Introduction to the CyBOK 1.1 Course Shell

Bastian Tenbergen[*]
Nancy Mead[#]
James Early[*]

[*] Department of Computer Science, State University of New York at Oswego

[#] Carnegie Mellon University, ret.

April 2023

Purpose

The Cyber Security Body of Knowledge (CyBOK) is the world's most comprehensive knowledge resource in the area of Cyber Security education. With 21 knowledge areas across four categories, CyBOK offers Cyber Security education in both breadth and depth for higher education learners and professional training alike.

In recent years, CyBOK-related resources for educators and trainers, developed through funded projects have been made publicly available[1], free of charge. These include, for example, a collection of robust case studies in support of all knowledge areas of CyBOK v1.1, educational video lectures, lab and practice materials, and reference material. Especially the CyBOK lecture videos by Cliffe Schreuders[2] and Case Studies by Mead and Tenbergen[3] are meant to provide educators with reusable, ready-to-apply resources, thereby saving instructors from researching or developing materials for their own instruction.

To further this goal and foster wide-spread adoption, we have developed a CyBOK-compatible course shell for an asynchronous, collaborative online course. The aim was to provide this course shell in a fashion to make it ready-to-deploy to a digital learning environment (DLE), regardless of which DLE the instructor's institution uses. The course shell contains modules for a six-week course that has been instructed at the State University of New York at Oswego with extraordinary success for more than five years. Originally based on the CompTIA Security+ curriculum, this course shell has been modified to make use of existing CyBOK educational resources. The course can be taught with or without CompTIA Security+ correspondence (CompTIA Security+ resource material must be purchased separately and are not included in the course shell). A provided correspondence table highlights coverage of CyBOK knowledge areas in the course modules, and relates CompTIA Security+ outcomes.

The course shell comes complete with course readings, assignments in the form of CyBOK Case Studies, peer learning activities, and topic discussions, course infrastructure such as discussion forums, and peer review instructions.

Learning Outcomes and Instructional Activities

Upon successful completion of the course, the learner will:

- have gained a solid background in basic concepts in information assurance;
- be able to apply these concepts to design an effective and implementable security policy;
- be able to audit a security policy;
- be able to discuss research articles and case studies in information assurance;
- be able to articulate principles of computer and network security.
- be able to define main terminology such as confidentiality, integrity, availability, and security fundamentals of computer networks, network security, basics of cryptography, mobile device security, access control mechanisms, and vulnerability assessment;
- be able to design for privacy and security constraints;
- be able to create and manage security networks applications;
- be able to design and manage a security policy;
- be able to create and manage data security policies;
- be able to create and manage virtual environments;
- be able to analyze and use the information generated from computing applications; and
- be able to integrate information from ubiquitous computing applications with information systems.

Learning activities include the following:

- Weekly ***reading assignments*** that students will be asked to complete on their own, supplemented with additional resources.
- Weekly ***discussion assignments***, in which students are asked to discuss amongst themselves what they've learned from the reading and additional resources. Students should make substantial contributions and supplement their contribution with online resources or accounts from their personal experience.
- Weekly ***Case Study assignments***, in which students are asked to complete one or more tasks pertaining to the material they have read and discussed. Case studies provided with this course shell are the complete case studies found on the CyBOK resource page[3]. These are instructor copies and contain application and grading suggestions and, in part, example solutions. It is recommended that the instructor modifies the case studies to suit their individual needs, at the very least by removing example solutions before assigning them to students.

- Regular ***peer reviews*** of Case Study solutions, in which students are asked to post their solution from the previous modules' Case Study assignments, as well as comment on the quality of at least two other students' solutions.
- A ***course-accompanying project*** with weekly milestones starting in week 2, in which students are asked to execute a penetration test against known-to-be vulnerable virtual machines, keep track of their efforts in a journal, and produce a penetration testing report to recommend methods to harden the virtual machines against attacks. The project may be collaborative in nature, i.e., allowing multiple students to share their attempts in dedicated discussion forum may help less experienced students to make quicker progress.

The course shell is designed to provide a collaborative, asynchronous learning environment. However, the course shell may also be offered as a self-study course by removing discussion activities and peer reviews and replacing them with instructor-graded learning activities (e.g., quizzes and graded assignments).

Components

This course shell consists of the following components:

