Academic Degrees and Professional Certification

Matt Bishop
University of California, Davis

Deborah Frincke
Pacific Northwest National Laboratory

Pick up any modern technical publication and you'll find a bewildering array of organizations ready and waiting to help you advance your career: Certified Information Systems Security Professionals (CISSP), Global Information Assurance Certification (GIAC), Microsoft Network Certification, BS, MS, and PhD programs, and so on. How should you invest your time and money in a lifelong learning program? If you're hiring personnel, what training and expertise should you look for?

In this installment, we discuss general professional certifications and compare and contrast them with a bachelor's degree to help you decide which is most appropriate.

Academic degrees

A BS, MS, or PhD indicates an institution's formal recognition that a student has completed an approved study plan. Two external indicators of an academic program's quality are reputation and accreditation.

Reputation

A degree's value is intertwined with the reputation of the university, department, and faculty in the program. A university puts its credibility on the line with each graduate. The degree committee's caliber is a key indicator of the expertise level expected from a student, especially for advanced degrees. University programs differ in how they present the discipline, the critical thinking skills they develop, and the breadth they require in liberal arts, social sciences, and mathematics.

Accreditation

For a program to earn accreditation, organizations such as the Accreditation Board for Engineering and Technology (ABET; www.abet.org) review it every few years for adherence to an accrediting body's standards. The Computer Science Accreditation Board (CSAB; www.csab.org), a participating body of ABET, is the lead society for computing, information, systems, and software engineering and cooperates in computer-engineering accreditation.

The process provides quality assurance and consistency of exposure to key underlying principles in a given discipline. Reviews are thorough and encompass such diverse criteria as classroom hours spent on specific topics and the quality of work produced by top, average, and lower-end students.

In addition to program accreditation, 19 recognized accrediting agencies (Council for Higher Education Accreditation; www.chea.org) generally review most US universities every four years. A typical accrediting agency considers the quality of many attributes, including finances, diversity, expected student achievement, faculty, and academics. Institutions also internally review departments, programs, faculty, and even individual classes. External forms of accreditation exist, including the Centers of Academic Excellence (CAE; www.defenselink.mil/nii/iasp/schoolsCAEList.htm) whose designation indicates that an information-assurance program meets specific requirements established by the US National Security Agency. Each accrediting organization uses its own criteria for accreditation, and its own method of determining which institutions and programs it accredits.

Of course, not all accredited programs are identical. While accreditation sets standards for a field's underlying principles, how it teaches them is up to the institution—two candidates with BS degrees from different institutions could have different strengths. While the value of a college experience is closely tied to a student's diligence, over time, most programs achieve a reputation for producing graduates with particular characteristics, such as leadership, formal methods, practical programming skills, or excellence in software processes.

Professional certifications

Like academic accreditations, there are a variety of professional certifications, which vary widely in purpose and requirements. We grouped the differing forms of professional certifications into three broad classes: vendor specific, domain specific, and practicum.

Vendor-specific certifications

These emphasize a particular skill set arrayed around a vendor's products and domain of expertise. For example, suppose the Blockade Company offers certificates in firewall management. People who earned this certificate will know how to configure Blockade's B123 firewall and use its features. They'll have a basic understanding of threats that the B123 can counter but might not understand other threats or how the B123 relates to other firewalls.

By contrast, a graduate with an MS—even one whose thesis concerned firewalls—probably won't know how to configure a Blockade B123 firewall. College education primarily uses domain- and vendor-specific knowledge as a vehicle to enhance the study of principles rather than as an end in itself. This graduate student should understand the principles underlying the B123 firewall and readily identify its relationship to other defense techniques. But the student will need training (or time) to discover how to configure one. On the other hand, a professional armed with only a Blockade certificate might lack the background to compare the Blockade B123 with other forms of system defense.

Vendor-specific certification identifies a student who's completed a curriculum that demonstrates mastery of particular tasks (such as configuring B123 firewalls) or equipment (such as the features of the B123 firewall). The student has acquired enough knowledge to understand why firewall configurations are important: what threats they counter, the consequences of particular settings, and so forth. Also, the student has seen the application of general principles of networking and security, as embodied by the firewall's characteristics.

Vendor-specific professional certification serves a different purpose than academic education. First, it should not take as long to achieve. Second, it is highly focused on a specific marketable skill. A company hiring someone with Blockade's firewall-management certification should immediately be able to put its new hire to work on its Blockade firewalls after explaining its local policies. A new hire with a graduate-level, security-focused academic education would need to learn how that particular firewall works, and might need extensive training or time for self-paced study before becoming productive.

By contrast, if a new kind of firewall were to become available, we could expect the university graduate to understand the differences between the two more rapidly than the Blockade firewall specialist. Also, the graduate should be able to readily learn other security-related tasks. Similarly, a computer-science degree could indicate that an individual would learn a new language or a new operating system more easily than someone with a professional certification in a specific language or operating system. (Of course, a degree or certification is only an indicator of what an individual might be able to do, and often establishes only the lowest threshold. The longer a person has been working, or the more self-motivated, the more likely the person has self-taught but unmeasured skills.)

