The Use of Simulations in Assessment and Certification

BJ Gleason†

ABSTRACT

Many organizations require their current and perspective employees to obtain industry-based certification to maintain, and seek promotions. However, many certifications are simple knowledge based examinations that reward memorization instead of actual performance. With industry's increased reliance and demand to hire certified professionals, there is much more dishonesty, as well as incompetence, entering the system. This paper examines the issues and difficulties faced by organizations trying to hire IT staff based on current certification methodologies and recommends that IT assessments should be shifted from knowledge-based to performance-based examinations through the use of scenario-based simulations. It also demonstrates how to integrate simulations into certification and assessment testing using a proposed digital forensics certification as an example.

Key Words : Simulation, Certification, Scenario Testing, Digital Forensics

1. Introduction

In the past, during the hiring process, there were few, if any, standards for hiring IT professionals. The hiring process was dependent on the evaluation of the applicant's resume and work experience. Resumes acted as a filter, and interviews were used to determine if the candidate possessed, and could demonstrate their skills. In the late 1980s, and early 1990s, companies such as Novell, Microsoft, and Cisco, started offering numerous certifications to individuals who could pass a single, or a series of exams[8]. These certifications started to become widely accepted in industry as a shortcut for the evaluation of an individual's abilities[10]. It is now common to see job posted requiring the possession of the certifications that the hiring organizations deem necessary for the position. Job position and resume databases such as Monster, Careerbuilder, and others, allow potential candidates to list their certifications, and employers to filter their search results based on specific certifications.

Based on the growing demand in certification, more vendors started producing their own certifications, to certify candiates in the operation of their own hardware and software. Other organizations, such as CompTIA, have been formed to produce vendor-neutral certification. Prometrics, Vue, and other testing centers have been set up world-wide to offer certification exams. Training institutions have started offering classes and

† University of Maryland, Asian Division.
Received : 2009-01-21, Accepted : 2009-03-10

boot-camps to prepare candidates for the certifications. Certification acronyms have become standard suffixes on titles, resumes, and business cards. Colleges have even started to incorporate certifications into their curriculum, or even offer college credit for those students possessing specific certifications. For example, Capella University's MSIT with an IA speciality program is not only "designed around the 10 domains of the CISSP certification"[6], but it will accept the CISSP and other certifications in place of several classes, to reduce the number of classes the student would have to complete to achieve their degree[7].

But as the reliance on certifications grew in the workplace, and their perceived value increased, it was inevitable that fraud would find its way into the certification process, and it is having a impact on the certification process[20]. Cheating has become rampant, and "paper certifications" - the ability to pass an exam via study with no actual experience - are becoming widespread. The author has personally witnessed numerous examples:

- Candidates taking digital photos of the exams
- Candidates writing down exam questions in notebooks
- Candidates assisting each other during the exam
- Candidates using cell phones, PDAs, and other devices during the exam
- Candidates using reference materials, such as books or notes, during the exam
- Website offering "brain dumps" - a list of questions compiled after an exam is completed
- Companies offering "practice tests" containing only slightly modified actual exam questions
- "Proxy" candidates hired to take the exams for the actual candidate
- Trainers handing out pirated exam study guides
- Training centers handing out the actual questions to the exam, and informing the students to take the exam before Friday, since a new set of questions will be distributed.

Rank	Certification Vendor	Braindump Sites*
1	Microsoft	328
2	Cisco Systems	326
3	Oracle	296
4	Citrix Systems	289
5	Sun Microsystems - SAI	286
6	IBM	283
7	CompTIA	281
8	CIW	272
9	CWNP	271
10	Hewlett Packard (HP)	269
11	Novell	269
12	Linux Professional Institute (LPI)	268
13	Apple	267
14	Check Point Software Technologies	266
15	EC-Council	263
16	Juniper Networks	260
17	EMC	259
18	Adobe Systems, Inc	254
19	Nortel	252
20	Lotus	250

*Information provided by and Copyright of CertGuard, Inc.

