Freely Available e-Resources as Collegiate Textbook in Undergraduate Cybersecurity Program
About UMUC

• One of 12 institutions under the University Systems of Maryland
• Over 94,000 students
• Largest public university in the U.S.
• Offered mostly online courses to non-traditional students
Undergraduate Cybersecurity

- Offered beginning Fall 2010
- Current enrollment: 3,891
- Bachelor of Science in Cybersecurity (120 credits):
  - 33 credits within the major
  - 41 credits in general education electives
  - 46 credits within minor or other general electives
- Can be completed fully online
- Two tracks: Policy and Technical
- Articulation agreements with all Maryland community colleges and many more across the U.S.
- Articulation agreement with UMUC Graduate School
E-Resources

• Initiated by UMUC Provost in Fall 2013
• Project Goal: 50% of all undergraduate courses will be using OER by Fall 2014 and 100% by Fall 2015
• Major revision in all courses to find OER
What is CSIA 303, Foundations of Information System Security?

1. Federal and State Laws influence information systems (IS) security policy
2. Standards and regulations also drive policy
3. As a result, IS security policy is then formulated
CSIA 303 E-Resources

- CSIA 303 students look at eResources to include:
  - NIST Publications
  - Public Laws (e.g., HIPAA, DCMA)
  - Standards (e.g., PCI/DSS and ISO-27000)
  - Current News Items and online publications
CSIA 303 E-Resources

• Benefit of e-resources within CSIA 303
  – Learning material is always fresh
  – Using same resources as practitioners in the field
  – Events receiving lots of public interest have students’ interests piqued
  – Processes of building IS security plans, disaster response plans, and business continuity plans are clearly visible
CSIA 413
Security Policy Implementation

Nancy M Landreville
Restructuring the Security Policy and Implementation Course

- E-resources
- Project focus
- Conference intensive
E-Resources


- Computer Forensics: A Pocket Guide by Nathan Clarke, IT Governance (c) 2010.
E-Resources

- NIST Guide to Information Technology Security Services
- NIST SP 800-53 rev. 4 – Security Controls
- NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014
- SANS 20 Critical Security Controls
- RAND Vulnerability and Assessment Guide
Project Focus

• Security Policy Framework (outline)
• Risk Assessment and Assignment of Security Controls
• Research Paper - (Security Policy)
• Business Continuity Plan
• Vulnerability Assessment Matrix
• Computer Forensic Analysis
• Organization Security Plan (comprehensive)
CSIA 459

• Course Objectives
  – research and evaluate emerging technologies objectively
  – identify new technologies for best-fit business solutions and determine secure implementation strategies
  – develop and communicate a recommendation based on research findings to the organizational stakeholders
  – define organizational considerations to implement recommendations
• Resources for Technology Life Cycles
CSIA 459

Source: http://www.atp.nist.gov/eao/gcr02-841/chapt2.htm
CSIA 459

• Resources for Researching Technologies
  – ACM Digital Library
  – Dissertations & Theses (Pro Quest)
  – IEEE Computer Society Digital Library
  – Science Direct
  – IEEE Spectrum (Web)

• Resources for Evaluation Methods
  – Shared Course Module with prerequisite course (Technology Evaluation)
  – Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340
• Resources for Evaluation Metrics
  – Five Pillars of Information Assurance: confidentiality, integrity, availability, authentication, and non-repudiation. Defined in CNSSI-4009 & discussed in Conflicts Among the Pillars of Information Assurance (IEEE IT Professional, July/August 2013)
• Content Resources
  – e-Books
    • Chapters 2 & 3 in *The Management of Technological Innovation: An International and Strategic Approach*
  – News Articles
    • *Cyber-Responders Seek New Ways to Respond to Cyberattacks*
CSIA 459

• Content Resources
  – Reports (Internet)
  – UMUC Produced Videos
    • Seven part interview with president of a local cybersecurity focused technology development firm.
CSIA 485
Practical Applications in Cybersecurity Management

Richard White
CSIA 485 E-Resources

- CSIA 458 Course Outcomes
  - **protect** an organization's critical information and assets by ethically integrating cybersecurity best practices and risk management throughout an enterprise
  - **implement** continuous monitoring and provide real-time security solutions
  - **analyze** advanced persistent threats and deploy countermeasures, and conduct risk and vulnerability assessments of planned and installed information systems
  - **formulate, update, and communicate** short- and long-term organizational cybersecurity strategies and policies

- Focus of each outcome is operational, which is best assessed using up-to-date and relevant case study examples from a wide variety of sources
CSIA 485 E-Resources

• Case Study – student activities that utilize e-resources
  – Risk Assessment
  – Gap Analysis
  – Technology Evaluation and Recommendations
  – Feasibility Assessment / Implementation
  – Policy, Training, Management

• E-resources provide the flexibility and specific “real world” context that help reinforce previous learning while providing a practitioner’s perspective.
CSIA 485 E-Resources

• Current e-resources within CSIA 485
  – NIST (various)
  – Daimler Chrysler Merger
  – Executive Guide to IT Architecture
  – Wachovia Merger
  – Conducting & Documenting a Security Gap Analysis
  – Current case studies (headlines, current events, and relevant cyber topics)
CSIA 485 E-Resources

• Benefit of e-resources within CSIA 485
  – Information is centralized
  – Resource diversity
  – Can be specific to course objectives
  – Provides more information from a variety of sources with an operational focus
  – On-demand and global accessibility
Questions?
Contact Information

• Jeff Tjiputra:
  – Jeff.Tjiputra@umuc.edu

• Ernest Rodgers:
  – Ernest.Rodgers@faculty.umuc.edu

• Nancy Landreville:
  – Nancy.Landreville@faculty.umuc.edu

• Valorie King:
  – Valorie.King@faculty.umuc.edu

• Richard White:
  – Richard.White@faculty.umuc.edu