https://doi.org/10.48009/1_iis_2010_410-416

FORMULATING AN EFFECTIVE CYBERSECURITY CURRICULUM

Terry Smith, Macon State College, Georgia, USA, terry.smith1@maconstate.edu
Alex Koohang, Macon State College, Georgia, USA, alex.koohang@maconstate.edu
Robert Behling, Arrowrock Technologies, USA, behlingr@hotmail.com

==========

ABSTRACT

Secure information systems are critical for the successful operations of business and government. With increased exposures and risk due to modern systems complexities comes increasing emphasis on cybersecurity. A key component to effective cybersecurity is knowledgeable and qualified employees. Because there is no license to practice in the IT field, professional certification is often used to validate knowledge and experience. While university IT programs often incorporate security components into the curriculum, they generally do not prepare candidates for certification. The role of university IT programs in providing the necessary knowledge and skills to allow graduates to function as computer security professionals is discussed. A model for a cybersecurity program development and evaluation is proposed, including mapping courses to desired program outcomes and competencies. Suggestions for future research include surveying IT security professionals to assess perceived value of certification and university programs.

Keywords: Cybersecurity Curriculum, Curriculum Design, Information Assurance, Professional Certification, Security Professionals

INTRODUCTION

Cybersecurity is playing an increasingly important role in protecting assets and operations for both business and government. As fraudsters become more adept at manipulating both public and private computer and telecommunications systems, the race is on for all organizations to establish and implement effective security measures. Secure information systems are critical to business success, critical to government programs, and critical for consumer confidence in the use of technologies in applications such as e-business. The foundation for all protective measures is well trained and competent workforce.

Increasing business complexity, expanding global markets, and increased business and government reliance on technology all contribute to creating greater risks and exposures, along with increasing the negative impact of a successful security breach. All modern organizations are exposed to greater risk as they deploy and utilize more sophisticated information systems, rely on these systems to support core business operations, and reach into markets in areas where laws, traditions and practices are very different from those found in the United States. Perhaps the most serious risk faced by all organizations is intentional system penetration and manipulation for fraudulent purposes. Usually financial gains are the fraudster's objective, which means that successful penetration results both business disruption and financial losses for the organization.

WHAT IS CYBERSECURITY?

Cybersecurity can be defined as the processes and procedures organizations, businesses, and governments must follow to protect computer assets and information from attack via the Internet. As straightforward as this may seem, the challenges to effectively protecting computer assets and information are enormous - but necessary. To do nothing could result in the loss of personal and private information, the inability to conduct transactions, or worse.

S.773 CYBERSECURITY ACT OF 2009

The Cybersecurity Act of 2009 is a Congressional bill focused on ensuring the " continued free flow of commerce within the United States and with its global trading partners through secure cyber communications, to provide for the continued development and exploitation of the Internet and intranet communications for such purposes, to provide for the development of a cadre of information technology specialists to improve and maintain effective cybersecurity defenses against disruption, and for other purposes." (http://www.opencongress.org/bill/111-s773/show)

REVIEW OF LITERATURE

In September 2005, hackers looted American money market accounts of $550 million in less than two hours (Cetron & Davies, 2009). In April and May 2008, Russian hackers "…subjected Estonia to a nationwide denial-of-service attack that effectively shut down the country's access to the Internet" (Cetron & Davies, 2009, p. 41). In June 2008, the Chinese military successfully hacked into the Pentagon's computer systems (Anonymous, 2008). Office Max, Sports Authority and BJ's Wholesale Club are among the companies hackers attacked in August, 2008, obtaining private information on over 40 million debit and credit card holders (Anonymous, 2008). In October, 2009, it was discovered that a "junior staffer improperly uploaded an internal document to a peer-to-peer file-sharing network, making it accessible to virtually anyone." (Wade, 2009, p. 12). Most recently, Google enlisted the assistance of the National Security Administration once it learned that an attack against its computer networks originated in China (Nakashima, 2010).

Listed above are just a few examples of cyber attacks and we continue to hear about more attacks each and every day. A cyber attack can be launched in many different forms, including viruses, denial of service, identity theft, phishing, malware, and spyware. It is clear that "…the expansion of the internet is opening up many new opportunities for criminals to exploit online vulnerabilities to commit cyber-crime acts or even deliberately attack the critical infrastructures of states" (Sund, 2007, p. 567).

