Syllabus for CS6863

Course Description and objectives

The course and lectures will cover some of the fundamental areas of information security including cyber threats, identity & access management, data protection, incident response, third party risk, security monitoring, security outsourcing, and mobile security.

This course will not be about the technologies of information security, rather management of information security. A broad (but not detailed) knowledge of information security technologies is assumed. CS6813 or equivalent. A working understanding of basic security threats and defensive technology from an undergraduate course or professional experience is sufficient. The full depth of these courses is not needed, and a single basic course in information security from another university is sufficient. Note that students who do not have the prerequisites in the past have often struggled to earn a grade of C.

Policies and Grading

Course policies, grading, contact information, etc. are in the “Policies and Grading” section in the General Course Information area on the course web site. All students are responsible to understand the contents of that document and follow the policies laid out there. That document describes a term project to be performed by student in teams. The teams will present reports on their projects to the class for discussion.
Week by week list of course topics

1. Introduction:
   - Fundamentals of information security management - course overview and expectations.
   - Term project approach goals, teaming, and expectations.
   - Weekly discussion topic and assignment.

2. IS program, policy management, and security governance
   - Information security program.
   - Security policy management.
   - Security governance.

3. Business priorities, secure development, and training & awareness
   - Business priorities and information security risks.
   - Integrating security into software development process.
   - Security training and awareness.

4. Cyber threats and information security risks
   - Cyber Threats, including motivation, trends, and threat monitoring
   - General principals of risk analysis

5. IT risk analysis, risk management, and security risk metrics
   - Major steps of risk analysis (probability, impact, prioritization, etc.).
   - Approaches to managing risks (reduction, mitigation transfer, and acceptance).
   - Managing risk with metrics.

6. Identity and access management (IAM)
   - What is it? Identity and access management approach.
   - IAM service components (manage access, enforce access, report access)
   - IAM reference architecture and strategy

7. Data protection
   - Identifying critical assets / data classification (data elements, PII, process)
   - Data loss prevention (data in motion, data at rest, and data at endpoint)
   - Data privacy (privacy laws, data flow, data inventory, integrated framework)

8. Incident response planning and business continuity
   - Security incident response planning (prepare, identify, assess, contain, investigate, resolve, learn).
   - Business Continuity Planning: making sure the organization can continue functioning after a security incident.
9. Term Project Preliminary Gate Review
   - Each team will present their preliminary (high level) project approach for instructor feedback and guidance.

10. Third party risk management
    - Third party risk management.
    - Third party risk assessment.

11. Security monitoring
    - Security monitoring overview and how it can help manage risk.
    - Overview of security monitoring data, logging requirements, and monitoring tools.

12. Cloud security
    - Models (SaaS, PaaS, IaaS).
    - Cloud security concerns and risks.
    - Which applications and data can be migrated to the Cloud?
    - Impact to traditional security management.

13. Mobile security, outsourcing, auditing
    - Approaches to securing mobile devices
    - Emerging challenges, including Bring your own device (BYOD)
    - Overview of managed security services.
    - Evaluation and assurance and information security audits.

14. Term Final Gate Review: each team will present their final (detailed) project design for class discussion and instructor feedback.
    - This review is essentially an outline of the project final report. Complete Term Project Report Due finals week.

Textbooks:

Please see the content item on textbooks in the “Course General Information” section of this course.