MORGAN STATE UNIVERSITY
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
COURSE SYLLABUS
FALL, 2015
ONLINE EEGR.483 INTRODUCTION TO SECURITY MANAGEMENT
CREDITS: 3

THIS COURSE IS A SENIOR ELECTIVE IN THE ECE DEPARTMENT.

INSTRUCTOR: THIERRY WANDJI
EMAIL: KETCHIOZO.WANDJI@MORGAN.EDU

CATALOG DESCRIPTION

This course will provide a background in the many aspects of security management associated with today's modern communications and networks. It includes the fundamentals of Risk Analysis, Risk Management, Security Policy, Security Operations, Legal issues, Business issues and Secure Systems Development.
Prerequisite: EEGR 317

COURSE OBJECTIVES

This course provides students with knowledge and skills in the fundamental theories and practices of Security Management Upon completion of the course a student is expected to:

CO1: Understand the role of Security Management in information technology systems

CO2: Quantify the properties of Information Security

CO3: Develop project plans for secure complex systems with knowledge of SANS 20 critical controls

CO4: Demonstrate understanding of the role of firewalls, guards, proxy servers and intrusion detection in networks on a Linux OS with traffic analysis

CO5: Evaluate the residual risk of a protected network

CO6: Provide forensics and other security management solutions in compliance with the policies and practices currently accepted in the industry as incident response.

CO7: Apply legal and ethical standards in the Information Security context.

COURSE CONTENT AND KNOWLEDGE BASES

This course will cover theory and application of: security management, security design, .network vulnerabilities, application of cryptography, risk analysis, and legal and ethical behavior.
The knowledge base is multidisciplinary and draws from which the course content is drawn is Business Management, Computer Engineering, System Management, and Sociology.

COURSE REQUIREMENTS

This course is an elective course for all engineering graduate students, especially those with the computer engineering, communications concentration, or cyber security interest. This course relates heavily to the EEGR410/480/481/482. In conjunction with the other courses, this course will help the student develop a breadth of understanding in security applications. Students are expected to prepare and participate in the lectures. Lectures will selectively cover material in the text and will draw from other reference sources.

Homework assignments and quizzes will consist of selected problems from the text and/or other sources. As this topic has a large applied element, class projects will be an important element of the learning experience for this topic. These projects will be accomplished using MATLAB and C programming languages or other Linux based platforms. Projects will represent a significant portion of the grade.

One examination will be given during the course. A comprehensive final project will be assigned in lieu of final exam. Depending on the scope of the project, working in a group is possible, given that the tasks of individuals are well defined in the project proposal.

Course Schedule/Session Format		
Content	**Date**	**Topic**
Module 1		**Introduction (CO1)** Brief introduction to security management and to the different cyber security courses taught at Morgan State. The topics in this module include cyber risks, basic computer security and network security concepts.
Module 2		**Threats, Risks and SANS 20 Critical Controls Overview (CO1, 3)** Describes SANS 20 critical control for security management as well as the following key cyber security concepts: Threats, Vulnerabilities. Also, in this module SANS 20 critical controls for security management will be identified, basic vulnerabilities and threats will be presented, key terms in will be defined.
Module 3		**Risk modeling and IT risk framework.(CO2)** In this module, a novel risk framework is introduced. Numerical risk computation is explained. Quantification of risk and costs associated with attacks are explained and determined this will help student to compare the advantages and disadvantages of various risk assessment methodologies. This module also explain how to balance the defense and control to minimize cost associated with successful breach. In this module the student will learn how to program the risk framework in MATLAB and simulate attacks. Simulate and illustrate Monte Carlo average of the cost based on different balancing strategies.
Module 4		**Risk decisions and IT risk framework analysis**. **(CO2, 4, 5)** In this module we continue analyzing the IT risk framework from the previous module but this time with a clear focus on MATLAB simulation of the risk and decision making. This module will teach students how to make reasonable decisions to minimize the cost of a cyber-attack based on simulation of the risk. Students will also be able to evaluate and categorize risk.

