Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors

Wm. Arthur Conklin
University of Houston
waconklin@uh.edu

Raymond E. Cline, Jr.
University of Houston
recline@uh.edu

Tiffany Roosa
University of Houston
troosa@uh.edu

Abstract

The need for cyber security professionals continues to grow and education systems are responding in a variety of way. The US government has weighed in with two efforts; the NICE effort led by NIST and the CAE effort jointly led by NSA and DHS. Industry has unfilled needs and the CAE program is changing to meet both NICE and industry needs. This paper analyzes these efforts and examines several critical, yet unaddressed issues facing school programs as they adapt to new criteria and guidelines. Technical issues are easy to enumerate, yet it is the programmatic and student success factors that will define successful programs.

1. Introduction

There is little argument that information security professionals are needed in our growing information based economy. Two of the top five job growth categories are in the field of IT. [1] Recently the IT security field has been reporting zero percent unemployment, indicating full employment opportunities for professionals. Yet graduates of many programs have difficulty finding employment. This paper will examine some of the issues associated with the mismatches between industry needs and the education pipelines designed to fulfill those needs.

The threat to IT systems has been growing over the past several decades. Attacks on US government systems have increased >650% over the past 5 years. [2] There is now a corresponding growth in the employment of security personnel, both in government and in industry. [3] The US government has responded to the shortage through the formation of the National Initiative on Cybersecurity Education. [4]

Information security as a discipline is built upon elements of information systems, computer science, psychology, and many other related disciplines. Operations in information security can be seen as a specialty operation that is above and beyond normal IS operations. As a specialization built on top of the base element, the skill levels associated with security personnel tend to be more advanced than those performing regular IT operations. Adding to the complexity of assessment of skill requirements is the risk associated with the security operations – security personnel tend to have greater levels of access to critical data and systems, and thus require greater scrutiny with respect to skills and abilities.

Education programs designed to meet the foundational disciplines of information security typically are accredited via programs such as Association to Advance Collegiate Schools of Business (AACSB) and Accreditation Board for Engineering and Technology (ABET).[5] One of the foundational elements of both ABET and AACSB accreditations is the concept of educational outcomes.[6, 7] Information security programs are not directly accredited, although they could be considered under ABET in the IT category. [7] The field of Information Systems has had storied arguments that it suffers from an identity crisis [8]. This confusion can be easily explained by the overlapping nature of MIS, CIS, IS, CS and IT programs. Security programs exist as a specialty under these programs, and thus can make the differentiation even more challenging.

The US government has recognized the importance of cybersecurity and has poured resources into programs and education. The most recent effort, the National Initiative for Cybersecurity Education (NICE) is an effort to define a framework to meet US government needs with respect to workforce.[4] A separate effort, the Department of Homeland Security (DHS) CyberSkills Task Force, led by a taskforce of industry and government leaders provided a separate series of recommendations. Neither of these efforts provided direct, actionable guidance for education.

In the US, there has been an ongoing program to address US Government needs with respect to Information Security graduates through a program

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.254

IEEE computer society

begun at the National Security Agency (NSA) and now shared with the Department of Homeland Security (DHS). This program, the Centers of Academic Excellence in Information Assurance Education (CAEIAE), has established criteria for two year institutions, four year institutions and research schools. Currently the NSA is leading an effort to revamp and modernize their curriculum based approach to the CAE program.

This paper looks at the need for educated professionals in cyber security, what this means in terms of specific skill development. We then present the current methodology behind several approaches to the curricula used in US universities. As the industry is experiencing a significant skills shortage, many have suggested a new course for cybersecurity education to remedy the skills shortage going forward. One approach, the re-engineering of the CAE program with the new knowledge unit based methodology being proposed by the National Security Agency is presented and analyzed. The paper concludes with an analysis of how these pieces can be used to create programs that act in the interest of education, industry and the student/graduate. A key element in our analysis is the use of programmatic and student success elements that are needed in a program if it is going to be successful as part of the analysis. Technical cybersecurity elements alone will not deliver the desired workforce results needed in today's cyber-enabled environment. If we are to have a better cybersecurity workforce, we need to change our education trajectory to meet the demands of government and industry jobs.