These are not isolated incidents, but are happening world-wide. Cisco Systems and Pearson VUE conducted a trial run of an anti-cheating system that they hoped would identify proxy test takers. Out of 200,000 tests given in eight countries located in Asia, Europe, the Middle East, and North America, over an 8 month period, they identified 1,400 possible cheaters, and were able to confirm that approximately 1,000 were taking the exam for someone else[3]. Microsoft has gone after Pass4Sure.com, who they believe are selling copies of their exams. Not only is Microsoft going after the companies who sell the exams, but also the candidates who make use of them. Microsoft has announced that buying exam answers Pass4Sure and other companies to be a form of cheating, and will imposed a lifetime ban for any candidates caught using these materials[5]. But this is only the tip of the iceberg-exam security vendor CertGuard found 328 braindump sites selling Microsoft exams, and 326 selling copies of Cisco certification exams. The chart shows how popular braindump sites are, and how widespread the problem is[31].

Cheating is even rampant in the military. The U.S.

Army is currently investigating whether thousands of soldiers cheated on various promotion exams by downloading copies of exam questions and answers from various websites. Over 1,200 different exams from a number of military schools have received over 500,000 hits per month[4].

Aside from the cheating and fraud that is starting to permeate the certification industry, there is even a more fundamental question that needs to be asked about the current certification process - does the current examination process really test the skills required, and allow the candidate to demonstrate mastery of the domain? Many of the current certifications are composed of multiple-choice questions, and there are specific strategies that students should use when taking multiple-choice exams. Eliminate distracters, taking a guess, favoring B & C over A & D, and other techniques might allow students to obtain a better grade and possible pass the certification, but how often on the job are employee presented with multiple-choice problems? Many of the multiple choice questions appear to be in the lower regions of Bloom's Taxonomy, and taken word-for-word from the training materials, so students can just use memorization to pass the exams. The validity of an exam is determined by how well it measures what it is intended to measure. To use an exam as a way to measure performance, there must be a relationship between exam score and the actual performance[32]. So it is possible that an exam might be a better measure of the individual's recall or even their test-taking ability rather than their ability to complete the actual task.

2. Simulations and Performance -Based Testing

Simulations have a long history and have been used for decades in aviation and medical fields for training and evaluation. The first crude flight simulators were developed in 1910, just a few years after the Wright brothers made their first successful flight in 1903 (Page, 2000). With the advent of computer technology and the growing sophistication of the aircraft, more sophisticated simulators were developed. Over time, the simulators have become so sophisticated that in the 1970s, the Federal Aviation Administration started to accept simulator flight time as actual flight for training and evaluation purposes. The medical field also has used simulations for diagnostics and to simulate surgeries. In 2004, in a decision very similar to that of the Federal Aviation Administration, the Food and Drug Administration started requiring the use of a high-fidelity, virtual-reality simulator for training doctors who were to perform a carotid artery stenting, a complex and risky procedure[12].

It is only logical that candidates should be tested in the manner in which they learned, and in the way they are expected to perform[11]. The assessment should be based on three factors: the candidate's expected knowledge and competence in the subject area, a way to test and observe the candidate's performance, and a way to evaluate their performance[19]. Simulations can address all three factors.

The goal behind simulation is to measure the ability to execute, not just the ability to memorize and repeat information. The advantages of using simulations are many - they are more realistic, more representative of the actual tasks that need to be performed, and more difficult to cheat on. Microsoft, Cisco and Oracle have started incorporating simulations into their certifications [29]. In lower-level, entry-level certifications, there are a few simulation-based questions, while in the higher-level certifications, such as the Cisco CCIE, student actually build and trouble shoot an entire network. Microsoft Office User Specialist exams are entirely software - simulation based.

