ISSN: 2167-1435
v29 n1957

# Developing an Undergraduate Degree Program in Cyber Forensics and Information Security

Karen Paullet
paullet@rmu.edu

Gary Alan Davis
davis@rmu.edu

Computer and Information Systems,
Robert Morris University
Moon Township, PA 15108, USA

## Abstract

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, Robert Morris University has developed a Bachelor of Science in Cyber Forensics and Information Security. This paper describes the rationale, development, and implementation of this new undergraduate degree program. Initial enrollment projections are cited in relation to actual student enrollment for the first year of the program. In addition, future enrollment projections for the new degree program are explored.

**Keywords:** Cyber Forensics, information security, degree programs, curriculum

### 1. INTRODUCTION

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, Robert Morris University has developed a Bachelor of Science in Cyber Forensics and Information Security.

During the 2006-2007 academic year the University began offering one single course in Computer Forensics. The enrollment of the initial course offering was at its maximum capacity of 28 students. As a result of significant student interest in the new course, the University developed a concentration in Cyber Forensics and Information Security. As an interim solution, a Concentration was developed as part of the existing B.S. in Information Sciences degree. The Concentration under the existing degree could be offered immediately, as opposed to requiring approval by the State's Department of Education. The concentration consisted of four courses related to Information Security and five courses related to Cyber Forensics. Initial enrollment in the Concentration during the 2009-2010 academic year was only five students. However, the following year, enrollment in the concentration tripled to 16 students. Due to the success of the Concentration, a B.S. degree in Cyber Forensics and Information Security was developed and proposed to the State's Department of Education. The degree was approved for delivery starting the Fall 2011 semester.

ISSN: 2167-1435
v29 n1957

## 2. CYBER FORENSICS AND 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 initially taught 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 was taught in academic programs. Today, 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 Information Assurance (IA) Education (CAEIAE) by the National Security Agency (NSA) and the Department of Homeland Security (DHS). In 1999, the goal of these centers was "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 with a 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.

## 3. EVOLUTION OF THE CYBER FORENSICS AND INFORMATION SECURITY FIELD

A 2012 study was conducted by the Verizon RISK Team, with cooperation from the Australian Federal Police, Dutch North High Tech Crime Unit, Irish Reporting Information Security Service, Police Central e-Crime Unit and the United States Secret Service to determine the level of data breaches throughout the world. The 2012 Data Breach Incident Report (DBIR) revealed 855 incidents compromising 174 million records. The number of compromised records drastically increased from the previous year by 170 million records. The results are based on first-hand evidence collected from forensics investigations through Verizon (Verizon, 2012).

Early attacks against corporate networks and databases were more of a nuisance, causing temporary loss of business and minor financial consequences. Current cyber attacks are designed to yield larger monetary payoffs for the criminal. The attacks are far more insidious than those of the past, making the attacks extremely difficult to detect and also making resulting financial loss more substantial (Sherstobitoff & Bustamente, 2007).

Due to the increasing risk of 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). 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.

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 seemingly 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).

ISSN: 2167-1435
v29 n1957

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 individuals are given more power, it may even become necessary to "monitor the monitors," in order to curtail abuse of power.

## 5. NEED FOR CYBER FORENSICS AND INFORMATION SECURITY

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.

For example, Kessler & Schirling (2006) developed a single course in Computer Forensics. The course reached maximum enrollment the first semester in which it was offered at Champlain College Vermont. Since the course was well received by students, the College developed a four-year degree in Computer Forensics. The Admissions Department immediately began receiving requests from students wanting to apply to the new Computer Forensics Program.

The approach taken at the researchers' University was similar to that of Champlain College. At the researchers' University, faculty immediately noticed increased student interest in the subject after a single course in Computer Forensics was offered. Students enrolled in the initial Computer Forensics course began to inquire if additional courses and/or a degree would be offered. At this time, faculty began to investigate the feasibility of a degree in Computer or Cyber Forensics.

As a first step, faculty researched the demand for professionals in this field. Faculty quickly realized that career opportunities existed in both the public sector (i.e., local, state and federal law enforcement) and the private sector. After this realization, the faculty consulted the U.S. Bureau of Labor Statistics data to determine employment demands in both the public and private sectors. Employment as a Computer Forensic Investigator in the public sector, as projected by the U.S. Bureau of Labor Statistics, is expected to grow 22% from 2008 to 2018. In the private sector, the overall employment of Computer Security Specialists is expected to grow by 30% from 2008 to 2018. Additionally, it has been projected that approximately 286,600 new Computer Security Specialists positions will be added over the ten year period in question. Growth in both sectors is considered by the Bureau of Labor Statistics to be *much faster than the average* for all occupations (Bureau of Labor Statistics, 2010).