Because vendor-specific certification's value is market-driven, it's volatile. The certification has value if the vendor's product is in demand, the specific skill set is in demand, and the certification appropriately measures the candidate's skill set. The value of most vendor-specific certifications diminishes as the underlying technology becomes outdated.

The value of most vendor-specific certifications diminishes as the underlying technology becomes outdated.

Domain-specific certification

This certification covers a broader class of knowledge. A professional organization defines a body of knowledge aimed at a practitioner category and offers a knowledge-mastery certification. Participants focus on this body of knowledge, rather than on the broad category of reasoning skills or the overall discipline of an academic program. Many domain-specific certifications require holders to also have professional experience, something an academic education won't provide.

A domain-specific certification attests to mastery via testing and, usually, through professional experience. The body of knowledge includes basic domain principles that a successful candidate can apply to realistic situations, even those that the testers never considered. The program's intent is to certify achievement of the organization's professional standards.

Domain-specific certification complements academic education because it covers a specific body of knowledge and its application in considerable depth along with field practice. A company hiring this person would have evidence of the person's experience and the areas of knowledge the person has mastered.

A key difference between this and a purely academic education is that new graduates might know the principles of a specific domain, but not yet applied them in their work experiences. Furthermore, the body of knowledge professional certifications cover supports existing professions more directly than degrees do; typically, an academic candidate's background might be more comprehensive, but lack some job-specific components.

Practicum certification

This category attests to practical application of specialized knowledge.

The practicum element might use one or more vendor systems.

Students demonstrate competence and experience in a particular subject area, such as firewalls in general, rather than a vendor's specific firewall offering. This type of certification assumes knowledge of key foundational material such as networking. As with an academic education, students learn to apply basic principles to diverse situations and environments, but (as with domain-specific certification) practicum certification emphasizes the ability to perform specific tasks to achieve specific goals rather than understand the principles that those tasks demonstrate.

The core knowledge needed to earn a practicum certificate is narrower than a domain-specific certificate, but broader in demonstrated skills. Assessment relies on a combination of knowledge testing and a project to which to apply that knowledge to achieve specific goals. The practicum element might use one or more vendor systems.

For example, an intrusion-analysis practicum certification might require an applicant to pass a test to prove mastery of basic concepts; in this, it resembles a restricted domain-specific certificate. Then the applicant must complete a project. For one such certification, the applicant uses network traces generated by intrusion-detection systems to determine what attackers did and then writes a detailed description of what the traces show. Experts review the analysis to determine whether it is correct and detailed enough. If so, the applicant receives the certification. This process describes the requirement for the GIAC certification offered by the System Administration, Networking, and Security Institute (www.sans.org).

(A person with an academic degree and practicum certification can draw on the theory and principles underlying a specific academic discipline, and also has the practical experience of extending and applying that knowledge in a particular area.)

What's right for you?

As we've shown, certification criteria vary. For example, someone who's CISSP certified has mastered the common body of knowledge promulgated by the International Information Systems Security Certification Consortium (ISC^2) organization (www.isc2.org), but its requirement differs from that to obtain a Cisco Certified Internetwork Expert (CCIE) certification. In academia, accrediting agencies like ABET or CSAB examine curricula and quality to ensure organizations meet minimum standards. But at present, no similar self-regulation exists. For professional certification, evaluation rests with the issuing organization, which leads to two observations about the quality of professional certification.

First, how can companies use a professional certification to determine a prospective employee's suitability for a particular job? The appropriate question is whether the certification measures what the employee needs to do. If employers find that employees who have a particular professional certification can perform their jobs well, and those without the certification perform the same jobs less well, the employer will probably prefer applicants that hold that certification. If they find that professional certification holders perform the job no better than those without it, they'll ignore them. The latter certification's credibility will decrease, making people less likely to obtain it.

Second, people tend to believe what they‘re comfortable believing. If all members of a company's management have an XYZ professional certification, they might believe that it is the mark of a top professional—regardless of whether that is true—and only hire people with that certification. In effect, enough professionals with the XYZ certification can maintain the certification's importance regardless of whether it actually enhances employee performance abilities on a particular job. This observation contradicts the first one, but it is a common human behavior.

The question of whether academic education or professional certification is more important than the other omits their differing goals. A better question is whether the education or certification of a particular prospective employee is appropriate for the job he or she will perform, and whether or how each will enable him or her to grow to handle new challenges and job responsibilities. Some jobs require understanding specific tasks or equipment, others require more general knowledge, and still others require both. But ultimately, candidates' abilities and character will determine how well they apply their learning. □

***Matt Bishop** is an associate professor in the Department of Computer Science at the University of California, Davis, and a codirector of the Computer Security Laboratory there. His research interests include vulnerabilities analysis, the design of secure systems and software, network security, formal models of access control, and intrusion detection. Contact him at bishop@cs.ucdavis.edu.*

***Deborah Frincke** is chief scientist for the Pacific Northwest National Laboratory's cybersecurity group in Richland, Washington. She is currently on leave from the University of Idaho, where she is an associate professor and was director of the Center for Secure and Dependable Systems. Her research interests emphasize system defense, especially intrusion detection, and the security of high-speed systems. Contact her at deborah.frincke@pnl.gov.*