Title:

Building an information assurance laboratory for graduate-level education

Authors:

LTC Craig E. Kaucher
Professor of Systems Management
Information Operations and Technology Department
Information Resources Management College
National Defense University
202-685-2079

John H. Saunders, Ph.D., GSEC
Professor of Systems Management
Information Operations and Technology Department
Information Resources Management College
National Defense University
202-685-2078

Presenter and author to contact:

LTC Craig E. Kaucher (kaucherc@ndu.edu)
Information Resources Management College, National Defense University
300 5th Avenue
Fort McNair
Washington, DC 20319-5066

Abstract

A recent innovation within the curriculum of the Information Resources Management College of the National Defense University has been the establishment of an Information Assurance Laboratory. The purpose of the laboratory is to support the delivery of the information assurance curriculum by providing an opportunity for students to gain some minimal hands-on experience with the technological aspects of information assurance. Although the students in the IRMC curriculum are working senior managers or prospective senior managers, who in practice, will likely have little hands-on interaction with information assurance technologies, we are finding that the lab experience greatly enhances their understanding of the theoretical aspects of information assurance technologies and provides a firm basis for their critical evaluation of the management-level considerations that they will face as information assurance managers or even chief information officers.

Introduction

Formal educational opportunities in the field of Information Assurance are rapidly expanding. An increasing number of public and private colleges and universities, as well as U.S. government educational institutions, are offering degrees or certificates at the graduate, undergraduate, and even the doctoral level in information assurance.

Some twenty-three colleges and universities across the United States have been granted a special distinction from the National Security Agency (NSA) as a "Center of Academic Excellence in Information Assurance Education" (National INFOSEC Education and Training Program: Centers of Excellence, 2001). An even more select group of schools has been certified by the NSA to award a certificate for Information Systems Security Professionals (NSTISSC, 1992).

The NSA certificate program is based on a seven-part body of knowledge and includes both awareness and performance-based levels of knowledge that students are expected to demonstrate. Appropriately for this management-level certification, the performance level elements of the body of knowledge consist of planning, management, policy, and procedural activities. Yet, as *information systems* security managers, these certificate holders will be engulfed by technology in the performance of their duties.

Among the schools offering this certificate is the Information Resources Management College (IRMC) of the National Defense University (NDU). The IRMC is a Department of Defense (DOD) college that offers accredited, graduate-level education to senior military officers and civilian employees of the DOD, as well as senior civilian employees of other federal agencies. Students in the IRMC program are working professionals, often with twenty or more years of experience in information management and technology. They typically hold management positions at various levels within their agencies. Most are enrolled in the certificate program because they have direct responsibilities for site or enterprise-wide information assurance.

The unique benefits of the IRMC curriculum in information assurance include courses tailored to the student's responsibilities within the federal government or the DOD. Successful completion of four courses is required in order to be awarded a certificate. The requisite courses are:

- Assuring the Information Infrastructure (AII)
- Enterprise Security Strategies, Guidelines and Policies (ESS)
- Managing Security in a Networked Environment (SEC)
- Critical Information Systems Technologies (CST)

These four courses include all aspects of the NSA certificate program and more. The curriculum covers the relationship between high-level information systems, critical infrastructure protection, and the nuts-and-bolts issues of network security. The context of the curriculum is the role of the student as an information assurance manager or even as a Chief Information Officer in the DOD or other federal agencies.

A recent innovation within the IRMC curriculum has been the establishment of an Information Assurance Laboratory. The purpose of the laboratory is to support the delivery of the information assurance curriculum by providing an opportunity for students to gain some minimal hands-on experience with the technological aspects of

information assurance, particularly within the SEC course. Although the students in the IRMC curriculum are working senior managers or prospective senior managers, who in practice, will likely have little hands-on interaction with information assurance technologies, we are finding that the lab experience greatly enhances their understanding of the theoretical aspects of information assurance technologies and provides a firm basis for their critical evaluation of the management-level considerations that they will face as information assurance managers or even chief information officers.

The use of technology in the classroom has become such a widely accepted practice in institutions of higher education, even at the graduate school level that, as one study put it, "the question for academicians is not whether we should or should not be using technology in our classrooms, but rather: How can we best use technology to improve learning outcomes"(McCallister, Matthews, 2001)? Another researcher has described technology tools as "becoming an inseparable part of good teaching" (Pierson, 2001).

