The Professional Certification Predicament

by Ben Rothke, CISSP

Professional certification is often a requirement for many information systems jobs. But certification is not an end in itself. Some of the important issues regarding certification are:

- ❒ Does certification equal value?
- ❒ The unique aspect of certification to information technology
- ❒ Education vs. certification
- ❒ Consistency between certifications
- ❒ Objective studies as to the value of certification
- ❒ Benefits of certification

Some certifications are valuable, others mere pieces of paper. Yet it is the skills and experience that a security professional brings to the table that is of value, not the number of suffixes after their name.

What do Ron Rivest, Adi Shamir, Len Adleman (creators of the RSA cryptosystem), Steve Bellovin (premier security researcher) and Marcus Ranum (Chief Technology Officer, Network Flight Recorder, Inc.) all have in common? Besides being some of the most innovative minds and creative personalities in computer security, they could not work at METASeS, Inc.

In May 2000, METASeS, a security solutions provider, announced that it would require CISSP (Certified Information Systems Security Professional) certification for all its consulting personnel. METASeS stated in its press release that the CISSP certification requirement for its consulting staff is compulsory to ensure that its clients receive the highest quality services available in the marketplace. Never mind that the creators of RSA forged an industry, Steve Bellovin is a recognized expert in firewalls and intrusion detection, and Marcus Ranum is a master of myriad security topics, the fact is that all five of them lack their CISSP certification, and this ostensibly makes them unemployable at METASeS.

It is simply distressing that companies are placing certification above crucial items such as experience, knowledge, and real-world know-how. Certification has somehow turned into a measure of value in and of itself; yet to a large degree, certification is often no more than a commodity. The fact that world-class security practitioners are categorized by their lack of a specific certification is an inequity, and ultimately a defeat for what is of lasting value, namely experience and skills.

In the press release announcing the requirement of the CISSP certification, Craig Robinson, Executive VP & COO of METASeS declared, "The [CISSP] certification guarantees that METASeS customers will receive the most efficient security solution from highly-skilled IT specialists. The CISSP is not about passwords and user ID's - it's about reducing business risks to produce more revenue and profitability".

While Mr. Robinson correctly noted that security is more that passwords and user ID's, the most important issues are - Does certification indeed mean that a client will receive the most efficient security solutions available? Are certifications in general necessary? Why is it in some IT groups a badge of honor to have a wall full of certificates, when similar professionals in non-IT divisions or other IT shops do not have the same need?

It would be a shame if METASeS , or any other organization, would forgo those with technical expertise and skills, simply because they lack an industry certification. Should METASeS stick to their guns and refuse to hire non-certified consultants, then their rationale for requiring certification in the first place (to ensure its clients receive the highest quality services available in the marketplace) would be nonsensical, in light that many, if not most, of the world-class security experts lack any type of certification.

Does Certification Equal Value?

Certification became in-vogue in the early 90's with the CNE (Certified NetWare Engineer) program from Novell. Job requirements often required CNE certification. The success of the CNE certification resulted in a glut of certifications and certification preparation pro-

grams. Within a few years, an entire industry was born around certification.

While Mr. Robinson of METASes stated that certification guarantees METASeS customers will receive the most efficient security solution; such a claim is difficult to verify. This is due to the fact that neither ISC2 (International Information Systems Security Certification Consortium, the group that manages the CISSP certification) nor any other information technology certification organizations offer any type of guarantee, assurance or indemnity for the parties they certify.

A further problem is that many certifications do not require any real-world experience. This condition has resulted in the term paper certified, as in He's a paper-CNE. Paper certification is where a candidate has certification, but has only understood the technology in the context of a test lab with technical definitions, as opposed to real-world production systems.

By way of analogy, if you were to have Lasik eye procedure, would you rather have your operation performed by someone who has done the procedure on thousands of people for a number of years, or someone who just got their Lasik certification? Shouldn't production systems also be managed by someone with real expertise and not just a piece of paper?

It is to the credit of ISC2 that they require proof of real-world experience. Candidates can only sit for the CISSP certification after having at least three years of direct work experience in one or more of the ten test domains of the information systems security Common Body of Knowledge (CBK).

