A MODEL PROGRAM IN INFORMATION ASSURANCE AND COMPUTER SECURITY

Dr. Terry Dennis, Illinois State University, terry.dennis@dsu.edu
Dr. Omar El-Gayar, Dakota State University, omar.el-gayar@dsu.edu
Kevin Streff, Dakota State University, kevin.streff@dsu.edu

ABSTRACT

With the ever-growing demands to better prepare information assurance professionals, this paper presents a model for IA and information security program development and outlines the Dakota State University Information Assurance Program. The program includes graduate and undergraduate components, emphasizes industry alliances, and engages in outreach programs. The programs at Dakota State can serve as model IA curriculum for other institutions.

Keywords: Information assurance education; Computer security education

INTRODUCTION

September 11, 2001 catalyzed the nation, bringing attention to a myriad of security issues. Computer breaches, viruses, and homeland security have become part of the day-to-day vernacular, and organizations are beginning to allocate a disproportionate share of their IT budgets on information protection projects. The Federal government and security experts alike fear that terrorists will again attack the critical sectors that are vital to the normal operation of our country. For example, the banking and finance industry in the United States safeguards over $21.5 trillion in credit assets (Allan et al., 2002). What would happen to the markets and consumer confidence in general if the stock exchanges were compromised, and the confidentiality, integrity, and availability of the banking infrastructure were disrupted for days?

Moreover, the 2003 CSI/FBI Survey found the highest level of financial fraud since the statistic was first gathered in 1997 (Richardson, 2003). Rarely a day goes by and the news features stories related to computer fraud or identity theft. Identity theft has been called the fastest growing crime in America" (Berghel, 2000), growing at an 80 percent rate from 2002 to 2003 (Pettey, 2003).

Accordingly, the federal government is encouraging universities to develop information assurance programs. For example, the National Security Agency has developed the Center of Excellence in Information Assurance Education program where universities serve as regional centers of IA expertise to provide more computer security programs aimed at retooling and retaining current federal and state information technology personnel. With the encouragement of the federal government, universities are building out their information assurance programs. This paper communicates a model information assurance program at Dakota State University, which was recently named a Center of Academic Excellence in Information Assurance Education.

INFORMATION ASSURANCE (IA)

Hayden (2003) defines information assurance as measures that protect and defend information and information systems by ensuring their confidentiality, availability, integrity, authentication, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

INFORMATION ASSURANCE AND SECURITY EDUCATION: A REVIEW

Yngstrom (1989) reports on one of the early attempts to develop designated information security educational programs. Since then, the number of programs has been steadily increasing. Nevertheless, unlike more mature disciplines like computer science, there is neither a universally accepted Common Body of Information Systems Security Knowledge (CBK), nor a model curriculum for Information Systems Security. In so far, models for information security education are results of government, industry, and academic efforts (Crowley, 2003).

Government efforts dates back to the 1987 Computer Security Act and are documented in various publications such as the National Institute of Standards' (NIST) 800-16 and the National Security Telecommunications and Information Systems Security Committee's (NSTISSC) 4011, 4012, 40123, 4014, and 4015. The NIST 800-16 and NSTISSI 4011 represent a CBK for information security at least from the US federal government perspective.

Industry efforts include various certification programs for IA professional. Such programs explicitly or implicitly define a CBK for their certification programs. Examples include the International Information Systems Security Certifications Consortium ((ISC)^2), the Systems Administration, Networks, and Security (SANS), the Institute for Certification of Computer Professionals (ICCP). Please refer to Laswell et al. (1999) for a comprehensive list of certification programs.

Academic effort ranged from presenting complete curriculum, to specific information assurance courses at the graduate and undergraduate levels, (Surendran et al., 2002). Examples of proposed curriculum include Crowley (2003) presenting the development of a graduate level information security specialization, Yang (2001) analyzing the impact of integrating computer security education within computer science education, and Kim et al. (2002) proposing an information security management curriculum based on an analysis of the job description of an Information Security Manager as perceived by the industry. Examples of specific courses include Troell et al. (2003) discussing the development of a forensic course, Cockcroft (2002) describing the planning and development of an information security management course, and Grimaila and Kim (2002) describing their experience developing a business undergraduate course on information security.

