Developing Security Competencies Through Information Assurance Undergraduate and Graduate Programs

Prepared for: NCISSE 2001, General Track

Prepared by: Mrs. Margaret K. Spanninger

BoozÆAllen and Hamilton Inc.
3190 Fairview Park Drive
Falls Church, Virginia 22042

e-mail: spanninger_margaret@bah.com
v-mail: (703) 289-5471
fax: (703) 289-5829

Abstract: This paper extends the current concepts of integrating information security topics within existing academic programs to actually establishing a new academic discipline for Information Assurance (IA). It explores the business drivers for such a program and the core body of knowledge required to establish a viable program of academic study in IA. Students of tomorrow should have the opportunity to pursue an IA degree at both undergraduate and graduate levels.

There are three basic business drivers for an academic program of study in IA. First, securing organizations from cyber attacks cannot be achieved without skilled and knowledgeable personnel at all levels of the organization. Second, private and public sectors are constantly challenged to hire skilled cyber security professionals with both specialized and broad cyber security capabilities. The marketplace is competing for a limited supply of cyber security professionals as demand for these professionals continues to rise. Third, organizations are challenged to bridge the gap between cyber security professionals and the workforce.

To this end, formal education is a critical component in establishing and maintaining an organization's security posture. It is a means of increasing the supply of cyber security professionals to meet increasing demand. Current academic programs have successfully integrated cyber security topics within the computer science domain to create a technical cyber security professional. However, colleges and universities have not addressed several topics that are needed to design, develop, implement and maintain managerial and operational cyber security controls that are required for an effective enterprise-wide IA program. The purpose of the proposed IA academic specialty is to provide a multi-disciplinary program to support a variety of managerial, policy, and business-related information security roles throughout the workforce. The program would complement existing academic programs in computer science and produce graduates who have a broad foundation in the full range of cyber security topics that compose Information Assurance.

Biography

Margaret (Marge) Spanninger is an Associate at BoozÆAllen and Hamilton Inc. where she leads the Risk Management Training Team of BoozÆAllen's Infrastructure Assurance Center of Excellence. She is graduated from West Virginia Wesleyan College with a B.S. in Accounting and from The George Washington University with an M.B.A in Information Systems Technology. Mrs. Spanninger has over 20 years of experience in technical and security training design, development and delivery. She has conducted security training for government clients that include Dept. of Energy, General Services Administration, and several agencies of the Intelligence Community.

Developing Security Competencies Through
Information Assurance
Undergraduate and Graduate Programs

INTRODUCTION

This paper extends the current concepts of integrating information security topics within existing academic programs to actually establishing a new academic discipline for Information Assurance (IA). It explores the business drivers for such a program and the core body of knowledge required to establish a viable program of academic study in IA. Students of tomorrow should have the opportunity to pursue a degree in IA at both undergraduate and graduate levels.

BUSINESS DRIVERS

There are three basic business drivers for an academic program of study in IA. First, securing organizations from cyber attacks cannot be achieved without skilled and knowledgeable personnel at all levels of the organization. Second, private and public sectors are constantly challenged to hire skilled cyber security professionals with both specialized and broad security capabilities. The marketplace is competing for a limited supply of cyber security professionals as demand for these professionals continues to rise. Third, organizations are challenged to bridge the gap between cyber security professionals and the workforce. The first part of this paper will address these issues.

All Employees Must Be Security Literate

The corporate need for IA cannot be met solely through information technology solutions. Organizations must have personnel at all levels that are skilled and knowledgeable in IA. At the Executive level, the CEO, CIO, CTO, and CFO must be knowledgeable about cyber security and the adverse consequences that could result from a security failure. Executives must understand the current status of their cyber security programs and controls in order to make informed decisions and investments to appropriately mitigate risks to an acceptable level. The corporate Manager of Security must posses a broad security foundation and a staff of cyber security specialists to address numerous cyber security issues. The system users must know their role and responsibilities for protecting corporate proprietary information. The goal is to protect corporate information as it exists in a variety of states and media. It includes tangible assets and intangible intellectual property.

