Thinking Across Stovepipes: Using a Holistic Development Strategy to Build the Cybersecurity Workforce

Lance J. Hoffman, Diana Burley, and Costis Toregas
The George Washington University

Report GW-CSPRI-2011-8

November 1, 2011

Abstract

This article proposes a holistic approach to developing the cybersecurity workforce based on careful integration of workforce development strategies into a plan that involves educators, career professionals, employers, and policymakers. First, it motivates this by describing how other fields such as medicine have successfully done this and arguing that cyber security is, like medicine, inherently cross-disciplinary at multiple levels of expertise and performance, making it similar in complexity to the medical profession and thus a good candidate for some of the solutions developed there. The article then focuses on one element of a holistic strategy – education -- and discusses the findings of a recent workshop on cybersecurity education. It then places those findings in the context of the broader discussion and suggests some practical steps. They encourage computer science educators, human resources professionals, and the functional experts from disciplines that will attract computer science graduates to think beyond their "stovepiped" fields and collaborate so that holistic, integrated solutions can be developed, accepted, and implemented.

Work supported by the Office of the Vice President for Academic Affairs and the School of Engineering and Applied Science of the George Washington University

This material is based upon work supported in part by the National Science Foundation under grants DUE-0621334 and CISE-1039564. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Introduction

"A critical element of a robust cybersecurity strategy is having the right people at every level to identify, build and staff the defenses and responses. And that is, by many accounts, the area where we are the weakest".[1] Indeed, it is generally accepted that the cybersecurity workforce suffers from an underinvestment in the relevant educational pipelines and a fragmented cadre of training and development programs.[2] The education and development of cybersecurity professionals is widely seen as a national security priority among government, industry, and academic stakeholders. Effectively addressing the national challenge to build a cybersecurity workforce from a current estimate of 1,000 individuals to the estimated required 30,000 specialists requires a comprehensive and coordinated strategy to educate and recruit cybersecurity professionals.[3] Although efforts, like the National Initiative on Cybersecurity Education (NICE) (http://csrc.nist.gov/nice/), emphasize the importance of a comprehensive approach to cybersecurity workforce development, there is limited empirical evidence available to inform the development of such an approach.

While the article draws from a United States base of priority concerns and responses, the topic of cyber security education and how best to prepare the next generation of cyber security workers is the focus of attention in many other nations. We try to summarize efforts of researchers in diverse nations to organize a common approach towards developing core curricula, and believe that additional collaboration across national boundaries may help develop stronger responses to the problem.

This article reaches into other disciplines to support the development of a holistic approach to developing the cybersecurity workforce. The approach is based on the careful integration of workforce development strategies into a coherent plan that involves educators, career professionals, employers and policymakers in the public and private sectors. The article is structured in three parts. First, we provide insight on how other fields have developed a holistic approach to workforce development and argue that the cyber security field is akin to those fields. Second, we focus specifically on one element of a holistic strategy – education – and discuss the findings of a recent workshop on cybersecurity education. Third, we place the findings of the workshop within the context of the broader discussion and suggest some practical steps for those who want to develop a strategy for cybersecurity workforce development.

A Holistic Approach to Workforce Development

A holistic approach to developing the cybersecurity workforce is one that considers the many disciplines that produce cybersecurity professionals – technical and nontechnical alike. This includes the computer science and computer engineering professionals, as well as those who were educated in management and policy related disciplines. The holistic approach respects the relative contributions of these different subfields, and recognizes that cybersecurity professionals must develop expertise within their individual subfield while simultaneously understanding how their work fits into the rest of the field. In this way, the holistic approach takes a systems perspective[4] that incorporates three key components: (1) activities that define the workforce structure; (2) continuous professional development opportunities to maintain the human resource; and (3) educational initiatives designed to build capacity in the pipeline.

Cybersecurity is not unique in the need for a holistic approach. Indeed, the development of other professions provides viable models for the structuring of this emerging field. For instance, those addressing the cybersecurity workforce development challenge often reference the healthcare field as a possible workforce development model.[5] [6] The field of cybersecurity today, it is suggested, is akin to 19th century medicine. Medical practitioners of the day, who were often self-taught and uneven in capabilities, functioned within an emerging field that addressed a complex, dynamic and somewhat unpredictable environment with no (or few) professional standards for performance. Needed was a landscape that was "coherent and consistent", much as cybersecurity doctrines are needed to foster those today.[7]

In 1908 the American Medical Association Council on Medical Education approached the Carnegie Foundation and asked their help in surveying and restructuring American medical education. A remarkable non-physician professional educator, Abraham Flexner, who also co-founded Princeton's Institute for Advanced Study, led the effort.[8] Over time, efforts by diverse groups helped the medical field evolve into a profession, and today its structure includes a host of fields and sub-fields with distinct career ladders, differentiated training and development programs, and strong standards of professional practice.