Security standards and guidelines have been developed to assist organizations and governments against internal and external threats. Ten countries worked together to develop a set of rules, practices, and principles, titled The Generally Accepted Systems Security Principles (Qingxiong, Johnston, & Pearson, 2008).

Organizations, businesses, and governments are not immune to cyber attack, despite the efforts to develop standards and guidelines to protect computer systems, networks, and information. The problem, according to Werlinger, Hawkey, and Beznosov (2009), is that beyond standards and guidelines there are a number of challenges that information technology organizations face. Among them are the lack of security training, the lack of a security culture, ineffective risk estimation, the complexity of systems, and a lack of security tools. Werlinger, Hawkey, and Beznosov (2009) found that organizations, business, and governments need IT security practitioners who understand the threats. The IT security practitioner must be able to effectively communicate with stakeholders who do not have the same concerns or priorities when it comes to understanding security.

Security risk can be monitored, managed, prioritized, controlled, and mitigated through a sound approach to information security governance (Cleary, 2008). It is through the offering of information security programs at higher education institutions that the skills to monitor, manage, prioritize, control, and mitigate cybersecurity risks may be obtained.

CYBERSECURITY PROFESSIONAL CERTIFICATION

Because there is no license to practice in the information technology profession, there is no standardized means for assessing skills and competencies of Information Security professionals. Voluntary certification programs have evolved to fill the credentialing void. Professional certification validates real world skills, examines technical and other knowledge, and provides assurance that certified individuals have minimum competencies, skills and experience. Information security certification has never been more important, with the movement being led by the U.S. Department of Defense requiring all workers with IT security responsibility to become certified (http://www.giac.org/).

A number of organizations operate certification programs, including: 1) International Information Systems Certification Consortium (ISC) [2]; 2) Global Information Assurance Certification (GIAC); and 3) Microsoft Corporation. There are many more, however these are a few of the more recognizable programs. Stated reasons for attaining professional certification include:

- Expand knowledge of concepts and practices
- Exhibit a commitment to professionalism
- Create networking opportunities with other certified professionals
- Enhance the resume
- Global recognition of knowledge and skills
- Enhance job opportunities and salary potential

A review of target markets and certification requirements for several of the more accepted certifications follows below. This is by no means a comprehensive listing of certifications available, but

it does illustrate several of the more universally accepted programs.

Global Information Assurance Certification (www.giac.org/)
- *GIAC Information Security Fundamentals*
- *GIAC Specific Certifications*

International Information System Security Certificate Consortium (www.isc2.org)
- *Certified Information Security Professional*
- *Systems Security Certified Practitioner*
- *Government Information Systems Auditor*
- *Certified Internal Auditor*

Microsoft Certification (www.microsoft.com)
Specialist Series
- *Microsoft Certified Technology Specialist*

Professional Series
- *Microsoft Certified IT Professional*
- *Microsoft Certified Professional Developer*

Master Series & Architect Series

While preparation for the examinations is done through a variety of activities, the SANS Software Security Institute (http://www.sans-ssi.org/) is directly aligned with the GIAC program to provide certificate specific targeted examination preparation. Training includes: 1) web security, hacking defense and security testing; 2) language specific secure software training; and 3) programmer/developer certification training. Microsoft also has targeted training programs. Other training and professional organizations offer workshops, seminars and technical training to assist security professionals prepare for the various examinations.

There are many Management Information Systems (MIS), Computer Information Systems (CIS), Information Technology (IT), and Computer Science (CS) undergraduate and graduate programs that include elements of, or offer concentrations in cybersecurity. These programs are also referred to as information security or information assurance. The following is a sample of higher education institutions that offer concentrations and/or programs in information security.