While it would be possible to cheat even on a simulated exam, the complexity of the answer, with possible variations, makes it much more difficult. In a recent brain dump put out by a commercial vendor, the answer to a CCNA simulation, with two variations, takes up 3 pages of single spaced type. In one of the Microsoft exams, the simulation answer goes on for 6 pages. The length and complexity of these answers (contained within a 1544 page brain dump), makes the process of memorization difficult - it could even be argued that it would be easier to learn the material. But

on many of these exams, simulation questions are actually just targeted pseudo-simulations. The complete environment is not simulated, many of the functions not needed for to complete the task are disabled and the simulation question typically begins at a logical starting point, all of which can provide additional clues to the candidate on how to solve the simulation[17].

3. Digital Forensics - A Complex, Growing Field

To see how simulation and performance - based testing can be used to assess competency, we will now examine how these techniques can be integrated into a certification program being developed for digital forensics. According to the Federal Bureau of Investigation[24], the amount of digital evidence processed from Fiscal Year 2000 to Fiscal Year 2005 has increased 3,060% to a staggering 1,426 terabytes of data. During the same time, the number of forensic examiners only increased by 182%, to a total of 264[24]. Shreeve (2005) also indicated that the field is growing at exponential rates and that the police and government agencies are not prepared to handle such growth[22]. In fact, a large percentage of cases dealing with digital evidence are being outsourced to private organizations, due in part to the lack of properly trained law enforcement professionals and increasing demand for digital evidence processing.

Whether collecting physical evidence, such as fingerprints or DNA, or digital evidence, a digital forensics investigator must follow certain laws and procedures. Digital forensics is the application of methodical investigatory techniques to solve criminal cases involving computer systems[9]. Digital forensics deals with the preservation, identification, extraction, documentation, interpretation, and presentation of data collected from a computer system. Digital evidence is hard to destroy but easy to damage. If not collected and preserved properly, the evidence, digital or otherwise, often cannot be used in a legal proceeding[9][27][28][30].

The National Institute of Standards and Technology has recommended that all organizations start incorporating digital - forensics processing into their incident-handling procedures[16]. In addition to the precautionary measures that sure procedures provide in the event that legal actions are necessary, forensic tools and techniques can be used for data recovery and troubleshooting. The major premise of Kent et al.'s report, however, was that "organizations should ensure that their [information technology] IT professionals are prepared to participate in forensic activities" (pg. ES-2). They stressed that incident handlers and first responders should receive forensics training and education so they know what they should and should not do when responding to a potential incident. They need to be prepared to cooperate with law enforcement and to make sure that they do not hinder the investigation or damage the evidence.

Digital evidence collection, preservation, and analysis are complex and time-consuming tasks. Forensic training is demanding and costly. Organizations have started to recognize the need to provide digital forensics advice and training for system administers[16], law enforcement[1], military personnel[14], and even college students[15][26]. Although there are now numerous digital forensics courses, college programs, and certifications, they tend to be very broad in scope, do not focus on any specific industry applications, and can take months or years to complete[15][25].

4. The Need for Simulation Based Certification in Digital Forensics

Aside from the basic knowledge, those out in the field also need to be kept up to date with the latest forensic applications being developed. This role is often filled by vendor-based certifications[13]. Only two vendor-specific, digital forensics certifications are currently available, the Encase Certified Examiner and the Accessdata Certified Examiner. However, both of these certifications are set up similar to the vendor-neutral certifications, wherein the student must take a multiple-choice exam and then has several months to process a sample digital forensic case using

that tool. With the numerous tools needed to complete complex investigations, the complex and time-consuming nature of vendor certifications, and the recertification processes, it is difficult for the digital forensic investigators to keep up to date and maintain their certifications.