In the healthcare arena, workforce development strategies embedded within the larger discussion of system-wide reform allow stakeholders to focus on the alignment of processes and people.[9] In this way, professional development strategies are designed to achieve the best fit between workforce and service needs as they emerge in the system as opposed to a focus on isolated positions.

Based on empirical evidence from a field with similarly complex and dynamic problem-spaces (healthcare), along with the informed opinion of cybersecurity education experts and lessons learned from existing education and training programs within the realm of cybersecurity, we support the notion that a well-considered cybersecurity workforce development strategy must be conceptualized holistically. We hope that an appropriate cybersecurity doctrine can be developed to achieve a positive state in a loosely affiliated but highly interdependent network (as health care is), learning lessons from its varied stakeholders as to what works and what does not work in getting to this state.

Cybersecurity Workforce Structure

Although often discussed as a distinct career field, the actual structure of the cybersecurity workforce is not well-defined. A 2010 Center for Strategic and International Studies (CSIS) report suggests that the cybersecurity workforce is comprised of those specialized technical professionals who self identify as cybersecurity professionals, as well as those generalists who build and operate systems and networks. More specifically, the US Office of Personnel Management identifies four occupational categories (2210-Information Technology Management Series, 0855-Electronics Engineering Series, 0854-Computer Engineering Series, and 0389-Telecommunications Series) under the public sector cybersecurity workforce umbrella. These classifications represent a high-level aggregation of cybersecurity professionals, and given the broad definitions, tend to mask members of the cybersecurity workforce who hold positions that are classified under other occupational categories. Moreover, they do not explicitly account for the vast number of professionals (both within the public sector and outside of it) who spend some portion of their workday addressing cybersecurity tasks even though their position

descriptions may not include such tasks. This is particularly true in small businesses where financial constraints limit the ability to hire dedicated cybersecurity specialists.

The complexity of the cybersecurity workforce is further complicated by the constantly evolving nature of cybersecurity tasks and technology. Even once a set of professional categories is identified, the evolving requirements necessary to achieve a level of successful performance in many positions (such as new certifications and additional expertise) make it difficult for human resource officials to identify career paths for advancement. Defining the workforce structure requires that human resource managers be able to identify professional expertise requirements at each step on the career ladder in order to articulate consistent metrics of evaluation and to offer appropriate professional development opportunities. The complexity and dynamism of cybersecurity problems present a challenge to identifying these career elements.

The career management behavior of many IT professionals also presents a challenge for workforce structuring. Because members of the cybersecurity workforce often exhibit career self-management behaviors through which *they* (as opposed to the organization) identify individual values, interests, and skillsets; determine career goals; and enact career strategies (networking, positioning, training), they tend to be less bound to organizationally constructed career paths Rather, they have a tendency toward a boundaryless career that is motivated primarily by personal achievement and external career dimensions such as organizational position, mobility, flexibility and the organizational work environment [10] instead of organizational goals.

The cybersecurity workforce is characterized by a complex cybersecurity problem space that requires public-private knowledge sharing relationships, trends toward outsourcing, and heavy uses of private sector contractors. Moreover, the tendency toward self-managed career development among IT workers (of which cybersecurity professionals are a subset) suggests that they are prone to leveraging organizationally-designed activities, as well as personal knowledge networks and self-identified development opportunities, to maintain career expertise and for career advancement. Current efforts (for example, the National Initiative for Cybersecurity Education activities under the direction of the U.S. Department of Homeland Security and Office of Personnel Management) to construct and identify cybersecurity career paths should consider non-traditional conceptualizations of career management like the boundaryless model in the structuring of cybersecurity workforce development strategies.