At the state level, similar employment demands were discovered. The State Department of Labor and Industry projects significant increases in Computer Forensic Investigator positions. Specifically, a 7% increase is projected in Private Investigation positions and a 15% increase is projected in Public Investigation positions. Both statewide projections are for the time period from 2008 to 2018. As for Computer Security Specialists, the State Department of Labor and Industry projects a 13% in positions between 2008 and 2018 (PA Department of Labor and Industry, 2010). Such increases in demand for Computer Security Specialists adds more pressure on academic programs to meet the increasing demand for information security professionals.

Further research determined that six Community Colleges/Technical Institutions in the surrounding area offer Associate's Degrees in Computer Forensics or Information Security. Bachelor's and Master's-granting institutions in the area offer either a degree in Information Security or a degree in Computer Forensics. Schools in the surrounding geographic area, however, do not currently offer a degree that is a combination of Computer/Cyber Forensics and Information Security.

After a review of both the labor statistics and surrounding schools, it was determined that an opportunity existed to develop a new and unique undergraduate degree. Specifically, the researchers determined that a combination of Cyber Forensics and Information Security was required to best meet the employment needs of this evolving field. In addition, this combination of disciplines would allow RMU University to uniquely prepare students for either the private sector (as Computer Security Specialists) or the

ISSN: 2167-1435
v29 n1957

public sector (as Computer Forensic Investigators). An examination of the surrounding schools in the region indicates that there is a strong market demand for Bachelor's-level programs in Cyber Forensics and Information Security. That market demand is further supported by an innovative Bachelor's degree program that would welcome transfer students from similar programs at two-year schools.

In the process of preparing the proposal for the degree, faculty consulted with local and federal law enforcement. Members of law enforcement provided guidance in terms of curriculum, course content, and sequence of courses, based on standards in the field. After the initial proposal was completed it was reviewed and affirmed by law enforcement.

## 6. CONTENT OF DEGREE PROGRAM

In preparing the proposal for the State Board of Education review, seven program objectives were developed for the new degree program. The program objectives were the following: 1) Demonstrate the proper use of cyber forensic tools and techniques, 2) Describe and be able to follow proper investigatory and legal procedures pertaining to cyber forensics, 3) 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), 4) Implement and evaluate the system of internal controls for any information system, 5) Use the Control Objectives for Information and Related Technologies (COBIT) as an assurance framework to describe Information Systems Security Assessment, Security Management, Security Testing, Disaster Recovery, Acquisition, and Risk Management, 6) Implement and improve controls assuring information integrity, 7) In addition, all programs in the CIS department of RMU must fulfill those core departmental requirements and the RMU core requirements.

In terms of curriculum content, the new degree in Cyber Forensics and Information Security was designed to contain 126 credits. The 126 credits were comprised of the following: 39 credits of the University core, 42 credits of the Cyber Forensics and Information Security major, 15 credits of a specified Area of Interest, and 30 credits of Open Electives. As a requirement for the degree, it was proposed that students choose 9 credits from the following list of "Legal" course topics:

- POLS2020 - Criminal Law and Evidence
- CRIM2000 - Criminology
- INFS3170 - Cyberlaw
- INFS3190 - Digital Evidence Analysis

As a further requirement for the degree, it was also proposed that students choose 9 credits from the following list of "Network/Information Security" course topics:

- INFS2150 - Intro to Web Development and E-Commerce Technology
- INFS3222 - IT Security, Control, and Assurance
- INFS3223 - IT Governance, Control, and Assurance
- INFS4180 - Network Forensics, Intrusion Detection, and Response

## 7. INITIAL ENROLLMENT PROJECTIONS

In terms of initial enrollment projections, the faculty estimated that a minimum of 10 students would be required to support sections of the new degree program. Further, it was anticipated that all students who were in the concentration would change to the new Bachelor's Degree Program. Based on student interest in related courses and the Cyber Forensics and Information Security Concentration, the faculty estimated that the program would grow to a maximum enrollment of 50 students within the first three years. For an academic program, 50 students may seem to be a low enrollment count. However, the student enrollment for all degrees within the Department of Information Systems for the 2011-2012 academic year was 685 for undergraduate, graduate, and doctoral programs. Undergraduate enrollment in the department, for the same year, was 435.

