Certifications: Are They Worth It?

By LTC BE Rhodes, Colorado Army National Guard

I walked into my first cybersecurity professional certification exam and needless-to-say, I was a bit nervous. It had been several years since I had taken a test that really counted for anything. This direct foray back into the cybersecurity world after some time away started because I had been assigned to lead an Army National Guard Defensive Cyber Operations Element. Having a high-end professional certification was a job requirement. Two months prior to the test, the Army sent me to a weeklong boot camp-style class to prep for the exam. The next seven weeks were then spent reviewing, studying, creating note cards, and doing it all over again. With that backdrop, I settled into the chair ready to take what turned out to be hardest test I have ever attempted.

Five and a half hours later, I was absolutely spent. I stared at my mouse pointer hovering over the "submit" button wondering if I had answered enough questions correctly to win the day. After some machination, I pressed submit and walked out of the test room wondering if the effort was worth it. As I awaited my results, I began to have serious doubts about my performance. I knew from my prep that if I had passed, the proctor would give me one piece of paper and if I was unsuccessful it would be two (one explaining where I had fallen short). The proctor handed me one piece of paper and said "Congratulations!". I thanked her and departed the testing center. I had just passed a major certification exam and I should have been jumping for joy, but I was so drained that I just wanted to get a bite to eat. After calling my wife with the great news, I stopped for "victory tacos." While I sat people watching, I began to realize the value of professional certifications in cybersecurity.

Cybersecurity is a unique discipline. Where else can anyone from any background get into the field for minimal cost? For less than 100 dollars today, you can set up a computing environment (Raspberry Pi kit with Wi-Fi, 16GB microSD card, keyboard, mouse, used monitor [or your existing HDTV], HDMI cable) at your home (I am assuming some type of internet access, realizing that is not necessarily ubiquitous). Next, you only need to peruse the Internet for skills you want to learn. I daresay, you can probably find YouTube videos with step-by-step instruction on everything you would ever want to learn in cybersecurity from coding to hacking and everything in between. Another free resource for newcomers to the field is Cybrary - an online learning resource which covers the gamut from beginning to advanced skills and classes on specific certifications (even micro certifications). I look back on my formative years and wonder where I would be today if I had access to the comprehensive and free educational resources available now.

Now that you've got a computer and access to learning resources, it is time to get that six-figure job, right? Not quite. Let's begin with the types of certifications (in no particular order) as I see them as cybersecurity professional*:

Knowledge-based – These certifications require you to know a large amount of information. Usually, the certification organization will have developed a series of "domains" to categorize the information. It is important to remember that each certifying body will ask questions their own way. Hence, it is not a good idea to try to study and attempt multiple certifications at the same time.

Example(s): CompTIA Security+, ISC2 Certified Information Systems Security Professional (CISSP), EC Council Certified Ethical Hacker (CEH), Cisco CCNA Cyber Ops

Hands On – These certifications provide a vehicle for applying the information learned. You may have to configure an actual (virtual) router, workstation, server, or firewall. *Example(s): Cisco CCNA Security, CompTIA Linux+, Microsoft Certified Systems Engineer*

Hybrid – This type of certification is becoming more prevalent. Any exam that mixes knowledge and hands on/semi-hands on can be considered hybrid. Additionally, many certifying entities are implementing adaptive exams. Adaptive exams have an algorithm that starts with an easy series of questions. If you get the easy questions right, the engine gives you a harder set of questions. Depending on your performance, your next questions may be easier or harder. In theory, an adaptive exam provides a more accurate assessment of the test taker. Example(s): Amazon Web Services (AWS) Certified Cloud Practitioner

General/Multidisciplinary – Most cyber security exams fall into this category by default. Depending on their field of work, cybersecurity professionals are expected to be multidisciplinary, walking in the door knowing a little something about everything from systems administration to networking to coding to defensive measures. *Example(s): GIAC Security Essentials Certification (GSEC)*

Specialized - These certifications focus on specialized aspects of cybersecurity. A good example here is cyber forensics. Many cyber forensics personnel start off general and become specialized. Organizations like the SANS Institute recognized this need and have created specialized certifications. *Example(s): GIAC Forensic Examiner Certification (GCFE), GIAC Network Forensic Analyst (GNFA)*

*Note: I am not endorsing specific certifications by providing examples in this list. You will need determine what is best for you based on personal interests and more likely job requirements. If you are in the Department of Defense (Military, Civilian, or Contractor), the listing of applicable certifications depending on Information Assurance role can be found here:https://iase.disa.mil/iawip/Pages/iabaseline.aspx

As a holder of multiple professional certifications, I will tell you that costs of each can vary widely for both training and exams (I will talk about cost shortly). If you are new to the field, I recommend against following my example (in other words: do not start with a high end, multidisciplinary

certification). So, what certification(s) should you pursue? I would answer that question with two questions: what do you want to do and what does your job require? With the breadth and depth of the cybersecurity field and the growing desire to put everything (including your crockpot) on the internet, finding a niche that gets you fired up is not hard to find. Many jobs in IT and cybersecurity require some basic level of certification (including the Department of Defense). Other opportunities will advertise a certification preference and if you do not have that or an equivalent you will not even get your foot in the door.

