Cyber Forensics and Security as an ABET-CAC Accreditable Program

David Wood
wood@rmu.edu

Frederick Kohun
kohun@rmu.edu
Computer and Information Systems, Robert Morris University
Moon Township, PA 15108, USA

Azad Ali
azad.ali@iup.edu
Technology Support and Training, Indiana University of Pennsylvania
Indiana, PA 15705, USA

Karen Paullet
paullet@rmu.edu

Gary Davis
davis@rmu.edu
Computer and Information Systems, Robert Morris University
Moon Township, PA 15108, USA

Abstract

This paper frames the recent ABET accreditation model with respect to the balance between IS programs and innovation. With the current relaxation of the content of the information systems requirement by ABET, it is possible to include innovation into the accreditation umbrella. To this extent this paper provides a curricular model that provides programmatic flexibility within the information systems environment that allows for innovation in the context of an accredited program. An innovative bachelor's degree program incorporating cyber forensics and information security is presented which can fit the ABET-CAC model for accreditation as an Information Systems degree. The paper argues for the usefulness of a cyber forensics security degree, and its positioning within the ABET accreditation framework.

Keywords: ABET, forensics, security, accreditation

1. INTRODUCTION

In the past 8 years, the total number of Information Systems (IS) programs attaining ABET-CAC accreditation has grown to 29. As the number of IS programs seeking accreditation is likely to increase, there is a need to assess not only the gains associated with the accreditation process but also potential unplanned negatives. This paper frames the recent ABET accreditation model with respect to the balance between IS programs and innovation. It can be argued that the ABET model focuses on Hardware, Software,

and Data, with a lesser degree of attention to people and procedures. For instance, while business courses had been a required part of the ABET accreditation and, since IS courses are not permitted to be counted as an IS Environment, there were no explicit requirements for IS related business courses in the information system environment. (DeLorenzo, Kohun, & Wood, 2006). While the IS business related courses are not specified by ABET, most accredited programs use essentially the same mix of business core courses. This has resulted in a degree of *de facto* standardization in accredited programs. However, with the current relaxation of the content of the information systems requirement by ABET, it is possible to include innovation into the accreditation umbrella. To this extent this paper provides a curricular model that provides programmatic flexibility within the information systems environment that allows for innovation in the context of an accredited program.

2. INFORMATION SECURITY – BRIEF HISTORY

"Information security" is not new; it has been used at different forums and introduced from different perspectives. Leeuw (2007) noted that the origin of information security dates back to when the scientific information became widely acknowledged and the need rose to safeguard this knowledge from being acquired or used by others without having the prior authorization. Innella (2008) on the other hand explained that the introduction of the Internet provided the spark which lead to increasing the use of Information security. The same author noted further that in 1969 when the Defense Advanced Research Project Agency (DARPA) solicited the effort of other institutions to design a network through which data could be passed and received. Some of these data were sensitive and this in turn led to establishing procedures for sharing sensitive information on the network and device technology to protect the information from being stolen.

Although introducing the Internet led to increase the sharing of information which in turn increased the use of information security, the swell of information security programs at academic institutions was not witnessed until the turn of the century. The wide spread use of business transactions electronically placed more urgency on delivering this information accurately. This in turn added to the importance of finding people who can protect this information from being tampered with. Academic programs realized this need and started different programs and courses to train people to acquire such skills.

3. INFORMATION SECURITY IN ACADEMIA

According to Innella (2008), securing computer networks had its roots in the 1960s when computers were connected through dumb terminals via networks and information exchanged through the network. Computer academic programs started initially teaching computer security in small doses, in a chapter or a few chapters in a book or through covering it with other topics in the same course. Later development increased the volume at which information security is taught at academic programs. In these days, nearly all computer programs have at least one course or topic that is devoted to teaching computer or information security in one form or another. Often an entire degree is devoted to teaching information security.

Governmental support for academic programs in information security has increased greatly in recent years. This support is exemplified in the establishment of the National Centers of Academic Excellence in IA Education (CAEIAE) by the National Security Agency (NSA) and the Department of Homeland Security (DHS). In 1999, the goal of these centers is "to reduce vulnerability in our national information infrastructure by promoting higher education and research in IA and producing a growing number of professionals with IA expertise in various disciplines (National Security Agency, 1999)". In the first year of the establishment of the center, seven universities were designated this status of excellence. The number of universities with this status has steadily increased since 1999 due to the increased demand for graduates trained in information security.