Over the past few years, the American Society for Industrial Security, and recently in conjunction with PricewaterhouseCoopers, have surveyed *Fortune 1000* companies in manufacturing, high technology, financial/insurance, and services industries to produce a report, *Trends in Proprietary Information Loss Survey.*[1] This report underscores the need of corporate America to protect proprietary information. Key findings from the survey germane to this discussion are:

- "In 1999, Fortune 1000 companies sustained losses of more than $45 billion from thefts of their proprietary information.
- Forty-four companies of the total 97 that responded reported a total of over 1,000 incidents of theft. Of these, 579 incidents were valued with a total estimated loss of

[1] http://www.pwcglobal.com/extweb/ncsurvres.nsf/DocID/36951F0F6E3C1F9E852567FD006348C5

nearly $1 billion. The average company responding reported 2.45 incidents with estimated losses per incident of over $500,000. The vast majority of the reported incidents were in High Technology (530) and Services organizations (356). Although Manufacturing reported only 96 incidents, the acknowledged losses of manufacturing companies accounted for the majority of losses reported in the survey, and averaged almost $50 million *per incident.*

- The global Internet and proliferation of information systems have significantly increased the risks to corporate proprietary information.
- The majority of companies responding to the survey have not effectively met the challenge of providing a framework in which to safeguard proprietary information."[2]

This survey supports the position that security continues to be a significant issue for corporate America and that although progress is being made, there is still so much more that needs to be done.

The cyber security needs of the Federal government are also growing at an accelerated rate. It is well documented that IA is a national priority cyber security has been on the General Accounting Office (GAO) high-risk list since 1997 when they noted that "growing evidence indicated that controls over computerized federal operations were not effective and the related risks were escalating."[3] With expanding connectivity and use of the Internet by the Federal workforce, it is evident that threats continue to increase while the government's ability to respond has not kept pace. In January 2000, the President issued the National Plan for Information Systems Protection [4] that identified 10 new programs that would be funded to strengthen the nation's cyber security posture. The programs were instituted to achieve two broad goals: to establish the U.S. Government as a model for information security, and to develop a public-private partnership to defend our national infrastructures. The broad scope of programs that were identified in the plan highlight the need for security within every Federal agency.

Although many improvements have been made, the GAO's high-risk report released January 17, 2001 states, "Critical operations, assets, and sensitive information gathered from the public and other sources continue to be vulnerable to disruptions, data tampering, fraud, and inappropriate disclosure."[5] Another GAO report states, we "have made scores of recommendations to agencies regarding specific steps they should take to make their security programs more effective. Most agencies have heeded these recommendations and taken at least some corrective actions. However, more needs to be done, especially in the area of security program management, which continues to be a widespread and fundamental weakness."[6] In all Federal agencies, cyber security program planning and management is critical to selecting appropriate and effective cyber security controls. The documented deficiencies in this area are widespread and remedies

---

2 American Society for Industrial Security International and PricewaterhouseCoopers. *Trends in Proprietary Information Loss Survey*, October, 1999, p. 3.

3 U.S. General Accounting Office, Performance and Accountability Series. *Major Management Challenges and Program Risks, A Governmentwide Perspective (GAO-01-241),* January 2001, p. 19.

4 Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to Dialogue, released January 7, 2000, The White House.

5 Op Cite, GAO-01-241. p. *19.*

6 U.S. General Accounting Office, Report to the Chairman, Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives. *INFORMATION SECURITY Serious and Widespread Weaknesses Persist at Federal Agencies. (GAO/AIMD-001-295),* September 2000, pp. 2-3.

are urgently needed. A more knowledgeable workforce would expedite the resolution of these issues and reduce the operational risks for many systems within the Federal domain.

The October 2000 Defense Authorization Act, Public Law 106-398 includes Title X, Subtitle G, the Government Information Security Reform Act addresses some of the cyber security deficiencies reported by GAO. The Act primarily addresses program management and evaluation aspects of cyber security. Requirements for both unclassified and national security programs include:

- annual agency security program reviews;
- annual Inspector General (IG) evaluations;
- agency reporting to OMB on the results of IG evaluations for unclassified systems and audits of IG evaluations for national security programs; and
- an annual OMB report to Congress summarizing the materials received from agencies.

