Curriculum Standards Panel

Foundation Series: Information Security Fundamentals

Charter and Project Plan

Released: August 21, 2017

Table of Contents

Introduction

Brief History of the National CyberWatch Center Curriculum Standards

When the National CyberWatch Center was launched in 2005, quality information assurance curriculum was in short supply, so the development of new curriculum was a necessity. In 2006, the National CyberWatch Center developed the nation's first model Information Assurance and Computer Forensics curricula. The development of standard curriculum has supported the growth of cybersecurity education nationally. Building on its model curriculum base, the National CyberWatch Center expanded the reach of cybersecurity education curriculum through the development and dissemination of stackable credential models.

In 2016, the National CyberWatch Center Curriculum Standards Panel (NCC-CSP) was established. Our mission is to identify the learning objectives, concepts, procedures, situational judgments, and intellective abilities required to develop capabilities maturity in cybersecurity foundational principles, techniques, tactics, and protocols. The standards produced by the NCC-CSP are the first to align instructional design, skill practice facilities, cybersecurity professional job performance standards, national workforce frameworks, and industry needs. The National CyberWatch Center Curriculum Standards Panels develop standards for instructional materials, assessments, hands-on labs or other learning programs. These curriculum standards align with national competency frameworks, such as the National Security Agency Centers of Academic Excellence Knowledge Units and the National Initiative for Cybersecurity Education (NICE) Workforce Framework KSAs.

In 2017, the standards panel architecture and mission was extended to develop course-specific standards panels to advance the models of instructional design used in cybersecurity education. Each standard course panel will develop a competency-based, mastery learning curriculum library. Competency-Based Education curriculum substantively differs from traditional instructional techniques used in most -cybersecurity education and training programs today. Competency-based objectives, principles, and techniques target increased cybersecurity capability maturity of the entrant and incumbent information technology workforce. By embedding assessments of capability maturity at each step of the learning process, readiness for instructional material is increased, thereby accelerating and deepening the comprehension or transfer of instructional material. Accordingly, a Curriculum Standards Course Panel (CSCP) process applies recent advances in learning science to innovate the conception, design and delivery of cybersecurity education.

What is different about Competency-Based Education—and why should we care?

Competency-Based Education (CBE) differs in several ways from Outcomes-Based Education (OBE). CBE seeks the achievement of learner improvement (regardless of outcome); while OBE seeks course or institutional achievements, such as grades, degree completion, or certification. These alternative approaches to education place different emphasis on the role and positioning of assessment. They also differ in the determinants of efficient operation. Consequently, they focus on different learning objectives and how the accomplishment of these objectives is measured. Essentially, CBE and OBE differ in their view of what constitutes a successful education program.

A primary purpose of OBE assessment is the classification of learners into groups, e.g., letter grades or certified/non-certified, based on designated score ranges. Since practitioners of OBE are comparing a learner with subjective distinctions, the OBE assessments are referred to as norm-referenced tests.

Conversely, CBE is guided by formative assessments based on valid predictors of job performance. Due to being grounded in evidence-based learning outcomes, CBE assessments are referred to as criterion-referenced tests.

Formative assessments within CBE enable "teaching-to-the-test" to ensure learners can accomplish *all* the task objectives. In contrast, summative assessments are common in most classrooms today. They enable "testing-what-was-taught" to ensure the most qualified individuals are selected through graded differentiation of achievements within a prescribed timeframe. The effect of this selection focus is to *reduce the number of the qualified* individuals in a competency domain to only those scoring above a "cutoff" on summative credentialing exams. OBE defines success as the number of individuals who obtained minimum proficiency in the time allotted—the *student success rate*.

CBE focuses on personalizing the educational experience in order to *increase the number of the capable* individuals who can perform the work. CBE instruction is driven by embedded assessments within each learning module that are designed to accurately identify and eliminate the obstacles to the development of competency. Whereas OBE focuses on what was understood, conceived and/or applied in order to recognize achievement, CBE focuses on what was misunderstood, misconceived, or misapplied in order to recognize readiness to learn subsequent material. Contrary to the OBE focus on the *ends* of learning, CBE is focused on the *means* of learning—the instructional techniques and readiness of the learner—with a primary goal of systematically reducing obstacles to achieving mastery in the shortest time possible—the *learning success rate*.