A MODEL FOR IA AND COMPUTER SECURITY PROGRAM DEVELOPMENT

Figure 1 presents a framework for developing undergraduate and graduate programs in IA and computer security. At the top level are certification considerations. Specifically, targeting a specific certification affects the program, the institution, the industry and the student. As noted in the previous section, there are a number of government and industry certification programs. While the CBK requirements for preparing for these certifications may overlap, there are specific requirements for each of these programs, thereby affecting the CBK addressed in the program. Moreover, certain industries and job description may prefer one certification over the other. Accordingly, job prospects for students graduating for the program are also affected by the decision. On the other hand, following federal guidelines required by the National Security Administration (NSA) allows institutions of higher education to receive recognition and funding to support their programs.

The CBK and the desired skill set for students graduating from the program are implied by the particular certification or standard followed by the institution. The CBK and skill set, in turn, guide the identification and description of the courses defining the program. However, particular

attention needs to be paid to the background of the students and the technical versus managerial mix. As noted by Surendran et al. (2002), IA is a multidisciplinary field encompassing computer science, communications, engineering, information systems, and management. Accordingly, infusing IA education for computer science students needs to address ethical, cultural, and managerial issues Yang (2001), while information security courses may need to be reengineered to target students with management focus (Hazari, 2002).

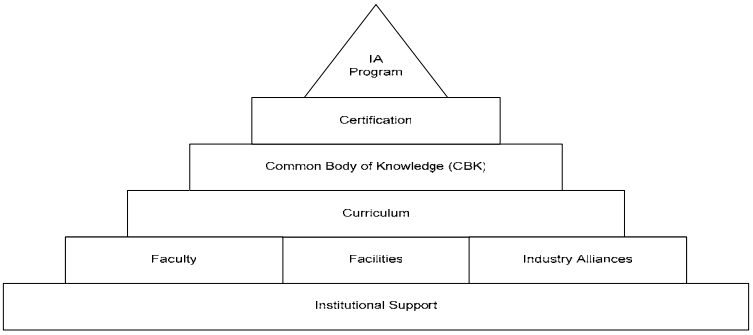

Figure 1. A Model for IA and Computer Security program development

As with other courses, faculty and facilities are needed to teach these courses. Nevertheless, IA faculty are in short supply and existing faculty need to be trained for the ever changing field of IA. Facilities required to demonstrate concepts and provide hands-on training require dedicated networking and computer labs that are not connected to the computing infrastructure. Moreover, to emphasize the hands-on nature of IA industry alliance is necessary to provide internship opportunities to students.

Institutional support is required to support the entire program. In particular, support is needed for faculty to acquire newer knowledge and skills, for investing in laboratories and other facilities, for fostering relationships with the industry, for reviewing and approving curriculum, and for a myriad of activities designated to meet certification requirements.

INFORMATION ASSURANCE AT DAKOTA STATE UNIVERSITY

In Executive Order 13231 (October 2001), the federal government outlines the nation's critical infrastructure, with banking and finance being one of these critical sectors (Bush, 2001). Dakota State enjoys a unique, rich partnership with the banking and financial services sector. When Dakota State focused its mission on technology in 1984, the governor of the state partnered the university with the emerging banking and credit card industry, just then locating in South Dakota. Executives from leading banks like Citibank were lent to the university to provide guidance and foster partnerships. With the emergence of IA as a strong emphasis at Dakota State, the strategic decision has been made to create an IA specialization in banking and financial services. This will allow DSU to build upon the relationships it has within this industry.

Central to the strategy to become a national program in information assurance, Dakota State has applied to the National Security Agency to become a Center of Academic Excellence in Information Assurance (CAE). To become a CAE, a university needs to demonstrate its commitment to information assurance education, research, and service. Centers of Academic Excellence must meet a minimum requirement on ten criteria that demonstrate depth and breadth of program.

Dakota State applied in December 2003 to the National Security Agency (NSA) to become a Center of Academic Excellence (CAE) in IA. Dakota State has received notification that it meets the NSA's curriculum requirements, with 100% for NSTISSI 4011 and 4013 national standards mappings and has been designated a Center of Academic Excellence in Information Assurance Education.

