Preparing for the CISSP Exam (4)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last three columns, I began responding to a former student who recently wrote to me with a request for suggestions on what to read in preparing for the CISSP exam. In this fourth and last article, I suggest a few valuable (albeit sometimes expensive) books and some (free) review materials for such preparation. Readers will find other lists of suggested readings on the Web by using search string “CISSP preparation course” in a Web search engine.

In my opinion, some of the most useful books for overall coverage of the field are as follows:


- _Handbook of Information Security_, 3-Volume Set (I chose this as the new textbook for our Master’s program at Norwich University) by Hossein Bidgoli <http://tinyurl.com/vf2549> (get your company to buy it for their library). I reviewed this enormous work in this column a year ago. <http://www.networkworld.com/newsletters/sec/2006/0410sec2.html>


In addition, the (ISC)^2 provides a slightly disorganized list of books at <https://www.isc2.org/cgi-bin/content.cgi?category=698>. For some reason it refers to the 3rd edition of the CSH (twice) but not to the CSH4.

Ideally, people preparing for any exam do best if they can study in teams. For example, they can use my own lecture slides as review material to quiz each other – they should be able to speak intelligently about every point on every slide. The files thus serve as one of the ways to check for holes in coverage of the material and also as a way of consolidating and strengthening knowledge.

- I340 Intro to IA lectures (last updated Fall 2005) <http://tinyurl.com/ydeo3> covers the first half of the CSH4.

- IS342 Management of IA (last updated Spring 2006) <http://tinyurl.com/csyny>. As you would expect, this course covers the second half of the CSH4.
• CJ341 Cybercrime & Cyberlaw (last updated Fall 2006) <http://tinyurl.com/yzgts8> is a mind-numbingly detailed look at how law enforcement has to deal with digital evidence, including the specific laws relating to computer crimes of all sorts. Personally, I love it, but I know that some people find it dry. Still, “Legal, Regulations, Compliance and Investigations” is one of the 10 domains of the CBK (Common Body of Knowledge) for the CISSP <https://www.isc2.org/cgi/content.cgi?category=8>.

In addition to all of this (mostly) free knowledge, it is also possible to enroll in a wide range of preparatory courses. I myself have taught for the (ISC)^2 and think their courses are good reviews. I am leery, however, of taking a short course _instead_ of reading and thinking for a long time about any subject beyond the purely technical. In my experience, the most important aspect of learning is thinking, not memory. Take a course if you like, but not just before your exam. Use the course as a form of review and verification – a tool for strengthening what you already know but above all for identifying what you have to think and learn about at greater length.

And good luck to all in your certification exams!

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.msia.norwich.edu> at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.