An efficient, effective way is needed to determine if a digital forensic investigator has sufficient expertise in operating a specific digital forensic application. Any digital forensic investigator should have a solid educational background in the field and should keep up to date with the latest technologies. Aside from being able to conduct the investigations, investigators often must present their findings in a legal proceeding, the results of which can have severe consequences. Since the improper operation of forensic software can result in a loss of data, misinterpretation of the facts, and possible exclusion of the evidence, the courts have become more concerned about the qualifications and abilities of the forensic investigators, and their mastery of the tools they use[23]. The opposing counsel also will attempt to discredit investigators or expert witnesses by challenging their abilities to process and interpret the evidence, and by questioning their credentials[2]. Thus, it is important that the investigator know how to properly operate the tools being used. A common way to establish credibility is to present various credentials, such as degrees and certifications.

There are two kinds of digital forensics certifications: vendor neutral and vendor specific. There are numerous vendor-neutral certifications of varying quality[18][21]. They range from requiring a multiple-choice exam to processing numerous, sample, digital forensic cases on supplied media. One of the most widely regarded is the Certified Computer Examiner certification, which requires a criminal background check, verifiable forensics training, and experience in the field. Candidates accepted for the certification process take a multiple-choice exam and then have to process three sample cases using any forensic tools they wish, documenting a complete report of their activities. The certification can take up to 90 days to complete[25].

There are numerous digital forensic applications, and researchers are developing more all the time; however, only two commercial vendors, EnCase and Accessdata require certification. Given the complexity of these certifications, it would appear that the vendors are trying to certify the overall investigative process instead of just the operation of the vendor's software.

If other vendors follow these existing, vendor-specific models for certification, it will place an overwhelming burden on an investigator who needs to be certified on several different software programs. In additional to obtaining the initial certification, there is typically a 2-year recertification cycle, which also requires processing additional simulated forensic cases.

Whereas many of the forensics certifications use multiple-choice questions and complex sample cases requiring the generation of detailed reports to test the candidates, a simulation-based examination would focus on common, specific tasks and would require the candidate to complete those tasks. This process would increase the authenticity and relevance of a simulation-based examination over a traditional knowledge-based exam. Rather than the candidate simply selecting one answer from a predefined list of possible choices, the candidate actually must operate the tool to solve the problem. Candidates would have to demonstrate how they would use the tool to solve the tasks required in a real-world investigation[29]. The simulation-based assessment process also would have the benefits of being faster to administer and complete (hours as opposed to months) and of not being dependent on a subjective human grader to interpret the results and assign a score.

5. Developing the Simulator Assessment Framework

Whether collecting physical evidence or digital evidence, certain laws and procedures need to be followed. The improper use of digital forensic software can compromise the evidence, making it inadmissible in a court of law. A simulator would be able to determine if the investigator can properly operate the digital forensic software, to ensure that the digital evidence is