Once again, these requirements underscore the need for a security-knowledgeable workforce at all levels of the Federal government.

Security Professionals Are In Short Supply

The second business driver for establishing an academic program of study in IA is that private and public sectors are constantly challenged to hire cyber skilled security professionals with both specialized and broad security capabilities. The marketplace is competing for a limited supply of IT and security professionals while demand for these professionals continues to rise. A study released by the Information Technology Association of America (ITAA) in April of 2000, stated, "There are more than a million good reasons to consider a career in the Information Technology (IT) industry today. That's because employers will create a demand in this country for roughly 1.6 million IT workers this year. With demand for appropriately skilled people far exceeding supply, half of these positions 843,328 will likely go unfilled." [7] The numbers in this study do not include jobs in government, non-for-profit organizations or small entrepreneurial firms. Clearly, demand for IT workers is large and growing! "According to Al Decker, CEO of information-security consultancy Fiderus, the U.S. alone will face a shortfall of between 50,000 and 75,000 security professionals in the next few years."[8] Mike Rothman, CEO of SHYM Technology, a maker of secure-digital-certificate software, states "There is generally a lack of good talent and skills across all technological specialties. It is especially acute in information security."[9]

The American Electronics Association (AeA) released a study in January 2001 that indicates that despite significant layoffs of dot-com and technology workers over the past eight months, skilled IT workers remain a scarce commodity. "Scarcity of qualified candidates, competition from high profile employers, and the potential for IT professionals to earn more as independent contractors were sited as the top barriers to recruiting IT workers."[10] The AeA CyberEducation Report[11]

---

7 Information Technology Association of America. *Bridging the Gap: Information Technology Skills for a New Millennium*. April 2000.

8 Salkever, Alex. BW Online, *Wanted: More Schoold for Security Pros*. November 28,2000.

9 Ibid.

10 American Electronics Association. AeA News Release:*AeA's 2000 Information Technology Workforce Survey Focuses on Job Attraction and Retention Techniques*. January 2001.

released in 1997 clearly shows that the number of computer science and electrical engineering degrees has declined over the last 10 years, and that of the total number of high-tech degrees that are being conferred, the percentage of degrees awarded to foreign nationals is growing. "Although all current projections anticipate tremendous growth and job creation in most of the high-technology sectors, the current labor pool of qualified workers is at best stagnant, and in some cases, shrinking. As the demand for technology workers and knowledge workers from key academic disciplines has grown stronger, the number of graduates in key technology disciplines has declined in many technical disciplines."[12] Although these studies indicate significant shortages of high-tech workers, the outlook for cyber security professionals is far worse. Today's cyber security professionals compose a fraction of the IT workforce. "Although precise figures for spending on information security education are hard to come by, the handful of U.S. academic programs with an information security emphasis turn out fewer than 200 graduates a year, and at the current rate, demand for security experts will vastly outstrip supply. Only 14 universities have been recognized for information security expertise by the National Security Agency. But some of those schools don't even offer an official curriculum in information security."[13]

In May of 1997, *InformationWeek* reported that information security professionals were in short supply based upon a Computer Security Institute (CSI) survey that addressed the need for more information security workers. Jose Grando, the manager of Ernst & Young's information systems assurance and advisory service stated, "The information security field is very young, and it can be difficult to find folks who have real, practical experience."[14] The survey indicated that an 18% increase in information security workers was expected. "The 340 organizations responding to the CSI survey averaged one information security specialist for every 1,600 employees. In contrast, these companies had 11 employees dedicated to physical security, and 56 information security professionals for every 1,640 workers.[15] In the 1999 Global Information Security Survey[16], conducted by PricewaterhouseCoopers LLP and *Information Week*, it was reported that 33% of companies with more than $500 million in annual revenue were spending less than $100,000 a year on security, including staffing, consulting, and technology. Overall, however, the survey showed that most companies were spending more on security than they did in the prior year. More recently, in September 2000, ComputerWorld noted that finding the right person to oversee an organization's information security efforts is not easy because of the significant shortage of knowledgeable candidates.[17]

The shortage of qualified IT and information security workers has been felt by the Federal government as well. The 1997, U. S. Department of Commerce, Office of Technology Policy, published *America's New Deficit: The Shortage of Information Technology Workers*. The report indicates that the education pipeline is trickling while demand is exploding. As the shortage of security professionals becomes more acute, recent steps have been taken to bolster the cyber security corps of the Federal government. In January 2000, $25 million in funding was provided for the Federal Cyber Services Training and Education Initiative. The initiative has five

---

11 American Electronics Association. CyberEducation Report, America's High-Tech Workforce: Supply of Workers not Satisfying Industry Demand. 1997.