A large body of research supports the relationship of the active involvement of the learner and greater learning, even in managerial programs. Joss (2001) states that the development of managerial capability involves acquiring both knowledge and experience. Other research concludes that learners retain only 10 percent of what they read and 20 percent of what they hear-but can retain 80 percent of what they experience personally and 90 percent of what they do and put into their own words (Linder, 2000). To quote the unattributed Chinese proverb, "I hear and I forget. I see and I remember. I do and I understand."

If anything, the use of technology in the classroom provides an alternative approach from the standard graduate school lecture and seminar format, while providing a meaningful exposure to technology (Brennan, Miller, Moniotte, 2001). And in fact, this alternative approach may be just what current and future information assurance managers need. The learning process has been depicted as a cycle involving four key activities: having a concrete experience, reflecting on what happened, conceptualizing the experience in terms of theory, and experimenting on ways to improve performance in similar future experiences (Kolb, Osland, Rubin, 1995; Raelin, 2000). Individuals tend to be predisposed toward one of these learning activities, yet effective learning is seen to require engagement in all four (Kolb et al., 1995, Raelin, 2000). Even faculty members possess the same predispositions, and generally fail to include all four in their courses (Watson, Temkin, 2000).

Information technologies of all kinds are cited as particularly well suited for a learner-centered or active learning paradigm (Albright, 1996). Some would even go so far as to say that action learning, namely the experience itself, even when not orchestrated or interpreted by professors, can be a powerful instrument for developing students (Casey, Pearce, 1977).

Perhaps the most focused articulation of the case for the inclusion of technology in the curriculum, and an accurate summation of our approach at IRMC, comes from the Gartner research organization:

> Technical training for managers needs to focus on providing a foundation for making technical decisions on architectural and design issues, based on input from a variety of internal and external sources. This

> training should be designed to enhance the manager's ability to make decisions about technology strategy – not to teach all the technical details that enable the manager to micromanage (Dallas, 2001).

It is with these principles in mind that we have undertaken to enhance the learning outcomes of our graduate-level students in information assurance by establishing the National Defense University Information Assurance Laboratory.

The IRMC IA Curriculum "Pre-Lab"

The ESS and AII courses within the curriculum focus respectively on the enterprise level and national/global level policy, planning and management aspects of information assurance. Consequently, there has been no real need for any extensive use of technology in the form of demonstrations or hands-on activities within these two courses.

Technology demonstrations have been a mainstay of the CST course, including a field trip for resident students to the nearby Naval Research Laboratory, where students observed demonstrations of some of DOD's most cutting-edge technologies. Several demonstrations of items such as wearable computers, wireless devices, and immersive virtual reality have also been a part of this course.

Prior to the formation of the IA lab, some form of technology had been previously used in the SEC course, also in the form of demonstrations by the instructor. These earlier demonstrations included a "hacking lab", where one or two instructors demonstrated several freely available hacker programs on a small, four-workstation laptop PC network, which was mounted on a wheeled cart, and rolled into the classroom. While students were usually appreciative of the opportunity to actually observe some of these hacking programs in operation, the artificiality of the classroom environment was magnified by the fact that only one laptop from the demonstration was able to be projected on the classroom screen at one time. Thus, the instructors had to use a video switching device and continuously switch between machines to show the class what was happening. Typically, at the end of the demonstration, the students would ask for the hacking lab cart to remain in the classroom so that those who wished to could try out some of the functions on their own.

Another demonstration previously conducted in the SEC course was the biometrics technology demonstration. Once again, this demonstration consisted of a laptop on a wheeled cart that was rolled into the classroom for a brief, instructor-conducted demonstration of several biometric technologies. Due to the relative simplicity of enrolling an individual into a biometric-based security environment, student volunteers were often used to demonstrate the utility of these technologies. However, in a class of normally twenty students, and given the length of the instructional period, only two or three students were normally able to participate in the demonstrations, while the rest of the class observed the demonstration on the projection screen.

When the SEC course is presented as an elective course to the other colleges of NDU (National War College and the Industrial College of the Armed Forces), as well as for IRMC's own Advanced Management Program, actual classroom hours become even

more constrained, with the result that these few demonstrations mentioned must be eliminated.