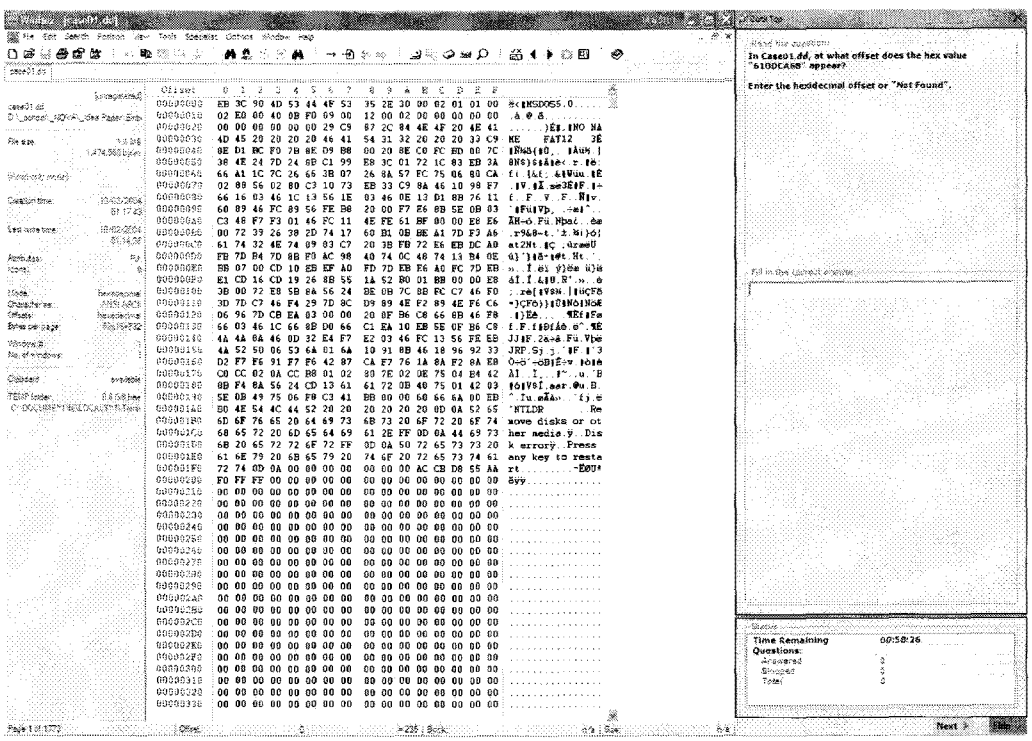
properly processed. The proposed Simulator Assessment Framework (SAF) would implement a criterion - referenced, performance - based assessment.

A survey of industry professionals and experts will be used to determine the basic sets of skills required of a digital forensics investigator. Once the skill sets have been identified, scenarios will be developed, and implemented in the simulator. In order to test the simulator, users who are considered by the vendor to be experts will test the simulation and provide feedback. In addition, the answers and time required for the expert to answer the question be collected to help establish a baseline that will be used to determine the proficiency of the candidate. Once the baseline is established, the simulator can be used to test candidates and see how they perform compared to the experts. The SAF environment would allow for multiple-choice, true-false, selection, short answer, and numeric response.

In order to increase operability, and maximize the number of applications that can operate within the environment, there is no coupling between the SAF and the application being used. The application doesn't have to be modified to work within the SAF, and the most current version of the application can be used as soon as it is released. The SAF requires the user to determine when they have answered the question, so the questions need to be design for the student to use the tool to derive the correct answer, and then move on. For example, a sample question might be, "In Case002.dd, how many deleted files appear in the root directory?" The answer could be a multiple-choice selection, but that might give the candidate a clue as to how many to look for. But using a numeric response, the subject would have to open up the case, examine the root directory, and on their own determine how many deleted files appear there. The questions should be focused on things can be found by using the tool, with a definitive answer being revealed.

When a candidate wishes to take the exam, they log in, select the test, and start the examination. The SAF environment is broken up into two parts - the simulation area and the testing area. In the illustration below, the simulation area is to the left, and the testing control area is to the right.

In the above simulation, the software being tested is



X-Way's Forensics WinHex, however due to the open design of the SAF, any software could be used. While the SAF environment is Windows-based, the area on the left could be used by any software, include virtualization software such as VMWare, Microsoft Virtual PC, QEMU, Xen, or VirutalBox, to allow testing of non-Windows environments or software. Since many forensic tools are Linux-based, such as Helix3, FBCD, Encase Linen, a virtual environment could be used within the SAF environment. With the proper drivers, the subject would be able to move seamlessly between the virtual system and the SAF environment. On the right, the testing control area displays the instructions, the questions, and provides a status window about the exam.

As the student completes each question, they click next, and move onto the next question. Once the student has completed all the questions or the time has run out, the results are calculated and displayed. In the SAF environment, the proficiency is based on two factors - speed and accuracy. Their answers and times are compared to the answers and time collected from the experts, and the score is calculated. The more questions the candidate can answer correctly in a given amount of time, the higher their score will be. Since time is a factor in this exam, this reduces the possibility that the candidate would be able to use other resources to find the answers. For example, the help files for the tools can be loaded within the environment, but the use of them to search for how to solve the current problem would increase the amount of time required to answer the question, and then, even if answered properly, would result in a lower score.

