

Luck, Career Goals and a CISSP Boot Camp

Editor's Note: This article was written in 2005 and was originally published on CSP Magazine. Due to numerous requests, it is being republished on EH-Net.

It is said that luck seems to find those prepared for it. And, as difficult as it is to admit, stuff happens. We may find that our current job doesn't satisfy our financial or intellectual goals, a natural disaster may strike or, the unthinkable, we may be deemed expendable! If you had to hit the pavement tomorrow, do you have the knowledge and experience to determine your own destiny? If not, what is lacking in your CV? What gaps in your knowledge or holes in the list of your credentials should you fill? What would make your resume stand out from the crowd? Could any of us be better prepared to take advantage of good luck or better yet overcome the bad variety?

As many in the IT field do from time to time, I too stopped recently to see where I stood in my career, where my chosen field is headed and what was my place in it? Think of it as a Personal Disaster Recovery Plan. Looking at my resume, I noticed a vast amount of experience, plenty of knowledge regarding the specific duties of each of the positions I held and a few certifications. What I seem to lack is a highly respected credential that would verify all of that experience, fill in some technical gaps of items I don't perform on a daily basis and be recognized by non-technical executives. That credential gap can clearly be filled by an IT certification, but which one is right for me and my career goals?

del.icio.us

Discuss in Forums {mos_smf_discuss:Editor-In-Chief}

The exact course reviewed in this article is offered at ChicagoCon 2008f

To get that answer, let's continue on with this little introspective exercise. So let's take a look... I've been an owner of a small consultancy, a CIO of a small software company and now a Director of IT at a university. Each has its benefits and rewards, but neither on its own would make an HR executive or recruiter stand on their head. After a careful and honest review of myself and the IT industry as a whole, I found that, although I've never had a title with the word 'security' in it, I have always had security as a main tenant of my duties. This is good for me, because the hot topic in all of IT right now just so happens to be security. I also have found it to be an area that truly holds my interest. With this information now clearly at the forefront of my mind, it starts to become clear that, for me, the only cert to fill this bill would be (ISC)2's CISSP with 35,767 certified professionals in 116 countries (as of 8-31-05).

Now that we have our goal, we must decide how to attain it. As with all certifications, there are numerous ways to prepare. Since I was looking at the CISSP as a career goal and not just something my boss asked me to do, I decided to combine many of the common methods of study into a single program. This personal program basically starts with experience, adds self-study and culminates with an instructor led class. This has worked for me in the past, so I'm confident, if I follow my plan, I will be a CISSP!

I'm a research nut. I looked at just about every piece of study material and boot camps available for the CISSP exam. I'll spare you the details, and go straight to my Recommended Study Method:

- Start simple with Free Study Guide from ISC2 to get the description of each domain from the horse's mouth. Know what you're getting yourself into.
- Get a good solid overview of the material with CISSP for Dummies. This is a good quick read to get your toe in the water.
- Go waste deep by double checking the info contained in the Dummies book by reviewing the CramSession Free Study Guide for CISSP.
- Dive in by using Shon Harris' All-In-One Exam Guide 2nd Ed. Keep an eye out for All-In-One 3rd Ed that will be updated with info on ISSEP.
- At least one book should be published by the organization giving the exam. This way you get used to their terminology and ways of thinking. In this case, the book is Official (ISC)2 Guide to the CISSP Exam.
- Review it all with CBT Nuggets. All told the Nuggets videos are 42 hours long! There is a setting to play the videos at a faster speed. You should know the info by now, so breeze through it as fast as you can.
- Now it's time for the Boot Camp. I decided on the 7-Day CBK Review Seminar (5-Day version also available) put on by The Training Camp. This one of the few if not the only training that offers an exam attempt at the end.

NOTE: The 'Recommended Study Method' is published in its generic form on CSP Online Magazine's Book Smarts Home Page.

I fully subscribe to the method of using multiple sources of study materials. It's not that (ISC)2 has bad material, it's just that not all ways of describing a topic sticks with all people. If a concept doesn't stick in your head for whatever reason, ask someone else to explain it to you. In other words, utilize another source of material. It also helps to fill in the gaps. As an example, the All-In-One book by Shon Harris dives deeper into a particular topic such as hacking history that the Official (ISC)2 Study Guide does not while (ISC)2 has practice questions that resembles the tone and difficulty of the real questions better than All-In-One.

NOTE: These are only recommendations. For more study resources, please see the end of this article.

Before we get to the actual boot camp diary, let me offer a word to the wise. Not only is it written as a requirement for achieving the CISSP credential, it is also highly recommended to have several years of security related experience. Have none, and chances of passing are greatly diminished. In addition to experience, try getting a lower level security cert such as Security+ from CompTIA. This will help greatly as a lot of similar ground is covered. If it is said that the CISSP material is a mile wide and a foot deep, then Security+ is a half mile and 6 in deep.