2. Industry Needs

The cyber security workforce needs are new to most firms. As an industry, cyber security has been around for quite a while, although the majority of the past four decades it has been concentrated in government sector. As e-commerce and other digital communities arose in business, the increasing need for cyber security has followed. Defining the needs has been challenging for a number of reasons. First, the digital revolution has been marked by sweeping technology changes. Second, with the rapid advance of new platforms, protocols and business uses, the driving force of advancement has been one of features, not security. Firms roll out new IT solutions for business reasons, and when it comes to resource allocation, the initial push has always been for more features. Security frequently takes a back seat, is seen as a cost, and the developmental resources for security have been scarce.

Even if the need is defined, there are additional daunting challenges. Security, by its very nature, requires a deep understanding not just of the technology, but of security principles as well. This means that the best candidates for security positions typically have significant technology experience and have many other career options. Growing security personnel from the ground up is a multi-year proposition, as it takes years of experience to develop maturity in the requisite knowledge, skills and abilities to perform many of the complex security tasks. The typical security functions in a modern enterprise include a mix of strategic and tactical operations. From deploying and monitoring security controls, to incident response, analysis, and forensics. The end result is a thorough capability in risk management. In an enterprise with many large scale critical systems, the detailed level of enterprise specific knowledge makes it difficult for someone to cover the entire spectrum of operations.

A recent analysis of the state of industry workforce preparedness characterizes the field as highly dynamic with the following specific challenges:[9]

- Conventional backward-facing protection methods often assume predictable, static infrastructure, when the reality is a dynamic, fluid environment;
- Asymmetric threats challenge traditional security methods and practices, demonstrating the growing need for better practices and more importantly, greater levels of expertise; and
- Professionals are often constrained by organizational silos that can isolate expertise – a challenge exacerbated by a lack of defined roles and advanced collaboration skills.

Professional development is characterized in three dimensions, knowledge, skills and ability, frequently denoted as KSA. Although considered by many to be equivalent terms, research has shown that KSAs differ across the novice to journeyman to expert categories of performance. [10] Professional development begins with the acquisition of knowledge, as this forms one part of the foundation of a practitioner's performance. The other part of the foundation, built upon the knowledge aspect is skills. Skills represent a consistent response, based on a knowledge component, to a particular set of situational criteria. Over time, with practice, the skill base can become more rapid in response, and more capable in an environment with uncertainty. Abilities are higher level functions, comprised of one or more skills, typically to a performance standard. A common belief is that to become an expert in something requires 10,000 hours of practice, over a period of as much as 10 years. This time is needed to develop the abilities based on the practiced application of an accumulation of skills and knowledge.

Industry needs in the realm of cybersecurity are not unidirectional, or targeted to a single professional.

There are a wide range of jobs that have different KSA's that are involved in cybersecurity. Some have lower required levels of knowledge and skills, while others have more advanced levels. This means that one-size does not fit all, with respect to jobs, KSAs, or education/training pipelines to develop talent.

Much like the medical profession, there is a need for doctors, nurses and technicians. In each of these major classes, there are separate types or specializations: pediatricians, surgeons, podiatrists, RNs, LVNs, LPNs, etc. Patients that require specific types of care dictate the professionals needed; no one substitutes a gynecologist for a neurosurgeon. Thinking all graduates of all programs are interchangeable can be as bad in information security as any other specialized profession.

3. Curricula

Accreditation is important to colleges and universities as the stamp of accreditation is seen as a measure of quality and a means of demonstrating that graduates meet educational requirements associated with many jobs. [11] Accreditation of University-wide programs is done in the US via six different regional accrediting bodies. This level of accreditation typically covers the bachelor's degrees being issued and ensures that the degree meets a minimum number of hours and specific content levels to ensure quality and uniformity. Accreditation of programs to specific degree program objectives is a separate effort, with this effort being more focused on the specific content of the degree and how the degree program is managed.