The Unique Aspect of Certification to Information Technology

Nearly every industry has some sort of certification, be it auto repair, culinary arts, respiratory therapy or criminology. Yet while other fields view certification as a means to an end, there seems to be the perception than within IT, certification has become an end in and of itself. One certification software company promotes this notion when their advertisements read "Collect certifications like a hunter collects trophies".

As an example, there are a plethora of certification magazines, software and training programs just to get people certified. There are even books about certifications, one with the title "Get Certified and Get Ahead ". Advertisements in professional periodicals have bylines of "Get certified – no experience necessary". Many examination preparation vendors offer certification guarantees. While there is nothing wrong with a vendor having confidence in the quality of their training and preparation materials, one would be hard-pressed to find such companies outside of IT providing similar guarantees of passing or entry into a specific job market.

Within IT, certification is a very profitable venture for those advocating it. There are massive revenue streams generated by the various certification schools, technology boot camps, publishing houses, etc. Specifically, certification boot camps frequently take people with aptitude, yet no real-world experience in technology, and within a week or two, cram them to pass the certification tests.

The truth is that to a large degree, IT managers in corporate America really do not know what to do with certifications. Corporate HR often uses certification programs as a way to assess skills, promotions, recruiting, pay increases, etc. Recruiting firms are utilizing certification to validate job candidates. Managers are often so out of touch with the technologies that they are managing, that they use certification as a crutch to assist them in their day-to-day management.

From the recruitment end, Lee Kushner, CEO of L.J.Kushner and Associates (Freehold, NJ www.ljkushner.com), an executive recruitment firm specializing in Information Security, states that the bottom line is that real security skills are the first priority. Management wants professionals who possess the skills and experience needed to navigate through the fast changing and developing field of information security. Kusher notes that "Employers who are searching for the industry's best qualified consultants look for the depth of experience that only the aforementioned experience can bring. However, CISSP certification is a tremendous enhancement to the information security professional's skills and experience". Kushner believes that while certification is indeed beneficial, it should be looked upon as a valuable enhancement or add-on, as opposed to a prerequisite for hiring.

Certification vs. Education

It should be noted that there is a large difference between certification and education. The goal of educa-

tion is to impart skills and knowledge to the student. The goal of certification is to evaluate whether that same student has successfully attained those skills and knowledge. The two generally hand-in-hand.

Commercial educational programs generally don't include any type of comprehensive testing. If a student paid for and attend a technical training class, then they passed. They could have slept though it all, but their attendance is all that mattered. Certification is an attempt to fill in that missing link to evaluate the efficacy of the training.

The larger problem is that within IT is that most employees lack a comprehensive technical education. Many companies do not what knowledge and skills are required to perform a specific job. Consequently, when they attempt to test an employee in those skills, the assessment is often flawed.

Where does the money go?

Many companies have spent significant sums on training and certification and often do not have a lot to show for it. They blindly send their staff to training and certification courses without a clear plan or expectation of what they hope to achieve from the training.

Changes need to occur. While IT managers may have naïvely approved open-ended certifications in the past, successful IT managers must now demand greater results from the training processes they are involved with, and the certification programs they send their employees to. Effective managers must seek out those certification programs that consistently produce graduates who are adaptable and well grounded, as well as immediately productive.

Vendors offering certification should also start replacing much of their product-specific minutiae in their programs with objective, real-world, hands-on expertise. Is it really necessary for an MCSE to know every parameter in the Windows 2000 route command? Or is it better to know its real-world use? Getting away from such product-specific minutiae can ensure that certifications are much more beneficial.

Are certifications of value? Yes, but only in the bigger context of real-world experience. As an example, there are a plethora of Internet web sites offering university diplomas. In truth, almost anyone can start their own university and offer degrees. Yet there is a significant difference between the University of Hoboken and Harvard University, namely accreditation and reputation. For certification to have greater value, management must understand what it takes to require the certification and what they are truly getting with a certified candidate.

Do company's require certification?

While METASeS may require certification, that is not necessarily standard across the industry. As an example, Bruce Schneier one of the world's leading experts on cryptography and President & CTO of Counterpane Internet Security, has no certification requirements for his staff and indeed is not a CISSP himself. Schneier states that "there are security experts who are not certified, and there are certified people who are not experts. I see value in training and experience; not in certification".