Professional Development

As in the public health example, the breadth of cybersecurity activities requires a highly diverse workforce. There is an exploding need for cybersecurity professionals in the field for government and industry jobs. Satisfying this need is made more complex by the fact that the potential entrants into academic or training institutions come from very different, non-homogeneous backgrounds:

- High school students with a general interest in computer science
- Students in two-year community colleges who are eager to join the work force
- The incumbent work force with needs for updating their skills
- Workers who have been laid off in allied fields with a desire to re-enter the workforce
- University students in a broad variety of fields that are tangent to cyber security

A host of academic, governmental, industry, and collaborative bodies that focus on cybersecurity education (or some aspect of the cybersecurity education space including: software assurance, information assurance, and secure coding) are engaged in complex projects to effectively meet the needs of this diverse population. These initiatives include: model curricula, common bodies of knowledge, principles and guidelines, certification matrices, training standards, special designations, cybersecurity workforce development programs, and student competitions; and are all designed to increase the quantity, quality and consistency of the production of cybersecurity professionals in the United States.

In addition, many of the potential entrant categories mentioned have major human resource development challenges well beyond the education realm, with articulation from two- to four-year colleges, government funding of career enhancement programs, employee-employer relations and other problems compounding the definition challenge and making a unified solution difficult at best. In one recent effort to outline a coherent roadmap for secure software education, Burley and Bishop suggest that all individuals who are involved in the development and deployment of systems and infrastructure, "from the policymakers who determine what requirements the systems must meet to the businesspeople who provide the support needed to create the systems to the architects, implementers, and operators of these systems," must be included in the career development educational, and professional training activities. They present roadmaps that outline essential concepts, appropriate instructional methods, and resource requirements and challenges for six cybersecurity workforce constituent groups (computer science students; non-computer science students; community college students; K-12 students; computer science professionals; and non-computer science professionals). Although, presented as distinct action plans, they suggest that the roadmaps are best considered as linked components of a holistic professional development strategy.

Workforce structure and professional development issues shape and in turn are informed by educational initiatives that build the next generation of workers in this field. The next section addresses this capacity building element and focuses on a 2010 U.S. National Science Foundation-sponsored workshop on cybersecurity workforce development that provided specific observations useful for forward progress.

Workforce Capacity Building -- The CyberCorps Workshop

"Cyber security risks pose some of the most serious economic and national security challenges of the 21st century".[11] An effective response to challenges in a complex and dynamic field demands a workforce capacity building approach "that recognizes the interaction of people, systems and processes and an evaluation framework that examines context, input, processes and outcomes in synergy rather than isolation".[12] The holistic approach described above used to underpin current workforce development strategies in the field of healthcare provides a usable framework for cybersecurity workforce development.

We now turn to observations of an October 2010 workshop to examine how one workforce capacity building program, called the CyberCorps by participants, is faring in the workforce development efforts. The report referenced in this section is just one of many sources that describe the need for far more graduates in information technology (IT), and specifically in

cyber security, to fill both public and private sector needs. Federal efforts to address those needs include the establishment in 2000 by the U.S. National Science Foundation of the Scholarship for Service program (SFS) (https://www.sfs.opm.gov/) to fund undergraduate and post-graduate education in exchange for entering the federal government's IT workforce after graduation. At approximately the same time, the U. S. Department of Defense started a similar effort, the Information Assurance Scholarship Program (IASP) (http://cio-nii.defense.gov/sites/iasp2/). Both programs also provide capacity-building grants to academic institutions to bolster cyber security education and workforce development (CSEWD).

Recognizing the potential for growth of educational opportunities in cyber security as well as the demand for cyber security skills in the workplace, a group of educators, IT professionals, program managers from government agencies, and other stakeholders and experts gathered at a workshop to reflect on the successes, lessons learned, and future challenges since the first formal government programs supporting CSEWD were launched. The National Science Foundation supported this effort[13] to explore the current weaknesses and strengths of the cyber security education system and ways in which it interacts with workforce development. The workshop focused on issues related to post-secondary cybersecurity education; its objective was to use lessons of the past to guide consideration of how CSEWD programs can meet the challenges of tomorrow's world—especially developing the government workforce—and to indicate how CSEWD programs can continue to produce post-secondary school graduates who bring up-to-date, applicable cyber security skills to their jobs. The ideas that resulted are formal recommendations, nor do they necessarily reflect consensus among all who took part. Rather, they represent the opinions of leading stakeholders in the field, to be used as a starting point in addressing CSEWD challenges.

We first describe a set of cross-cutting principles that participants felt should inform efforts to address CSEWD needs. Next, we present a summary of the pervasive barriers to improving CSEWD identified by the workshop participants. We end with observations about SFS in particular and CSEWD in general, as well as potential approaches for addressing these.