6. Conclusions

The early testing of the SAF has generated positive feedback from the experts and candidates who have participated. It appears to be easy to develop questions for, and provides a more realistic environment to assess the skills of the candidates. It could be used as part of a certification process, or used as part of an in-house hiring process to quickly assess the skills of candidates, based on common tasks they will be required to perform and should already possess.

The proposed SAF environment should not be the only requirement used to determine if a candidate is qualified to process digital forensics, or any other field in which they are applying. Instead it should be seen as a way to validate a portion of the candidate's qualifications, in addition the other skills and requirements needed for the tasks they are to perform.

With the proper controls, and the dynamic variations allowed for and provided by a sufficiently large enough test bank, it should greatly reduce the possibility of candidates cheating or revealing the questions and answers to others. Even if some of the information about the examination process were to leak out, it is more likely that what would be revealed are the skill sets required by the candidates - which is exactly what we hope the candidates possess, rather than the exact questions and answers.

References

[1] Armstrong, H., & Russo, P. (2004, June). *Electronic forensics education needs of law enforcement.* Paper presented at the 8th Colloquium for Information Systems Security Education, WestPoint, NY.

[2] Ball, C. (2004). Cross-examining the computer forensics expert: Getting to the truth means understanding not just computers, but also those who examine them for evidence. *Trial*, 40(7), 78-81.

[3] Baron, K., & Wirzbicki, A. (2008). Study confirms widespread cheating on job exams. Retrieved September 24, 2008, from http://www.boston.com/jobs/news/articles/2008/07/22/study_confirms_widespread_cheating_on_job_exams/

[4] Bender, B., & Baron, K. (2007). Army probes alleged exam cheating - Answers to tests for promotions found on websites. Retrieved September 15, 2008, from http://www.boston.com/news/nation/washington/articles/2007/07/22/army_probes_alleged_exam_cheating/

[5] Brodkin, J. (2008). Don't be fooled by suspicious test preparation Web sites. Retrieved September 23, 2008, from http://www.networkworld.com/newsletters/edu/2008/090108ed1.html?hpg1=bn

[6] Capella University. (2008a). Information Technology Online Degree Programs. Retrieved September 20, 2008, from http://www.capella.edu/information-technology-online-degree.aspx

[7] Capella University. (2008b). Transfer credit & credit for prior learning. from http://www.capella.edu/schools_programs/credit-for-prior-learning.aspx

[8] Carrion, J. (2002). The State of Microsoft Certification. Retrieved September 25, 2008, from http://mcpmag.com/columns/article.asp?editorialsid=420

[9] *Casey, E. (2004). Digital evidence and computer crime : forensic science, computers, and the Internet* (2nded.). Amsterdam ; Boston: AcademicPress.

[10] Cegielski, C. G. (2004). Who values technology certification? *Commun. ACM, 47*(10),103-105.

[11] Crisp, G. (2007). *The e-assessment handbook*. [London]; NewYork:Continuum.

[12] Dawson, D. L. (2006). Training in carotid artery stenting: Do carotid simulation systems really help? *Vascular, 14*(5),256-263.

[13] Dean, H. (2001). IT certification: What it is and where it's headed. *TechDirections, 61*(3),24-27.

[14] Giordano, J., & Maciag, C. (2002). Cyber Forensics: A Military Operations Perspective. *International Journal of Digital Evidence*, 1(2),NA.

[15] Gottschalk, L., Liu, J., Dathan, B., Fitzgerald, S., & Stein, M. (2005, February 23-27). *Computer forensics programs in higher education: A preliminary study*. Paper presented at the annual meeting of the Special Interest Group on Computer Science Education, St.Louis,MO.