Although not officially named a boot camp, I chose InfoSec Academy's 7-Day CISSP CBK Review Seminar for several reasons. First of all, the InfoSec Academy is part of The Training Camp, a well respected and (ISC)2 endorsed training facility. Being (ISC)2 endorsed, our instructor came directly from (ISC)2 giving the students a leg up in preparing for the exam. The InfoSec Academy is also an SC Magazine finalist for best training facility of 2005. Last and certainly not least, they offer the ability to take the exam at the end of training. A fellow student traveled all the way from Georgia (the country not the state) for this very reason. Those of you who have attended any type of instructor led training knows how valuable of an offering this is. Waiting a week or two (or maybe even longer) to take the exam outside of the immersive environment makes it that much more difficult to pass.

Speaking of immersive environments, I chose InfoSec Academy's 7-day course instead of the 5-day course for this exact reason. The 5-day course is just like most weekly seminars with your normal 8-hour days, Monday through Friday. The 7-day course follows the same exact schedule with additional features such as evening sessions with review questions, hotel accommodations, some meals and the exam attempt. Our instructor stayed in the same hotel and made himself available during our stay. The 2 extra days made all the difference in the world. The 6th day offers the students a timed practice exam made up of retired questions directly from old CISSP exams, a post-exam review and plenty of time to cover weak areas. The 7th day is for the 6 hour, 250 question exam. And in the unfortunate event that any 7-day student fails the exam, the next review seminar is offered free of charge courtesy of the InfoSec Academy. In some instances, even your second exam fee is covered. Discuss the details with the InfoSec Academy.

Due to its ANSI Accreditation, (ISC)2 is unable to provide pass / fail rates. But based on unofficial research, it seems as though an average pass rate for the CISSP exam is around 60 - 65%. The InfoSec Academy with their 7-day immersive course increases that passing rate to approximately 90% based on information compiled by their customer service department over the past 6 months. With an average of 18 attendees per course taught by a total of 43 available (ISC)2 Authorized Instructors, I felt very comfortable putting my career goals in the hands of the InfoSec Academy.

Even though our first official day of camp was on a Monday, many of us checked into the hotel on Sunday night. We had a meet-and-greet that same evening with our instructor and our 7-day classmates. I made sure to find out the order in which the domains would be covered, so I could skim the corresponding chapters of the material I had already read the night before class. The schedule was as follows:

Monday: Security Management Practices & Security Architecture and Models

Tuesday: Business Continuity Planning, Access Control Systems & Applications Development

Wednesday: Cryptography & Physical Security

Thursday: Law, Investigations and Ethics, Operations Security then a Review of the 1st 9 domains

Friday: Telecommunications and Network Security

Saturday: Practice Exam & Student Requested Reviews

Sunday: Exam

Keep in mind that this is a Review Seminar that is officially endorsed by (ISC)2. This has 2 important meanings. First of all, the InfoSec Academy uses presentations prepared by (ISC)2. This is just as important as reading Microsoft books when taking a Microsoft exam. You learn their way of thinking as well as their terminology which may differ from 3rd party materials. If you can't attend an official seminar, then be sure to get the (ISC)2 Official Guide To The CISSP Exam as

your main foundation of material. Our instructor had only a single copy that he let the students borrow, so purchasing your own copy is recommended. Secondly, by being named a Review Seminar, it implicitly states that the student should bring prior knowledge, experience and invested study time to the process before attending. The amount of each is up to you, but the amount directly correlates to your chances of passing. Being a review of the Common Body of Knowledge (CBK), even if you have experience, it is rare for a candidate to possess experience in all 10 domains of the CBK. It is essential to study many of your materials before ever considering landing in a classroom. This is not to say that it is impossible to pass the exam with only attending the course, but most who try do not have a positive result.

Like many who endeavor to achieve a lofty goal, the road to the destination sometimes feels disorienting and sometimes flat out unnecessary. The start of the first day of class truly felt unnecessary as we covered simple information about (ISC)², exam details such as number of questions and time allowed and the requirements for achieving as well as maintaining your CISSP certification (visit CSP Mag's CISSP Page for more details). This is another classic example of letting professionals do their job and trust that their experience and knowledge will eventually make the necessary evils later prove to be highly valuable. One such tidbit is the fact that 25 questions on the CISSP exam are considered beta questions. In an attempt to remain up-to-date and relevant, (ISC)² constantly is evolving the exam by slowly retiring old questions with new ones covering latest technical and conceptual security topics. The candidate will not know which of the 25 questions out of 250 on the exam are the beta questions. This is their way of anonymously getting feedback on the fairness and level of common knowledge expected of security professionals. I will later share with you how important this information was to my confidence during the lengthy exam.