In addition to certifications, many cybersecurity jobs have a "desired years of experience" requirement. This can be challenging for many people coming into the cybersecurity field right out of college or making a mid-career transition. Do not let your lack of in the cybersecurity field experience hold you back. Cybersecurity is a field where ongoing self-learning is expected, encouraged, and seen as desirable as employers. Apply whether you have the years of experience or not; you really have nothing to lose.

Back to costs, certifications that are viewed by the industry as less difficult cost less for both training and the associated exams (on average between $300 to $800 per sitting). Depending on what you want to do in cybersecurity, paying for an initial certification yourself may be a good investment based on potential future earnings. Always look for ways to reduce your out-of-pocket costs. If you are a veteran or military member with the GI Bill, you can use those benefits to cover both training and certification costs. There also opportunities in the civilian community. For example, from time-to-time, certifying organizations will offer pilot programs for new certifications at little to no cost to the participants. Cisco just did that with the CCNA Cyber Operations certification. When you are interviewing for that dream cybersecurity job, a reasonable question for your prospective employer is do you offer reimbursement for certifications? I am not saying to not take a job if they do not; however, organizations that make cybersecurity a priority see value in keeping their talent well trained.

Most, if not all, cybersecurity professional certifications require maintenance. That maintenance usually includes an annual fee (varies between $50 to $100 annually) and the completion of some amount of Continuing Education Units (CEU) or Continuing Profession Education (CPE) credits. Certifications that are viewed as difficult to achieve cost less to "maintain" in both fees and CEUs/CPEs. Some certifications are lifetime, while others have a cycle of renewal (usually three years). In short, if you are paying the maintenance annual fees and completing the required CEUs/CPEs, renewals are easy. As you progress in your cybersecurity career, you will likely let low-end certifications lapse while you keep up high-end certifications. Do not ever let a high-end certification lapse unless you really want to take an exam again. It is advisable to check with your employer or prospective employer if they help cover the cost of annual maintenance fees; many do.

In addition to maintaining current certifications, it is quite common for cybersecurity professionals continue to pursue additional ones. Many in the field believe you should pursue at least one new certification per year to drive your learning focus. While that is certainly a worthy concept, due to the expense and time commitment required of each certification it may not be the best option for everyone. I recommend a measured approach; if your position requires a specific certification you should obtain and maintain it. Similarly, if you want to move into another part of the cybersecurity field, it may make sense to get certified in that area (for example moving from network defense to malware analysis). While is not possible to have too many certifications, it is better to focus on those that advance your field of interest (wide or narrow).

At the start of this discussion, I noted there is value in professional certifications in cybersecurity. First off, professional certifications are a reasonable way to demonstrate your knowledge in the field, general or specific. Many of my fellow cybersecurity professionals will argue that knowledge does not mean experience. I agree; however, everyone must start somewhere and as leader in the field I do consider professional certifications when assessing the potential aptitude of candidates (especially if they completed it on their own). Next, many positions require certifications (including my current jobs), so it is difficult for me to ignore their merit. The good news is that the types of certifications described previously help employers find the best fit for a job. For example, if you have advertised a job that requires some knowledge of routing and switching, and you do not hire a person with a requisite certification, you are asking for trouble. Finally, professional certifications are a beginning not an end! Cybersecurity is a growing, ever-changing, complex, and multi-disciplinary field that needs motivated self-learners to shape the future. Certifications are one of many ways to get started. What are you waiting for? It is time to jump in!

LTC BE Rhodes leads an Army National Guard Cyber Protection Team. In his civilian job, he is a Cybersecurity Professional for a global consulting firm. He has more than 20 years of experience in cybersecurity, the DoD, Intelligence Community, and industry. He is a CISSP, CEH, CCNA Cyber Ops, CNDA, Security+, and GIAC-GLEG. BE is a founding member of the MCPA-Denver Chapter. Follow him on Twitter @cyberguy514.

Certification Resources

(List does not constitute endorsement by MCPA or Author)

Amazon Web Services (AWS)
https://aws.amazon.com/certification/

Cisco
https://www.cisco.com/c/en/us/training-events/training-certifications/overview.html

Cybrary
http://cybrary.it

CompTIA
https://certification.comptia.org

DoD Approved Baseline Certifications
https://iase.disa.mil/iawip/Pages/iabaseline.aspx

EC-Council
https://www.eccouncil.org

(ISC)²
https://www.isc2.org

SANS
https://www.sans.org

Microsoft
https://www.microsoft.com/en-us/learning/certification-overview.aspx