[16] Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response* (NISTSpecialPublication 800-86). Gaithersburg,MD:National Institute of Standards and Technology.

[17] Neilson, G. (2005). Microsoft's New Simulation Questions: Report from the Field. Retrieved September 29, 2008, from http://certcities.com/editorial/columns/story.asp?EditorialsID=194

[18] Palmer, C., Newsham, T., Stamos, A., & Ridder, C. (2007). *Breaking forensics software: weaknesses in critical evidence collection*. Paper presented at the BlackhatUSA 2007.

[19] Pellegrino, J. W., Chudowsky, N., & Glaser, R. (2001). Knowing what students know: The science and design of educational assessment. Retrieved September 29, 2008, from http://books.nap.edu/openbook.php?isbn=0309072727

[20] Reese, B. (2007). The cheating industry that is devaluing IT certification - Part one. Retrieved September 25, 2008, from http://www.networkworld.com/community/?q=node/13341

[21] Ridder, C. K. (2007). Evidentiary Implications of Potential Security Weaknesses in Forensic Software. Retrieved May 1, 2008, from http://www.isecpartners.com/files/Ridder-Evidentiary_Implications_of_Security_Weaknesses_in_Forensic_Software.pdf

[22] Shreeve, J. L. (2005). Cyber sleuths. Retrieved Aug 18, 2005, from http://policeone.com/topic_internal.asp?view=99719&cat=articles&vid=118102

[23] Smith, F. C., & Bace, R. G. (2002). *A guide to forensic testimony: the art and practice of presenting testimony as an expert technical witness*. Boston: Addison-Wesley.

[24] Talley, J. (2006, April 25-28). *Computer Analysis Response Team (CART) unit overview*. Paper presented at the United States Forces Korea Information Assurance Conference, Osan Air Force Base, Seoul, Korea.

[25] Taylor, C., Endicott-Popovsky, B., & Phillips, A. (2007, April 10-12). *Forensics education: Assessment and measures of excellence*. Paper presented at the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), Seattle,WA.

[26] Troell, L., Pan, Y., & Stackpole, B. (2004, October 28-30). *Forensic course development - One year later*. Paper presented at the annual meeting of the Special Interest Group for Information

Technology Education (SIGITE), SaltLakeCity, UT.

[27] US Department of Energy. (2000). *First Responder's Manual.* Aiken,SC.

[28] Vacca, J. R. (2005). Computer forensics: *Computer crime scene investigation* (2nded.). Hingham, MA:CharlesRiverMedia.

[29] Vaglio-Laurin, M. (2006). *Don't just tell us - Show Us! Performance-based testing and the SAS® certified professional program.* Paper presented at the annual meeting of the SUGI, SanFrancisco, CA.

[30] Whitman, M. E., & Mattord, H. J. (2007). *Principles of incident response and disaster recovery.* Boston: Thomson Course Technology.

[31] Williams, R. (2008). Top 20 Most Braindumped Certification Vendors. Retrieved September 24, 2008, from http://www.networkworld.com/community/node/26055

[32] Witnah, D. (2004). A Practical Guide to Simulation Development. Retrieved June 1, 2006, from http://www.performancetest.org/members/files/testdesigndox/backgrounddox/Simulation%20Development.pdf

BJ Gleason

BJ Gleason has been teaching computer science and information systems classes for 25 years, and was a recipient of the 2007 Stanley J. Drazek Teaching Excellence Award for his innovative classroom techniques. He holds an Educational Specialist degree (Ed.S) in Computers in Education, as well as B.S. and M.S. degrees in Computer Science, B.A. in Asian Studies, B.S. in Criminal Justice, M.S. in Educational Leadership, and is currently working on his PhD at Nova Southeastern University. In addition, Mr. Gleason holds over 25 computer industry certifications, including Microsoft MCSE, CompTIA Security+, CISSP and is a Certified Computer Examiner from the International Society of Forensic Computer Examiners.