In the case of accreditation of programs, one of the first considerations revolves around the issue of focus of the program. Programs are accredited to meet a standard. In the case of information systems, the most common standard is the IS 2010 Curriculum standard, promulgated by ACM and IEEE-CS. [12] There are numerous other related computer science standards, including ones for software assurance, computer science, and computer engineering, however there is not a specific one for information security. [13, 14] This is one of the issues that the current effort being led by NSA is attempting to rectify, to produce a de-facto base set of information security standard curricula.

The IS 2010 Curriculum is designed around a series of outcome objectives and fundamental resource elements such as laboratories and instructors. A set of seven proposed courses is outlined, demonstrating a path to operationalize the material into a manageable form for delivery across a wide range of undergraduate programs. [12] There is flexibility built in so that the material can be morphed into existing programs to enable ready adoption. The seven courses are:

IS 2010.1 Foundations of Information Systems
IS 2010.2 Data and Information Management
IS 2010.3 Enterprise Architecture
IS 2010.4 IS Project Management
IS 2010.5 IT Infrastructure
IS 2010.6 Systems Analysis &Design
IS 2010.7 IS Strategy, Management, and Acquisition

The program document lists specific learning objectives for each of the above courses. While institutions have leeway in how they adapt this material into their programs, the above material provides a reasonable foundational basis upon which any institution specific specialization can be undertaken. For instance if a program adds programming classes, then it can produce web developers, programmers, etc.

For a foundational curriculum, such as IS, this method of documentation works well. Arguably the basics are covered by this approach, and although detractors have stated that security, or ethics, or other elements are not given their proper perspective. The response from members of the committee that created the curriculum has always been – "it can be built inside this framework". This is a reasonable expectation for a foundational curriculum with built in flexibility. For a curriculum with multiple diverse options, such as information security, the "all-in-one" approach will not work well. The diversity of information security as an academic topic, as well as its reliance upon and IT/IS foundation, has been documented in several studies. [15, 16] The development of a single foundational curriculum that can meet all major requirements is not a possibility for a field as diverse as information security.

Information security is a field that has both breadth and complexity. Security can be impacted by virtually any and all technologies employed in the enterprise; as well as actions by people in the enterprise, whether governed by procedure or not. This makes the domain of study very large and one with lots of detail. If a person is involved in securing operating systems, they first need advanced knowledge on the operating system, how it works and where vulnerabilities have occurred. The level of detail is significant, making it extremely rare for someone to be good at both Windows and Linux.

Success in educational programs can be viewed from a variety of aspects. Student success can be examined from either successful completion of program, or career progression upon graduation point of view. Since successful completion typically precedes the career aspect, this paper will focus on that aspect in its analysis. As students self-select their educational paths, and outcomes do weigh in their decisions, student success is an important issue of an institution is going to have a thriving program. Cybersecurity classes will not have throngs of students enrolling and then washing out like biology and chemistry programs are famous for in higher education. For students to embark on the challenging program of study, they need to perceive the usefulness of the program, and this is typically done through job placement history. This makes alignment of program objectives and hiring firm's requirements a factor in student success. Student success is also influenced by creating a learning community where they can belong to a larger group with similar goals and objectives. The inclusion of student groups and other forms of community act to increase student success and are important to a successful program.

4. New NSA driven model

At the time of this paper, the new NSA curriculum based model for determining CAEIAE status is still under development, and the final outcome may indeed look slightly different. The methodology being employed to date to build the model has been one that has been highly inclusive of academic and industry involvement. Numerous workshops have been hosted across the country to facilitate academic involvement in the development of the criteria. The new criteria is based around a concept of a knowledge unit (KU). A KU is a midlevel grouping of knowledge and skill in an area of cybersecurity. Examples of KU's include, networking concepts, introduction to cryptography, information security fundamentals and basic scripting. Some KU's are comprised of more detailed elements than others, but each is geared towards introductory knowledge and skills around a central topic.

Within a given KU, a series of topics are covered. At the time of the drafting of this paper, not all KU's have been completely detailed, nor have knowledge and skill components been defined for each topic in the KU. One of the issues faced in cybersecurity is the ever advancing nature of technology. What was new yesterday, is old today, then something newer, and typically not even on the radar of most, arises and demands security attention. This occurs for both technology and the attacks against it. An example of the topics for the KU networking concepts includes:

- Overview of Networking (OSI Model)
- Network Media
- Network architectures (LANs, WANs)
- Network Devices (Routers, Switches, VPNs, Firewalls)
- Network Services
- Network Protocols (TCP/IP, HTTP, DNS, SMTP)
- Network Topologies
- Overview of Network Security Issues

Each of these topics is still high level enough to have several knowledge and skill elements defined.