Classes started promptly at 8:00 AM every day and continued until 5:00 PM with those in the 7-day course continuing after 5 with practice questions followed by reviews and explanations of each answer. All of the students were treated very well with more than enough supply of a variety of soft drinks, snacks and my personal favorite, coffee. The staff's attitude was to allow the students to concentrate on the material without having to worry about the small details. As for those in the 7-day course, we were served daily hot lunches. High marks for the creature comforts.

WARNING: The CISSP exam by definition is vendor neutral. This means that there will be no labs for hands-on practice of the information taught during the never-ending PowerPoint Presentation. In order to do so, we would have to have actual computers and equipment from specific vendors thus breaking from its own definition. This lends itself to the other definition of the CISSP credential... it's a security management certification. Therefore, it covers history, concepts and theories. Practical hands-on experience helps greatly in understanding these concepts, but the seminar is very old fashioned right down to the Scantron paper and pencil exam.

So it is no surprise that it took effort by the students to remain involved during the lectures themselves. This is where the talents of our instructor showed both breadth of knowledge and a gap in interactivity. He clearly had a command of the material having years of CISSP instructing experience with even more practical security experience. He works in the continuity planning field, so we all rocked the BCP portion of the exam. I did feel however that he occasionally got lost in the slides, trying to blast through them to get to the juicy part of the steak, the domain reviews and Q&A. Also during the classroom sessions, he often would tell the students not to worry about certain topics as much as others. We initially felt that this lacked the depth needed to fully understand a given topic well enough to pass the exam. But to his credit, he ended up being completely correct. So even though it would be wise to include more visual aids and real-time drawing of relevant diagrams to describe concepts, his years of training CISSPs and the feedback offered to him by his former students definitely paid dividends to those who followed.

With all of the different types of study materials available, I felt I might as well address the elephant in the room - Brain Dumps. I checked many forums including my own at CSP Online Magazine for thoughts on the subject. I am a blunt person, so I will choose not to stop now. **DO NOT WASTE YOUR TIME ON DUMPS!** We had students who brought copies of dumps to share with their classmates. Take my word on it... enough answers are wrong to make you wonder if any are correct. This led to a group of us that formed a study group at the hotel to debate whether the dump was correct or the (ISC)² material. Once again, go with the organization that created the exam. In very short time, we tossed the

dumps and never looked back.

The best part of any training is the ability to hang out with other people like yourself. This experience was no different. During the breaks, lunches, evening sessions and study groups back at the hotel, the off time with the other students was almost as valuable as the class itself. I can't with any certainty conclude that this is because of the CISSP credential, the field of IT security or The Training Camp marketing efforts, but the caliber of talent in the room would be the envy of any major corporation, educational institution or government entity anywhere in the world.

With such an experienced and intelligent crowd, we were able to cover the scheduled domains pretty closely to our predetermined path, but did deviate based on student progress and requests. Saturday morning we all took a practice exam of 100 questions in 2 hours. If you scored better than 80% on the practice exam, you could feel relatively confident you were on track to passing the real exam. We had the rest of the morning, afternoon and evening to study on our own in preparation for the exam on Sunday morning from 9:00 am - 3:00 pm.

Before being released on the exam like blood-thirsty hounds, some final items were covered. Not only did we all receive certificates of completion (of course only after we filled out evaluation forms), but we were also given the chance to receive test-taking advice from our instructor and from our fellow students. Suggestions included the always good idea of getting to bed early the night before the exam. Other common thoughts were to not get overconfident or unduly stressed, read the questions and the answers completely before choosing your final selection and always answer every question no matter what. If you are unsure of an answer, mark it for review during a second or even third pass through the questions. For this reason, time management was also discussed as it becomes vastly important on such a difficult exam. Since it is now allowed to write in the test booklet, use this as a visual tool to mark not only those questions you want to review but also those you feel were quite easy. It is also wise to use this technique to highlight key words in questions to help eliminate wrong answers or to add confidence in correct answers.

All of these are great, but, in my honest and humble opinion, the most valuable advice is to force yourself to take mandatory breaks during the exam. Each candidate is given 6 hours to complete the test. Most complete it in 3 to 4 hours, giving the average person 2 hours of unused time. Once again reminding you that this is a task that most of us chose willingly as an opportunity to advance our careers and have spent countless hours in preparation, it only stands to reason that everyone should use those 2 hours to their advantage. So, every time you complete 50 questions, close your exam booklets and ask to be excused to the bathroom, get coffee or simply get out of the exam room to stretch. This break helps both those students who are breezing through the exam as well as those struggling. For those breezing, it prevents you from skimming the questions as opposed to reading them thoroughly simply because you are on a roll. For those struggling, it gives you time to reflect or get a fresh start. Either way, on an exam this long, this is the single best method of time management. And let's face it, in the grand scheme of things, what's a couple more hours if it increases your chances of passing? Who cares if you're the last one in the room? Take this advice and just do it!

