



May 26th, 3:30 PM

AACSB-Accredited Schools' Adoption of Information Security Curriculum

Linda Lau

Longwood University, Farmville, Virginia

Cheryl Davis

Longwood University, Farmville, Virginia

Follow this and additional works at: <http://commons.erau.edu/adfsl>

Scholarly Commons Citation

Lau, Linda and Davis, Cheryl, "AACSB-Accredited Schools' Adoption of Information Security Curriculum" (2011). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 3.

<http://commons.erau.edu/adfsl/2011/thursday/3>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University[™]

SCHOLARLY COMMONS

(c)ADFSL



AACSB-ACCREDITED SCHOOLS' ADOPTION OF INFORMATION SECURITY CURRICULUM

Linda Lau

Longwood University
Farmville, Virginia

Cheryl Davis

Longwood University
Farmville, Virginia

ABSTRACT

The need to professionally and successfully conduct computer forensic investigations of incidents has never been greater. This has launched an increasing demand for a skilled computer security workforce (Locasto, et al., 2011). This paper examines the extent to which AACSB-accredited universities located in Virginia, Maryland and Washington, D.C. are working towards providing courses that will meet this demand. The authors conduct an online research of the information security courses and programs offered by the 27 AACSB-accredited business schools in the selected area.

The preliminary investigation revealed that eight of the 27 participating universities did not offer any courses in cybersecurity, digital forensics, and information assurance. However, nearly 70% of the participating universities have included at least one or more information security courses in their curricula and some universities have implemented more extensive information security programs. This paper will describe the research methodology and results of the study.

Keywords: digital forensics, information assurance, cybersecurity, information technology, information security, computer security

1. INTRODUCTION

Technology has redefined the process of criminal and business investigations. Investigations can involve forensics, information assurance and cybersecurity. Computers are not only part of everyday activities but are also used in criminal activities. The need to professionally and successfully conduct computer forensic investigations of incidents has never been greater. Digital information is increasingly being used as evidence in criminal and civil cases. Law enforcement and security agencies are using digital forensics not only as a tool to solve cases but to prevent them. After the tragic terrorist events that unfolded on September 11, 2001, there has been an increase in the focus on security – at airports, immigration centers, and federal and government buildings. Cybersecurity has since become a major component of that security. In November 2010, WikiLeaks exposed secrets of the inner workings of the U.S. diplomats (Rayfield, 2010). This breach of security may have put some diplomats and intelligence professionals lives at risk. These events have not only dramatically changed the way we view security, they have increased our reliance on cybersecurity and they have drastically changed the way we live.

In this study, information security will include three areas: cybersecurity, digital forensics, and information assurance. Cybersecurity refers to the protection of information and property from unwanted computer behavior with the objective of allowing the information to remain accessible and productive to its intended users (Cybersecurity, 2011). Digital forensics is defined as the process of investigating and retrieving information from a variety of electronic devices, including computer hard drives, cell phones, file servers and e-mail servers (Duerr, et al., 2004). Information assurance is the field of practice focused on managing the risks associated with storing, processing, and transmitting information (Marchant, et al., 2009).

2. LITERATURE REVIEW

Security and privacy have become the most complex and pressing subjects of information technology. From the demands of government and homeland security to the nature of the information age itself, employers -- including the government -- are faced with serious challenges of how to obtain a reasonable balance with dwindling resources. Experts agree that obtaining this balance will be found in education as information technology plays an important role in modern education (Gong, Xu, and Yu, 2004). State and local governments are showing their support for reforms through the passage of Bills. In 2006, the Virginia General Assembly passed Senate Bill 494/House Bill 1307, requiring the Governor of Virginia to develop a statewide strategic plan to address the need for reforms in workforce policy, which includes the implementation of workforce development and training initiatives (Governor Kaine's Workforce, 2011). This Bill was passed to allow Virginia to build a skilled workforce able to compete effectively in the technological 21st century.

Over the past decade, compared to the national average, fewer and fewer working-age adults in Virginia are continuing with their higher education and/or upper level training (The National Center for Public Policy, 2006). On the other hand, the Occupational Outlook Handbook predicted that the job outlook is very favorable for those in computer security (2006). However, the demand for computer security skilled professionals is much greater than the supply. The 2006 Occupational Outlook Quarterly stated that employees in the diverse field of computer security typically work very long and irregular schedules. This could be a direct result from not having enough universities offering programs to train skilled employees needed to meet the demand of employers. In February 2009, President Obama ordered a 60-day review of the federal government's various cybersecurity programs which have set the stage for a substantial overhaul of government's cybersecurity activities as well as new legislation for data protection and security breach notification (Vijayan, 2009). The Cybersecurity Enhancement Act of 2009 will provide up to \$396 million in research grants over the next four years to develop best practices and standards to protect computer networks (Montalbano, 2011).