In sum, in CBE assessment is formative, precedes or drives, and is embedded in instruction whereas in OBE assessment is summative, occurring after learning and often as an afterthought in instructional design. CBE seeks to improve efficiency of learning where OBE seeks to improve efficiency of instruction.

Outcomes-based assessments measure the *learning objective* of assimilating the content transmitted. Each learner is scrutinized to determine if they can provide the minimum number of *correct answers*. The efficiency of information transmission is measured by the number of individuals achieving *completion* of the course or degree program in the expected amount of time, e.g. 4-6 years for an undergraduate degree. This focus on efficient information transmission minimizes the time and cost investment in limited instructional resources (talent and technology). The trade-off is that not all learners will achieve proficiency of understanding or competence in application in the time provided.

Conversely, the *learning objective* of CBE is mastery of each concept, action, or judgment required by a competence domain. The *mastery threshold* determines the optimal content to be fully comprehended and applied. Each instructional module is scrutinized to determine if it possesses the minimal level of "correct instruction" necessary to eliminate misunderstanding, misconception and misapplication of course material. The efficiency of each individual's learning curve is measured by the breadth of mastery achieved by the learners, within the time provided. The trade-off is that the economic basis of education must shift from seat time to learning time. This necessitates a change in metrics from credit hours to credentials achieved. In Thus, success in OBE is measured by how quickly (and how many) individuals complete the course while CBE is measured by how quickly and how many requisite capabilities are mastered. OBE rewards successful students while CBE rewards successful learning.

Developing Pathways to Mastery

The current project, funded by a grant from the National Security Agency, will extend the initial work

of the NCC-CSP. The Curriculum Standards Course Panel (CSCP) will apply psychometrically-valid, competency-based instructional design techniques to develop the model domain taxonomy, assessment items, instructional content, and the sequencing plan for that content necessary to overcome constraints to developing mastery of the fundamentals of information security. The model is intended to provide guidance towards standardization of cybersecurity curricula. Further, the model curricula will facilitate rapid prototyping, development and dissemination of adaptive, accelerated learning systems that can substantially improve cybersecurity workforce capability maturity. The result will not be a course, in the traditional outcomes-based sense. Instead, a library of learning objects will be assembled. These learning modules may be mixed and matched based on learner readiness, institutional goals, and career requirements. In analogical terms, *the CBE course is a step along a pathway to mastery, not a serving for a meal to complete the menu in a course catalog*.

A pathway crosses thresholds, passes milestones and checkpoints, with crosswalks or exit ramps connecting one pathway to another. Similarly, the CSCP process is designed to identify the pavers, gates and intersections for each CBE course. Four types of pavers will categorize knowledge as declarative, procedural, conditional or situational. The transfer from knowledge to skill is assessed by passing through a performance gate which assures consistency of skilled application. Intersections demark a milestone or checkpoint (achievement of a badge or certificate) earned when skilled application has been demonstrated across a series of scenarios of increasing difficulty. Finally, when the necessary and sufficient milestones and checkpoints have been achieved, the pathway may lead to other courses for which prior learning serves as pre-requisites.

Over the long term, a series of CSCP processes will define the entire Information Assurance and Cybersecurity Foundation Series. These courses will provide the competency prerequisites for mastering Career Pathway courses enabling the capability to perform one or more specialty job roles. Figure 1 depicts the vision for the CSCP program supporting development of both Foundation and Career Pathway courses. Figure 2 depicts the Foundation and Pathway Series as a holistic approach to enhancing the nation's cybersecurity capability maturity. Together these series of CBE curricula will support learning pathways for traditional and continuing education, facilitate articulation agreements between Cybersecurity Centers of Academic Excellence, and accelerate the transition of entrant and incumbent works to meet the growing demand for cybersecurity capabilities.