According to Frost & Sullivan (2008), technology by itself does not solve security problems; people must be trained on the use of technology in order to properly use it to solve anticipated problems. In a survey of 7548 professionals in the information security that was conducted by Frost & Sullivan to

study the status of jobs available on information security professionals, they estimated number of information security professionals employed worldwide in 2007 to be approximately 1.66 million. This number of positions available is expected to increase to almost 2.7 million professionals by 2012. This increase from 1.6 million to 2.7 million represents a 10% increase each year from 2007 to 2012.

Such increase in demand for information security professionals adds more pressure on academic programs to meet the increasing demand for information security professionals. Information systems and information technology programs kept steadily making modifications to their programs to include information security to keep pace with the demand for such professionals. The continuing modifications are more apparent in the representation of information security in IT model curriculum. The earlier version of these model curricula hardly suggested the inclusion of information security in their suggested topics. However, later versions suggested the inclusion of courses as well as programs in information security.

4. INFORMATION SECURITY IN THE MODEL CURRICULA

Many organizations work to model curricula for various technology fields: The Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE), the Association of Information Systems (AIS) and the Association of Information Technology Professionals (AITP). These organizations have worked at many levels to develop model curriculum for different computer disciplines. They have developed a number of documents in this regard and indicated that they will continue to do so as the need arises The initial focus of these efforts was to develop a model curriculum for computer science programs. This evolved into a larger number of model curricula to cover a wider range of computer related programs.

The documents that are developed by these organizations are labeled as computing curriculum, though not officially considered "standards"; they have been widely used in curriculum development and accreditation. In fact, due to their wide use in higher education, these documents are considered as de facto standard or pseudo standard curriculum in the computing technology fields.

The latest incarnation of these model curricula include IS2002, CC2005, IT2005 and IT2008.

IS2002

IS2002 (Gorgone et al., 2002) included a table titled "Representative Capabilities and Knowledge Expected for IS Program Graduates". This table included four areas, one of which is technology. Under the technology heading, lists Database Design and Administration and beneath it suggested the topic of "Administration, security, safety, backup, repairs, and replicating" as topic coverage areas.

In addition to the representative capabilities figure, IS2002 included 12 learning units, each of which can serve to be courses in traditional IS programs. Security was mentioned as a topic of coverage under two learning units, IS 2002.1 – Fundamentals of Information Systems and IS 2002.2 – Electronic Business Strategy, Architecture and Design.

CC2005

The development of Computing Curriculum 2005 (CC2005) served these two purposes: First, it identified the fields or the academic programs that encompass computer related programs. Secondly, it listed specific fields that are included under each domain.

CC2005 identified five computer related programs: Computer Science (CS), Information Systems (IS), Information Technology (IT), Computer Engineering (CE) and Software Engineering (SE). Along with a list of the five technology fields, CC2005 provided a scoring mechanism for the coverage (or domain) area for these five technology fields. Although there is some overlap in the coverage area among these five fields, CC2005 provided ample description of each of the coverage areas for all five.

One of the tables included in CC2005 provides Comparative weight of computing topics across the five kinds of degree programs mentioned above. Two topics were mentioned in this table regarding security: Security issues and principles, and Security implementation and management. Both of these categories were present in computer

engineering, computer science, information systems, information technology and software engineering.

IT2005, IT2008

Both the IT2005 and IT2008 standard curricula have been developed regarding the latest emerging field of information technology. Information Assurance and Security are listed as one of twelve knowledge areas included in the body of knowledge for this field. In addition, information assurance and security is included as one of the "Pervasive Themes" that are prominent in all of the knowledge areas.

5. ABET-CAC INFORMATION SYSTEMS ACCREDITATION

An analysis was performed of previous research by examining ABET IS accreditation in areas such as the value in receiving accreditation, the value in positioning the program in the school of business, and its relationship to AACSB accreditation. The review included an analysis of the prior work on ABET IS accreditation by Gorgone, Hilton, Jones, Lidtke, and MacKinnon. (DeLorenzo et al., 2006). A synopsis of their findings was presented that supports the position taken in this paper.