Surveying the need for an IA Lab

As the technology of information assurance continues to rapidly evolve, IRMC faculty have continued to update the curriculum, particularly in the most "tech-heavy" course, SEC. Where once straightforward classroom discussions of topics such as computer viruses, or worms, or other malicious code were conducted, backed by easy to understand PowerPoint graphics, the evolution of these threats to information security has become so complex as to defy simple explanation and illustration. Likewise, discussion of topics such as firewalls, intrusion detection systems, and virtual private networks (VPN) have required updating. The topic of firewalls, for example, has evolved from a theoretical discussion of packet filtering to the inclusion within the curriculum of discussion of multifaceted products that provide packet filtering, proxy, and stateful inspection firewalling, as well as intrusion detection and VPN capabilities.

From a practical perspective, an increasing percentage of students also have become interested in discussing the relative merits and shortcomings of actual products and vendors within the various technical sectors of information assurance. An increasing number of students in each SEC course come to the college with working experience in some aspect of information assurance. For these students, basic theoretical discussions of technology do little to advance their understanding of the topic. These students are interested in hearing from their peers what works and what doesn't in the real world. While the faculty does not endorse any particular products or vendors, such discussion seems to prove beneficial, especially when it comes to enhancing the understanding of the roles of the various technologies in an overall information assurance program, and the important considerations for management-level personnel, such as the IRMC student body.

These two trends, increasing complexity in threats and technical defensive measures, as well as an increasingly sophisticated student body, pose a dilemma to the faculty: how do we cover the basics mandated by the certificate program, while keeping the curriculum timely and relevant to a student body with a wide range of experience.

Our methodology for resolving this dilemma has been to consider a broader approach to information assurance education. A laboratory environment provided an approach that could offer a technologically relevant educational environment while at the same time assisting the information assurance novice in understanding basic concepts, and allowing the more experienced student to explore advanced concepts. As we undertook to plan for possible building and implementation of the Information Assurance Lab, we thought it best to validate some of the considerations for its construction and operation by conducting a survey of the students. A brief (seven question) survey was developed and validated by the SEC course manager, the demonstration instructor, and the department chair.

Two consecutive offerings of the SEC course were surveyed. Each course consisted of twenty students. Each saw the "hacker lab" and the biometrics demonstrations during the course, as described earlier. The surveys were voluntarily completed on the final day of class along with the normal IRMC end-of-course student

survey. Identical survey questions were used for both classes. An analysis of the completed surveys showed similar responses to each question. The following analysis is therefore based upon the composite results of the two surveys conducted.

The first question asked: "Which of the following best describes your general outlook on the use of technology in this course?" The responses occurred as follows:

Table 1: Question 1

Keep the computers out and give me more PowerPoint	Show me demonstrations	Allow me or some of my classmates to participate in demonstrations	Let us interact with the technology in group exercises	Provide each individual student with the opportunity to perform exercises with the technology
2.2%	33.3%	13.3%	26.7%	24.5%

The responses were nearly evenly split between those who wanted to either see demonstrations or voluntarily participate in some demonstrations, and those who wanted to interact with the technology in either group or individual exercises. Only a small percentage wanted no technology used. Our conclusions from this data were that the students felt that technology definitely had a place within the classroom in the SEC course, and that a significant number of students believed that they would benefit from some interaction with the technology.

The next four questions were closely related. The questions, in sequence, asked students to select technologies that they would like to see in demonstrations (question 2), participate with in demonstrations (question 3), perform group exercises with (question 4), and perform individual exercises with (question 5). The list of eight technologies was identical for each question and consisted of biometrics, firewalls, intrusion detection systems, public key technologies, virtual private networks, anti-virus technologies, hacker-ware (simple level), advanced hacker techniques, and other. Students could select as many responses for each question as they wanted. The following table depicts responses to questions 2 through 5:

Table 2: Questions 2-5

	Biometrics	Firewalls	IDS	PKI	VPN	Anti-virus	Hacker-ware (simple level)	Advanced Hacker Techniques	Other
Question 2	44.4%	53.3%	60%	64.4%	44.4%	26.7%	37.8%	57.8%	5%
Question 3	33.3%	33.3%	37.8%	44.4%	24.4%	13.3%	22.2%	35.5%	0
Question 4	17.8%	33.3%	40.0%	42.2%	28.8%	13.3%	17.8%	28.9%	0

Question 5	28.9%	22.2%	24.4%	35.5%	17.8%	8.9%	17.8%	26.7%	0

Perhaps not surprisingly, students responded that they would like to see demonstrations (question 2) of nearly everything. The most popular technologies for demonstrations were public key technologies, intrusion detection systems, advanced hacker techniques, and firewalls. Biometrics and virtual private network demonstrations were also supported by a significant percentage, while simple hacker-ware and anti-virus technologies were the least desired for demonstrations.