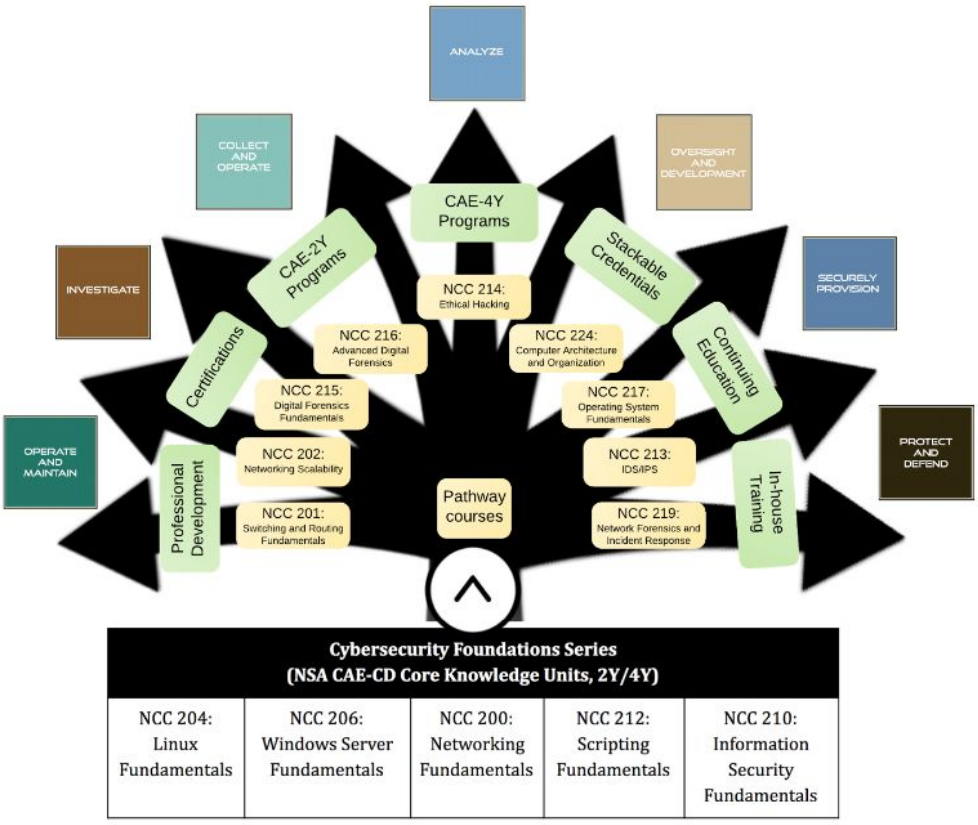

Figure 1: Foundation and Pathway Series Curriculum Standards

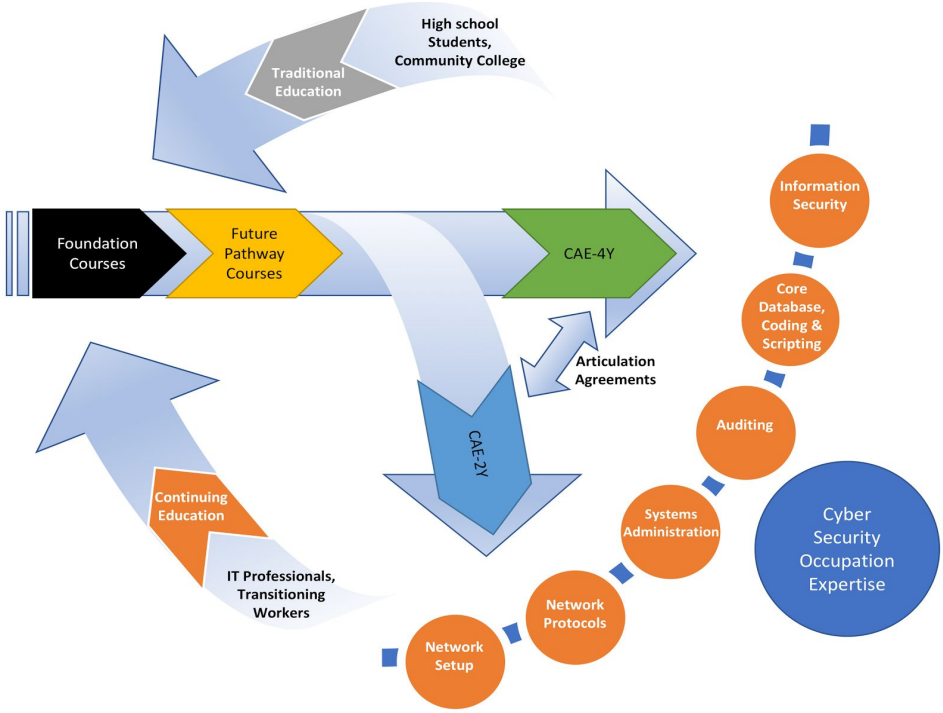

Figure 2: A holistic pathway to enhance cyber career readiness

The CSCP Process

The Cybersecurity Foundations Series Curriculum instructional design process applies evidence-based principles in competency-based learning (Jones & Voorhees, 2002). CBE research has identified eleven practices are needed to design curriculum that is valid and reliable for maturing job- and career-ready capabilities. Each of these eleven practices will be applied in producing the Foundation Series instructional materials.

Core Curriculum Development Process

1. A chair of the course curriculum panel is named as the managing editor of the CBE Mastery Learning Course Library being designed and developed by the CSCP.
2. 30-50 subject matter experts (instructors, industry practitioners, and instructional designers) are assigned to a Topic Area Working Group (TAWG) to identify, define, and agree on competencies required for mastery in their assigned area.
3. Competencies are clearly defined, understood, and accepted by relevant stakeholders. Competencies are defined at a sufficient level of specificity that they can be assessed (measured) to assure learning effectiveness.
4. Multiple learning paths and related assessment item topics are identified to guide attainment of mastery in course content.
5. The assessment team considers precision, reliability, validity, credibility, and cost requirements in making decisions about the use of commercially developed assessments and/or panel-developed assessments.
6. The panel of experienced faculty and practitioners participate in the design of new instructional materials and related assessment items (as required).
