Cybersecurity Workforce Development Directions

R.C. Dodge[1], C. Toregas[2] and L. Hoffman[2]

[1] United States Military Academy, West Point NY, 10996
[2] The George Washington University, Washington, DC 20052
e-mail: ronald.dodge@usma.edu; {toregas1, lance.hoffman}@gwu.edu

Abstract

The cybersecurity workforce is one of the most critical employment sectors in the world. The systems supporting the information technology requirements of the world's government, power, and financial systems are interconnected more than any other system in the world. Despite the criticality and interconnectivity of these systems, the workforce has developed without a concentrated and standard view of its requirements. In this paper the authors report on efforts in the last two years to define the requirements for developing the cybersecurity workforce.

Keywords

Cybersecurity workforce, security education, training, awareness

1 Introduction

The cybersecurity workforce is failing to meet the demands of a society with deep reliance on information technology. This failure is abundantly evident in many security assessment reports. Identifying the requirements of this career field and creating a holistic approach to defining accreditation guidance to certify an individual's competence to be a part of this workforce has been the topic of several workshops in the USA in the past two years. While there was no overlap in planning or participation in the workshops, they arrived at the same conclusion – change is needed now in the way we develop and manage the cybersecurity workforce.

In 2011, the United States Department of Homeland Security sponsored a workshop executed by the Institute for Information Infrastructure Protection (I3P). In this workshop, approximately 40 representatives from the US government, international corporations, and academic institutions met to discuss and outline the demands within each sector for cybersecurity workforce professionals. The final report highlighted the sense that the cybersecurity workforce resembled an ecosystem comprised of expertise in complementary knowledge, skills, and abilities (Goodman et al., 2011). The domains of expertise, however, are nearly impossible to all master within a specific job function in the career field. Unfortunately, if one is lacking, the system is vulnerable to attack or failure.

A second effort sponsored by the National Science Foundation and executed by the Cyber Security Policy and Research Institute (CSPRI) of The George Washington University (GW) started to explore the integration of workforce development strategies into a plan that involves educators, career professionals, employers, and policymakers.

The healthcare and legal professions may serve as potential models for the development of a cybersecurity workforce management plan. In both of the fields, an educational foundation is important yet due to the very specialized nature of the many sub-disciplines within the career fields, a specialization path and possibly a certification structure could be helpful.

A first step in constructing a development model for a career field is to detail the components of the career field and the specific functional requirements within each component. In a multiagency effort, the United States launched the National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) in partnership with the Department of Homeland Security. The goal of this effort is to create a Cybersecurity Workforce Framework that defines the architecture and specific functional requirements for all job functions within the cybersecurity workforce.

The referenced workshops and the proposed NIST workforce model serve as informed starting points in the discussion on how to rationally develop the cybersecurity workforce. The cybersecurity workforce career fields must transform to assist organizations managing and securing our IT infrastructures and services, to ensure the employees are competent, and to support the development of education and training programs. In this paper, we discuss the findings of the I3P and CSPRI workshops and how the NIST NICE workforce model can be used as a starting point in a full career development and management structure.

2 Three significant efforts

In order to develop new directions in cybersecurity workforce development, it is important to look at a variety of discussions and make sure that no one sector or special interest dominates the conclusions. Too much is at stake to develop the "favorite flavor of the month" approach to new directions in cyber security. The authors have identified three recent events in which significant number of important stakeholders assembled to discuss cyber security workforce issues, and present the problem they were organized to address, the discussion which took place and the recommendations which emerged. In this way, while not claiming exhaustive coverage, the paper is able to provide diverse ideas from an illustrative subset of discussions (which however surprisingly tend to similar conclusions and observations!)

2.1 I3P workshop on Cybersecurity Workforce Demand

Problem. Much attention has been paid to devising better ways to educate and train cybersecurity professionals; however this effort was supported only by calls for a more talented workforce, not by a specific problem statement. To begin to address the lack of originating guidance from the employment sectors, the Institute for Information Infrastructure Protection (I3P) ran a workshop in 2011 to gain a better understanding of the demand for cybersecurity workers in government and private industry. At this workshop, participants listened to keynote talks from leading figures from government, industry, and academia and participated in collaborative working sessions to transpose the discussion points into statements about the need for cybersecurity workers.

The workshop participants shared their specific workforce needs in order to collectively develop a more complete and nuanced understanding of the demand. Among the workshop's goals were to:

1. Develop a more complete understanding of employer demand for cybersecurity skills so that employers and educators can work together to meet the demand.
2. Facilitate communication and cooperation between cybersecurity workforce customers and providers so that supply will more closely track demand.
3. Recognize emerging trends in cybersecurity workforce demand so that training programs can be developed or enhanced to provide new capabilities when they are needed.
4. Provide a framework for needed research and action in the future.