Student willingness to participate in demonstrations (question 3) was somewhat less than their desire to simply view the demonstrations, although the popularity of technologies remained relatively consistent. Public key, intrusion detection and advanced hacking led the way once again, followed closely by firewalls and biometrics. Simple hacking and anti-virus technologies drew minimal support.

When asked about their choices for technologies to participate with in group exercises (question 4), student responses were nearly identical to the previous question. Public key, intrusion detection, firewalls, advanced hacking and VPN all showed a fairly strong support. Simple hacking and anti-virus trailed in popularity. One notable difference was in biometrics, where the percentage of students wanting to participate in group exercises dropped significantly in comparison to the other technologies.

As for participation in individual exercises (question 5), student willingness basically dropped across the board, with the exception of biometrics, where a greater number of students responded that they would like this level of interaction with the technology rather than for biometrics group exercises. Even so, public key technology led the way for individual exercises

Based upon these results to questions two through five, we have concluded that a significant percentage of students desire some level of interaction with six of the eight technologies surveyed. Anti-virus and simple hacking technologies are least desired for interactive learning, while public key technologies, intrusion detection, firewalls, VPN, biometrics and advanced hacking techniques are technologies with which students desire interaction.

Students seemed to recognize the individualized nature of the use of biometric technologies in information assurance as evidenced by their stronger support for individual, as opposed to group exercises with that technology.

Public key technologies received the strongest support for all forms of interaction. Anecdotal information from various faculty members who teach public key technology topics indicates that this is one topic where, through simple lecture and slide presentation, most students either quickly understand the technology or struggle with it. In one singular instance from our Advanced Management Program, where the timing permitted an SEC elective class to perform a public key technology exercise (installing and using PGP), several students came away from that event declaring that they now finally understood the basics of public key technology.

Question six of the surveys asked students to categorize the general level of instruction of the SEC course, notwithstanding the demonstrations presented, on a five-part scale. The results were as follows:

Table 3: Question 6

Much too technical for your level of job responsibility	A little more technical than you need for your job/career	About right in technical level for your job/career	Not quite technical enough for your job career	Much too non-technical for your job/career
0	2.6%	57.9%	34.2%	5.3%

This data indicates to us that the level of technical instruction in this graduate-level course is on track, although the data also supports an observation of a trend in increasing technical sophistication among our student population, as shown by the "not quite technical enough" response by just over one third of those surveyed.

The final question of the survey (question 7) was addressed specifically to those students whose response to the previous question indicated that they felt the SEC course needed to be more technical in nature. The question requested students to describe in narrative form what subject matter shortcomings of themselves and their classmates that they perceived would hinder a more technical level of instruction. Student comments basically centered around the wide range of technical skill levels within the class and the impact that this would have on the quality of the instruction, given the amount of time available. A sample of the comments includes "time might be a limiting factor", "Instructor would have to be sure everyone was on the same page", and "[I] have no technical background at all"

From these and other comments we conclude that our students correctly recognize that technology should play a role in their education, but within the proper context of the management-level curriculum.

Building the Lab

Having sensed and measured the need and value of an information assurance laboratory, we set out to begin the development of the NDU Information Assurance Laboratory and insertion of exercises into various elements of the curriculum. This mission has been undertaken with the following principles in mind:

- Utilize technology in the classroom to enhance lecture and seminar discussion
- Show real, current technology in the lab; expect to turn over technologies rapidly
- Demistify the technology to the greatest extent possible by making the whole lab network visible; no hidden cabling or terminations into wall jacks
- Work in groups; students for the most part prefer this anyway
- Keep exercises simple and in support of larger learning objectives; we are conducting graduate level education, not tech school training
- Make the whole thing portable; we can make better use of our limited space and also deliver instruction and workshops "on the road"

We decided to build a lab that provided a general diversity of platforms into

which we could insert a variety of technologies. Thus our lab includes UNIX (Sun Solaris) and Linux (Red Hat) servers, MS Windows 2000 servers, Windows NT servers, and Windows 95, 98 and XP workstations. Interconnection is currently provided through 3Com hubs, while a CISCO router and a CISCO switch are available to become a part of the network. A CISCO PIX firewall appliance is also available to become a part of the configuration. Currently the network is in a standalone configuration with no external connectivity to the university network or the internet.