It is interesting to note that after the initial year of the new program, enrollment exceeded the three year estimate. Specifically, student enrollment during the first year of the Cyber Forensics and Information Security degree was 52. This high-level of enrollment underscores student interest in this burgeoning field.

## 8. INDIVIDUAL CLASS ENROLLMENT TREND

Since the B.S. in Cyber Forensics and Information Security started in Fall 2011, sufficient data do not exist to show a

ISSN: 2167-1435
v29 n1957

longitudinal trend of enrollment. However, certain individual courses within the new degree have been offered since the 2007-2008 academic year. Therefore, the enrollment trend can be analyzed for these individual courses. For example, the Computer Forensics course had an initial enrollment of 19 students during the first academic year that it was offered. During the second academic year, the Computer Forensics course increased in enrollment to 25 students. The enrollment for this course actually declined until the B.S. in Cyber Forensics and Information Security degree was launched during the 2011-2012 academic year. As seen in the table below, enrollment for the Computer Forensics course more than tripled after the new bachelor's degree started. See Figure 1 below for the Computer Forensics enrollment trend.

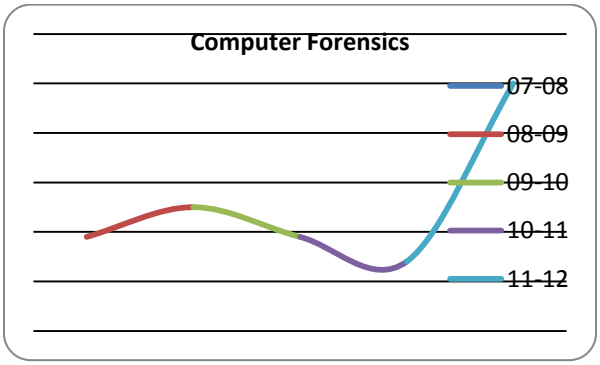


Figure 1. Computer Forensics Enrollment Trend

Cyberlaw was first offered in the 2009-2010 academic year, during which time, ten students enrolled in the course. Enrollment remained almost flat until the degree was offered. Following a similar trend as the Computer Forensics course, the Cyberlaw course took an upward trend, almost tripling in student enrollment. See Figure 2 for the Cyberlaw enrollment trend.

Two newer courses in the concentration, Digital Evidence Analysis and Network Forensics were offered starting in the 2010-2011 academic year. Initial enrollment in the Digital Evidence Analysis and Network Forensics courses was 12 and three, respectively. As depicted below, both courses had an ascending trend in student enrollment following the start of the new degree. See Figure 3 for the enrollment trend of these two new courses.

