Toward Curricular Guidelines for Cybersecurity

Report of a Workshop on Cybersecurity Education and Training

Executive Summary

The *Cyberspace Policy Review*, published in 2009, argued for a national strategy to develop a cybersecurity workforce adequate in numbers and expertise to secure the United States in cyberspace. In assessing education and training, the Review said, "Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees."[i] A number of workshops and a wide range of initiatives have been undertaken in recent years to help develop a comprehensive and coordinated plan to build a cybersecurity workforce adequate to meet the pressing needs of business and government.

A Core Leadership Group comprising cybersecurity experts in government, industry, and academia gathered in Atlanta 21-22 February 2013 to discuss current cybersecurity education initiatives and make recommendations that will inform near-term and long-range curricular guidance in cybersecurity for colleges and universities. The group also discussed the roles for government and private industry to play in building a broad cybersecurity workforce ranging from proficient technicians and practioners to policy makers and thought leaders.

Workshop participants embraced the philosophy expressed by ACM's policy arm (USACM) and the Computing Research Association (CRA) that computer science and computer engineering graduates should possess a thorough **education** in cybersecurity and related fundamentals and principles as well as **training** in cybersecurity-specific technologies, tools, and skills. The balance between education and training may vary for particular knowledge areas or sub-specialties, but a strong underpinning of basic knowledge and principles to complement technical skills should form the basis of a curriculum in cybersecurity.

The leadership group offered perspectives on the educational components that should be incorporated into traditional degree programs.

Doctoral degrees support next-generation cybersecurity education and research in academia, and provide thought leadership and advanced expertise necessary for industry and government. Our best and brightest have much to contribute:

- Ability to think, set, and achieve long-term research goals
- Ability to apply theoretical foundations of cybersecurity to real-world challenges
- Ability to combine theoretical and practical understanding to inform cybersecurity policies and assess innovations
- Ability to mentor the next generation of students and potential leaders
- Willingness to seek career aspirations both within and outside academia

At present, few PhDs in information assurance and cybersecurity return to academia to educate future generations.[ii] We need a vibrant mechanism to create PhDs in cybersecurity. An important step in that direction would be to better leverage the Department of Homeland Security (DHS)/National Security Agency (NSA) Information Assurance Scholarship Program, designed to assist in recruiting and retaining highly qualified personnel to meet the Department of Defense's

(DoD) information technology requirements for national defense and the security of its information infrastructure; as well as NSF's investment in the CyberCorps® Scholarship for Services (SFS) to allow SFS-funded graduates with advanced degrees to serve their government service requirement in academia where they can help to enhance the security component of existing courses, develop new ones, and contribute to faculty professional development.

Master's degrees are essential for providing a cybersecurity workforce with advanced capabilities. Building on a sound baccalaureate degree in computer science or related area, an additional two years of education could cover important technical cybersecurity topics. A master's degree in cybersecurity would, in a 2-year timeframe, allow suitably prepared graduates to master the knowledge, skills, and abilities (KSAs) specific to advanced topics in cybersecurity.

Universities should provide several master's degree options addressing cybersecurity issues:

a. **Cybersecurity for computing professionals**--Strongly technical cybersecurity-specific degree programs focusing on cybersecurity built upon a rigorous undergraduate background in computer engineering, computer science, or software engineering
b. **Cybersecurity in society**--Master's programs in non-computing disciplines that emphasize cybersecurity challenges and vulnerabilities and their implications for various professions, including law, business, economics, and medicine
c. **Cybersecurity operations**—Practical techniques and technologies for recognizing vulnerabilities and preventing security breaches

Business and government could encourage and improve cyber expertise by funding scholarships to help students afford master's-level courses in cybersecurity.

Associate degrees in computing disciplines focus on graduating a technically proficient and employable workforce in a relatively compressed timeframe. They help to feed technically-adept practitioners into the cybersecurity workforce pipeline. Two-year colleges are doing an excellent job in addressing cybersecurity education at the college level, graduating students directly into the workforce as well as transferring students into baccalaureate degree programs. Community colleges and other two-year institutions tend to coordinate their curricula with KSAs needed by local businesses. Community colleges should be generously funded and supported in their efforts by the community of cybersecurity stakeholders, including government and private industry.

