by Cara Tang,
*Portland Community College*

# Cyber2yr2020: ACM Guidelines for Associate-Degree Cybersecurity Programs

Cybersecurity has emerged as an academic discipline as demand for cybersecurity professionals burgeons. As the field develops and grows, projections of the shortage of cybersecurity workers continue, and the growth of cybersecurity jobs continues to accelerate. In their 2017 Global Information Security Workforce Study, (ISC2),[1] a worldwide organization of cybersecurity professionals, projected the global cybersecurity workforce shortage to reach 1.8 million by 2022 [9]. In 2019, Cybersecurity Ventures predicted there will be 3.5 million unfilled cybersecurity jobs globally by 2021 [7]. The U.S. Bureau of Labor Statistics projects that in the period 2018-2028, all occupations in the U.S. economy will grow by 5%, computer occupations will grow by 12%, and information security analyst occupations will grow by 32%, which is "much faster than average." [13] The projected 32% growth rate is a dramatic increase over already-high previous projections, as shown in Table 1.

**Table 1:** U.S. Bureau of Labor Statistics growth projections

| 10-Year Period | U.S. Bureau of Labor Statistics Growth Projection for Information Security Analysts |
|---|---|
| 2014-2024 | 18% |
| 2016-2026 | 28% |
| 2018-2028 | 32% |

Academic institutions are racing to build and update cybersecurity programs to help meet the growing demand for cybersecurity professionals; community and technical colleges in the U.S. and similar schools around the world have an important role to play.

## Cybersecurity Curriculum Guidelines

In December of 2017, the Joint Task Force on Cybersecurity Education published *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity* (CSEC2017) [10], representing a new discipline in ACM's Computing Curricula Series. The volume was endorsed by four professional societies: Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS), Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC), and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8). Offering guidance for a broad variety of cybersecurity programs at the post-secondary level, CSEC2017 is a first effort at comprehensive cybersecurity curriculum guidelines.

Following on the CSEC2017 effort, the ACM Committee for Computing Education in Community Colleges (CCECC) has led the creation of a similar set of guidelines for two-year Cybersecurity programs at the associate-degree level, called Cyber2yr2020. In addition to CSEC2017, other relevant sources that have influenced the associate-level guidelines include the CAE (Center of Academic Excellence) in Cybersecurity 2019 knowledge units (requirements of the U.S. National Security Agency and Department of Homeland


ILLUSTRATION: ©CAN STOCK PHOTO/MCARREL

Security National Centers of Academic Excellence in Cybersecurity) [12] and the NICE (National Initiative for Cybersecurity Education) Cybersecurity Workforce Framework [11]. Cyber2yr2020 aligns with 100% of the CAE Foundational Core and Technical Core knowledge units. The scope of Cyber2yr2020 includes both career-oriented (intended to lead to a job) and transfer (intended to lead to transfer into a four-year program) associate-degree programs in cybersecurity.

## Development Process

The ACM CCECC formed the Cyber2yr2020 task force in early 2018 consisting of ten community college educators from schools across the United States and representing a variety of focus areas within cybersecurity. The task force met online close to monthly, with occasional in-person meetings of subsets of the group. The task force members are listed here.

- Markus Geissler, Cosumnes River College, CA (steering committee)
- Nancy Jones, Coastline Community College, CA

[1] 2017 Global Information Security Workforce Study is referred to as ISC2 or ISC[2]. We use the former so there is no thought that the superscript is to a footnote.


ILLUSTRATION: ©WWW.ISTOCKPHOTO.COM/OSKANOV

- James Kolasa, Bluegrass Community and Technical College, KY
- Amelia Phillips, Highline Community College, WA
- Lambros Piskopos, Wilbur Wright College, IL
- Pam Schmelz, Ivy Tech Community College, IN
- Christian Servin, El Paso Community College, TX (steering committee)
- Melissa Stange, Lord Fairfax Community College, VA (steering committee)
- Cara Tang, Portland Community College, OR (steering committee, task force chair)
- Cindy Tucker, Bluegrass Community and Technical College, KY (steering committee)

In addition to the focused work and contributions of the Cyber2yr2020 task group, significant input came from the community through a variety of means including face-to-face breakout groups at a pre-NICE Conference event in November 2018; survey responses; feedback on drafts; interactive sessions at conferences; and input from the project's advisory group of professionals from industry, government, four-year schools, and the CSEC2017 task force. Two drafts were presented for public review and comment: StrawDog (March – April 2019) and IronDog (July – August 2019). All of the input and feedback significantly improved the guidelines. The ACM Education Board endorsed the guidelines in January 2020, and they are available on the CCECC website at [3].

## Cyber2yr2020 Curricular Framework

The Cyber2yr2020 guidelines for two-year programs maintain the CSEC2017 division into eight knowledge areas/domains, plus "cross-cutting concepts" representing pervasive themes that cut across knowledge areas. The eight knowledge areas are Data Security, Software Security, Component Security, Connection Security, System Security, Human Security, Organizational Security, and Societal Security. The cross-cutting concepts include Confidentiality, Integrity, Availability, Risk, Adversarial Thinking, and Systems Thinking.