Students in the twenty-person class are organized into five groups of four. Each group works from a Windows XP laptop, with a secondary flat panel monitor to make viewing by all group members easier. Student workstations will be used for both attack and defense purposes.

A group of laptops consisting of two Windows NT servers, one Windows 98 workstation, and two Windows 95 workstations serves as the primary target machines for any attacking.

Two Windows 2000 servers, the Solaris and Linux servers, and an additional XP workstation are controlled by the instructor, and may play attack, defense or neutral roles. These servers and the primary target servers now host or may host web and email servers, and serve as domain controllers and as name servers.

In addition to the basic lab platforms, technical arrangements are being undertaken to permit the projection of all of the machines onto three large screen displays within the classroom, so that students can more easily view activity on servers, attack target platforms, and other student workstations.

The First Lab and Feedback

The first SEC course after the lab equipment was acquired and installed occurred in December 2001.

The first lesson in which it was used was a new form of the hacker demo. The lab exercise for this initial event was closely modeled after the demo, with students participating to perform the "hacks" themselves from their group workstations primarily against the NT, Win95 and Win98 target machines. Student exercises consisted of a combination of detection and analysis activities using some inherent operating system functionality, as well as the use of some highly scripted and command-line attack tools.

Several key observations were made during the conduct of this class. First, there was a very wide range of technical proficiency among the students. Given the configuration of the room and one laptop workstation per group of four students, the student who sat within easiest reach of the laptop keyboard became the defacto operator, assisted and advised perhaps by the individuals seated to either side, and usually observed only by the fourth member of the group, who was seated two places to either the left or right of the operator. Thus, the operator's ability to understand and execute directions from the instructor was a decisive factor as to whether the group worked through the exercise on pace with the instructor, or lagged behind. In some groups very minimal direction from the instructor was all that was necessary to launch the group on a new exploit, giving them time for repeated attempts, and extended discussion among themselves of the results. In other groups, basic instructions such as "open up a console and get to the C prompt" resulted in confusion and eventually required step-by-step

intervention by the instructor, i.e. “go to Start, then Programs, then Accessories, then Command Prompt” while leaning over the student operator’s shoulder and pointing to the screen.

As a result of this observation, in future hacker labs, instructors will make an attempt to balance the technical proficiency composition of the groups so that all groups can proceed at the same pace. Instructors will also encourage the more technically proficient members of each group to take control of the keyboard for more advanced hacking and guide other group members, while yielding control to less experienced group members for less difficult techniques.

Another related observation was that despite survey data indicating that large percentages of students preferred exercises with more advanced hacker techniques, the observations from this initial class indicate that few students may in fact be ready to perform such exercises. In fact, several students from this first hacker lab class requested, and were granted, additional lab time due to their lack of understanding of the basics covered in the lab. A few students requested additional lab time for performing advanced techniques, although none took advantage of the opportunity during the week.

The second lesson of this SEC course in which the lab was used was the Firewall and Intrusion Detection class. For this initial class, no additional lab time had been allotted to an already tight schedule, so the lab exercise had to be quick and effective in order to support the instruction.

Building on the students’ experience from the hacker lab two days earlier, students where first directed to scan the lab network using an automated tool and observe all of the hosts that were revealed. Next, students were introduced to the basic functionality of the Windows XP Internet Connection Firewall. By activating the firewall in its default configuration and then rescanning the network, students observed that all other student workstations had “disappeared”. Students then continued to experiment with permitting and denying various services and protocols, rescanning, and observing the results.

The students apparently found observations of this simple example of the configuration and utility of firewall technology useful. Several students commented that this was the first time that they had actually observed a firewall in action and that they felt they understood the principles of firewall technology better as a result. Students also better understood a key learning point of the relationship of information assurance policy (“we don’t want to allow our network to be pinged”) to technology implementation (“deny the ICMP echo request service at the firewall”).

At the conclusion of this SEC course, another survey on the lab was conducted. The first question was identical to that asked in the earlier surveys regarding the students’ general outlook on the use of technology in the class. In this survey, 72.2% of respondents indicated that they would like to interact with more technologies in group exercises and 27.8% indicated that they would like to perform individual exercises. Nobody indicated a desire to voluntarily participate in demonstrations, observe more demonstrations, or eliminate any use of technology in the class.