Bachelor of Science
- Capital College
- Indiana University of Pennsylvania
- Kennesaw State University
- Macon State College
- Norwich University
- University of Detroit Mercy
- University of Maryland University College
- Utica College

Master of Science
- Carnegie Mellon University
- Georgia Institute of Technology
- Kennesaw State University
- Norwich University
- Nova Southeastern University
- Regis University
- University of Detroit Mercy

Doctor of Philosophy
- Nova Southeastern University

Do these programs provide students with the necessary skills to operate effectively in the public and/or private information security sector? Are current programs providing the right kind and level of education and training to produce productive and effective security professionals? Do the mission statements recognize the importance of the program? Should the mission of the program be modified to recognize the impact of the Cybersecurity Act of 2009 and address the certification issues? Is there a better way for universities to prepare students for a career in information systems? Will the current academic programs give students the necessary skills to be competitive when taking certification examinations?

The purpose of this paper is to present a model for designing cybersecurity programs that address the above question. This design of the model also includes the quality standards for a sound cybersecurity program.

DESIGNING THE CYBERSECURITY CURRICULUM

In designing the cybersecurity program, whether as a full bachelors program or a concentration with an IT, CIS, CS, or MIS program, it is a good practice to consider quality standards that are established by accreditation bodies such as ABET. ABET accredits programs in computing, engineering, and technology. Although accreditation is beyond the scope of this paper, embracing ABET standards within the design of cybersecurity curriculum can help to ensure the quality standards of the program will be met.

Our model consists of the program' framework and the program's course design. The program's framework is the backbone of the curriculum. The program's framework builds the necessary criteria for the successful design of the coursework within the curriculum.

The Program's Framework

The program's framework includes three parts: 1) formulating the program's mission; 2) constructing program's educational objectives/career goals; and 3) determining program outcomes/competencies. All three parts are necessary to support the program's coursework design and consequently the successful implementation of the program.

Formulating the Program's Mission

Normally, the mission of the program is aligned with the department/school and the overall mission of the institution. The mission, in general, must clearly articulate the goals and directions of the program and define what the program will provide (Koohang, et al, 2010). The cybersecurity program's mission should recognize the impact of the Cybersecurity Act of 2009 and address the certification issues. An example of a mission for the cybersecurity program is as follows:

The mission of the cybersecurity program is to educate students in all aspects of cybersecurity in ways that lead to rewarding careers. The cybersecurity program ventures to provide for continued development and exploitation of the Internet and Intranet communications and the development of a cadre of information technology specialists to improve and maintain effective cybersecurity defenses against all forms of disruption and manipulation as recommended in the Cybersecurity Act of 2009. In addition, the cybersecurity program endeavors to provide competencies and skills for students preparing them for professional certification in cybersecurity.

Constructing Program's Career Goals

The careers must be central to the design of the cybersecurity program. ABET refers to the program's career goals as the Program Educational Objectives. It defines the Program Educational Objectives as "broad statements that describe the career and professional accomplishments that the program is preparing graduates to achieve." (http://www.abet.org/)

The career goals are linked with the mission of the department/school and/or the institution as a whole. In addition, the career goals should be derived from the needs of constituents. The constituents can include employers, students, and the regional community (Koohang, et al, 2010). In addition, Security Certification Consortiums such as the ones mentioned in Table 1 are appropriate constituencies that can guide the standards for Cybersecurity programs. Constructing career goals requires that attention be given to not only the job titles, but also the job descriptions and the required skills and knowledge. This will ensure an effective construction of program career goals (Koohang, et al, 2010). An example of the career goals for the cybersecurity program is as follows:

The cybersecurity program requires that graduates will assume productive roles in cybersecurity positions.

Determining Program's Competencies

Program competencies are the knowledge and skills students should have by the time they conclude the program. Determining program competencies grants clear direction for working effectively through the details of program course design. ABET refers to program competencies as program outcomes. Program outcomes as defined by ABET are "*Narrower statements that describe what students are expected to know and be able to do by the time of graduation. These relate to skills, knowledge, and behaviors that students acquire in their matriculation through the program.*" (See http://www.abet.org/_TrainingCD/data/Glossary/glossary.htm)

The program's outcomes/competencies are based on the needs of the program's constituencies. The program outcomes must be measurable and linked to program's educational objectives/career goals. Involvement of the program constituencies and their input are used to continuously improve the program outcomes/competencies (Koohang, et al, 2010). Rather than reinventing the wheel, university programs can take advantage of work already done

by the certification organizations to chart a course towards providing relevant content.