Discussion. The problem space presented while assessing the workplace requirements for cybersecurity professionals is daunting. One aspect of the challenge was well articulated when one workshop participant summed up the pace of change by observing that none of the cybersecurity jobs he has held in the last 20 years existed when he started his career. This is very characteristic of the career field. Employers and employees have struggled to keep pace with change, making the development of a formalized career model very challenging. Because specific job roles will shift with the advent of new threats and new technologies, participants agreed that competency in core skills is essential. These capabilities include both quantitative skills such as engineering, mathematics and computer science, as well as behavioral skills such as management, communication and the ability to think creatively. Thus, the demand for cybersecurity expertise cannot easily be described with a uniform skill profile. Rather, needed expertise encompasses an ecosystem of complementary knowledge, skills and abilities

The workshop consisted of three primary keynote presentations, each followed by a breakout session to discuss the presentation and assess the viewpoints in context of the workshop goals.

First, Roberta G. Stempfley, Deputy Assistant Secretary for Cybersecurity and Communications and Principal Deputy Manager, National Communications System,

Department of Homeland Security, described the landscape she surveys from the perspective of leading the US federal government's efforts in this space: the challenges are constantly changing, the demand is outpacing the number of employees, and the workforce must understand the broad aspects of the mission. Using the automobile industry is indicative of the pressures being placed on the IT industry, she noted that Ford produces 2 million cars annually; Apple sells 12 million iPods in the same period. Ford executives therefore say they have no choice but to put iPod connectivity in every car. Consumers demand it, so Ford provides it. The Apple technology is integrated into Ford automobiles, presenting potential new threats to functions and features. Distributed computing and Smartphone are two more worrisome examples. During roughly this same year-long period, the cybersecurity workforce with the Department of Homeland Security grew from 38 to over 200 employees. The rapid pace of change and growing landscape of integration and services requires its employees to be well-rounded professionals who can make security decisions in the context of their organization's mission and resources.

The second keynote talk, by William G. Horne, Research Manager, Systems Security *Lab*, Hewlett-Packard, described the challenges posed to one of the largest technology providers in the world, consisting of 325,000 employees operating in 170 countries. He described the security workforce development challenges: a competitive recruiting and retention environment, the lack of a cybersecurity skills taxonomy, and an uncertain business environment.

He stated that no universal system exists to classify cybersecurity skill sets. HP employs 325,000 people, including a large and diverse cybersecurity workforce. Still, he noted, "there's no database I can query to find out how many of those people know government and risk management and how many people know incident response." This is further challenged by the large collection of corporations seeking to offer high performing employees lucrative offers to change companies. Lastly, Mr. Horne noted the complex environment that his cybersecurity professionals are responsible for. He noted that cybersecurity encompasses a broad and rapidly expanding group of capabilities, and it involves supporting activities in nearly every facet of the economy.

In this respect, security is much like health care. There's more to medicine than hiring the best doctors and nurses; an effective health care system requires a broad diversity of roles: EMTs, medical equipment providers, hospital administrators, pharmaceutical research and manufacturing, and insurance services. Similarly, cybersecurity requires an ecosystem of skills, both general and specialized, among them computer scientists, programmers, forensic analysts, cryptographers, white-hat hackers, and risk-management specialists. A Venn diagram of all these necessary skills would have very little overlap.

Finally, Stephen J. Lukasik, of the Center for International Strategy, Technology and Policy at The Sam Nunn School of International Affairs, Georgia Institute of Technology, discussed how to develop an integrated cybersecurity workforce. He advocated a multi-disciplinary approach to cybersecurity, rejecting "Edisonian"

thinking in favor of a methodology based on established sciences that study active agents. He quoted James Lewis, Director of the Technology and Public Policy Program at the Center for Strategic and International Studies, saying that "there is no correlation between the training cyber professionals receive and the job they have to do." One of the greatest misperceptions is defining cybersecurity as a technical problem. Doing this only addresses about 50 percent of the problem, Lukasik said. Effective cybersecurity demands a mix of skills, including law, diplomacy, and management in addition to information technology. Additionally, the workforce at large needs to understand their responsibility to exercise due care and "IT hygiene".