Module 5		**Risk management**.**(CO5, 6)** In this module, we will analyze NIST 800-30 and 800-39 documents. We will also learn how to assess security risks and costs based on NIST 800-30/39 document and discuss risk assessment from NIST POV. Lastly, students will learn various risk analysis methodologies and how to Make decisions on risk management issues based on the NIST guidelines and Program a risk assessment model to understand the relation between risk and system security policy.
Module 6		**Forensic and incident response**. **(CO6)** In this module, we will start the discussion on monitoring, forensics and incident response. Identify key terms in security monitoring, identify key concepts in forensic analysis, and make recommendation on incident response given any scenario.
Module 7		**More on Incident response. (CO6)** In this module, we will have a closer look of the NIST SP800-61 document and we will identify SP800-61 key goals. Also, incident response mechanisms will be explained as well as how to select the best response possible in any given situation.
Module 8		**Forensic and Exam review. (CO6)** In this module, we will have a closer look of the NIST SP800-86 document. Students will be able to describe the methodologies used in network forensics. Cyber forensics will be studied in details as well as how to select the best forensic analysis in any given situation.
Module 9		Midterm Exam
Module 10		**Forensic (CO6)** In this module, we will continue the analysis of the SP800-86 document. After completion of this module students will successfully be able to identify key steps to handle an incident, integrate forensic techniques into incident response, and use data from data files for forensic analysis, use data from operating systems for forensic analysis. Lastly, detect and prevent intrusion.
Module 11		**Linux Operating System**. **(CO4)** In this module, we will analyze NIST SP800-69 document in details as well as different forensic topics and will identify core components of OS. As a hands-on activity, student will download and use LINUX OS to perform different forensic analyses and capture packet for analysis which will enable students to analyze and decipher network traffic, identify anomalous or malicious activity and provide a summary of the effects on the system.
Module 12		**Supply Chain Risk Management Practices. (CO6)** In this module, we will review NIST SP800-161 (Supply Chain Risk Management Practices for Federal Information Systems and Organizations). After completion of this module students will be able to identify core components ICT SCRM controls, integrate ICT SCRM into organization wide risk management, and identify ICT supply chain threat events.
Module 13		**Policy, legal and ethical implications of the security management. (CO7)** In this module, we will look into data security and its importance. Also, we will look into Legal, Ethical and compliance issues regarding data security and identity theft. After completion of this module students will be able to identify the risk of identity theft, distinguish different data handling policies, and explain different federal and statewide policies related to cyber security and acts addressing issues of data security such as HIPAA/FERPA.

Module 14		**LEGAL AND ETHICAL ISSUES IN COMPUTER SECURITY.(CO7)** In this module we will continue evaluating legal, ethical and compliance issues regarding computer security. Also, we will review the materials summary of all the modules presented throughout the semester in order to get ready for the final exam. After completion of this module students will define the key legal terms in computer security such as Patents, copyrights, and IP in Information Concept. Identify different computer crimes, examine a computer fraud case for ethical issues, and comply by the rules of the ethics as dealing with cybercrimes.
Module 15		Review of the course and Final project discussions

FORMAT

Online

GRADING

Projects and assignments	**20%**
Midterm Exam	**20%**
Quizzes	**20%**
Discussion board	**20%**
Final Project	**20%**

NOTE: Any material submitted that is substantially copied from other students without citation or from the Internet will receive a zero grade.

EXPECTATIONS AND REQUIREMENTS

- Students are expected to log on to at least Bb 3 times a week.
- Students are expected to be actively engaged on the discussion board conversations.
- Homework and other assignments are due by midnight of the given due date. 5% Late penalty will be deducted for late submission.
- Academic misconduct or cheating during an exam will result in an F grade for the course.

RELATIONSHIP TO CURRICULUM SEQUENCE

This course is part of a Cyber Security series of courses EEGR480, 481, 482, 483

BIBLIOGRAPHY

Required: Whitman, M Management of Information Security, Thompson,

Recommended: Pfleeger, C.P., Security in Computing, Prentice Hall, Copyright 2010 ISBN 0-13-239077-9

Schneier, Bruce. *Applied Cryptography*, Second Edition, John Wiley & Sons, 1996. ISBN 0-471-11709-9