There are 10 security domains created by the International Information Systems Security Certification Consortium (ISC, http://www.isc2.org) to: 1) offer a universal body of knowledge for information security professionals; and 2) provide a foundation for security practices and principals in all industries. These domains are as follows:

- Information Security governance and risk management
- Access control
- Telecommunications and networking security
- Cryptography
- Security architecture and Design
- Operations security
- Application development security
- Physical (Environmental) security
- Business continuity and disaster recovery planning
- Legal, regulations, investigations, ethics and compliance (ISC, http://www.isc2.org)

An example of a cybersecurity program's outcome/competencies can easily be derived from the International Information Systems Security Certification Consortium (ISC) – "10 security domains" (isc2.org). These are clearly relevant to university course design as well.

- *An ability to demonstrate and apply security management practices*
- *An ability to identify access control systems and methodology*
- *An ability to describe telecommunications and networking security*
- *An ability to use and apply current techniques, skills, and tools necessary for cryptography*
- *An ability to identify and apply security architecture and models*
- *An ability to identify current techniques and tools necessary for operations security*
- *An ability to identify and analyze application and systems development security*
- *An ability to identify and use physical security*
- *An ability to identify and apply business continuity and disaster recovery planning*
- *An ability to describe and apply security laws, investigation, and ethics*

In addition the abilities to demonstrate independent critical thinking and problem solving skills; work effectively in teams; and communicate effectively are general requirements that must be central to the above program outcomes/consistencies for all graduates. Direct and indirect assessments to measure achievements of the competencies must be carried out continuously. The assessments ensure the continuous improvement of the program competencies.

The Program's Course Design

In this part, the attention turns into designing courses based on the program's mission, the program's career goals, and the program's competencies that are formulated, constructed, and determined. A total of 5 to 6 courses shall constitute a cybersecurity program. Listed below is an example of 6 courses that are mapped to the program outcome/competencies. Mapping the courses to the program competencies is important for the measurement and continuous improvement.

Course: Cybersecurity Management

- *An ability to demonstrate and apply information security governance and risk management*
- *An ability to identify access control*
- *An ability to identify current techniques and tools necessary for operations security*
- *An ability to identify and protect physical security*

Course: Server/Client Systems Security

- *An ability to use and apply current techniques, skills, and tools necessary for cryptography*
- *An ability to identify and apply security architecture and models*

Course: Business Continuity and Disaster Recovery Planning

- *An ability to identify and apply business continuity and disaster recovery planning*

Courses: Software Security

- *An ability to identify and analyze application and systems development security*

Courses: Network Security

- *An ability to describe telecommunications and networking security*

Courses: Security laws, investigation, and ethical Issues

- *An ability to describe and apply security laws, investigation, and ethics*

Independent critical thinking & problem solving skills; an ability to work effectively in teams; and effectively communicating are the program outcome/competencies central to all coursework.

In summary, the courses within the program must link to one or more program competencies. The course will have a set of topics. The course will have a set of learning objectives based on the course topics. The course will have a set of assessments to measure the course's learning objectives. Successful completion of the assessments satisfies the program competencies that are linked to the course. For example, the course software security has one program competency: *An ability to identify and analyze application and systems development security*. The course software security must be able to successfully measure this competency. A set of learning objectives related to the course topics should be designed. The learning objectives should be assessed. Successful assessments of the learning objectives ensure that program competency has been achieved.

Listed below are the program competencies matched with their key security issues/topics. The security issues/topics for each competency are compiled from Dougherty (2010). A compilation such as this one can be used as a guide for including the appropriate learning objectives/topics in each course within the program.

An ability to demonstrate and apply security management practices

- Security concepts; Security controls; Security definitions
- Security practices measurement: confidentiality, integrity, and availability

An ability to identify access control systems and methodology

- Maintaining information confidentiality, integrity, and availability determined by an organization's risks, threats, and vulnerabilities

An ability to describe telecommunications and networking security

- *Confidentiality*: Network security protocols, Network authentication services, Data encryption services
- *Integrity*: Firewall services, Communications security management, Intrusion detection services
- *Availability***:** Fault tolerance for data availability, Acceptable logins and operating process performance, Reliable and interoperable security processes and network security mechanisms

An ability to use and apply current techniques, skills, and tools necessary for cryptography