A project manager at a leading investment bank states, "I could care less about certification. I want a person who understands in depth the technology they are running". This manager felt that when certification test stress the finer points of a technology or product to a high degree of detail (as they often do), many people unfortunately get tied up in this and then lose the perspective of what the technology they are using is all about. More importantly, he stated that "those who ride the banner of certification often become wedded to the technology they are certified in, and don't have the sense when to use a hammer instead of banging away with their favorite wrench."

Char Sample, Principal Architect at Symantec, notes that many employers are often unable to discern truly experienced candidates from those who simply know a few buzzwords. Employers in that state use certification as the vehicle to differentiate between the experienced candidate and the neophyte. However, what most employers really want (or need) is a candidate who is a critical thinker and problem solver. Unfortunately, for those types of individuals, there are no certifications, not even college degrees, that can attest to their competence. Sample notes that some of the best minds around do not have a degree, and even of those that have degrees, many are not in traditionally technical disciplines (such as computer science, engineering and math).

Barbara Dijker is president of the System Administrators Guild (SAGE), which is currently developing a cer-

tification program for system administrators. Dijker opines, "The value of certification is 100% dependent upon the particular certification program. So the question of value can only be answered specifically for a particular program." Dijker believes that few technical managers require certification of their staff because they recognize that one can be highly skilled and qualified without it. She personally would not require certification of a prospective employee if she were confident of their abilities. She would rather have the best person for the job rather than the most credentialed. Dijker observes that "requiring existing staff to gain certification is career development, not training and it could potentially backfire and allow your staff to find more lucrative employment elsewhere".

Michael Ressler, division manager for security consulting services at Global Integrity, states that Global Integrity requires all its consultants obtain their CISSP certification. Ressler comments, "Our clients are the primary driving force behind our efforts to have all of our consultants obtain their CISSP certification. Since it is important to many of them, it is important to us". Ressler notes that his main concern though is to have well trained, knowledgeable consultants who have extensive backgrounds in the areas in which they consult."

Consistency between certifications

A problem that many managers face is that there is a lack of consistency and uniformity between certifications. While most managers are able to discern the value of a bachelor's degree between an accredited Ivy League school and an Internet degree mill, they can't discern the value between a CCIE (Cisco Certified Internetworking Expert) and a CLP (Certified Lotus Professional), or the difference between a CCSA (Checkpoint Certified Security Administrator) and a CCSE (Checkpoint Certified Security Engineer).

This problem is exacerbated in that the companies that issue the certification are often not forthcoming in what the certification signifies. When a manager meets a person with a specific certification, there should be some type of way to clarify what the certification means and what one can expect.

Studies to the value of certification

Anyone seeking to research the overall effectiveness of certification, will find that there is not a lot of long-term and objective and impartial studies showing the value of certification. In addition, even those studies that lack objectiveness and impartiality are often conducted by web, telephone or mail, making them on occasion statistically meaningless, due to the ineffective methodologies used in the surveys.

David Goldstein, a well-respected marketing executive in the financial services industry has been conducting demographic marketing surveys for nearly 20 years. Goldstein notes that many surveys are simply marketing tools used for lead qualification. Marketing groups use this method of lead qualifications to ascertain if an individual is suitable for a specific product or service.

Goldstein remarks that conducting an effective survey with meaningful questions is not such a simple endeavor. Those developing the questions should in no way tailor the question to affect the outcome. While asking about gender is as simple as male or female, many other question are more abstract, and do not fall into a simply yes or no answer scheme. To ask a meaningful question, the questioner must be well versed in the specialty of market research. To get a valid response, questions have to be carefully constructed and qualified.

For those that attempt to glean some information from any type of survey, Goldstein notes some critical question to ponder before relying on the data:

- ❒ What methodology was used in the research
- ❒ Does the sample represent the population you want to survey
- ❒ Were the respondents qualified
- ❒ What is the sampling error
- ❒ Are the rating scales (very good ..... very poor) balanced
- ❒ Does the question bias the response
- ❒ Are the questions sequenced properly

One study that does a provide a good methodology and evaluation overview is Criterion Validity of Microsoft's Systems Engineer Certification: Making a Difference on the Job by Jack McKillip of the Southern Illinois University at Carbondale.

Benefits of certification

There are indeed benefits to certification, but those benefits need to be understood within a larger context. Using product certification as an initial example, Microsoft has used the Windows NT C2 security rating as

a proof to the strength of Windows NT. The problem is that C2 certification requires (amongst other things) that the host be disconnected from the network . So while your Windows NT server may be C2 certified, none of your 50,000 users can access it. Is that value?