Recommendation. The keynote presenters, while coming from varied positions within the "cyber economy", all posited viewpoints that were very consistent. Throughout the discussions the concept of a diverse workforce that requires both a broad understanding of the landscape and also a deep understanding of very specific areas kept reappearing. The lack of a taxonomy that defines the cybersecurity worker's initial and continuing education and training requirements is a significant deterrent to meeting the needs of the workforce.

To address the underlying concerns raised, the working groups adopted and expanded upon some recommendations from the keynotes and provided insight into additional areas. The first and foremost need was for a skills taxonomy that defines roles for the cybersecurity employee. This would serve as the foundation for a workforce management strategy. A strong recommendation from the working groups was to not exclude the non-cybersecurity workforce in the roles discussion. Every employee with computer access has a cybersecurity role as much as an employee is responsible to safeguard his or her door keys or access codes. This was commonly referred to as "cyber hygiene".

Once a taxonomy of roles is established, the initial and continuing education and training requirements must be established. We have seen an initial attempt at this in the United States Department of Defense with the 8500 series directive (DoD 8500.01E). In this model, a very rough roles taxonomy was created (and refined/expanded in subsequent updates) along with a representative commercial certification that must be obtained in order to serve in a specific role. (In Section 2.3 of this paper we review the new NIST proposed cybersecurity workforce framework.) The definition of frameworks however is not sufficient to ensure workforce competency due to the rapidly changing setting. The working groups proposed a system of practical internships and residency (to borrow a term from the medical field) where practitioners apply their education and training in order to gain an appreciation of the complex environment.

While creating a taxonomy and an educational/training support structure is an important foundation, without requirements for organizations to comply with the framework, the solution will not meet the demand of a highly interconnected IT infrastructure. The requirement for regulations that cross international borders was deemed an important facet of this proposed solution. However, it was admitted that this was the least likely to be adopted.

2.2 CSPRI Workshop on Cybersecurity Education and Workforce Development

Problem. Even while the education and development of cybersecurity professionals is increasingly seen as a priority, the cybersecurity workforce suffers from a fragmented cadre of training and development programs (Assante and Tobey, 2011). The breadth of cybersecurity activities requires a highly diverse workforce. Potential entrants into academic or training institutions come from very different, non-homogeneous backgrounds:

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

An October 2010 workshop organized by the George Washington University Cybersecurity Policy and Research Institute (CSPRI) and sponsored by the National Science Foundation explored issues related to post-secondary cybersecurity education and workforce development (CSEWD). Participants agreed that while the university model does not completely satisfy all cybersecurity education and training needs, employers 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. Participants also agreed that cybersecurity requires a multi-disciplinary, holistic, approach. On the other hand, they could not reach consensus on how to integrate cybersecurity education into current academic settings, nor could they agree on whether barriers to cybersecurity education and training could or should be addressed through standardization. Details of the workshop findings and expanded work that uses it are available elsewhere (Hoffman, 2010; Hoffman et al., 2012).

Discussion. A holistic approach to developing the cybersecurity workforce is one that considers the many disciplines that produce cybersecurity professionals – technical and nontechnical alike, in a coherent fashion. It 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. Such an approach incorporates (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.

The development of other professions provides a historical model for the structuring of this emerging field. For instance, cybersecurity today can be compared 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 (Schneider and Mulligan, 2011).

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 (Starr, 1982). 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. This model could inform the current cybersecurity workforce discussions and provide replicable models for consideration.

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

1. **Curative—not palliative**—approaches to address causes rather than symptoms of the continuing security breaches in computer systems.
2. The **development of metrics and processes for evaluation** to identify successes and areas for improvement.
3. **Long-term integration** of CSEWD efforts including a **lifelong learning continuum**

Workshop participants also saw a need for the development and launch of coordination and disagreement resolution mechanisms for multiple organizations, since no single organization holds the key to preparing the cybersecurity work force of the future.

Finally, they agreed that non-traditional approaches to education and training should be incorporated side-by-side with university-delivered courses. These approaches include:

1. Well designed two-year community college curricula that either produce strong, desired skills for market-ready workers or articulate seamlessly to baccalaureate programs
2. Degrees which span, in a holistic manner, the entire offerings of a university and its diverse schools and departments and which prepare the cybersecurity worker with a full set of skills that truly address the problem
3. Academic and private efforts that enable job-specific challenges to be addressed in long term, educational environments
4. Different delivery mechanisms for education modules that take full advantage of today's technology capacity (for example, wikis, podcasts, social media, virtual laboratories, and cloud computing).