Each knowledge area/domain is divided into "Essential" and "Supplemental" portions. This recognizes the fact that there can be a variety of flavors of associate-degree Cybersecurity programs. A two-year Cybersecurity program could be crafted by starting with the Essential content and adding selected Supplemental content to meet local needs.

The heart of the curricular framework is a small set of competencies for each knowledge area/domain, along with a variety of student learning outcomes organized by knowledge unit/subdomain within each knowledge area. The competencies follow the definition presented in Modelling Competencies for Computing Education beyond 2020: A Research Based Approach to Defining Competencies in the Computing Disciplines [8]: "Competency integrates knowledge, skills, and dispositions and is context-situated." Knowledge ("know-that") refers to "mastery of core concepts and content knowledge." Skills ("know-how") are "qualities that people develop and learn over time with practice and through interactions with others."

Dispositions ("know-why" and "know-yourself") include "attitudinal, behavioral, and socio-emotional qualities of how disposed people are to apply knowledge and skills to solve problems." Context is the setting in which competencies manifest, the "authentic situations related to problems/issues and aspects of work." [8]

To facilitate integration into competency-based curricula, competencies and learning outcomes are expressed using action verbs from Bloom's Revised Taxonomy [6]. The Bloom's level—Remembering, Understanding, Applying, Analyzing, Evaluating, or Creating—represents the depth of cognition for a given competency or learning outcome. In addition, Essential learning outcomes are accompanied by a three-tiered assessment rubric. Each knowledge area/domain is summarized with a "domain card" giving the definition of the knowledge area, the Essential and Supplemental Competencies, and a list of the knowledge units/subdomains. Figure 1 shows the Software Security card.

Table 2 shows a selection of Essential learning outcomes from the Data Security knowledge area/domain along with the associated assessment rubrics. The first column of the three-tiered rubric, Emerging, represents an emerging grasp of the desired outcome, without yet achieving it. The middle tier, Developed, is the learning outcome itself. The higher tier, Highly Developed, represents going beyond the learning outcome. Readers are invited to interactively explore the full list of competencies, learning outcomes, and assessment rubrics at the ACM CCECC website [5].

## Mappings

The Cyber2yr2020 guidelines have been mapped to a number of related frameworks. Many U.S.-based community and technical colleges with Cybersecurity programs are interested in the designation by the NSA (National Security Agency) and DHS (Department of Homeland Security) of Center of Academic Excellence (CAE) in Cybersecurity [12]. The Cyber2yr2020 guidelines have been mapped to the CAE knowledge units, and the Cyber2yr competencies and learning outcomes align with 100% of the Foundational Core and

### Software Security

**Definition**
**Focuses on the development of software with security and potential vulnerabilities in mind so that it cannot be easily exploited.**

**The security of a system, and of the data it stores and manages, depends in large part on the security of its software. The security of software depends on how well the requirements match the needs that the software is to address, how well the software is designed, implemented, tested, and deployed and maintained. The documentation is critical for everyone to understand these considerations, and ethical considerations arise throughout the creation, deployment, use, and retirement of software.**

**Essential Competencies**

- **[SOF-E1] Write secure code with appropriate documentation for a software system and its related data.** *Applying*
- **[SOF-E2] Analyze security and ethical considerations at each phase of the software development lifecycle.** *Analyzing*
- **[SOF-E3] Use documentation, such as third-party library documentation, in a given secure computing scenario.** *Applying*

**Supplemental Competencies**

- **[SOF-S1] Implement isolation to secure a process or application.** *Applying*
- **[SOF-S2] Discuss the relationship between an organization's mission and secure software design.** *Understanding*
- **[SOF-S3] Write software specifications, including security specifications, for a given process or application.** *Applying*
- **[SOF-S4] Assess a given test plan, from a security perspective. Evaluating**
- **[SOF-S5] Examine social and legal aspects of software development from a security perspective.** *Analyzing*
- **[SOF-S6] Develop user documentation for software installation with security appropriately included.** *Creating*

**Knowledge Units**

**Fundamental Principles**
**Design**
**Implementation**
**Analysis and Testing**
**Deployment and Maintenance**
**Documentation**
**Ethics**

Data | **Software** | Component | Connection | System | Human | Organizational | Societal