Certification can only be meaningful when used in the appropriate context. That context mandates understanding the value of the specific certification, what was required to obtain it, the vendor's commitment to quality, and the inherent capabilities of the individual. As an example, one of the most respected certifications is the CCIE (Cisco Certified Internetworking Expert). To obtain a CCIE, one must pass a number of tests, in addition to successfully completing two days of lab work. The CCIE prerequisites are so extensive, that it is recommended that those with less than 3 years of Cisco experience not bother taking the test. Because the CCIE is such a complex exam, there are a limited number of people who have passed (as opposed to nearly one million Microsoft Certified Professionals). As a result, because of its daunting requirements and required lab work, there is no such thing as a paper CCIE. Cisco has architected the CCIE certification to place value over the sheer number of those being certified.

Some of the direct benefits that certification may offer from most vendors include:

❒ Discounted technical support calls

❒ official recognition from the vendor

❒ personalized certificates and plaques

❒ use of the official certification logo

❒ newsletters with technical information

❒ access to technical and product information

❒ access to exclusive discounts on products and services

❒ priority invitations to conferences, technical training sessions and special events.

❒ personal recognition

❒ product and training discounts

❒ beta product and early releases

❒ for Microsoft certification, potential college credit for certification through Regents College.

❒ Increased charge-out rates to customers, leading to greater profitability

In addition, certification is also a good way to inspire motivated employees who are quick learners and looking to advance themselves and in fact may be a way to increase employee retention. While the common wisdom is that employees often leave the sponsoring company after they have achieved certification, this isn't always true. The reality is that employees at companies that invest in their ongoing professional development are significantly less likely to leave the company than those who work at companies that don't invest in certification. When employers sponsor certification training, employees generally feel a greater sense of loyalty.

New trends in information security certification

The newest certification in the information security space is SANS' GIAC (Global Incident Analysis Center) certification program (www.sans.org/giactc.htm). The two GIAC certifications are the GIAC LevelOne Security Essentials and the GIAC Certified Intrusion Analysts (GCIA).

GIAC was designed to be of value to systems administrators and managers of systems that require systems and network security. The GIAC course specifications were developed via the consensus of many veteran security professionals and attempted to coalesce the varied talents necessary for the multi-disciplinary art of information security.

The CISSP certification on the other hand isn't designed for those who actively implement products, says Rick Koenig, VP of sales at ISC2, but for professionals who develop policies, manage security functions, and perform consulting, and need a good understanding of how security realms interrelate.

The main difference between the two is that CISSP teaches and tests on the basic information that security professionals should know. It emphasizes theory and concepts and avoids any type of specific products. With GIAC, the specific tools, technique and product commands used are tested on, as well as some of the theoretical concepts.

So while you may want to hire a CISSP as your information security manager, a GIAC may be better as a network security architect. It remains to be seen if GIAC will live up to its promise, or if it will even catch on in the industry. But it looks like a promising start, though.

Conclusions

Certifications, when used and understood in context do indeed offer value. Yet a certification must not be valued above experience and in-depth knowledge. Skills and experience are what are of key value within infor-

mation systems security, and they are what is often in short supply. While anyone with a pulse can get some sort of certification, experience must be unquestionably of prime significance.

Managers looking to grow their organizations with qualified staff need to appreciate certification for what it is; namely a small item in a large pond. Those that attempt to place innate value on certifications are either shortsighted or perhaps have some sort of financial interest in the certification. Bruce Schneier has often stated the security is a process, not a product. So too with certification, it is a single element in the large process of technical development and education.

The FUD (fear, uncertainty and doubt) factor is pervasive in the technology industry. Press releases about vaporware products are not uncommon. But let there be no fear, uncertainty or doubt about certification: it is overall a small thing, from which we hope, big things, namely experience and skills , will one day come.

Ben Rothke is a New Jersey based security consultant with eB Networks. Those wishing to know which certification he has can reach him via e-mail at brothke@ebnetworks.com

The views expressed are his own.

Ben would like to thank Alan Lustiger, CISSP of Datek Online Brokerage Services, Inc., for his assistance reviewing and critiquing this article.

[[Insert Table 1. Some Random URLs about Certifiction--see text box outside of page]]