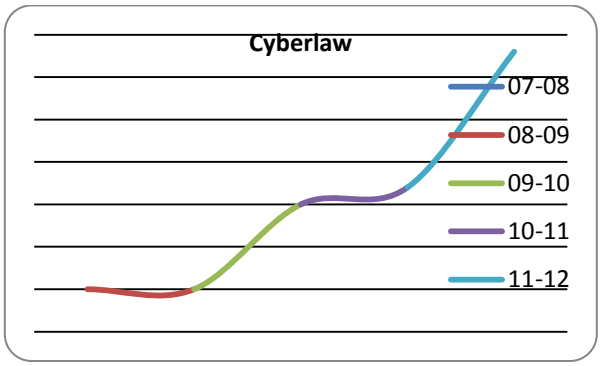


Figure 2. Cyberlaw Enrollment Trend

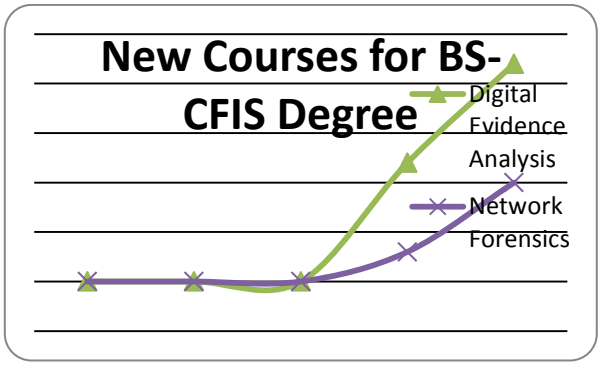


Figure 3. Digital Evidence Analysis and Network Forensics

## 9. IMPLEMENTATION OF THE DEGREE

In order to introduce the new B.S. in Cyber Forensics and Information Security degree, a major campus event was planned with the local branch of the F.B.I., the District Attorney's Office, the Sheriff's Office, and the Mobile Crime Unit. It was decided that a hands-on event with current and potential students would be the best way to generate interest in the degree and the field. Therefore, the event was designed around hands-on, forensic activities that were overseen by law enforcement professionals. Specific activities at the event included fingerprint dusting, fingerprint analysis, hair sample analysis, vision impairment activity, and a campus-wide game of clue. After the forensic activities, the students were encouraged to stay for various speakers from law enforcement and the field of cyber forensics. The keynote speaker of the event was an agent from the Cyber Crimes Unit of the F.B.I. The agent's presentation discussed various criminal activities related to the Internet and Cyberspace, such as identity theft, credit card theft, cyber-stalking,

ISSN: 2167-1435
v29 n1957

child-pornography, and cyber-gangs. In addition to the forensic activities and speakers, the new B.S. in Cyber Forensics and Information Security degree was introduced to the attendees. To further promote the new degree program, printed materials and web-links were made available to potential and prospective students. Admissions counselors were also present at the event to answer enrollment questions from prospective students.

The F.B.I. event was promoted to the local campus, the local community, local high schools, and two-year colleges within the area. More than 200 people attended the event.

## 10. FALL 2012 ENROLLMENT PROJECTIONS

Since the degree program starting in the Fall of 2011, it is difficult to forecast future enrollment. However, the time-series data from individual courses can be used to approximate enrollment growth, since certain courses in the program have been offered since the 2007 - 2008 academic year. Using Excel's Linear Regression function, the enrollment of four core courses within the degree were forecast out five years into the future. As depicted in Figure 4, all four courses show positive growth in enrollment over the next five years.

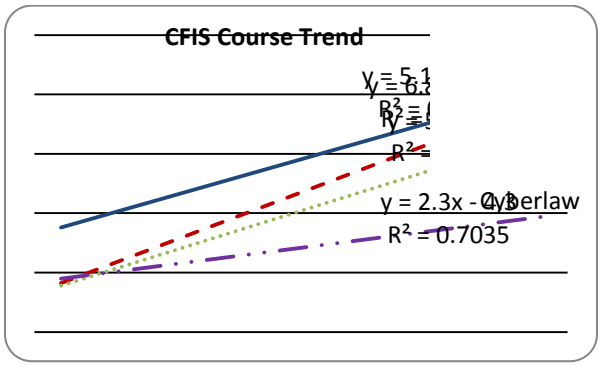


Figure 4. CFIS Course 5 Year Forecast

To further support the demand for this new program, freshman and transfer student enrollment can be analyzed. For the Fall 2011 start of the program, there were 16 incoming freshmen and four transfer students for the new degree. In comparison, for the Fall 2012 semester, there are 27 incoming freshmen and 14 transfer students (at the time of this research). The freshmen and transfer student enrollment for Fall 2012 seems to support the individual course enrollment forecasts depicted in Figure 4.

## 11. CONCLUSION

In five years (and among numerous challenges) a single course in Computer Forensics has evolved into a successful, four-year degree. Within only one year since the launch of the degree, there are approximately 75 students enrolled. This level of enrollment has exceeded the initial project of 50 students over a three-year period.

In addition to interests in the cyber forensics and security field, the success of this new program could also be attributed to the active involvement of working professionals and law enforcement. By soliciting input from professionals and law enforcement, our University's faculty were able to design a degree program that was practical and adequately met the needs of the growing workforce in this new area. Only time will tell, but all current indications point to a successful and prosperous degree program.

## 12. REFERENCES

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

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

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

Kessler, G.C., & Schirling, M.E. (2006). The design of an undergraduate program in

ISSN: 2167-1435
v29 n1957

computer and digital forensics. *The Journal of Digital Forensics, Security and Law,* 1 (3)m 37-50, 2006.

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

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.

U.S. Department of Labor Statistics, (2010). Economic releases.

Verizon. (2012). 2012 Data breach investigations report. Retrieved June 20, 2012 from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

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