Strengthening the Nexus: Government-Business-University cooperation and collaboration on security, training and research

November 1, 2011

Susan C. Aldridge, PhD
University of Maryland University College
UMUC’s Unique Attributes Contribute to Building a Pipeline of Cyber Warriors
University of Maryland University College

- Largest State University; 94,000 Students
- 28 Countries; 150 Locations
- Face to face instruction
- Award winning virtual campus
- 25,000 military service members
Workforce Relevant Degree Programs

• Mapped to industry standards
• Taught by scholar practitioners
• Close relationship to DoD and First Responders
• NSA/DHS Center of Academic Excellence in Information Assurance Education
UMUC was uniquely positioned for growth

- Global
- High tech
- Agile – ability to launch new programs
- Large contingent of clearance – ready students
- Creation of Cybersecurity Panel of Experts
GROWTH PROGRAMS: Cybersecurity Enrollments

Since unveiling its three degree programs and three graduate certificate programs, UMUC has received 5,300 applications, and enrolled close to 3,200 students.
Graduate School Approach

• Establish new Department for Cybersecurity and Information Assurance
  – Current IA specialization
  – 2 New Cybersecurity degree programs
  – Center for Security Studies
Degree Format – 36 credits

- CSEC 610 Cybersecurity and Cyberspace
- CSEC 620 Human Aspects in Cybersecurity: Ethics, Legal Issues, and Psychology
- CSEC 630 Prevention and Protection Strategies in Cybersecurity
- CSEC 640 Monitoring, Auditing, Intrusion Detection, Intrusion Prevention, and Penetration Testing
- CSEC 650 Cyber Crime Investigation and Digital Forensics
- CSEC 635 National Cybersecurity Policy and Law
- CSEC 645 Enterprise Cybersecurity Policy
- CSEC 655 Global Cybersecurity
- CSEC 670 Cybersecurity Capstone

MS Cybersecurity
Career Paths

• MS Cybersecurity
  – Chief security officer
  – Cybersecurity manager or administrator
  – Cybersecurity architect
  – Cybersecurity operations analyst
  – Cybersecurity engineer
  – Secure software assurance engineer
  – Cyber operations planner
Career Paths

- MS Cybersecurity Policy
  - Cyber policy analyst
  - Cyber intelligence analyst
  - Federal, state, and local government manager
  - Legislative aide
Program Articulations

- Articulation with Community Colleges
- Articulation with UMUC Graduate Programs
School of Undergraduate Studies Approach

- Integrate Cybersecurity with existing major in Information Assurance (IA).
- IA and Cybersecurity are closely related (but distinct) disciplines.
- Major is interdisciplinary – includes courses from several majors.
- External Consultant supported broadly-based undergraduate curriculum.
CSIA Degree Structure (33 sh)

Foundation Courses (9 sh):
- CSIA 301  Information System Architecture
- IFSM 304  Ethics in the Information Age
- CSIA 302  Telecommunications in Information Systems
  OR
- CMIT 265  Networking Essentials

Core Courses (12 sh):
- CSIA 303  Foundations of Information System Security
- CSIA 412  Senior System Managers and Security
- CSIA 413  System Administrators and Information Security
- CMIT 320  Network Security

Supplemental Courses (9 sh) chosen from:
- CCJS 421  Computer Forensics
- CSIA 454  Information System Security Mechanisms
- CSIA 457  Cybercrime and Cyberterrorism
- CSIA 459  Security Issues and Emerging Technologies
- IFSM 432  Disaster Recovery Planning
- IFSM 433  Information System Security Needs Assessment & Planning
- CMIT 321  Ethical Practice of Intrusion Prevention & Detection
- CMIT 425  Advanced Network Security

Capstone Course (3 sh):
- CSIA 485  Trends & projects in Cybersecurity & Information Assurance
Career Paths

B.S. Cybersecurity

A degree in cybersecurity prepares students for careers as information systems security professionals, senior systems managers and system administrators responsible for information systems and security of those systems.

- Systems security analyst
- Information security officer
- Systems administrator
- Security architect
- Malware analyst
- Computer crime investigator
- Security operations center analyst
- Intrusion analyst
- Vulnerability analyst
Course Components

- Interactive Case Study
- Technical Primers
- Reading Assignments
- Virtual Lab Exercises
- Learning Objects
- WebTycho LMS
- Threaded Discussions
Virtual Cybersecurity Lab

- Practical, hands-on exercises with live software (e.g., password cracking)
- Delivery at a distance
Learning Object - Content

Module Introduction

Like www.somebooks.com, most businesses today rely heavily on information technology (IT) and information systems (IS) to conduct key business operations. Information systems help organizations streamline their processes, automate activities, and increase efficiency. Many businesses implement basic security measures such as firewalls, antivirus software, and proxy servers to secure their IS from malicious attacks.

A security incident such as the one at www.somebooks.com can have serious consequences especially for online businesses. Therefore, it is critical for organizations to take cybersecurity seriously.

Before you get into the intricate maze that is cybersecurity, it is important to gain some ground knowledge about IS.

In this module, you will learn about IS and the need to secure these systems.
Learning Object – Computer Forensics

Figure 1.5
Hard Drive Platter and Read/Write Heads

- Platter
- Read/write head
- Actuator arm

Stop animation
Learning Object - Multimedia

Why Is Cyber Crime Increasing?

Before you learn about IS and the need to secure them against cyber crime, consider the conditions and factors that make cyber crime attractive to criminals.

Click Play to review each video. Then, click the Reflect button to ponder over a few related questions.

In this video, Harry D. Raduege Jr., Chairman, The Deloitte Center for Cyber Innovation, helps us understand why cyber crime is increasing.
New Undergraduate Courses Developed

- Social Networking and Cybersecurity Best Practices
- Basic Security Measures in Cyberspace
Cybersecurity Scholarships

• Through its successful Cyber Gala, UMUC raised $470,000 for cybersecurity scholarships.
• Awarded more than $362,000 in scholarships to nearly 100 students.
• Scholarships are merit-based.
Corporate Cyber Programs

- UMUC’s Corporate Learning Solutions (CLC) team signed 10 new alliance agreements this spring; currently has 28 prospects in the pipeline.
- Booz Allen Hamilton has more than 100 employees enrolled in one of UMUC’s three graduate cyber certificate programs.
Testimonies at Hearings

- UMUC Provost Dr. Greg von Lehmen testified in July before a Senate Small Business and Entrepreneurship Committee, chaired by Senator Ben Cardin (D-MD).

- UMUC staffing a 3 year legislative taskforce on Cybersecurity in Maryland.
Career Services

- 2 Virtual fairs - global
- 1 Face to face fair including Maryland Colleges and Universities.