From this data, we conclude that the lab in general was a success for this class. Students clearly desire to get their hands on the technology at some level of interactivity. As a result, we will attempt to continue to adjust the SEC course to allow a sufficient amount of lab time for group exercises in as many technology-based classes as

appropriate. We will also attempt to make lab time available during non-class hours for students who desire to do additional individual work for both basic understanding and advanced techniques.

The next two questions again asked students to chose technologies that they would like to interact with in either group exercises or individually. The results were similar to the earlier surveys with biometrics, firewalls, intrusion detection, public key and VPN technologies again being the most popular in both responses. We will continue our plans to focus on introducing these technologies into the lab environment.

When asked the question about the technical level of instruction in the course, the student responses indicated an almost perfect balance. An overwhelming 83.3% indicated that the technical level was "about right" (up from 57.9% in the earlier surveys). Just 11.1% indicated that it was "a little more technical than you need" (up from 2.6% earlier), and 5.5% indicated that it was "not quite technical enough" (down from 34.2% previously). Since this was the first class surveyed following use of the lab, and taking into account the small population size (18) for this survey, the most notable shift that we can observe from the previous surveys appears to be away from where "not quite technical enough" held a substantial percentage in the earlier survey. Apparently the exposure to the lab satisfied the technology desires of some students who otherwise may have wanted more.

The remaining narrative responses to the questions of this survey indicated a general satisfaction with the group exercise format, with minor dissent, and a greater understanding of the subject matter gained through participation and observation in the lab scenarios.

Conclusions

From our experiences thus far, we conclude that hands-on interaction with the technical aspects of information assurance education in a graduate-level setting can prove beneficial to the students in several ways:

- By supporting instruction in the basics of information assurance technologies for those who lack first-hand experience, the lab environment can help to even the playing field for further discussions in class of management-level issues.
- Hands-on experience assists senior managers in understanding and correlating the input of various technical and non-technical subordinates.
- The lab provides an environment that demonstrates the necessity of information assurance policy to drive the requirements for technology solutions.
- The small group format of the lab allows students to participate in teaching as well as learning in a true seminar style.
- The lab provides a no-risk environment for these senior managers to experiment and learn within that they are unlikely to see back at their jobs.

Our intent is to continue to survey the students of future courses (7 more scheduled through August 2002). We will continue to develop and integrate lab experiences into the course, based upon the technology priorities indicated by the students, and we hope to present further research based upon our experiences in the future.

References

Albright, M. (1996, February 5). Speech delivered at the Southern Regional Faculty and Instructional Development Consortium, Baton Rouge, LA.

Brennan, Linda L., Miller, John R., and Moniotte, Susan M. (2001). Hearding cats to water: benchmarking the use of computers in business education. *Journal of Education for Business,* 76,(6), pp. 345-352.

Casey, D. and Pearce, D. (1977). More than management development: Action learning at GEC. New York: AMACOM.

Dallas, Susan (2001). *Training for IT Managers: Why Now?* The Gartner Group. Note Number: TG-13-2618. Retrieved on 8 January 2002, from http://www4.gartner.com/DisplayDocument? id=328761&acsFlg=accessBought

Joss, Robert L. (2001). Management. *Australian Journal of Management,* 26, pp.89-103.

Kolb, D. A., Osland, J.S., and Rubin, I.M. (1995). Organizational behavior: An experiential approach (6th ed.). Englewood Cliffs, NJ: Prentice Hall.

Linder, J. (2000). Old dogs, new tricks. *Outlook Anderson Consulting*, no. 1

McCallister, Linda. and Matthews, Linda. (2001). Electronic MBAs: The future is here. *S.A.M. Advanced Management Journal*, 66(1), pp. 41-47.

National INFOSEC Education and Training Program. Fort George G. Meade, MD. Retrieved on 8 January 2002, from: http://www.nsa.gov/isso/programs/nietp/newspg1.htm#Universities

National Security Telecommunications and Information Systems Security Committee. (1992). National Training Standard for Information Systems (INFOSEC) Professionals (NSTISSI No. 4011). Fort George G. Meade, MD: National Security Agency.

Pierson, Melissa E. (2001). Technology integration practice as a function of pedagogical expertise. *Journal of Research on Computing in Education*, 33(4), pp. 413-430.

Raelin, J.A. (2000). Work-based learning: The new frontier of management development. Upper Saddle River, NJ: Prentice Hall.

Watson, Carol, and Temkin, Sanford (2000). Just-in-time teaching: Balancing the competing demands of corporate America and academe in the delivery of management education. *Journal of Management Education*, 24(6), pp. 763-778.