships with local or nearby high schools and technical and community colleges, to sustain the recruitment of diverse students for associate or bachelor's degrees in areas relevant to cybersecurity. Today many academic institutions promote and support experiential training for students in the areas of computer science, information technology, and cybersecurity. Essentially, current computer science, cybersecurity and information technology degree programs that mandate experiential learning or capstone requirements should engage and mobilize more students to serve as role models for recruiting students from high schools and two-year institutions. College students should be guided by faculty and staff members to design academic and co-curricular skill-enrichment mathematics and computing activities for motivating youngsters to pursue bachelor's degree programs in cybersecurity and related areas. The enrichment activities should be delivered by college students to high schools on convenient periodical schedules.

Faculty members at four-year academic institutions ought to sign more articulation student transfer agreements with two-year institutions that offer associate degrees in areas related to cybersecurity education. Moreover, faculty members at two and four years institutions in areas of cybersecurity should meet periodically, to review and recommend changes in the educational training of students at two-year institutions for successful careers.

2. **Retention**

Clearly, it is not enough to recruit diverse students into cybersecurity programs without a strategic plan to cope with students who end up struggling with core courses in areas such as mathematics and computer programming. A comprehensive cybersecurity program in associate or bachelor's degree ought to have alternative plans for guiding students with deficiencies in mathematics, scripting, programming, and/or installation and applications of cybersecurity tools to success. Retention strategies might include the use of currently high-achieving cybersecurity majors or alumni or industrial partners to mentor and serve as role models to future cybersecurity experts. Retention of minority students in cybersecurity programs might be considered intrusive, but there is reason to believe that a carefully outlined alternative plans for guiding students with various academic, family, social and financial issues, will promote more diverse students for the cybersecurity workforce.

3. Cybersecurity Skill Training Requirements

The question naturally arises on the skills required for graduates with two-year or four-year degrees in cybersecurity. Should associate and bachelor's degree programs in cybersecurity be designed and offered based on the existing and future anticipated faculty strength? Regardless of the faculty strength what skills should graduates with associate or bachelor's degrees in cybersecurity demonstrate upon graduation, and perhaps in long-life learning?

In agreement with the ABET requirements for the accreditation of current and future cybersecurity programs, herein are long-life skills for future cybersecurity training:

Student learning outcomes for cybersecurity majors should mirror the ability to:

1. Write correct, well-documented and readable programs.
2. Describe and use networks.
3. Describe and use operating systems.
4. Articulate ethical, professional, and legal standards of behavior.
5. Communicate effectively in written and oral exchanges.
6. Design and implement secure network architecture based on security policies.
7. Identify and correct security weaknesses in operating systems, networks, and applications.
8. Demonstrate understanding of theoretical foundations of security by solving problems.

9. Design and implement effective defensive and offensive strategies in cyber security.

But, what kinds of courses should be designed to satisfy the current and future needs of cybersecurity workforce? Here are a few examples:

- A Course in Firewall and Penetration Testing might include Knowledge of common network tools:
    - Knowledge of Computer Network Defense and vulnerability assessment tools, including open source tools, and their capabilities
    - Knowledge of Defense-In-Depth principles and network security architecture
    - Knowledge of general attack stages Knowledge of network security architecture concepts including topology, protocols, components, and principles
    - Knowledge of penetration testing principles, tools, and techniques
    - Skill in applying host/network access controls
- A Course in Offensive and Defensive Security might cover:
    - Knowledge of different classes of attacks
    - Knowledge of front-end collection systems, including network traffic collection, filtering, and selection
    - Knowledge of host/network access controls
    - Knowledge of incident response and handling methodologies
    - Knowledge of intrusion detection system tools and applications
    - Knowledge of network traffic analysis methods
    - Knowledge of the common attack vectors on the network layer
- Applied Cryptography
    - Knowledge of cryptology
    - Knowledge of encryption methodologies
    - Knowledge of network access, identity and access management
- Database
    - Knowledge of database management systems, query languages, table relationships, and views
    - Knowledge of database theory
    - Knowledge of query languages such as SQL

    - Skill in developing data models
    - Skill in generating queries and reports
    - Skill in maintaining databases
    - Skill in optimizing database performance
- Operational Safeguards
    - Knowledge of policy-based and risk adaptive access controls
    - Knowledge of current and emerging threats/threat vectors
    - Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins
    - Knowledge of system and application security threats and vulnerabilities
- OSI Layer Security
    - Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol (TCP) and Internet Protocol (IP), Open System Interconnection Model (OSI), Information Technology Infrastructure Library, v3 (ITIL))
    - Knowledge of IA principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation)
    - Knowledge of network security architecture concepts including topology, protocols, components, and principles
    - Knowledge of VPN security
    - Skill in securing network communications
- Computer Forensics
    - Knowledge of anti-forensics tactics, techniques, and procedures
    - Knowledge of basic concepts and practices of processing digital forensic data
    - Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data
    - Knowledge of seizing and preserving digital evidence
- **Security Policy and IT Risk Management**
    - Knowledge of Computer Network Defense policies, procedures, and regulations
- Computer Networks
        - Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services

Summary

The industry is already infusing DevOps tools and agility into business operations. The need exists to develop case-based projects for training the future cybersecurity workforce about agile skills and rapid applications and network monitoring using DevOps tools. If I have the opportunity to participate in this panel discussion of the long-overdue recruitment and retention of the Cybersecurity Workforce, I will be willing to demonstrate creative projects that can be used to motivate, recruit, and retain more students into the current and future cybersecurity workforce.

Bio Sketch of Amos Olagunju

Amos Olagunju is a professor in the Computer Science and Information Technology Department at St. Cloud State University (SCSU) in Minnesota. He previously served as the interim dean of undergraduate studies at SCSU. Under his leadership, SCSU experienced the highest levels of enrollment, retention and graduation of students for minority students in STEM areas. He has served as the School of Graduate Studies Dean and Chief Research Officer at Winston Salem State University. A faculty fellow and later a senior faculty fellow selected jointly by the American Society of Engineering Education and the Navy, Amos developed manpower mobilization and data-mining algorithms for monitoring the retention behaviors of personnel. Under the leadership of Amos as a Professor and Chair of the Computer Science Department, Delaware State University established a reputable computer science degree program for minority students. As a visiting scholar at Michigan State University, he investigated the barriers to the retention and graduation of minority students in computer science and published a solution manifesto for international audience in computer science education. Amos is an ABET Program Evaluator. He has participated in the Carnegie African Diaspora Fellowship Program and the Specialist Fulbright Scholar Program.