The Exam

Be afraid. Be very afraid... Just kidding. Although I swear they front loaded the exam with those beta questions that don't count! Since beta questions may cover topics you didn't cover during your own personal study method, they got me so discouraged, I thought I could never pass. But I kept telling myself that this is a marathon and not a sprint. I got up and took one of my personally scheduled breaks, went to the bathroom, splashed water on my face, cleared my head a little and went back into the testing room. I found that as the test went on, it got easier for me. But having such difficult questions in the beginning set the tone for the entire experience. So, like most who have taken the exam, I had no idea whether I had passed.

But I stuck to my plan of going through every question once, highlighting key words, answering every question on the scantron sheet and marking each question with one of three marks: 'X' (Knew it 100%) '?' (Was not 100% confident) '*' (Had no idea). You may also mark a question that relates or is similar to another question by writing the previous question number next to the similar question. This will help you cross-reference questions to increase your confidence in other answers. All the while taking my breaks, I eventually made a second pass only ignoring questions with a 'X' over the entire question. Slowly after 2 - 3 passes, I whittled down the questions until there were very few for which I was still unsure. Having eliminated all but 2 answers on each unsure question, I made educated guesses.

The CISSP examination truly was an endurance test just as much as it was a test of knowledge. I guess this is a good metaphor for the security field... or at least it should be. I took the exam on Sunday and got the email on Thursday afternoon. "Congratulations!" it read. I was elated, relieved, excited and more.

As Sun Tzu said, 'Every battle is won or lost before it is fought.' I had a plan for preparing and a plan for taking the exam. I was not able to read every book or take every practice test, so I had to be flexible. But I still stuck to the plan. Was there any luck involved? Sure. What was the end result? Goal achieved. What now?

From the beginning, we always had the CISSP credential as a career goal. So, what does this mean for my career? Just to test the waters, I updated my resume and posted it on CareerBuilder.com with the title, 10+ yrs exp, CISSP, MCSE 2003. Low and behold, perspective and reputable employers in the IT / Security fields began contacting me - not the other way around. I don't know if this is more a reflection of the economy, the credential or just blind luck. Either way, it has garnered the attention of my intended audience, and that's proof enough for me.

Donald C. Donzal

Editor

The Certified Security Professional Online Magazine

Additional Study Resources:

The Certified Security Professional Online Magazine

(ISC)² eLearning

PrepLogic

The Training Camp's InfoSec Academy 5-Day Course

CISSP Related Links:

General

<http://www.ethicalhacker.net/>
<http://www.isc2.org/>
<http://www.cccure.org/>
<http://www.searchsecurity.com/>
<http://www.cissps.com/>
<http://www.nsa.gov/>
<http://www.nist.gov/>
<http://www.ansi.org/>
<http://www.iso.ch/>
<http://www.ieee.org/>
<http://www.sans.org/>

CBK Domains

Access Control

<http://www.cert.org/advisories/>
<http://www.symantec.com/securitycheck/>

Application

<http://java.sun.com/>
<http://www.phase-one.com.au/>
<http://www.ansi.org/>

Architecture

<http://whatis.techtarget.com/>
<http://www.tech-faq.com/>

BCP

<http://www.drj.com/>
<http://www.drii.org/>
<http://www.disaster-resource.com/>
<http://www.bci.com/>

Crypto

<http://www.cryptography.com/>

<http://www.techtarget.com/definitionalpha>

<http://www.howstuffworks.com/>

<http://www.homenethelp.com/>

Law, Invest & Ethics

<https://www.isc2.org/cgi-bin/content.cgi?category=12>

<http://www.iab.org/>

<http://www.ietf.org/rfc/rfc1087.txt?number=1087>

<http://www.cert.org/>

<http://staff.washington.edu/dittrich/forensics.html>

Ops

Most material in this domain is covered in other domains. Use many of the resources already listed.

Management

<http://www.securityauditor.net/>

<http://www.microsoft.com/technet>

http://www.rcmp_grc.ca/tsb/pubs/index_e.htm

Physical

<http://www.asisonline.com/>

<http://www.security.org/dial-80/links.htm>

Telecom

Way too many to list. Use many of the resources already listed.

Donald C. Donzal

Editor-In-Chief

The Ethical Hacker Network