12 Ibid. p. 7.

13 Op Cite. Salkever.

14 Wilde, Candee. *InformationWeek*, "Hunt for Security: Information Security Pros aren't easy to come by." May 26, 1997.

15 Ibid.

16 Larsen, Amy K., *Information Week*, "Global Security Survey: Virus Attack." July 12, 1999.

17 Radcliff, Deborah. *Computerworld*, "Wanted Security Superman." September 25, 2000.

programs that address the shortage of cyber security professionals. Specifically, the Scholarship for Service program enables the government to attract and retain people to fill IT security positions.

Every Employee Has a Security Responsibility

The last business driver that I will address is one that challenges virtually every type of organization and industry. It is the challenge to bridge the gap between security professionals and the workforce. An enterprise-wide IA program involves all employees. Each employee must be cognizant of his/her security responsibilities and sufficiently trained to perform them. Organizations must bridge the gap between cyber security professionals and all levels of management, cyber security professionals and IT professionals, and between cyber security professionals and system users. Management must realize that not only are technical skills needed, but non-technical qualifications, such as the ability to assess risk, develop information security procedures, write policy statements, and educate employees are just as important. Securing information must be an organizational priority and as such, security practices must be totally integrated with the numerous business processes of an organization.

On the technology front, as the world economy moves to e-business, the need for IT specialists to be more skilled and knowledgeable in the implementation of cyber security controls, practices and procedures has become more critical. In both public and private sectors, security is still a subordinate duty that suffers from neglect as technicians are more focused on system performance and strive to keep the systems up and running and the users happy.

On the user front, there is much to be done to bridge the security gap. In general, users want to do what is right, but they often don't know what that is. Whether it's using weak passwords, monopolizing bandwidth by playing music via the Internet, or spamming co-workers, users play a crucial role in protecting the information resources of an organization. As long as people are in the security equation, they will pose the biggest threat to critical system resources. Ignorance should not be an excuse for putting an organization's information assets at risk. Awareness programs can be extremely effective in combating user-related security issues and bridging the gap between security professionals and users, yet they are rarely funded in any organization.

CERTIFICATIONS BOLSTER SUPPLY

In response to the explosive demand for cyber security expertise, a number of professional societies have developed certifications in or relating to information security. The common cause was to identify "competent professionals" in information security or related professions. The common goal is to raise the bar in terms of minimum cyber security competencies and demonstrated proficiency in the field. Although the requirements for certification are vastly different, there is some commonality among the programs. Let's wade through the alphabet soup of professional certifications.

For starters, there's the ASIS CPP program. ASIS is the American Society for Industrial Security and CPP is a Certified Protection Professional. This program is the granddaddy of all programs. It began in 1977, when information security was less focused on technical solutions and more interested in managerial solutions. There are almost 4,000 current CPPs, which are about 44% of total ASIS membership. The program has evolved and there are seven domains of knowledge: security management (38% of certification test), physical security (19% of test), investigation (15% of test), personnel security (9% of test), legal aspects (7% of test), and protecting sensitive

information and emergency management (each is 6% of test). To sit for the exam, candidates must have nine years of relevant experience with at least three of those years in a position responsible for some aspect of security. If the candidate has a Bachelor's degree, the experience requirement is reduced to seven years. Re-certificatoin is required to promote professional development and requires nine maintenance credits within three years. The goal of the CPP is to certify "competent professionals who can effectively manage complex security issues that threaten people and assets of corporations, governments, and public and private institutions."[18]