The KU program is a key component of the Centers of Academic Excellence in Information Assurance Education (CAEIAE) program. The CAEIAE program is designed to recognize schools that offer security programs that meet a certain minimal level of coverage. One of strengths of the KU based program is its ability to recognize schools that have differing programs. The program is designed around a core component of KUs with additional KUs that act as specializations. This aligns with the industry demands for a broad spectrum of different worker capabilities.

The overall structure of an academic program will be built around a set of core KUs, with institutions then picking additional optional KUs to build out a program around their own specific themes. By grouping KUs around themes, institutions can specialize their offerings around specific job areas, incident responses, operations, digital forensics, etc. This flexibility provides a much better ability to match education offerings to industry needs than previous approaches to alignment.

Core Knowledge Units - 2 Year degrees

- Basic Data Analysis
- Basic Scripting or Introductory Programming
- Cyber Defense
- Cyber Threats
- IA Fundamentals / Security First Principles
- Intro to Cryptography
- Introduction to Digital Logic
- IT Systems Components
- Networking Concepts
- Policy, Legal, Ethics, and Compliance
- System Administration

Core Knowledge Units – 4 Year degrees (2Y Core Knowledge Units plus)

- Database Management Systems
- Human Machine Interface
- Network Defense
- Networking Technology and Protocols
- Operating Systems Concepts
- Probability and Statistics
- Programming

Individual KUs are not the same level as courses and a single course can meet elements from multiple KUs. The challenge is in determining what needs to be in courses to have a complete education and the KUs provide a mechanism for managing this complex task. The use of specialty areas, which are comprised of groupings of different KU's, works towards overcoming the challenge of aligning education to job requirements.

Job titles, requirements and details vary all over the map, but they do tend to fall into groupings; forensics, incident response, etc. By driving the education programs to specialize in an area, this enhances the ability for students to maximize their education against job opportunities upon graduation.

5. Aligning Objectives

One of the missing elements from both the curricula models and to a degree the KU model is the use of outcome objectives to guide student learning. Whether called learning objectives, or outcome objectives, the result on the student learning process is dependent upon the quality of the objective, not how it is labeled. [17] When examining security and IT objectives, the Mager model of condition, behavior and standard is well suited. [18] These objectives can be then structured like the topics in a class, from general to specific. General: Given a computer and vulnerability scanner, the student will be able to identify the vulnerabilities. More specific: Given a computer and a vulnerability scanner, the student will be able to identify the specific vulnerabilities on the computer, correct them and rerun of the vulnerability scanner to demonstrate that the system no longer shows the vulnerabilities. You can even create highly specific ones such as Students will be able to configure Snort rules to detect a SSH login from outside the corporate network.

For learning outcomes to be effective at guiding student learning, there are several traits needed. They need to provide an intuitive, student-friendly and transparent framework for guiding the learning process. When learning outcomes emphasize a broad overview with a top-down design approach to a more detailed specification, this results in key areas of learning being emphasized, making it easier for students to navigate toward key concepts and issues in a complex environment. By making the important elements more evident, the student is guided towards a pathway of learning designed to be more comprehensive and achievable.

6. Analysis of Gaps

One of the biggest current gaps in alignment between education and industry is a complaint that graduates do not have sufficient hands-on skill sets to make them ready to perform jobs. Highly noted in the recent DHS CyberSkills Report, one proposed remedy is the tightening up of criteria associated with NSA/DHS certifications, so that programs will respond with more hands-on content. [19] This issue of hands-on experience has been a long standing criticism of many higher education programs. The central theme of this issue is training versus education. Training tends to be oriented towards the how and is focused on the current technology and methods. Teaching a student to develop and implement specific firewall rules on a Cisco router is training. Education tends to focus on the why, the theory and mechanisms behind the material. Teaching a student about firewall rules, how they are used to implement a perimeter defense, their strengths and weaknesses, this is the role of education.