2.3 NICE Cybersecurity Workforce Framework

Problem. The Cybersecurity Workforce effort by the National Institute of Standards and Technology (NIST) was embarked on because there is very little consistency throughout the United States about how cybersecurity is defined and how the workforce is trained. To have a comprehensive understanding of the cybersecurity workforce, additional human capital data beyond the competencies and data on knowledge, skills, and abilities (KSAs) is needed. The framework developed by NIST presents a very detailed analysis of roles and responsibilities within the cybersecurity career field and is not limited to government roles. It is possible to consider applying it across sectors and international lines.

Discussion. The Framework organizes the cybersecurity workforce into seven high-level categories, each comprised of several specialty areas (Homeyer and Maxson, 2012). In developing the framework, NIST coordinated with all sectors of the US federal and state government(s) as well as a large number of not-for-profit organizations including educational, security practitioners, and professional societies. The high-level categories are:

1. Securely Provision: Specialty areas concerned with conceptualizing, designing, and building secure IT systems.
2. Operate and Maintain: Specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.
3. Protect and Defend: Specialty area responsible for the identification, analysis and mitigation of threats to IT systems and networks.
4. Investigate: Specialty areas responsible for the investigation of cyber events or crimes which occur within IT Systems and networks.
5. Operate and Collect: Specialty areas responsible for the highly specialized and largely classified collection of cybersecurity information that may be used to develop intelligence.
6. Analyze: Specialty area responsible for highly specialized and largely classified review and evaluation of incoming cybersecurity information.
7. Support: Specialty areas that provide critical support so that others may effectively conduct their cybersecurity work.

Each of the categories is further defined to address the specific specialty areas. For example the "Operate and Maintain" category is further defined to include the following specialty areas: Data Administration, Information System Security Management, Knowledge Management, Customer Service and Technical Support, Network Services, System Administration, and Systems Security Analysis. These seven areas make up the functional requirements within this category.

While the breakdown of the categories into specific specialty areas is important, more details are needed to ensure the functions are uniformly understood and supported. To meet this requirement, each specialty area is further defined using the taxonomy shown in Table 1. Each of the rows in Table 1 are explained in detail for

each specialty area so that the job functions within the specialty area are clearly articulated and measurable.

Cybersecurity Category	**A generalized grouping of specialty areas**	**Can have one or more unique specialty areas associated with a category**
Specialty Area (SA)	Defines specific areas of specialty within the cybersecurity domain	•Belongs to one and only one cybersecurity category •Can have any number of unique tasks and KSAs associated with it
Task	Defines high-level activities that codify a specialty area	•Belongs to one and only one cybersecurity specialty area •Tasks are not linked individually to competencies/KSAs
Competency	A measurable pattern of knowledge, skills, abilities, or other characteristics that individuals need to succeed and that can be shown to differentiate performance.	•One or more KSAs are assigned to each competency •The same competency is likely to be needed across multiple specialty areas
KSA	Defines a specific knowledge, skill, ability.	•Assigned to one or more specialty areas •Each KSA has exactly one competency associated with it

Table1: Function Framework Taxonomy

Recommendation. The details of the NIST cyber security workforce framework lay out a single component of a wide ranging program designed to meet the demand for our cyber workforce. The Department of Homeland Security in the United States is testing the framework to provide structure to its cyber security workforce, trying to develop consistency in terminology across all agencies and components. Lessons learned from the pilot should be gathered and integrated into larger adoptions of a workforce model.

3 Three efforts – fitting the puzzle pieces together

The workshops both identified the need for a new, more holistic way to look at cybersecurity education requirements from the government and commercial market places and major structural descriptors that a good solution must have in order to be viable. Inputs were sought from a wide group of stakeholders, and there was surprising agreement on this need to rethink cybersecurity education. At about the same time, the US Government began its NIST/NICE effort, identifying actual skill sets needed in a structured methodology. The workshop outcomes and NIST/NICE

results are consistent with one another and represent a framework that begins to inform decision makers as to needed strategies to improve the workforce, both in quantity number as well as its ability to respond to market needs.

Of course there are many ways to address cybersecurity needs in the government and industry market place. A dominant one is the entire industry of training and accreditation which takes a skills-dominant approach and delivers in a manner authorized by a recognized national or international body a set of skills to workers and students alike. Many times, efforts to define needed reforms and changes in cybersecurity strategies come up short because the academic and training disciplines do not effectively integrate into a coherent set of action strategies for industry, government and academia to consider simultaneously. Figure 1 provides a pictorial flow diagram to help visualize and see the interconnections within the process for cybersecurity workforce development.