7. The course instructional and assessment design is aligned with the developing National CyberWatch Center Core Curriculum Standards Curriculum Map. The curriculum map provides institutional guidance for course, certificate, degree, and career development pathways associated with the National Cybersecurity Workforce Framework Specialty Areas
8. Assessment items are directly mapped to learning goals in competency profile scorecards that will support individual or personalized development plans (IDP/PDP) for each learner.
9. A pilot implementation of the course enables critical decisions about strategies to improve student learning and program effectiveness. Aggregation of pilot competency profiles demonstrates a more rigorous and performance-based institutional program evaluation and accreditation process that includes formative guidance to policy makers.
10. The pilot implementation results are disseminated through public review and comment workshops to ensure all relevant stakeholders fully understand the findings.
11. The pilot implementation results are used to experiment with new ways to document students' mastery of competencies that supplement the traditional transcript.

Panelist assignments and responsibilities

As referenced above, panelists will be assigned to one or more of the TAWGs based on their expertise in teaching, designing, or having relevant work experience in the focal topic area. Each working group will include a minimum of 30 panelists. Panelists must be willing to: 1) participate in at least one of the online discussions scheduled each week of active panel work; 2) contribute to the accomplishment of the session objectives after the weekly online meeting in asynchronous activities; and 3) review the

TAWG and final CPSP deliverables. Panel activities will be facilitated by the National CyberWatch Center Research Team supported by an online brainstorming and collaboration system.