Cross-Cutting Principles for Addressing Cyber Security Education and Training

Workshop participants identified a number of cross-cutting principles—concepts that should be applied to any efforts to improve CSEWD:

- Cyber security is an **international issue**. Strategic planning should go beyond the federal level, taking into account needs, concerns, and opportunities at the national and international levels.
- Cyber security requires a **multi-disciplinary approach**. Efforts should be made to educate and partner with disciplines not always thought of as related to cyber security (e.g., decision sciences, forensic sciences, public policy, law). A holistic approach will foster more collaboration across disciplines, increase interest in cyber security as a necessary component of nearly all types of work, and increase resources and support for cyber security.
- **Curative—not palliative**—approaches are needed to address causes rather than symptoms of the continuing security breaches in computer systems.
- The field of cyber security education requires the **development of metrics and processes for evaluation** to identify successes and areas for improvement. Tools to

measure, monitor, and track programs should be developed, tested, and validated, then made available to educational institutions and programs to implement as appropriate.

- **Recruiting and retaining minorities and women** into cyber security education and the cyber security workforce is vital to meet the workforce demand. Women and minorities make up an increasingly large proportion of the workforce. "Unless the science, engineering, and technology labor market becomes more representative of the general U.S. workforce, the nation may likely face severe shortages in science, engineering, and technology workers".[14]
- **Long-term sustainability and integration** of CSEWD efforts must be considered, given the scope of the need and the rapid pace of developing technology. Better strategies are needed to connect the currently unconnected segments of cyber security education and awareness from kindergarten through graduate school and beyond. A **lifelong learning continuum**, or "K-through-gray" approach, should be developed.

Barriers to Advancing CSEWD

Despite the pressing need for more workers skilled in cyber security, CSEWD continues to face barriers—notably, a lack of consensus on how to integrate cyber security education into current academic settings. The CSEWD workshop participants identified several "inconvenient truths," or entrenched barriers that inhibit efforts to advance CSEWD:

- **The university model does not completely satisfy all cyber security education and training needs**. Traditional undergraduate and graduate programs tend to take several years to complete and include general courses not related to cyber security (in service of the larger educational mission). Because university programs often do not address the time-specific needs of industry and government, they sometimes face difficulties educating students about a rapidly changing field. They often do not meet the needs of people who cannot take time out of the workforce to pursue a degree. They are generally not intended to provide short, intensive courses that respond to specific and current concerns.

- **Academic silos prevent collaboration and integration**. Cyber security is a relatively new field that does not always integrate neatly with other computing programs. Academic departments are notorious for guarding their resources and are justifiably resistant to giving up faculty spots, laboratory space, or funding opportunities. Most academic programs have tended to build their own tools rather than exchange resources with others, and they tend to hold firm ownership over whatever they create. Alternative approaches to education, such as online learning and co-op education, sometimes are seen as a threat or as too difficult to incorporate while maintaining a core mission of the university (education, as opposed to training). Often, universities lack incentives to try new approaches; that is, the current system of rewards is insufficient.

- **Experiential education is not popular with employers**. Employers want cyber security graduates with real-world experience but are reluctant to provide that

experience through internships or part-time work because (1) the return on investment is uncertain, (2) screening and training interns for meaningful work is expensive and time-consuming, and (3) organizations cannot afford to make their systems vulnerable to possible threats. Some organizations want students to have specialized education but don't provide the state-of-the-art tools and related resources (training, maintenance) that correspond with their specific needs.

- **Upper-level management generally does not buy in to advanced education and training**. Few opportunities are available for working people to increase their cyber security knowledge and skills without leaving their jobs permanently. Even fewer opportunities are available to those at the highest levels of an organization—the people with the most influence in their companies.

- **The Information Assurance CAE designation lacks solid prestige**. As of June 2011, 123 institutions have been designated by the U. S. government as a "Center of Academic Excellence in Information Assurance Education" (CAE), a "Center of Academic Excellence in Information Assurance Research" (CAE-R), or a "Center of Academic Excellence in Information Assurance 2-Year Education" (CAE-2Y). Granting CAE status to so many institutions has diluted the cachet of the label, and private-sector employers don't see CAE as a meaningful credential. Some of the most prestigious universities that produce technically accomplished graduates with computer security knowledge are not CAEs. Historically, universities have selectively applied for designations such as "CAE" on the basis of their goals and aspirations, internal competencies, target student audiences, and budgets. Because university departments have not traditionally taught courses geared toward standards such as those that CAEs and CAE-2Ys and, until recently, CAE-Rs are required to teach, it is not surprising that many fine universities have not applied to become CAEs. Even among CAEs, there is no independent mechanism for validating outcomes or results, so it is not clear to what extent institutions that receive scholarship grants under this program actually teach to the required standards.