A Washington Post article highlighted the need for a dramatically different approach to cybersecurity education, outreach, as well as the hiring by the federal government (Cyber Help Wanted, 2009). This need is further complicated by the fundamental discrepancy between the users and employers' expectations, the scarce work force, and the underdeveloped educational mechanism (Locasto, et al., 2011). Because cybersecurity, digital forensics, and information assurance are constantly evolving fields, universities must offer programs that promote life-long learning in these areas.

The Association for Computing Machinery (ACM) *IS 2010 Curriculum Guidelines for Undergraduate Degree Programs in Information Systems* is a model curriculum intended to provide flexibility in designing Information Systems (IS) curricula to satisfy various local requirements. IS faculty may be affiliated with schools of business, schools of public administration, schools of information science or informatics, stand-alone schools of Information Systems, or other variations (Topi, et al., 2010). This flexibility also fuels an ongoing debate regarding the nature and identity of information systems as a discipline. The ACM guidelines suggested that universities should offer information security courses across campuses. Unfortunately, the interdisciplinary content and complexity of the information security courses require instructors to possess appropriate training in diverse contents in the field of information security (Shing, et al., 2007). A 2006 research concluded that although several entities in this country offered various certificate programs, these certifications provided limited knowledge and skills that may not be sufficient for employers (Hentea & Dhillon, 2006). The third largest reason for the high turnover of IT security employees is due to the fact that they were inadequately trained and ill-prepared for the jobs (Furnell & Clarke, 2005). A case study conducted in 2004 revealed that programs in fields such as computer science and information technology lack an emphasis on security issues in their curriculum (Bogolea & Wijekumar, 2004). A Web-based survey collected data from IS faculty members in several business colleges (Foltz & Renwick, 2010). Sixty-one instructors completed the survey, 50 of the completed surveys came from AACSB-accredited business colleges. A strong majority (73%) of the respondents

indicated that IS security needs to be addressed and that the present curricula are not meeting those needs, especially in the required courses.

Current literature revealed two main concerns with the current workforce. First, there is an employer demand for a computer security skilled workforce, and this demand for computer security skilled professionals is much greater than the market can supply. Although universities play a vital role in providing this skilled workforce, there is a shortage of universities offering technology programs to meet the demand of employers. Further, there is no existing benchmark to measure the quality of the current programs. Hence, this paper will examine the information security curricula at AACSB-accredited universities located in Virginia, Maryland, and Washington, D.C.

3. RESEARCH STUDY

This section of the paper will describe the research methodology used to collect the data needed for this study. Twenty-seven universities were selected as participants for our research. The research data were collected via the Internet, summarized using Excel 2007, and the results are discussed in the Data Analysis subsection. Research limitations that may affect the validity of this research and topics for future research are also presented in this section.

3.1 Research Methodology

This research explores the information security programs offered by 27 universities located in Virginia, Maryland, and Washington, D.C. These universities are selected based on their AACSB-accredited business programs (Accredited Institutions, 2011). As of March 2011, there were 16 AACSB-accredited universities in Virginia (with two business colleges in University of Virginia), seven in Maryland, and four in Washington, D.C. The authors visited each university's Web site and performed a comprehensive search at each Web site using keywords such as cybersecurity, forensics, digital forensics, and information assurance. This online search documented pertinent information regarding the information security courses and programs, such as the field in which the courses are offered, the number of credits for each course and/or program, and the departments/schools offering courses and programs. The search results were collected, summarized, and tabulated in tables.

3.2 Data Analysis

Table 1 showed that two of the 16 Virginian universities offered at least one information security course. However, seven Virginian universities do not offer any information security courses and another seven of the Virginian universities offer some sort of information security programs. In the state of Maryland, one university does not incorporate any information security courses into its curriculum, while four universities taught at least one course in the three selected fields, and two universities have a structured information security program. Finally, the District of Columbia housed two universities that offered at least one information course and two universities have a structured information security program. Of the 27 AACSB-accredited universities surveyed, nearly one-third of the participating universities do not offer any information security courses and another one-third of them offer at least one information security course. The remaining 40% (11) have a formal structured program in this area.

Table 2 provided a more detailed description of the information security programs offered by the 11 universities: seven in Virginia, two in Maryland, and two in the District of Columbia. Of the seven Virginian universities with a more comprehensive information security agenda, four of them – James Madison, Norfolk State, Radford, and Virginia Commonwealth – have an undergraduate degree in various majors and concentrations. Three of them – George Mason, Norfolk State, and Virginia Commonwealth – have a master's degree in information security. Only two of these seven universities – Norfolk State and Virginia Commonwealth – offer both undergraduate and graduate degrees in information security. Three Virginian universities – George Mason, Longwood, and Radford – offer a minor in information security, and two of them – George Mason and Virginia Tech – offer graduate certificate programs in this area.