1. A spreadsheet on the design of ***Course Modules and Coverage Correspondence*** to CyBOK Knowledge Areas and CompTIA Security+ outcomes. These help the instructor to tailor outcomes, learning activities, and the overall educational experience by providing an overview that makes obvious to what degree changes in coverage alter CyBOK knowledge area coverage.
2. Two ***example schedules*** to show how modules can be distributed in a six-week summer course, one with only CyBOK resources, and one with corresponding CompTIA Security+ resources. The CyBOK example schedule is also contained in the course shell and most certainly requires updating on part of the instructor.
3. An ***example syllabus*** to show how the course can be meaningfully administered with different learning activities. This syllabus is also contained in the course shell. It is strongly recommended that the instructor replace this with their own syllabus. Nevertheless, instructors may seek guidance to derive their own scoring schemes for assignments and learning activities from this document.
4. The ***course shell*** itself, in Common Cartridge 1.2 format[4]. This 700+Mb .imscc-file contains all course materials, resources, assignments, etc. No other resources are necessary. The file can simply be uploaded to your Common Cartridge 1.2 compatible[5] DLE. Dates, deadlines, and learning activities will require tailoring to instructor preference and educational circumstance.
5. A file describing the ***Course Project "Penetration Test"***, a CyBOK Case Study taken from the resource page[3]. Although the course shell includes a module for the course project, some virtual machine infrastructure must be set up by the instructor and is not otherwise explained in the course shell (with the exception of getting started texts and videos on the matter). This file describes the entire case study as implemented in the course shell and includes a description of the required preparation.

The dates for module releases and assignment deadlines in the course shell follow the example schedules for Summer 2023 and require adjustment for your course offering.

Technical Prerequisites

To apply the course shell, you must have access to a Digital Learning Environment (DLE), such CANVAS, BrightSpace, or Blackboard. Most likely, your institution already has access to one. Moreover, your institution should provide you with an empty course shell for your course. You may import the .imscc-file into this course shell using your DLE's import/export feature. Please refer to your institution's resources on these matters for guidance.

Guidelines to Adopt the Course Shell

To adopt the course shell, the instructor will have to enact some minor modifications, depending on the educational circumstance in which this course shell shall be introduced. These are as follows:

1. **Study** the Course Modules and Coverage Correspondence spreadsheet as well as the example schedules and **decide** which modules and learning activities to include in your course. Also decide on a grading scheme, etc.
2. **Edit** the example syllabus based on your decision from Step 1, instructional preferences, and institutional context. Be sure to edit contact information in your syllabus.
3. **Edit** the example schedule to match the course offering and time span for your instruction.

4. **Import** the course shell into your Common Cartridge compatible DLE by uploading it and using the import wizard (see above). Make the following modifications:
   a. In the Course Information module, **change the instructor information** to match your own details.
   b. **Replace the syllabus** with your own syllabus from Step 2.
   c. **Replace the course schedule** with your own schedule from Step 3.
   d. **Modify module release and due** dates as well as assignment due dates based on the schedule from Step 3. Some DLEs (e.g., BrightSpace) allow automatic off-setting of course dates. It is recommended to double-check dates if you use this feature.
   e. In each module, find the CyBOK case studies. Download the material and **change the case study description and tasks** to suit your instructional needs, **at the minimum by removing example solutions**, grading guidelines, and instructor resources.
5. **Set up virtual machines for the course project** based on the description that can be found in the CyBOK Penetration Test Case Study document.
6. **Write an opening post** in the discussion forum "Introductions" and introduce yourself to your students.
7. **Have fun!** 😊

The course shell is designed to provide a collaborative, asynchronous online learning experience to the learners with minimal grading and preparatory effort on part of the instructor. Nevertheless, it is advisable for the instructor to check daily on discussion posts, moderate discussions by prompting students, and track student progress during peer reviews as well as the course project. In particular, the course project might require some helpful hints to be occasionally offered in the project discussion forum to students who are less experienced with Linux command line. Be sure to identify struggling students by observing their life progress in their project journals.

This course shell can accommodate a more self-directed, non-collaborative asynchronous learning experience if such is desired. In this case, discussion forums and peer reviews may be removed from the learning activities in the syllabus and the appropriate provisions removed from the course shell. Simply delete them. It is recommended to provide regular student feedback through promptly graded assignment solutions as well as weekly quizzes instead.

Acknowledgement

This course shell is based on the course design by our colleagues, for whom we are deeply appreciative for giving us permission to use their work as the base for this CyBOK-specific extension:
Dr. Nafees Qumar, *Governors State University*
Dr. Christpher Harris, *University of Northern Colorado*

References

1) CyBOK consortium: CyBOK-related resources for educators and trainers, developed through funded projects, 2022. Online resource, available at https://www.cybok.org/resources_developed_through_funded_projects/, accessed April 2023.
2) Cliffe Schreuders: Lecture Videos and CyBOK, 2022. Online resource, available at https://github.com/cliffe/SecGen/blob/master/README-CyBOK-Lecture-Videos.md, accessed April 2023.
3) Nancy Mead, Bastian Tenbergen: Case Studies in Support of CyBOK 1.1, 2022. Online resource, available at: https://www.cybok.org/media/downloads/CyBOK_1.1_Case_Study_Library_upload.zip, accessed April 2023.
4) IMS Global Learning Consortium: Common Cartridge. Open Standard, available at: https://www.imsglobal.org/activity/common-cartridge, accessed April 2023.
5) eLearningIndustry: MS Common Cartridge Compliant Learning Management Systems, 2023. Online resource, available at: https://elearningindustry.com/directory/software-categories/learning-management-systems/compliance/ims-cc, accessed April 2023.