fissea

Federal Information Systems Security Educators' Association

AWARENESS • TRAINING • EDUCATION

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

University of Maryland University College

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

University of Maryland University College

CSIA 303
Foundations of Information System Security

Ernest E. Rodgers

CSIA 303 E-Resources

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

University of Maryland University College

CSIA 413
Security Policy Implementation

Nancy M Landreville

Restructuring the Security Policy and Implementation Course

- E-resources
- Project focus
- Conference intensive

E-Resources

- Building an Effective Information Security Policy Architecture by Sandy Bacik, Auerback Pubications (c) 2008.

- A Manager’s Guide to ISO 22301: A Practical Guide to Developing and Implementing a Business Continuity Management System by Tony Drewitt, IT Governance (c) 2013.

- 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 Evaluating Emerging Technology

Valorie King

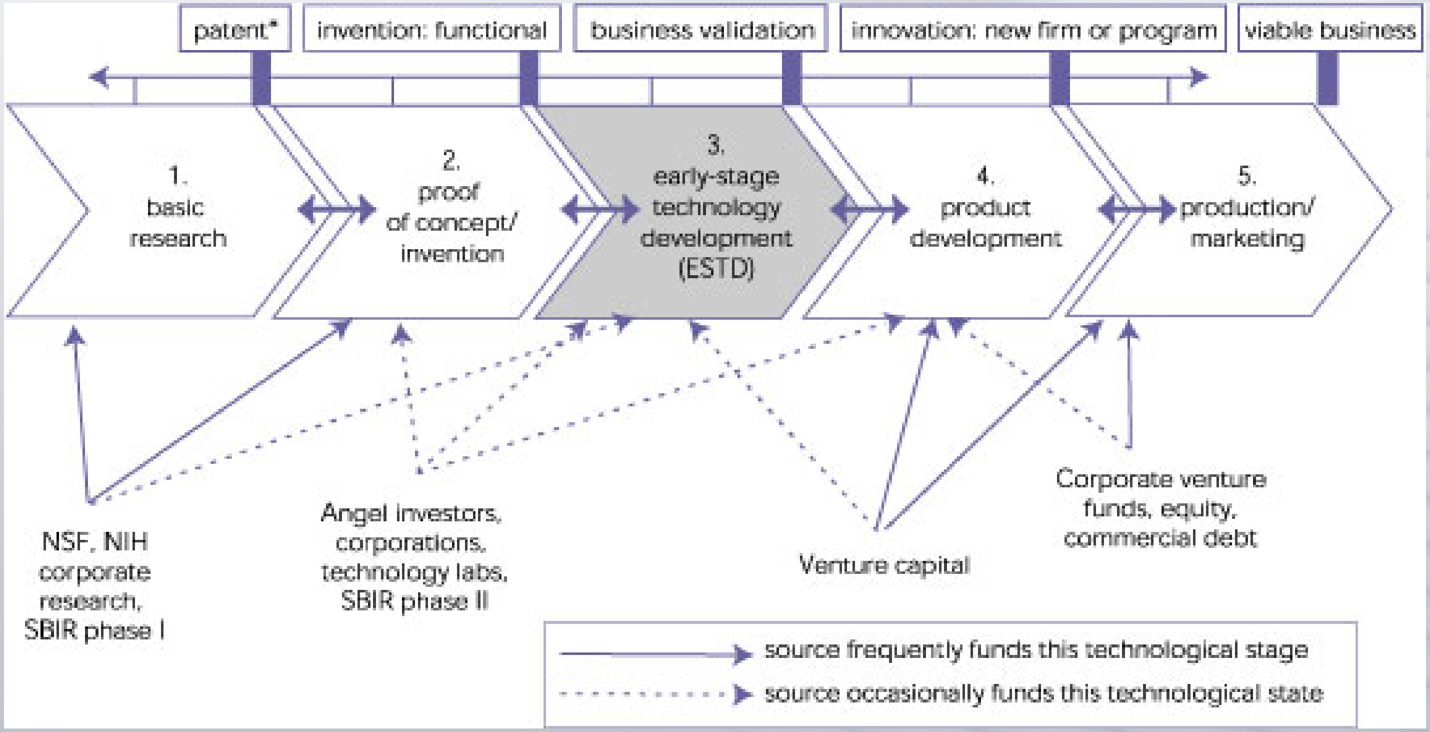
CSIA 459

- 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

CSIA 459

- Resources for Technology Life Cycles
  - **Technology Innovation Life Cycle** adapted from National Institute of Standards and Technology. (2002/2005). *Between invention and innovation an analysis of funding for early-stage technology development* (NIST GCR 02-841).
  - Viewpoint: Ready technology. *Communications of the ACM, 57*(2), 40-42.

CSIA 459



patent*

invention: functional

business validation

innovation: new firm or program

viable business

1. basic research

2. proof of concept/ invention

3. early-stage technology development (ESTD)

4. product development

5. production/ marketing

NSF, NIH corporate research, SBIR phase I

Angel investors, corporations, technology labs, SBIR phase II

Venture capital

Corporate venture funds, equity, commercial debt

source frequently funds this technological stage

source occasionally funds this technological state

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
  - The Delphi Technique http://www.britishcouncil.org/eltons-delphi_technique.pdf

CSIA 459

- 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)*
  - **Five Pillars of Information Security: protection, detection, reaction, documentation, prevention.** Original article by Amir Ameri in *Risk Management Magazine* http://cf.rims.org/Magazine/PrintTemplate.cfm?AID=2409

CSIA 459

- 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* http://www.govtech.com/security/Cyber-Responders-Seek-New-Ways-to-Respond-to-Cyberattacks.html?page=2
    - Malykhina, E. (2014, March 3). Feds look to Big Data on security questions. *Information Week.* Retrieved from http://www.informationweek.com/government/big-data-analytics/feds-look-to-big-data-on-security-questions/d/d-id/1114062

CSIA 459

- Content Resources
  - Reports (Internet)
    - U.S. Department of Homeland Security (DHS) Science and Technology Directorate. (2013). *Transition to practice (TTP) technology guide* (vol 2). Retrieved from https://www.dhs.gov/sites/default/files/publications/csd-ttp-technology-guide-volume-2.pdf
    - *Research Questions and Challenges for a Smart and Sustainable Community System* (Carnegie-Mellon). http://www.cmu.edu/silicon-valley/smart-communities/research-questions-and-challenges.pdf
  - UMUC Produced Videos
    - Seven part interview with president of a local cybersecurity focused technology development firm.

University of Maryland University College

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