As noted by Hilton (2003), MIS programs in a business school provide "business graduates with [adequate] education in a major change lever" and "to ensure that a large number of technology professionals are adequately educated in basic business concepts". ABET accreditation of an MIS department housed within a college of business would only increase the credibility and quality of both the department and the college. However, ABET IS accreditation presents curriculum challenges on the balance of business and IS courses for those programs seeking AACSB accreditation, as noted by Jones (2004). Given the recent national decline in IS majors and the inclusion of typical IS curriculum into mainstream business majors (i.e., database, data mining, systems analysis, web design), IS curricular innovation is needed in order to attract students including women. One proposed strategy is to include an information systems environment that is an area of interest to the current contemporary population of young adults.

One area of interest that has attracted national attention is forensics. What follows is a curriculum offered at a mid-Atlantic university combining the core requirements and focus of an ABET-CAC IS accreditable curriculum with a focus on cyber forensics and its counterpart information security.

Cyber Forensics

Cyber Forensics is an emerging discipline offering significant career opportunities. Professionals in this discipline combat identity theft, corporate theft, cyber terrorism, and the exploitation of minors. To meet the current and growing need of these professionals, a hybrid program was created incorporating the needs of cyber forensics, and those of information security. The proposed degree is a Bachelor of Science in Cyber Forensics and Information Security. Possible careers include private industry, government (including law enforcement), and the legal profession.

As new technological innovations continue to proliferate in our society, so do the opportunities for technology exploitation. Once the purview of a few "geeks" and "hackers," cyber and computer crime has evolved to include a large following of increasingly sophisticated and organized criminals. As cyber crime continues to expand, the need for highly-skilled professionals in cyber and computer forensics also increases.

6. CYBER CRIME

Corporate/Business Theft

A recent survey of 494 U.S.-based companies found that the average annual loss per company due to cyber crime jumped to $550,424 during 2006. This increase in corporate loss more than doubled from the 2005 estimate of $168,000 (Kelly, 2007). There are several trends within corporate cyber crime that contribute to this increase in losses. First, the very nature of the cyber criminal has changed. Early attacks against corporate networks and databases were more of a nuisance, causing temporary loss of business and minor financial consequences. The cyber thief of the mid to late 2000s, however, has designed extremely organized attacks that yield larger monetary payoffs for the criminal. Also, the attacks are far more insidious than those of the past, making the attacks extremely difficult

to detect and also making the resulting financial loss more substantial (Sherstobitoff & Bustamante, 2007).

Due to the increasing risk to cyber theft, corporations are under an increasing bevy of regulatory requirements from government and quasi-government agencies. Federal mandates such as Sarbanes-Oxley have required U.S. corporations to address cyber security and tighten all potential exploits. Specifically, the central role of the Information Technology (IT) department has shifted ". . . from technology to corporate governance. Government mandates and compliance issues continue to be a hot topic within the IT department" (D'Amico, 2007, p. 29).

Since cyber crime in corporate America directly affects profits, ". . . cyber security is becoming more of a boardroom issue." (D'Amico, 2007, p. 29). To help fight the growing liability of cyber crime, business organizations need to employ people who have both business acumen and the necessary technology skills for mitigating cyber attacks.

Personal Property/Identity Theft

Advances in technology have dramatically increased the storage capacity and availability of personal information. Our networked-lives have made socializing, purchasing, banking, and healthcare convenient; however, this interconnectivity has also exposed private citizens to identity theft and other vulnerabilities. In 2007, the theft or loss of personal information in the United States alone, such as credit card data and Social Security data, climbed to record levels. A 2007 study found that 79 million personal records were reported as compromised; a statistic that is nearly four times the volume reported for 2006 (Associated Press, 2007).

A recent incident involving TJX Cos. (the parent company of T.J. Maxx and Marshalls department stores) shows the vulnerability of private consumers' data. During the "hack" of its network and associated databases, TJX acknowledges that up to 46 million private records (i.e., credit card numbers) were compromised. Third-party consumer groups have estimated this number to be much higher; as much as 94 million (Associated Press, 2007).