The next professional certification is the CISA from ISACA. This is the Certified Information Systems Auditor program sponsored by the Information Systems Audit and Control Association. The CISA has been available since 1978. Last year, 6,458 people took the exam and 52% passed. Over the last five years, the number of applicants has been rising 20% per year and the annual passing rate has been 50 — 51%.[19] The exam covers process and content specific to the information systems (IS) auditor job function. The seven domains of knowledge for CISA are: the IS audit process (10% of test); management, planning, and organization of IS (11% of test); technical infrastructure and operational practices (13% of test); protection of information assets (25% of test), disaster recovery and business continuity (10% of test); business application system development, acquisition, implementation, and maintenance (16% of test); and business process evaluation and risk management (15% of test). Certification requirements include: passing the exam, a minimum of five years professional IS auditing, control, or security work experience (or a combination of experience and college degree or credits), compliance with the ISACA Code of Professional Ethics, and continuing education. The continuing education requirement is for 120 contact hours during a fixed 3-year period with a minimum requirement of 20 contact hours in any given year.[20]

The next program is the CISSP from $(ISC)^2$. The International Information Systems Security Certification Consortium was established in 1989 as an independent, non-profit corporation whose sole charter is to develop and administer a certification program for information security practitioners. They developed the Certified Information Systems Security Professional program and have certified over 3,000 security professionals over the last four years. They have recently established a System Security Certified Practitioner (SSCP) program as well. The CISSP covers 10 domains of knowledge: access control; computer operations security; cryptography; application program security; risk management and business continuity planning; communications security; computer architecture; systems security; physical security; policy, standards and organization; and law investigations and ethics. Applicants are required to subscribe to the $(ISC)^2$ Code of Ethics, have three years of direct work experience in one of the 10 domains, and to pass the test. CISSP requires 120 hours of continuing professional education, 80 related to information security and 40 in other professional development activities, over a three-year period for re-certificatoin.[21]

Finally, we have the SANS GIAC programs. SANS is the System Administration, Networking, and Security Institute. They recently began to offer training and certification programs through their Global Incident Analysis Center. Unlike the other programs that rely heavily on experience, the GIAC programs have a well-defined curriculum to support the certification process and provide practical application activities. It has foundation training through the

---

18 http://www.asisonline.org/ [click on Certified Protection Professional].

19 Statistics provided by Christen Gunning of ISACA, March 2001.

20 http://www.isaca.org

21 http://www.isc2.org

Information Security KickStart course that provides systems knowledge and skills for the novice security practitioner and LevelOne security essentials to introduce and reinforce security concepts through demonstrated practical application of security knowledge. There are six LevelTwo modules that provide specialized instruction in firewalls, perimeter protection and VPNs; intrusion detection in depth; advanced incident handling and hacker exploits; securing Windows; Securing UNIX; and auditing information systems. Certifications are available to students who have completed practical assignments and the tests can be taken online whenever the student is ready. This year, GIAC is starting to make the certifications available to anyone who wishes to take the exam, independent of SANS GIAC training.[22]

This trend toward the professionalization of cyber security via certifications is desperately needed. Security is becoming a viable career path as organizations realize the importance of security in maintaining a competitive edge in today's dynamic markets and in protecting the bottom line. However, of the certification programs that exist, only GIAC offers substantial training in any of the domains of knowledge. The others are focused on certification. The "review" sessions that are offered to help candidates pass the exam are not focused on education. They provide insight into the test and what is expected. This level of detail and knowledge will not help the novice, nor help those who wish to enhance and augment their skill set. As demand for cyber security professionals continues to surge, it is apparent that we must do more than offer on-the-job training to our security workforce who currently learn information security through ad-hoc, unstructured activities. We must provide a means for employees to gain the required knowledge and skills through higher education. An academic discipline in IA would support the professionalization process and could also provide opportunities for students to gain significant experience as they complete their academic course of study.