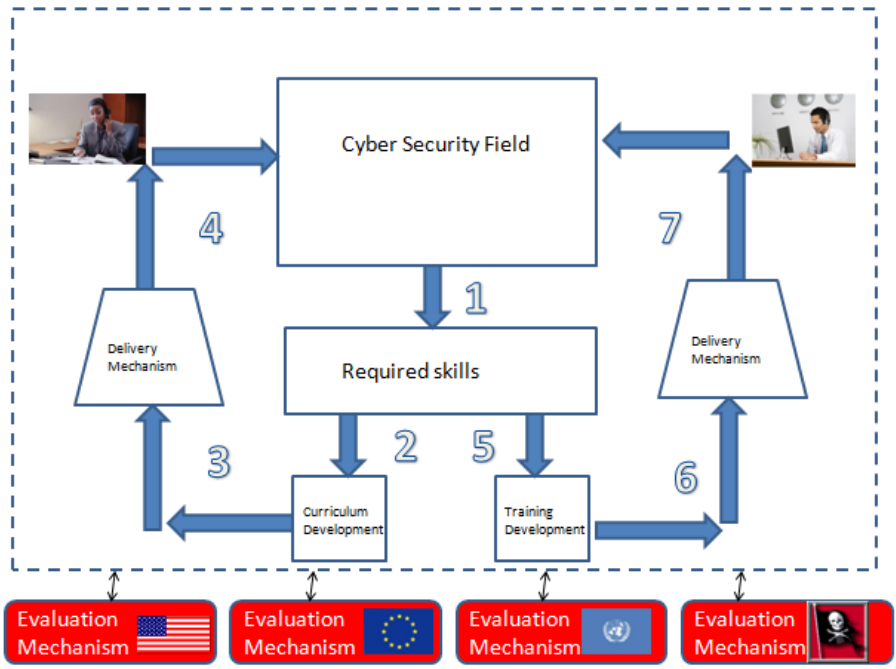

Figure 1: Process for Cybersecurity Workforce Development

Intervention strategies in various stages of the process flow can help fine tune the work force quality and quantity, and also establish the relativities with other parts of the interconnected system. As an example, creating a way to link a set of skills to curriculum development (#2 in the diagram) would modify the outcomes emanating from the related delivery mechanisms (#4).

The details of the NIST cybersecurity workforce framework layout a single component of a wide ranging program designed to meet the demand for our cyber workforce. The Department of Homeland Security in the United States is piloting the framework to provide structure to its cybersecurity workforce, gaining consistency in terminology across all agencies and components. Lessons learned from the pilot should be gathered and integrated into larger adoptions of a workforce model.

4 Conclusions and Recommendations

Cybersecurity workforce development is an international issue. Although the work described here was set in the United States, the cybersecurity workforce challenges are global. 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." (Perez et al., 2011). The focus of this work has been on creating a rigorous set of academic modules that work together and define a robust set of outcomes responsive to perceived cybersecurity education needs. The efforts of this group are consistent with the findings presented here.

The international cybersecurity education community can be strengthened through a coherent discussion of the entire Needs-->Responses-->Delivery mechanism action flows. This paper attempts to establish an initial framework for this needed discussion.

5 Acknowledgements

This material is based upon work supported in part by the National Science Foundation under grants DUE-0621334 and CISE-103956 and in part upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P)

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.

6 References

Assante, M., Tobey, D. 2011. "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.

Department of Defense Directive 8500.01E, www.dtic.mil/whs/directives/corres/pdf/850001p.pdf

Goodman, S., Lawrence Pfleeger, S., Dodge, R., Longstaff, T., I3P Workshop Report Workforce Development: Understanding the Demand, 27-28 April 2011. Available at: www.the**i3p**.org/docs/publications/432.pdf

Hoffman, L.J. 2010. Building the Cybersecurity Workforce of the 21st Century: Report of a Workshop on Cybersecurity Education and Workforce Development, *Report* GW-CSPRI-2010-3, December 15, 2010. http://www.cspri.seas.gwu.edu/Seminar%20Abstracts%20and%20Papers/2010-3a%20Building%20the%20Cyber%20Security%20Workforce%20of%20the%2021st%20Century.pdf

Hoffman, L.J., Burley, D., Toregas, C. 2012 Thinking across Stovepipes: Using a Holistic Development Strategy to Build the Cybersecurity Workforce, to appear, IEEE Security & Privacy Magazine, March 2012.

Homeyer, J., Maxson, M. 2012. Introduction to NICE Cybersecurity Workforce Framework, available at: http://csrc.nist.gov/nice/framework/documents/NICE-Cybersecurity-Workforce-Framework-printable.pdf, last accessed 17 Jan 2012

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

Schneider, F., 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.

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