Demand for computer security education increases as interest in computer science programs decline (Traugot, 2002). However, the Upper Midwest lacks comprehensive programs in information assurance. No university in Montana, Wyoming, North and South Dakota, Minnesota or Wisconsin is a Center of Academic Excellence. Most of the IA expertise is concentrated on the East coast near the Washington, DC area. This fact presented Dakota State an opportunity to meet the IA needs of the Upper Midwest. Each of the major components of Dakota State's Information Assurance program is described next.

Educational Programs

Dakota State University currently offers four separate information assurance related degrees, including a Master of Science in Information Assurance and Computer Security, Master of Science in Information Systems with a Network Administration and Security Specialization, Bachelor of Science in Electronic Commerce and Computer Security, and a Minor in Computer Networking and Security. These programs are important because all students at Dakota State can integrate security into their programs. Each program is briefly described next.

Master of Science in IA and Computer Security (MSIA) - Dakota State will offer a MSIA degree beginning Fall 2004, consisting of 36 credits of IA coursework, including eight core courses and four specialization courses in Wireless/Mobile Security, Banking/Financial Security, or Cybersecurity. The MSIA degree is designed to prepare professionals who will have the skills to both develop and implement security strategies to improve the security posture of organizations, and provide technical leadership for the organization's efforts to adopt new technologies, implement security strategies, and protect organizational assets against attack.

To meet this objective, a unique program was created that offers the people, process, and technology education required to protect organizations in today's hostile environment. Dakota State's IA program is based on the defense in depth model which is widely held as the de facto standard that organizations and government agencies use to protect their organizations from threats. The model was developed by the National Security Agency (NSA), and purports a holistic approach to defend the organization against a variety of threats, including natural disasters, insider, outsider, accidental and intentional attacks by nation states, criminal elements, hackers, corporate competitors, and terrorists. The defense in depth approach involves building layers of defenses using three components: people, operations, and technology. While many organizations have focused primarily on the technology component, the defense in depth model suggests that people and process investments are also necessary to protect critical infrastructures and assets of organizations and government agencies. The model advocates that vulnerabilities and threats should be mitigated based on using a trained workforce each of whom follows clear, explicit security policy that is enforced and augmented with technology.

The MSIA curriculum was developed to address the technical skills identified by governmental organizations such as the United States Department of Defense and National Security Agency. The National Security Telecommunications and Information Systems Security Committee of the National Security Agency have developed a common, agreed-upon body of knowledge to be covered in the information assurance area. The standards developed by the National Security

Agency, known as NSTISSI 4011, were used as the model for the development of the MSIA program.

Master of Science in Information Systems Program (MSIS) - Dakota State offers a MSIS degree designed to prepare graduates for leadership positions in the technology field with a networking/electronic commerce security specialization. The MSIS program is very successful at Dakota State, with 126 students from 21 states and 7 countries represented in the program.

Bachelor of Science in Electronic Commerce and Computer Security Program - In 2000, Dakota State received approval from the South Dakota Board of Regents for delivery of an undergraduate degree program in Electronic Commerce and Computer Security with a specialization in computer security. Forty-eight students are enrolled in the degree program and, interest and participation in the program continues to rise. Dakota State used the NSTISSI 4011 standard to develop and certify its Bachelor of Science in Electronic Commerce and Computer Security program (McConnell, 1994).

Minor in Computer Networking and Security Program - Dakota State also offers a minor in computer security, where students can take a sequence of six classes to specialize in computer security. This minor is popular with students majoring in Computer Information Systems or Computer Science. This program offers students who elect more traditional technology majors to integrate security education into their programs, making them more marketable upon graduation.

Research

Dakota State formed a banking industry advisory board in 2003 to facilitate dialogue and partnerships between the university and industry. The board provides guidance to industry information needs and concerns, access to industry contacts, speakers, internships, research projects to provide application-oriented experiences, and faculty development opportunities in industry. Because of Dakota State's expertise and efforts in IA and its longstanding relationships in the banking and finance sector, the South Dakota Board of Regents (Board) approved the creation of a Center for Information Assurance for Banking and Finance (CIABF) at Dakota State. Such centers are reserved for those programmatic areas for which the institution has specialized abilities, recognized expertise, and an ability to make a real difference to the region.