In Maryland, Towson University is heavily involved with the information security curricula, offering

various undergraduate, graduate, and certification programs. It is also note worthy to mention that, of the 27 universities surveyed, only Towson University has established a Center of Excellence that is devoted to the education of information assurance. This sole establishment is known as the National Centers of Academic Excellence in Information Assurance Education (CAEIAE), and was approved by the National Security Agency and the Department of Homeland Security as a National Center of Academic Excellence (CAIT, 2011). University of Baltimore offers a bachelor degree in Forensic Studies. In the Capital, both George Washington University and Georgetown University offer master's degrees and certifications in the area of information security.

3.3 Research Limitations

The reliability and validity of this research depends on the accuracy of the information collected from the Internet during the research period, which is beyond the control of the authors. Further, the authors selected the participating universities based on one accreditation, AACSB. This accreditation was selected based on the authors' affiliation with teaching in an accredited business college. However, there are many other universities located in the three selected regions that offer courses and programs in information security whose curricula are approved by other types of accreditation. Unfortunately, the lack of resources delimited the number of universities that could be included in this study.

3.4 Future Research

The authors plan to continue with the current research. First, the authors plan to examine the formal structured information security programs in more details. For instance, pertinent information such as the number of credits needed for each program, the disciplinary area, the department and college offering the course, etc., will be collected, summarized, tabulated, and then analyzed further. The authors also intend to contact the participating universities to confirm the number of faculty who are teaching those courses, the number of students enrolled in those courses, as well as the date of creation of those courses. If more resources are available, the authors will increase the sample size to include AACSB-accredited universities in neighboring states such as West Virginia, Pennsylvania, Delaware, North Carolina, and South Carolina.

4. CONCLUSION

This research provided some insight into the information security curricula offered at 27 AACSB-accredited universities in Virginia, Maryland, and Washington, D.C. The conducted research supports the concerns found in the literature review, mainly: (1) There is a shortage of universities offering information security programs; and (2) There is a lack of benchmarks used to measure the quality of the current programs being offered. Only one of the 27 universities surveyed has established a Center of Excellence for information security programs. We would like to see more universities establishing their own centers of excellence and utilizing the federal and states monies set aside for the development of best practices for computer security programs.

REFERENCES

- Accredited Institutions. Retrieved from <http://www.aacsb.edu/> on January 3, 2011.
- Bogolea, B. & Wijekumar, K. (2004). Information security curriculum creation: A case study. Kennesaw, GA, InfoSecCD Conference, October 8, 2004.
- Center for Applied Information Technology (CAIT): Information Assurance Resources. (2011) Retrieved from <http://www.towson.edu/outreach/cait/informationAssurance/> on March 25, 2011.
- Cybersecurity. (2011). *Wikipedia, the Free Encyclopedia*. Retrieved from http://en.wikipedia.org/w/index.php?title=Computer_security&oldid=414432823 on February 17, 2011.