- **There is strong disagreement over whether barriers to cyber security education and training could or should be addressed through standardization**. Standardized curricula, program accreditation, and specialty certification have all been recommended as mechanisms to improve CSEWD. But cyber security threats change rapidly, as do technology and platforms, so standards must be updated in a timely manner. If consensus were reached about some minimum guidelines around a set of generally accepted skills, organizations would have to emerge that can be trusted to take responsibility for applying appropriate metrics impartially (to accreditation or certification programs, for example).

- **National security concerns can hinder international collaboration.** The Internet is global, and while cyber security issues are international **and** multi-national, they are also nation-specific and intertwined with national security, competitiveness, and wide variations in the laws that govern privacy and data protection.

- **Current efforts to link employers with high-quality students are not positioned to meet large-scale needs**. Within SFS, the SFS job fair brings together a wide range of employers and students. This functions reasonably effectively for this relatively small pool of candidates. However, to become more effective and efficient, a larger, more general mechanism is necessary, one that scales well to meet the generally acknowledged need for more college graduates educated in cyber security and can address the needs of various types of employers and job-seekers.

Workshop Findings and Practical Steps for Workforce Development

The workshop's findings align well with the workforce structure and professional development observations we presented in the beginning of this paper and with a recent "doctrinal thesis" that presents a number of interesting analogies between cyber security and public health.

The dynamic nature of the cybersecurity field, where both the threats and responses, as well as the underlying technology foundation are constantly changing, suggest that long term responses must be carefully constructed and be flexible in order to accommodate these changes. Rather than a single, iron-clad solution that is to work for everyone, concerned employers, academics and government officials must rather turn to construct a *process* or *roadmap* which will provide flexibility in terms of content, delivery mechanism, and financing of the education component for the cybersecurity student. At the same time, non-traditional approaches to education and training will have to be incorporated side-by-side with university-delivered courses. These approaches will include:

- Well designed two-year community college curricula that either produce strong, desired skills for market-ready workers or articulate seamlessly to four-year baccalaureate programs
- Degrees which span, in a holistic manner, the entire offerings of a university and its diverse schools and departments and which prepare the cyber security worker with a full set of skills that truly address the problem (curative rather than palliative approach)
- Academic and private efforts that enable job-specific challenges to be addressed in long term, educational environments
- Different delivery mechanisms for education modules that take full advantage of today's technology capacity (wikis, podcasts, social media, virtual laboratories, and cloud computing -- to name but a few)
- The development and launch of coordination and disagreement resolution mechanisms for multiple organizations, since no single organization holds the key to preparing the cyber security work force of the future.

This last approach especially is important because "Success in [both public health and cybersecurity] ultimately depends not only on technical progress but on reaching a political agreement about the relative value of some public good in comparison to other societal values

and the institutions granted authority to resolve conflicts (along with the methods they might use)."

International Work

Cybersecurity workforce development is an international issue. Although the focus of the workshop presented here has a primary focus on the United States, we recognize the need for a global mindset in addressing the cybersecurity workforce challenge. To that end, we highlight the relationship between the findings provided here and those of a related international working group. Since 2009 an international group of educators has focused on the education aspects of workforce development in Information Assurance (IA). (We consider IA to be a component of cybersecurity.) Through the Innovation and Technology in Computer Science Education (ITiCSE,) working group meetings, faculty, researchers, and government officials from Australia, Sweden, the UK and the US collaboratively examined the "history of IA education efforts, current academic, government and industry guidelines, standards, and recommendations with respect to IA and computing education, and how the quality of IA programs might be assessed." In addition, ITiCSE participants are working "to develop a model of curricular guidelines for IA education," and to examine "the educational missions and curricula of two and four-year institutions with respect to IA education."[15] The efforts of this group are consistent with the findings presented here.

Future Work

Reconciling education and training goals with workforce development goals will require a coordinated approach. This paper suggests guidelines and strategies that speak to the academic cyber security community and the career development community alike. The two disciplines must begin to collaborate far more intensely than has been the norm. When a holistic approach is recommended, it is more than a holistic approach to integrating the cybersecurity disciplines (forensics, secure coding, network security and other fields); it is a call to a coordinated approach between educators and human resource professionals who must help the students and workers eager to retool themselves for a different future to come together, establish common vocabularies and action strategies, and establish a team approach to responding to the call for more cybersecurity experts.