AN ACADEMIC PROGRAM OF STUDY IN INFORMATION ASSURANCE

With these business needs and the push for professionalization of the cyber security career field, it is apparent that formal education is a critical component in establishing and maintaining an organization's cyber security posture. It is a means of increasing the supply of cyber security professionals to meet increasing demand. In general, current academic programs have successfully integrated cyber security topics within the computer science domain to create a more technical security professional. However, colleges and universities have not addressed several topics that are needed to design, develop, implement and maintain managerial and operational security controls that are required for an effective enterprise-wide IA program. The purpose of the proposed IA academic specialty is to provide a multi-disciplinary program to support a variety of managerial, policy, and business-related cyber security roles throughout the workforce. The program would complement existing academic programs in computer science and produce graduates who have a broad foundation in the full range of security topics that compose Information Assurance. The remainder of this paper is devoted to an assessment of where we are today and what is needed tomorrow for establishing a viable framework for providing undergraduate and graduate degree programs in Information Assurance.

Current State of Affairs

There are only 14 universities that have NSA approved curricula in IA. The IA courses are generally offered as a specialization to an MS or PhD in Computer Science. Only a handful of these schools offer MBAs or Certification programs. An article in *BusinessWeek online*,

---

[22] http//www.sans.org

November 28, 2000, titled "Wanted: More Schools for Security Pros" laments that there are so few schools with academic programs with an emphasis on IA and that the few programs that do exist turn our less than 200 graduates a year. Of the schools that do have IA programs in place, recruiting and retaining qualified professors is an enormous challenge.

A New Academic Discipline

The basis for an academic program in IA exists among government training standards and guidance, professional organizations that currently offer security certifications, and industry best practices in cyber security training and education. It is only through the combined efforts of these organizations that significant progress can be made in addressing and alleviating the severe shortage of cyber security professionals.

There are fundamental cyber security concepts that establish a foundation for training and education. Within the Federal government, there are two primary standards and guidance documents that identify content that is required for cyber security training and education. The National Institute of Standards and Technology Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model* (NIST SP 800-16) presents a thoroughly documented model for cyber security training and education. The National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4011, *National Training Standard for Information Systems Security (INFOSEC) Professionals* identifies minimum course content for information systems security professionals. In combining the content specified in these documents we can define a core body of knowledge (CBK) that is key to role- and performance-based cyber security training and education. The CBK from these sources is comprised of the following topics:

- Laws and regulations
- IT security program
- System environment
- System interconnection
- Information sharing
- Risk Management
- Life Cycle controls
- Management controls
- Operational controls
- Technical controls
- Awareness, training, and education
- Handling sensitive and classified information

These topics are the building blocks that establish the foundation for a successful and relevant IA program of academic study.

To compliment the CBK defined in NIST SP 800-16 and NSTISSI 4011, ASIS, ISACA, and $(ISC)^2$ have worked with professional testing organizations to develop their certification exams. ASIS has developed role delineation and job analysis surveys to identify specific security tasks that are performed through various roles. ISACA has developed the CISA Practice Analysis that identifies security tasks and the knowledge required to perform the tasks for several domains of knowledge. These task analyses are invaluable sources of information in identifying what skills are needed in the workplace and what knowledge is required to perform the skills. This information could be adapted to an academic program of study in IA.

Another source of IA expertise in education can be found in a handful of training organizations such as the Computer Security Institute (CSI), the Management Information Systems Training Institute's (MISTI) Information Security Institute, and SANS. These organizations represent industry best practices in cyber security education. These organizations have discovered a niche market in providing cyber security training and education. They have responded to the needs of the marketplace by offering cyber security courses, seminars and conferences. The courses they

offer address both technical and managerial aspects of security programs. The SANS training program and recently developed GIAC program were developed through community consensus. These programs establish a foundation and support specialized training in technical solutions. Partnerships between these organizations and academia would provide immediate returns. Offering these courses for college credit would broaden their appeal and allow one more avenue for students to take on the road to becoming a cyber security professional.

Professional certification programs can assist in the definition, development and delivery of academic programs in two important ways. First, practicing security professionals have identified essential domains of security knowledge and created training materials to support the domains. These existing materials could certainly "jump-start" an academic program of study in IA. Second, as there is a shortage of qualified professors, certified professionals should be encouraged to teach college and university courses for credits toward re-certification. This would provide valuable expertise in the classroom and allow students to benefit from real world lessons learned.