- Cyber Help Wanted: The federal government lacks a sensible hiring process – and enough good candidates – to guard computer networks. (August 1, 2009). *Washington Post*, p. A16. Retrieved via Greenwood Library LexisNexis database on March 25, 2011.
- Duerr, T., Beser, N., and Staisiunas, G. (2004). Information assurance applied to authentication of digital evidence. (Research and Technology) *Forensic Science Communications*, October 1, 2004. Retrieved from <http://www.highbeam.com/doc/1G1-137921545.html> on February 21, 2011.
- Foltz, C., & Renwick, J. S. (2010). Information Systems Security and Computer Crime in the IS curriculum: A detailed examination. *Journal of Education for Business*, 86(2), 119-125.
- Furnell, S. & Clarke, N. (2005). Organizational security culture: Embedding security awareness, education, and training. *Proceedings of the IFIP TC11 WG 11.8, 4th World Conference Information Security Education*, Moscow, Russia, 4: 213-222.
- Gong, M., Xu, Y., & Yu, Y. (2004). An enhanced technology acceptance model for Web-based learning. *Journal of Information Systems Education*, 15(4): 365-374.
- Governor Kaine's Workforce Development Strategic Plan. (2011). Making connections: Virginia's new direction for workforce development. Filed on February 12, 2011 with the www.nationalskillscoalition.org. Retrieved on March 25, 2011.
- Hentea, M., & Dhillon, H. (2006). Towards changes in Information Security education. *Journal of Information Technology Education*, 5: 221-233.
- Locasto, M., Ghosh, A., Jajodia, S., and Stavrou, S. (2011). Virtual Extension The ephemeral legion: Producing an expert cybersecurity work force from the air. *Communications of the ACM*, 54(1): 129-131.
- Merchant, R., Cole, R., and Chu, C. (2009). Answering the need for information assurance graduates: A case study of Pennsylvania State University's security and risk analysis major. *Information Systems Education Journal*, 7(75): 3-11.
- Montalbano, Elizabeth (February 4, 2010). Cybersecurity bill calls for research, task force. *Information Week*. Retrieved from <http://www.informationweek.com/news/government/policy/showArticle.jhtml?articleID=222601110> on March 25, 2011.
- Shing, Marn-Ling, Shing, C., Chen, K., and Lee, H. (2007). Issues in information security curriculum: Collaborative learning and team teaching. *International Journal of Innovation and Learning*, 4(5): 516-529.
- The National Center for Public Policy and Higher Education. (2006). Virginia, Measuring Up 2006: The State Report Card on Higher Education, p. 1-16.
- Rayfield, J. (November 2010). *Gibbs On WikiLeaks: Stealing and Disseminating Classified Info is a Crime*. Retrieved from <http://tpmdc.talkingpointsmemo.com/wikileaks/2010/11/> on February 18, 2011.
- Topi, H., Valacich, J, Wright, R., Kaiser, K., Nunamaker, J., Sipior, J., and Vreede. G. (2010). IS 2010 curriculum guidelines for undergraduate degree programs in Information Systems. Joint IS 2010 curriculum task force-Association for Computing Machinery (ACM) and Association for Information Systems (AIS).
- Vijayan, J. (May 29, 2009). Obama's cybersecurity plan gets cautious praise. *ComputerWorld*. Retrieved from http://www.computerworld.com/s/article/9133687/Obama_s_cybersecurity_plan_gets_cautious_praise on March 26, 2011.

Table 1 Information Security Courses and Programs at 27 Universities

No information security course	Offers 1 or > information security courses	Has an information security program	TOTAL
Virginia			
Christopher Newport University	Virginia Military Institute (2)*	George Mason University	
College of William and Mary	Virginia State University (1)	James Madison University	
Old Dominion University		Longwood University	
Shenandoah University		Norfolk State University	
University of Richmond		Radford University	
University of Virginia**		Virginia Commonwealth University	
Washington and Lee University		VPI and State University	
TOTAL	7	7	16
Maryland			
Salisbury University	Frostburg State University (1)	Towson University	
	Loyola University Maryland (5)	University of Baltimore	
	Morgan State University (5)		
	University of Maryland (2)		
TOTAL	1	2	7
District of Columbia			
	American University (2)	The George Washington University	
	Howard University (1)	Georgetown University	
TOTAL	0	2	4
	8	11	27
	29.63%	40.74%	

* Number in parenthesis indicates the number of courses.

** University of Virginia has two business schools - Darden and McIntire.

Table 2 Information Security Programs and Certifications at 11 Universities

	Undergraduate	Graduate	Minor	Certifications
Virginia				
George Mason University		Forensic Science, MS Computer Forensic, MS ISA, MS Computer Science, BS/ISA, Accelerated MS IT, BS/ISA, Accelerated MS IT, PhD, concentration in ISA	Forensic Science	Forensics, Graduate Certificate Telecommunications Forensics and Security, Graduate Certificate Forensic Nursing, Graduate Certificate ISA, Graduate Certificate
James Madison University	Pre-Professional Health Programs/Pre-Forensic Studies in Forensic Biology, Forensic Chemistry, or Forensic Anthropology			
Longwood University			Cyber Security, Forensics, and Policy	
Norfolk State University	Computer Science-Information Assurance, BS	Computer Science-Information Assurance, MS		
Radford University	Chemistry /Concentration in Forensics, BS Anthropological Sciences/Concentration in Forensic Anthropology, BS or BA		Forensic Science	
Virginia Commonwealth University	Forensic Science, BS	Forensic Science, MS		
VPI and State University				Information Assurance Engineering, Graduate Certificate
	7	4	3	2

Table 2 Information Security Programs and Certifications at 11 Universities (cont'd)

	Undergraduate	Graduate	Minor	Certifications
Maryland				
Towson University	Forensic Chemistry Major/General Forensic Science Track	Forensic Science, MS		ISA, Certificate
University of Baltimore	Forensic Studies, BS			
	2	1	0	1
District of Columbia				
The George Washington University		Forensic Sciences, MS, concentrations: crime scene investigation, forensic chemistry, forensic toxicology, forensic molecular biology, high- technology crime investigation		Forensic Investigation, Graduate Certificate
Georgetown University		Professional Studies in Technology Management/ Information Security/Information Assurance Track, MS		Forensic Accounting, Certificate
	2	2	0	2