Industry wants workers to arrive ready to work day one, on their equipment, configured as they have configured it, and able to immediately add to the team strength. Industry also expects their workers to have the knowledge (read education) that they can adapt to technology changes and continue to contribute as systems, equipment and processes change. Although many refer to this as an "or" proposition (you can be educated, or you can be trained) the reality is that industry needs this to be an "and" relationship. It is important that students learn the theory, the why, as well as how to implement it on current equipment, the how. The relationship of training to education is illustrated in Figure 1.

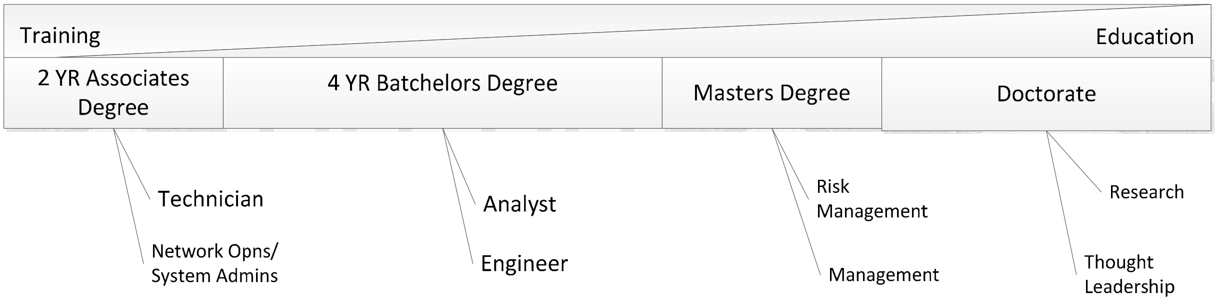

Figure1. Pipeline for Information Security Education and Training

Figure1 also illustrates a pipeline from community colleges through doctoral programs associated with information security. This figure illustrates several things. First, there are several different degree program levels that will provide information security workers to industry. This is important as the field needs a wide range of workers with differing skillsets. The figure shows the higher training component of community college programs, which goes towards the "we need workers now" issues facing many firms and government agencies. Ensuring that the education pipeline dovetails with industry needs will enhance student opportunities at the end of their education. This will strengthen programs in many ways including increasing the factors that support student success.

The current practice of accredited university education is typically grounded in theory, and has less room for training opportunities. Students that take all the hands-on courses at a community college have troubles applying most of their work towards a 4 year degree, should they choose to go further with their education. This creates a wall for students allured by the immediate job prospects of the technical hands-on operator training found in community college programs. This also creates a long term issue for the industry, as it creates a class of workers without the skills to move forward in a career in information security. These students will never possess the university degrees or understand all of the theory behind the driving forces in the industry.

Students self-select their education programs; which university, which major, which classes (electives) and which professor (when there are options). This too can have adverse effects, as students will self-select based on self-desired items such as "cool classes", easy grades, etc., instead of focusing on the quality of education with respect to future opportunity. The result is the education system with its gaps in desired outputs as being experienced today. There is a strong desire on the part of students to take classes such as pen-testing, as the allure of the topic and the opportunity to "hack" and the ability to put it on a resume. This, in turn, drives professors to build these classes to meet a "market demand" in their programs. In today's economic times, "butts in seats" is a measure most programs monitor and report to their administration.

Students that have participated in the National Collegiate Cyber Defense Competition (CCDC) have demonstrated a high employability value, with members of teams that compete in the National Finals all receiving serious job offers from the biggest names in the industry. Team members after 5 years of employment have demonstrated solid career progression. This serves as a possible example that a proper mix of training and education can be achieved. Hands-on programs increase self-efficacy on the part of students and research has shown that this is an important element in building student success. These are important lessons to be learned from a student success point of view and warrant the consideration of activities such as these directly in a program rather than optionally on the side.