It is commonly known that there is no environment in greater need of cyber security than that of colleges and universities. By fostering open systems for research and sharing information, universities provide a fertile environment for hackers to exploit. Academic programs that require practical application of what is learned could bolster security initiatives on campus and through work-study programs provide resources that would otherwise be unavailable. Providing supervised activities for students to learn and apply what they learn in an academic environment would significantly enhance the learning experience and make the students more valuable to the workforce.

With these many programs and resources, I believe academia can design and develop both undergraduate and graduate programs in IA. With the wide range or topics that compose IA it is conceivable that in addition to the programs already in place, programs of study can be developed to support BA, BS, MA, MS and PhD degrees in IA. These programs should be designed to take a novice and guide him/her through appropriate courses to graduate both generalists and specialists in IA. The programs should not only provide the knowledge and concepts that support the security discipline, but also provide hands-on training in defending and securing the campus environment. Clearly all facets of security would be needed for such an undertaking and significant benefits could be achieved for all parties involved.

An Approach

Using the NIST SP 800-16 model as a template, universities can build a program of study to accommodate the different types of courses that are required. First, there are concept courses that target the novice. They establish a foundation for further discussion and learning. Next, an enterprise-wide security context must be established to provide a macro view of the components that compose a corporate/government security program. At a minimum, the relationships among the components and how the components are integrated into a total solution should be identified. From here, I suggest two tracks a management based program of study and a complimentary technology based program. Each track should support both generalists and specialists.

The cyber security management program of study will focus on the management controls that must be implemented in an enterprise-wide cyber security program. In managing a cyber security program, requirements are identified, solutions are implemented, and periodic reviews take place to assess the "reality" of the environment. A reconciliation process occurs as reality is

evaluated against the requirements and deficiencies are discovered. It is a process that must be documented and understood because what takes years to build can be compromised in seconds. Cyber security management is the linchpin to the security solution. The program of study for cyber security management is comprised of the following topics:

- Security Planning
- Security Management
- Risk Management
- Legal Aspects & Ethics
- Security Policy
- Risk Assessment
- Personnel Security
- Investigations
- Physical Security
- Emergency Management
- Disaster Recovery
- Rules of Behavior
- Protecting Sensitive Information
- Security Audits
- Security Integration with Corporate Business Processes

The technology-based program of study will focus on the technological controls that are an integral part of the security solution. The technology controls help enforce security policy. The program of study for security technology is comprised of the following topics:

- Security Architectures
- System Vulnerabilities
- System Development
- Applications Development
- Configuration Management
- Cryptography
- Access Control
- Identification and Authentication
- System Audit and audit data analysis
- Intrusion Detection
- Anti-Virus
- Telecommunications & Network Security
- Computer Operations Security
- Firewalls
- Incident Response

These lists represent topics that support the identified programs of study and are not exhaustive, nor all-inclusive. With the wide range of topics, it is easy to identify 30 to 45 credits for a major in an undergraduate program of study and 30 to 45 credits for a graduate degree that is completely focused on IA. It would also be possible for a student to major in computer science and minor in IA at the undergraduate level.

Meeting the Challenge

With all this said, progress cannot be made without cooperation and attention from academic, corporate, and government organizations. In January of this year, 19 of the nation's leading high tech companies formed the not-for-profit Information Technology Information Sharing and Analysis Center (IT-ISAC) to cooperate on cyber security issues so we are better prepared to respond to threats and to minimize the impact of major incidents. We need this same level of commitment and investment for security education. Universities must extend their reach and partner with security professional organizations and cyber security training specialists to further develop their programs and to augment their staff. As many professors are lured away from the classroom by corporate salaries, perhaps universities can seek federal grants or corporate endowments for cyber security positions. As there are not enough cyber security professionals to go around, reaching back to academia puts many programs at risk. To mitigate this risk, universities could adopt the government's Scholarship for Service programs for PhD candidates. This program could specify a fixed period of service or allow for academic service in lieu of payback. Expanding academic programs in IA has many challenges and we must continue to look for ways we can leverage existing business and government resources to the academic sector. If we do not succeed in these efforts, we will not be able to fill a critical gap in the workforce of today and into the future.