Consumer advocacy groups, as well as law firms representing both private and class-action suites need skilled individuals who understand the technical intricacies involved in identity theft cases. In addition, local, state, and federal laws and regulations need to be updated to combat cyber crime and prosecute offenders. Again, highly-skilled individuals must be hired to aid in this effort.

Cyber Terrorism

Cyber terrorism takes cyber crime to a whole new level. Unlike traditional cyber crime, the motives of cyber terrorism are social, political, or religious. Cyber terrorism can be financially motivated, however, most attacks are designed to deny service or compromise key infrastructure systems.

Since virtually all infrastructure systems are computer-controlled or linked via networks, any type of system could be at risk. In an attack, cyber terrorists could sabotage or cripple mundane systems such as electricity, telephone, and automated banking. However, cyber terrorists could also target more critical systems, such as public water supplies, air traffic control systems, and military defense systems (Wagner, 2007).

The U.S. Department of Defense considers the Internet and cyberspace as the "fifth operating domain for war fighting" and adds that cyber terrorism attacks could range from ". . . simple disruption of communications systems to loss of combat capability" (Wagner, 2007, p. 35).

As the United States and allies work to tighten physical security, terrorists may favor cyber attacks that bypass physical security measures. Although, a full-scale "cyber jihad" has not yet been launched, there have been sporadic attempts by extremists in the Middle-East and China to infiltrate U.S. systems. As expected, terrorist cells in different geographic locations use the Internet to communicate and to distribute plans and information.

Monitoring terrorist communications and securing critical private and governmental systems from cyber attacks requires a growing arsenal of professionals. Local law enforcement and government, as well as state, and federal levels all require a growing number of individuals who have the technical expertise to guard our cyber-borders. As

these monitors are given more power, it may be necessary to also increase the need to monitor the monitors, protecting from abusing this power.

Exploitation of Minors

Finally, among the most heinous of cyber crimes involve the exploitation of children. Criminals in this realm can be involved in crimes ranging from child pornography to abduction, molestation, and murder of children.

Unfortunately, the connectivity of the Internet and the proliferation of social sites such as MySpace and Facebook have spawned a whole new medium for child predators. Recent FBI crime statistics show that six out of ten children who are online have received an e-mail or instant message from a total stranger. Even more alarming, approximately one in every 33 children who are online will be coaxed by a stranger to meet in person (Murphy, 2008).

Online websites, chat rooms, and Internet Service Providers (ISPs) must continue to work with legislators and all levels of law enforcement to fight against child predators and protect children while they are online. A growing number of highly-trained and skilled individuals are needed in the private and public sectors to prosecute child predators and to make cyberspace safe for everyone.

7. B.S. IN CYBER FORENSICS AND INFORMATION SECURITY

Program Objectives

When a student successfully completes all requirements for the B.S. in Cyber Forensics and Information Security, he/she will be able to . . .

- Demonstrate the proper use of cyber forensic tools and techniques.
- Describe and be able to follow proper investigatory and legal procedures pertaining to cyber forensics.
- Properly report the findings of a cyber forensic investigation in both written form (using proper grammar, writing style, and citation) and in oral form (i.e., within the context of a trial, hearing, or deposition).
- "The final skills that IT professionals have to develop relate to security. … The IT professional must understand, apply, and manage information assurance and security in computing, communication, and organizational systems." (Ekstrom et al., 2006, p. 355).

The course titles used in this proposed program are found in the Appendix.

Thus, we have presented a way to use the existing ABET accreditation standards to present a a program in Cyberforensics and information Security which can enable graduates to meet the needs of industry while satisfying academic excellence standards.

8. REFERENCES

Associated Press. (2007, December 31). "Data security breaches reach a record in 2007". The Wall Street Journal , p. B5.

D'Amico, E. (2007). "Cyber crimes continue to plague business and keep security software spending high." Chemical Week , 169 (21), 29.

DeLorenzo, G., F. Kohun, & D. Wood (2006). "ABET-CAC IS Accreditation: Curricular Standards and Program Rankings." Issues in Information Systems, VII (1).