**Figure 1:** Software Security card

**Table 2:** Selected Data Security essential learning outcomes with assessment rubric.

| Emerging | Learning Outcome - Developed | Highly Developed |
|---|---|---|
| **Explain hash functions for checking integrity and protecting authentication data.** *Understanding* | **Investigate hash functions for checking integrity and protecting authentication data.** *Applying* | **Examine hash functions for checking integrity and protecting authentication data.** *Analyzing* |
| **Define the concept of digital forensics.** *Remembering* | **Discuss the concept, need, and value of digital forensics.** *Understanding* | **Illustrate the concept, need, and value of digital forensics.** *Applying* |
| **Recognize the benefits and challenges of multifactor authentication.** *Remembering* | **Summarize the benefits and challenges of multifactor authentication.** *Understanding* | **Illustrate the benefits and challenges of multifactor authentication.** *Applying* |
| **Describe data access control to manage identities, credentials, privileges, and related access.** *Understanding* | **Implement data access control to manage identities, credentials, privileges, and related access.** *Applying* | **Choose data access control to manage identities, credentials, privileges, and related access.** *Evaluating* |
| **List various cryptanalysis attacks.** *Remembering* | **Classify various cryptanalysis attacks, such as ciphertext only, chosen plaintext, chosen ciphertext, man-in-the-middle, and brute force.** *Understanding* | **Carry out various cryptanalysis attacks, such as ciphertext only, chosen plaintext, chosen ciphertext, man-in-the-middle, and brute force.** *Applying* |

**Readers are invited to interactively explore the full list of competencies, learning outcomes, and assessment rubrics at the ACM CCECC website.**

Technical Core knowledge unit outcomes and topics.

Readers familiar with ABET may be aware that ABET developed program-specific criteria for accrediting cybersecurity programs at the baccalaureate level [1] and ABET is working on establishing accreditation for two-year programs in cybersecurity. The Cyber2yr2020 guidelines were used by ABET to develop draft program criteria for two-year cybersecurity programs.

The NICE Cybersecurity Workforce Framework [11] is a resource that categorizes and describes cybersecurity work. The Cyber2yr2020 competencies have been mapped to the seven categories of the NICE Framework. Visit the CCECC website to view these classification mappings and others [5].

## Call for Program Examples

A collection of examples of two-year cybersecurity programs is being assembled, including degrees, certificates, or collections of courses (such as those used in a CAE designation). A program example aligns an actual cybersecurity program with the competencies in Cyber2yr2020, showing the competencies that appear in each course that makes up the program. Seeing how the curricular guidance plays out in a real program can help with program updates as well as implementation of new programs.

If you would like to correlate your program to the Cyber2yr2020 guidelines, or to see the existing program examples, visit [5] and select the Program Examples tab. For any questions or suggestions, use the contact form at [5] (Contact tab) or email me. ❖


**References**

1. ABET. Accreditation Criteria & Supporting Documents; www.abet.org/accreditation/accreditation-criteria. Accessed 2020 January 28.
2. ACM Committee for Computing Education in Community Colleges. Computer Science Curricular Guidance for Associate-Degree Transfer Programs with Infused Cybersecurity. (New York, ACM, 2017). doi: http://dx.doi.org/10.1145/3108241.
3. ACM Committee for Computing Education in Community Colleges. *Cybersecurity Curricular Guidance for Associate-Degree Programs*. (New York, NY, ACM, 2020); http://ccecc.acm.org/Cyber2yr2020. Accessed 2020 January 17.
4. ACM Committee for Computing Education in Community Colleges. *Information Technology Competency Model of Core Learning Outcomes and Assessment for Associate-Degree Curriculum*. (New York, NY, ACM, 2014); doi: http://dx.doi.org/10.1145/2686614.
5. ACM Committee for Computing Education in Community Colleges; http://ccecc.acm.org/. Accessed 2020 January 17.
6. Anderson, L.W. and Kratwohl, D.R. eds., *A Taxonomy for Learning, Teaching and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives*. (New York, Longman, 2001).
7. Cybersecurity Ventures. Cybersecurity Talent Crunch to Create 3.5 Million Unfilled Jobs Globally By 2021, October 24, 2019; https://cybersecurityventures.com/jobs/. Accessed 2020 January 17.
8. Frezza, S., Daniels, M., Pears, A., Cajander, Å., Kann, V., Kapoor, A., McDermott, R., Peters, A., Sabin, M., and Wallace, C. Modelling Competencies for Computing Education beyond 2020: A Research Based Approach to Defining Competencies in the Computing Disciplines. In *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, (Larnaca, Cyprus, ACM, 2018), 148-174; https://doi.org/10.1145/3293881.3295782.
9. (ISC2). Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes Rise Higher, June 7, 2017; https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage/. Accessed 2020 January 17.
10. Joint Task Force on *Cybersecurity Education. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. (New York, NY, ACM, 2017); doi: http://dx.doi.org/10.1145/3184594.
11. National Initiative for Cybersecurity Education (NICE). *NICE Cybersecurity Workforce Framework*, August 2017; NIST Special Publication 800-181; doi: https://doi.org/10.6028/NIST.SP.800-181.
12. NSA and DHS, Centers of Academic Excellence in Cyber Defense 2019 Knowledge Units; https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf. Accessed 2020 January 17.
13. U.S. Bureau of Labor Statistics. *Occupational Outlook Handbook*, Information Security Analysts; https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm. Accessed 2020 January 17.



**Cara Tang**
Portland Community College
12000 SW 49th Ave.
Sylvania, TCB 312
Portland, OR 97219
*cara.tang@pcc.edu*


**DOI:** 10.1145/3388862 