Undergraduate baccalaureate degrees present serious challenges to enhancing cybersecurity education because to some extent adding knowledge areas at the baccalaureate level is a zero-sum game. The curriculum for any computing major already has tight time allotments, and "elbowing in" cybersecurity knowledge areas must be done carefully so as not to "elbow out" topics deemed essential by other faculty members.

Workshop participants offered suggestions that educational institutions should consider when weaving cybersecurity topics into undergraduate curricula.

For all undergraduates:

- At all levels, there is a need for understanding and practicing cybersecurity in a human context, taking into consideration workflow, human nature, and other practical constraints. A recent report[iii] recommends adopting a doctrine of public cybersecurity that envisions cybersecurity as a public good. In this view, institutions would set standards and educate citizens similarly to promulgating public health policies and practices. Educational

institutions have a vital role to play in raising the security awareness of citizens and influencing their security behavior.
- Many disciplines (law, medicine, business, international studies, publishing, and many more) have related cybersecurity issues that should be part of each student's curriculum. Indeed, awareness of the principles and challenges of information security and privacy should be woven into the entire curriculum, though finding or training faculty members to add this dimension could well be challenging.

For computing majors:

- Each student in a computing-related degree program should be required to take at least one technical course in a security-related knowledge area.
- Faculty should exemplify to students a responsible attitude toward security issues.
- Faculty with a low comfort level in teaching security topics are prone to give security topics inadequate attention. Faculty members should gain competence and confidence to teach cybersecurity in its many contexts, or be willing to have colleagues with that expertise collaborate with them on teaching security topics.
- Where appropriate, institutions should create credentials or certificates in security-related topics to give their computing graduates competitive advantage with employers. Few exist currently, and none has achieved ascendant respect in the market. A meaningful credential must:
    - Align with the institution's aspirations.
    - Represent demonstrable skills.
    - Become a permanent part of the graduate's professional qualifications and transcript.
    - Require critical thinking and not merely "check the box" exposure to credentialing criteria.
    - Emphasize best practices and not mandated standards.
    - Support a mechanism for keeping knowledge and skills current and relevant.[iv]
- A set of guidelines for degree programs in computer science, entitled CS2013, a collaboration between ACM and the Institute of Electrical and Electronics Engineers Computer Society (IEEE-CS) has taken an outward-facing approach to the development of the curriculum and has incorporated relevant cybersecurity concepts within the various computer science knowledge areas.[v]

Community support

Development and adoption of a cybersecurity curriculum would be greatly aided by an organized community of practice combining industry, government, and academia. A committed and active community would help to coordinate initiatives, distribute tools, share courses and best practices, and provide funding and other resources.

Building a bigger and better pipeline for a cybersecurity workforce will require a commitment from business and government to collaborate with educational institutions to provide:

- Funding
- Curriculum advice
- Courseware and software tools
- Internship and capstone experiences
- Mentoring
- Job opportunities

[i] National Initiative for Cybersecurity Education (NICE) Strategic Plan: *Building a Digital Nation.* September, 2012. http://csrc.nist.gov/nice/documents/nicestratplan/nice-strategic-plan_sep2012.pdf

[ii] Piotrowski, Victor. *Remarks on the US Cybersecurity Education Landscape*. [PowerPoint slides] Presented February 21, 2013

[iii] Mulligan, D. Schneider, F. *Doctrine for Cybersecurity.* Daedalus. Fall 2011, 70-92
Also available as Cornell Computing and Information Science Technical Report, April 2011.

[iv] Schneider, Fred B. *Labeling-in Security*. IEEE Security & Privacy 7(6): 3 (2009)

[v] *Computer Science Curricula 2013 (CS2013).* ACM/IEEE-CS Joint Task Force
http://www.cs2013.org