Ekstrom, J., S. Gorka, R. Kamali, E. Lawson, B. Lunt, J. Miller, & H. Reichgelt (2006). "The Information Technology Model Curriculum." Journal of Information Technology Education, V5,

Frost and Sullivan (2009). Global UDC Industry Analysis March 2009.

30 Sep 2009 | Information & Communica

Gorgone, J.T, G.B. Davis, J.S. Valacich, H. Topi, D.L. Feinstein, & H.E. Longenecker (2002). "IS 2002: Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems." Association for Information Systems, Atlanta, GA.

Hilton, T. (2003). "MIS Program Accreditation: Comparing AACSB and ABET." Proceedings of ISECON 2003 §2211.

Hilton, T.S.E., D.A. Johnson, & G.M. Kasper (2004) "ABET Accreditation of MIS Programs in AACSB Schools." Proceedings of ISECON 2004, 21, 1-16

Innella, P. (2008). "A Brief History of Network Security and the Need for Adhe-

rence to the Software Process Model." Retrieved December 10, 2008 from http://www.tdisecurity.com/resources/assets/NetSec.pdf

Jones, C. (2004). "An Analysis of Programmatic Differences between dual ABET/AACSB and ABET-Only Accredited Information Systems Programs." Issues in Information Systems. V(2).

Kelly, S. (2007). "Computer crime losses double." Business Insurance , 41.

Kohun, F.G., & D.F. Wood (2003). "The ABET CAC Accreditation Experience – Intent and Reality – the Information Systems Perspective." Information Systems Education Journal, 1(43), 3-11

Kohun, F.G., & D.F. Wood, (2004). "The ABET CAC Accreditation – Is Accreditation Right for Information Systems?" Proceedings of IACIS 2004, V2, 579-583

Leeuw, K. D., & J. Bergstra (2007). The History of Information Security: A Comprehensive Handbook. New York, NY: Elsevier

Lidtke, D.K. & G.J. Yaverbaum, G.J. (2003). "Developing Accreditation for Information Systems Education." IT Professional. 41-45.

MacKinnon, R. J., & E.S. Butler (2005). "How Do IS Programs Compare With ABET Accredited Programs?" Proceedings of IACIS 2004, V1, 332-338

Murphy, M. (2008, May 9). "Facebook, states set predator safeguards." Tribune Business News .

National Security Agency (1999). National Centers of Academic Excellence. Retrieved July 27, 2009 from http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml.

Sherstobitoff, R., & P. Bustamante, (2007). "You installed Internet security on your network: is your company safe?" Information Systems Security , 188-194.

Wagner, B. (2007). "Electronic jihad: experts downplay imminent threat of cyberterrorsim." National Defense, 92 (644), 34-36.

APPENDIX

CYBER FORENSICS AND SECURITY PROGRAM:

BS Information Sciences: Cyber Forensics Checksheet

UNIVERSITY CORE 39 Credits Required Including

3 cr	Fund of Info Systems
3 cr	Statistics I

BS IS -- PROGRAM REQUIRED COURSES 36 Credits

3 cr -- one from	Finite Math and Applied Calculus
	Statistics II
3 cr	Quan Analy For Inf Sys Prof
3 cr	Glob, Econ, Soc, Eth Iss Comp
3 cr	Visual Basic Programming
3 cr	Adv Web Page Design/Ecomm
3 cr	Operating Systems Concepts
3 cr	Intro Web Dev & E-Comm Techn
3 cr	Systems Analysis and Design
3 cr	Advanced Sys Analysis/Design
3 cr	Network Technology & Mgt (N+)
3 cr	Database Management Systems
3 cr	Project Management

TRACK CONCENTRATION 12 Credits Required

3 cr	Info Tech Security, Control, and Assurance
3 cr	IT Governance, Control, and Assurance
3 cr	Network Security
3 cr	Network Forensics, Intrusion Detection, and Response

IS ENVIRONMENT – 15 Credits Required

3 cr	Criminal Law and Evidence
3 cr	Criminology
3 cr	Computer Forensics
3 cr	Cyberlaw
3 cr	Digital Evidence Analysis

OPEN ELECTIVES 24 Credits Required