We also have seen cases where some of the "best and brightest" jumped ship early in the education pipeline, lured by good starting salaries, but then became trapped in dead-end jobs because they don't have the necessary education to move up the corporate career ladder. In spite of the immediate need for well-trained people, the industry as a whole might be better served by not eating the seed corn, as the best and brightest should be encouraged to go as far up the education ladder as possible. This is how we will truly advance new ideas and innovations. Aligning student achievement and potential to ensure student success is an important programmatic element. Virtually all students, each with their own abilities and background will enter the Figure 1 pipeline on the left. How far they progress through the pipeline is a result of many factors. Because of the multitude of different jobs in cybersecurity, it is important to realize that the objective is not to move all students as far through the pipeline as possible. A more optimal outcome will be to move students as far as possible based on each student's ability, something easily measured with success indicators such as GPA. Identifying the best paths for individual students, based on their abilities, will increase student success and help the entire program to grow and thrive.

As for all programs, we need to determine the correct mix of theory and practice. Information security classes without hands-on exercises, dealing with the operationalization of the theory and concepts from lectures, have little place in our field. There are few, if any jobs, for those who cannot do some of the security tasks. Students need the ability to implement, as well as the ability to understand. Simply memorizing things from Google will not produce the level of worker that is needed. We must move classes up the Bloom's Taxonomy and a proper implementation of the elements of the KU based program being developed by the NSA can go a long way toward this objective. Even the course structures from the accrediting standards are useable, as instructors are given significant leeway within the structures to incorporate material of their own choosing.

Objectives can be the guide that assists students in navigating the material in the pursuit of learning the essential elements with respect to developing useful ability through the course of study. This places the responsibility of aligning the objectives to create a bridge between material and job needs upon the course designer and instructor. This level of essential detail is missing from the curricula and KU models described and needs to be addressed if a program is going to produce graduates that can assume roles in the security field without additional post-graduation training.

Examining all the options, it is recommended that the course structures accreditation provides be re-engineered to include the KU material, including hands-on laboratory exercises. In every class, there should be a conscious decision about the ratio of training vs. education, ensuring all levels of students get sufficient levels of each. Actual demonstrations of the classroom material in operational settings, such as the CCDC exercises or internships, should be highly encouraged. Practice makes perfect and a lot of practice is needed by all participants at all levels. Using the KU's as a list of essential elements, that fit into the curricula (class) container scheme is relatively easy. The missing element is the development of the learning objectives at several levels, from course, to lecture, to assignment, that enable students to navigate the complex subject matter of security and IT.

The KU effort is a great first step toward providing a framework for educators to align information security programs with industry needs. But as already discussed, this is not a single dimension issue, security has many different dimensions, with divergent needs. This means that the information security training and education environment serves a family of needs, and without the basis of solid learning outcomes, these needs are still poorly defined. Much work needs to be done in defining the learning objectives across the KUs so that the landscape can be navigated and consumed by students in a productive fashion.

Another missing element of the KU based system is the determination of appropriate coverage of material. In the past, programs such as the CAEIAE program have operated on a 100% or nothing basis. You either possessed ever element to a desired degree or you did not obtain recognition. This concept works when the list of elements is fairly limited, but in the current KU system, the list has grown tremendously. This creates a situation that is currently being debated across secondary school systems across the country – do we teach what needs to be learned, or do we teach to the test. In an ideal world, these are the same, but in a dynamic world such as cybersecurity, this can lead to programs not teaching what employers want, either because it is too new and not on the list yet, or because there isn't room in the curriculum because of other items an employer doesn't care about but needed to maintain program recognition. There is an easy fix, set a percentage, such as 90%, and expect programs to cover at least 90% of the listed elements. This provides flexibility and also will dramatically reduce criticism of specific individual program elements as they will not all be required. Again, making things more achievable and credible will enhance student success and assist in industry acceptance.

The role of the government in building a successful cybersecurity education system goes beyond just detailing a list of technical elements that need to be covered. Creating a program with the level of flexibility to allow institutions to dovetail technical program elements, with programmatic elements that build student success and meet industry needs will strengthen the outcomes of the programs. Acknowledging the need for more than just a set of technical outcomes will not be enough. Any government recognition program designed to assist in cybersecurity education needs to pay more than just lip service to the complete set of elements that drive student success and outcomes. Providing resources, in terms of funding, time and materials, across the entire spectrum of an educational program is needed to create a new profession of highly skilled workers. We are not suggesting more regulation, but are suggesting that addressing student success factors as well as industry accepted outcomes are needed to achieve the goals associated with creating a professional cybersecurity workforce.