Beyond approaches focused on small portions of the educational puzzle, we argue for a comprehensive, collaborative approach. The academic environment provides strong incentives for research, which stays within fairly rigid discipline boundaries. The coordinated approach we suggest will have to compete with the existing reward mechanisms and hopefully overcome the seemingly natural proclivity for education to stay within broad walls of a given established discipline.

As with the fields of law and medicine, the professionalization of the cybersecurity field requires a three-pronged approach that defines the workforce structure, provides continuous professional development opportunities, and develops effective educational initiatives. This holistic approach requires a true partnership between educators, human resource professionals, and cybersecurity practitioners.

References

[1] J. Gosler, "Cyberwarrior Shortage Threatens U.S. Security," *NPR Morning Edition*, July 19, 2010, http://www.npr.mobi/templates/transcript/transcript.php?storyId=128574055.

[2] M. Assante and D. Tobey, "Enhancing the Cybersecurity Workforce," *IT Professional*, vol. 13, no. 1, pp. 12-15, Jan.-Feb. 2011, http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5708280.

[3] Partnership for Public Service and Booz Allen Hamilton, "Cyber IN-Security: Strengthening the Federal Cybersecurity Workforce," July 2009, http://www.boozallen.com/media/file/CyberIn-Security_2009.pdf.

[4] A. Roach, J. Kidd, and T. Freeman, "Achieving professional practice change: From training to workforce development," *Drug and Alcohol Review*, vol. 28, pp. 550–557, Sept. 2009, http://onlinelibrary.wiley.com/doi/10.1111/j.1465-3362.2009.00111.x/pdf.

[5] D. Burley and M. Bishop, "Final Report: Summit on Education in Secure Software," June 2011, https://public.me.com/profdee27/.

[6] K. Evans and F. Reeder, "A Human Capital Crisis in Cyber Security," *Center for Strategic and International Studies*, Nov. 2010, http://csis.org/publication/prepublication-a-human-capital-crisis-in-cybersecurity.

[7] F. Schneider and D. Mulligan, "A Doctrinal Thesis," *IEEE Security & Privacy Magazine*, vol. 9, pp. 3-4, July-Aug. 2011, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5968081&tag=1.

[8] P. Starr. *The Social Transformation of American Medicine*. Basic Books, 1982.

[9] J. Conway, M. McMillan, and J. Becker, "Implementing Workforce Development in Health Care: A Conceptual Framework to Guide and Evaluate Health Service Reform," *Human Resource Development International*, vol. 9, no. 1, pp. 129-139, Mar. 2006, http://www.tandfonline.com/doi/abs/10.1080/13678860500522975#preview.

[10] M.B. Arthur and D.M. Rousseau, (eds.), "The Boundaryless Career: A New Employment Principle for a New Organizational Era," New York: Oxford University Press, 1996, http://findarticles.com/p/articles/mi_m4035/is_3_43/ai_53392863/.

[11] White House Report, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," p. iii, May 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[12] D. Koo and K. Miner, "Outcome-Based Workforce Development and Education in Public Health," *Annual Review of Public Health*, pp. 253-269, 2009, http://www.annualreviews.org/doi/pdf/10.1146/annurev.publhealth.012809.103705.

[13] L. Hoffman, "Building the Cyber Security Workforce of the 21st Century: Report of a Workshop on Cyber Security Education and Workforce Development," GW Cyber Security Research and Policy Institute Report #GW-CSPRI-2010-3, Dec. 2010, http://www.cspri.seas.gwu.edu/Seminar%20Abstracts%20and%20Papers/2010-3a%20Building%20the%20Cyber%20Security%20Workforce%20of%20the%2021st%20Century.pdf.

[14] U.S. Congressional Commission on the Advancement of Women and Minorities in Science, Engineering and Technology Development, "Land of Plenty: Diversity as America's Competitive Edge in Science, Engineering and Technology," Sept. 2000, http://www.nsf.gov/pubs/2000/cawmset0409/cawmset_0409.pdf.

[15] L. Perez, et al., "Information Assurance Education in Two and Four Year Institutions," http://www.iticse2011.tu-darmstadt.de/sites/default/files/wg3_0.pdf.