- Protection of the confidentiality and integrity of data – encryption/decryption

An ability to identify and apply security architecture and models

- Framework to organize and formalize security policies
- Access control Model; Integrity Model; Information flow Model

An ability to identify current techniques and tools necessary for operations security

- Implementing appropriate controls and protections on hardware, software, and resources; Maintaining appropriate auditing and monitoring; Evaluating system threats and vulnerabilities

An ability to identify and analyze application and systems development security

- System feasibility, Software plans and requirements, Product design, Detailed design, Coding, Integration product, Implementation, Operations and maintenance

An ability to identify and use physical security

- Environment surrounding the information system; Appropriate countermeasures to physically protect the system; Hazard vulnerability assessment such as emergencies, service interruptions, natural disasters, and sabotage

An ability to identify and apply business continuity and disaster recovery planning

- Preserving business in the wake of a disaster or disruption of service with business continuity planning and disaster recovery planning

An ability to describe and apply security laws, investigation, and ethics

- Understand the US and international laws pertaining to information security; Types of computer crimes that can be committed; Issues unique to investigating a computer crime; Breach notification procedures; Ethics

Additional courses such as Internship in Cybersecurity, Emerging Issues in Cybersecurity, etc. can be added to the curriculum if the program allows for more courses to be included in the program. Furthermore, advanced courses can be designed outside the core knowledge depending on the type of the program, credit hours needed to graduate, etc.

Program Continuous Improvement

Once the program is in place, attention ought to turn into program's continuous improvement. A cybersecurity program is not an idle program. The program requires constant change, update, and improvement. Direct and indirect assessments must be in place to continuously improve the program competencies. These assessments can ensure that the program competencies are being attained. Indirect assessments can be achieved by administering surveys to measure students' opinions/attitudes toward the program. These surveys can be administered to existing students, graduating students, and alumni of the program. Direct assessments of the program competencies take place within courses in the program. These assessments can be achieved by activities, assignments, and/or exams.

CONCLUSIONS

University cybersecurity programs need careful design and monitoring if they are to be effective. Cybersecurity certification programs provide valuable insights into what industry professionals see as important knowledge, skills and issues. Understanding these views and incorporating relevant topics into the IT curriculum can strengthen university programs and provide students with a more robust academic experience.

As it currently stands, we could do a better job of preparing students to meet the cybersecurity challenges. University programs are criticized as being too "generic" and not giving students the skills they need to immediately be productive security specialists. Proprietary training programs provide focused training in specific skill sets, but do not develop the IT professional to meet the challenges beyond operational issues. Both are important! University programs can take the best from the training programs, incorporate it into the curriculum, and strengthen their programs.

This is a preliminary look at curriculum issues and developing an IT cybersecurity curriculum model to meet the challenging security needs. The next logical step would be to survey cybersecurity professionals to determine their perceptions of certification programs, university programs and the perceived value of the various educational programs and certification.

REFERENCES

1. Anonymous. (2008). Digital risk trends 2008. *Risk Management, 55*(10), p. 32-36.
2. Cetron, M. J., & Davies, O. (2009). World Ware 3.0: Ten critical trends for cybersecurity. *The Futurist*, September-October, 40-49.
3. Cleary, B. (2008). How safe is your data? *Strategic Finance, 90*(4), 33-37.
4. Dougherty, M. (February 2010). 10 Security Domains (Updated). *Journal of AHIMA 81(2),* 57-61
5. Nakashima, E. (2010). Google to enlist NSA to fight off cyberattacks. Washingtonpost.com
6. Koohang, A., Riley, L., Smith, T., & Floyd, K. (2010). Design of an Information Technology Undergraduate Program to Produce IT Versatilists. *Journal of Information Technology Education*, *9*, 99-113.
7. Qingxiong, M., Johnston, A. C., Pearson, J. M. (2008). Information security management objectives and practices: a parsimonious framework. *Information Management & Computer Security, 16*(3), 251-270.
8. Sund, C. (2007). Towards an international road-map for cybersecurity. *Online Information Review, 31*(5), 566-582.
9. Wade, J. (2009). Security breach on capitol hill. *Risk Management, 56*(10), p. 12.
10. Werlinger, R. W., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, *17*(1), 4-19.