7. Future work

The shift to a KU based cybersecurity education platform is just beginning, with many of the details still not determined as of this paper. As the industry shifts to this new paradigm, it remains to be determined whether the new criteria alone will make enough of a skills based shift to move the industry where it needs to go. The addition of student success factors into the design of a new curriculum will result in better assimilation of the material as shown in other education areas where these techniques are used. To fulfill the objective of producing the best trained and educated cyberskills workforce possible, the inclusion of elements such as student success factors into the final education model will assist in achieving the object. The exact roles, levels of these factors and best method to employ them needs further study to optimize the results.

8. References

1. Choudhury, V., A. Lopez, and D. Arthur, *"Issues and Opinions - IT Careers Camp: An Early Intervention Strategy to Increase IS Enrollments".* Information Systems Research. **21**(1): p. 1-14.
2. Noland, K., *GAO: Federal Cyberspace Incidents Up 680% Over 5 Years*, in *ExecutiveGov*. 2012, ExecutiveGov.
3. Vijayan, J., *Demand for IT security experts outstrips supply*, in *ComputerWorld*. 2013.
4. NIST, *National Initiative for Cybersecurity Education Strategic Plan*, National Institute of Standards and Technology (NIST), Editor. 2012, NIST: Washington, DC. p. 26.
5. Attaway, A.N., et al., *An Approach to Meeting AACSB Assurance of Learning Standards in an IS Core Course.* Journal of Information Systems Education, 2011. **22**(4): p. 355-366.
6. AACSB International, *Eligibility Procedures and Accreditation Standards for Business Accreditation*. 2006, The Association to Advance Collegiate Schools of Business.
7. ABET. *Criteria for Accrediting Computing Programs, 2013 - 2014*. 2013 [Last; Available from: http://www.abet.org/DisplayTemplates/DocsHandbook.aspx?id=3148.
8. Benbasat, I. and R.W. Zmud, *The identity crisis within the IS discipline: Defining and communicating the discipline's core properties.* MIS quarterly, 2003: p. 183-194.
9. Assante, M.J. and D.H. Tobey, *Enhancing the Cybersecurity Workforce*, in *IT Pro*. 2011, IEEE Computer Society.
10. K.A. Ericsson et al., *The Cambridge Handbook of Expertise and Expert Performance*. 2006: Cambridge Univ. Press.
11. Saulnier, B. and B. White, *IS 2010 and ABET Accreditation: An Analysis of ABET-Accredited Information Systems Programs.* Journal of Information Systems Education, 2011. **22**(4): p. 347-354.
12. Association for Computing Machinery (ACM), A.f.I.S.A., *IS 2010 Curriculum Guidelines for Undergraduate Degree Programs in Information Systems*. 2010, Association for Computing Machinery (ACM) and Association for Information Systems (AIS).
13. ACM and IEEE Computer Society, *CS 2008: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*. 2008, IEEE/ACM Joint Task Force on Computing Curricula.
14. IEEE Computer Society and ACM., *CE 2004: Curriculum Guidelines for Undergraduate Degree Programs in Computer Engineering*. 2004, IEEE/ACM Joint Task Force on Computing Curricula.
15. Rowe, D.C., B.M. Lunt, and J.J. Ekstrom, *The role of cyber-security in information technology education*, in *Proceedings of the 2011 conference on Information technology education*. 2011, ACM: West Point, New York, USA. p. 113-122.
16. Ma, J. and J.V. Nickerson, *Hands-on, simulated, and remote laboratories: A comparative literature review.* ACM Comput. Surv., 2006. **38**(3): p. 7.
17. Harden, R.M., *Learning outcomes and instructional objectives: is there a difference?* Medical Teacher, 2002. **24**(2): p. 151-155.

18. Mager, R.F., *Preparing instructional objectives*. 1962.

19. DHS Task Force on CyberSkills, *CyberSkills Taks Force Report*, D.o.H. Security, Editor. 2012: Washington, DC. p. 1-41.