Outreach

Equally important to the IA education and research activities are the outreach activities. Dakota State made a decision to also focus resources on extending the reach of the university beyond its traditional borders, and promote security awareness and training to anyone in the Upper Midwest. Several of the important outreach components are: an IA portal to promote IA awareness in the state, region, and beyond; an annual IA Symposium; the formation of chapters on campus to pull together IA professionals, academics, law enforcement, and IA professionals across the Upper Midwest, e.g., InfraGard and International Information Systems Forensics Association (IISFA); and a Business & Education Institute for outreach training

Facilities

To compliment the aforementioned programs, Dakota State has invested over $1,000,000 in outstanding facilities conducive to superior IA education and research. Two facility highlights include an attack/defend lab and distance education facilities. In 2003, Dakota State created an attack/defend lab to help students learn and defend against the tools that hackers use to penetrate and cause havoc. Dakota State received a grant from Cisco Systems to partially equip the attack and defend lab. Dakota State has also added two dedicated distance education classrooms that will be important to offering distance IA education.

CONCLUSION

Dakota State University has developed a strategy for growing a comprehensive, nationally recognized information assurance program. The decision was made to grow both graduate and undergraduate offerings by building upon an already strong security curriculum. Today, four unique IA degree programs are offered, including a Master of Science in Information Assurance. The decision was also made to grow within the program hands-on experience for students and faculty by partnering with the banking and finance industry, leading to the establishment of a national center for banking and finance research in information assurance. State of the art computer technology and facilities were acquired to support these IA initiatives.

REFERENCES

1. Allan, C. A., Anderson, C., Axelrod, C., Bender, M., Callahan, R., Gerbracht, F. W., et al. (2002). *Banking and Finance Sector: The National Strategy for Critical Infrastructure Assurance*.
2. Berghel, H. (2000). Digital village: Identity theft, social security numbers, and the Web. *Communications of the ACM, 43*(2), 17-21.
3. Bush, G. W. (2001). *Executive Order 13231*. Washington, DC: The White House.
4. Cockcroft, S. (2002). Securing the commercial Internet: Lessons learned in developing a postgraduate course in Information security management. *Journal of Information Systems Education, 13*(3), 205-210.
5. Crowley, E. (2003). Security : Information system security curricula development. *ACM Press NY*, 249-255.
6. Grimaila, M. R., & Kim, I. (2002). An undergraduate business information security course laboratory. *Journal of Information Systems Education, 13*(3), 189-195.
7. Hayden, M. V. (2003). *National Information Assurance Glossary*. Ft. Meade, MD: Committee on National Security Systems.
8. Kim, K., & Surendran, K. (2002). Information security management curriculum design: A joint industry and academic effort. *Journal of Information Systems Education, 13*(3), 227-235.
9. Laswell, B. S., Simmel, D., & Behrens, S. G. (1999). Information assurance curriculum and certification: State of the practice.
10. McConnell, J. M. (1994). *National Training Standard for Information Systems Security (INFOSEC) Professional*.Unpublished manuscript.
11. Pettey, C. (2003). *Gartner Says Identity Theft Is Up Nearly 80 Percent.* Retrieved January 14, 2004
12. Richardson, R. (2003). *CSI/FBI Computer Crime and Security Survey* (Survey). Washington, DC: CSI/FBI.
13. Surendran, K., Kim, K.-Y., & Harris, A. (2002). Accommodating information security in our curricula. *Journal of Information Systems Education, 13*(3), 173.
14. Traugot, C. L. (2002). *Enrollments up in computer security*. Retrieved April 7, 2003, from http://triangle.bizjournals.com/triangle/stories/2002/09/23/focus4.html
15. Troell, L., Pan, Y., & Stackpole, B. (2003). Forensic course development. Proceeding of the 4th conference on information technology curriculum on Information technology education. *ACM Press NY*, 265-269.
16. Yang, T. A. (2001). Computer Security And Impact On Computer Science Education. *The Journal of Computing in Small Colleges, 16*(4), 233-246.
17. Yngstrom, L. (1989). Experiences from a one-year academic programme in security informatics. *Information Age, Guildford, 11*(2), 77-82.