Panelists who are unable to commit to a minimum of two hours for any weekly session should notify the Panel Administrator at least two week prior to the scheduled session. A schedule of activities will be posted to Google+ Community to provide logistical and communication support for the panel activities. Each panel or TAWG session will involve a series of online activities that will be included in a Session Agenda announcement on the Google+ Community site and discussed at the opening of each session conference call. Each week will include at least three independent conference call events to accommodate panelist schedules. **Panelists are requested to attend at least the conference call of one session each week in which they will participate**. Panel activities can be accomplished asynchronously, if desired. However, panelists should find they will benefit from the interactive, collaborative, synchronous sessions and that they will experience higher productivity during synchronous activity.

The purpose of each session conference call is to provide a scheduled time for synchronous, collaborative input from panelists. The scheduled weekly calls will ensure: 1) appropriate time is allocated for completion of session activities; 2) assignment of panelists to breakout working groups as necessary; 3) sequencing of working group activities is most efficiently accomplished; and 4) data aggregation, analysis, and reporting of session output supports the weekly session activity schedule.

Prior to the first mapping session a survey will be distributed to request preferences for days and times for synchronous sessions.

Summary of CSCP Mission

Expected outcomes

1. Demonstrate the rapid development and renewal of instructional materials that closely aligns with the National Institute of Standards and Technology's National Cybersecurity Workforce Framework (NCWF) by implementing effective practices in crowdsourced, competency-based instructional design, supporting scaling of the full program across both Foundations and Pathway Course designs.
2. Demonstrate the feasibility and agile development benefits of inductive, psychometric classification methods for identifying common misunderstandings and misconceptions of concepts, procedures, conditions, or situations, which must be remedied for accumulation of cybersecurity expertise to occur. These competency-based assessment models will apply Diagnostic Classification Modeling to produce detailed competency profiles and personalized (differentiated) learning paths for each learner as a complement to current grade-based or portfolio-based assessments.
3. Demonstrate the platform independence of the differentiated instruction modules through use in both hosted and locally established infrastructure learning environments.
4. Demonstrate the feasibility of raising the cybersecurity capability maturity levels of learners, both traditional and non-traditional, through the application of formative, mastery-based learning techniques.

Project Deliverables

Outcome: Crowdsourced Instructional Designs Aligned with NCWF
Deliverables: Library of conceptual, procedural, conditional and situational instructional modules covering all NCWF Competency Areas that were designated by the National CyberWatch Center CSP as applicable for the course (draft syllabi available upon request).

Outcome: Inductive Concept Inventory Development
Deliverables: A minimum of three concept inventory assessment items will be identified for each instructional module discussed above. These will be validated and improved throughout the prototype development period.

Outcome: Platform Independence
Deliverables: The demonstration of this platform independence will be evidenced by three use-case implementations of the Fundamentals of Information Security course: 1) selective module use as a supplement to existing course syllabi using textbook or other traditional instructional techniques; 2) implementation in a standard off-the-shelf LMS which offers differentiated or mastery learning paths; and 3) implementation in a hosted environment which provides integrated, adaptive learning.

Outcome: Increasing Capability Maturity
Deliverables: Each participant in the pilot will receive a personalized competency profile showing their capability maturity within the NCWF model. This data will be aggregated to support workforce planning. Finally, a pre-post analysis will permit evaluation of maturity level increase.

Final Deliverable

The cumulative process will produce a curriculum model for cybersecurity professionals consistent with the requirements of the U.S. Equal Employment Opportunity Commission (EEOC), the International Organization for Standardization (ISO), and the American National Standards Institute (ANSI) guidelines for development of recruitment and selection programs. The model will contribute to the development of standards for aptitude testing, instructional design, performance evaluation and electronic performance support systems in both academic and corporate training environments.

Panel Chair and Managing Editor

Alan Watkins
ABW Consulting Services
Phone: (n/a)
Email: abwatkins.consulting@gmail.com

Panel Administrator and Session Facilitator

Dr. David H. Tobey
Indiana University South Bend
Phone: (540) 860-0360
Email: dhtobey@indiana.edu