River Valley Community College
One College Place
Claremont, NH 03743

March 2012

ENTERPRISE SECURITY MANAGEMENT

CURRICULUM AND COURSE NUMBER: CYBS 130R
DEPARTMENT: Business/Computer Technology
CREDIT HOURS: 3
SEMESTER HOURS: **CLASS:** 2 **LAB:** 2
PREREQUISITES/COREQUISITES: CYBS 120R

COURSE DESCRIPTION

Students will understand the principles of risk management, security architectures, incident handling, disaster recovery, and secure systems administration.

Course Competencies:
Upon successful completion of this course, the student will be able to:

1. Contingency Planning: In this topic, you will take a look at various types of disasters that can befall an organization and put it out of business—unless the organization has implemented some form of business continuity planning. You will look at how such plans can be developed and tested.
    a. Identify disaster types, examine issues relate to contingency planning, and consider the role of security policies as part of an overall contingency planning strategy
    b. Analyze contingency planning goals, and review the testing of such plans
    c. Study the effect of electrical power loss for networks and the backup planning required to prevent such events
    d. Examine data-backup strategies for various operating systems and perform tasks related to backups
2. Performing a Risk Analysis: In this topic, you will be introduced to the concepts and issues surrounding one of the more debated areas of security – Risk Analysis. You will see different methods of risk analysis, different standards, and different techniques to minimize risk. All of these issues, concepts, and techniques lead up to the same goal, to perform a risk analysis.
    a. Define the concepts of risk analysis
    b. Examine the methods of risk analysis
    c. Describe the process of risk analysis
    d. Describe the techniques available to minimize risk
    e. Examine the principles of performing a continuous risk assessment
3. Creating a Security Policy: In this topic, you will examine the concepts of security policies and their implementation. You will be introduced to different methods of policy creation and implementation, and you will create a policy document. You will also examine the methods of security response and how response is related to policy.
    a. Describe the concepts of security policies
    b. Examine the standards of security policy design

c. Describe the individual policies in a security policy
d. Examine a detailed, complete policy template
e. Describe the policy procedures for incident handling and escalation
f. Define the common procedures for strategic partner connections in a security policy
g. Create a scenario-based security policy document

4. Certification and Accreditation: In this topic, you will examine the certification and accreditation process of information systems as outlined for the federal government. You will study in detail the four phases of the process used and the duties and responsibilities of the key participants. You will also explore applications of the certification and accreditation process for non-government organizations.
    a. Examine and understand the background information for the Certification and Accreditation Process
    b. Identify the laws and regulations governing the Certification and Accreditation Process
    c. List the phases of the Certification and Accreditation Process and give a definition for each of those phases and their associated activities and tasks
    d. List and define the roles and responsibilities of the individuals involved in the Certification and Accreditation Process
    e. Understand the System Security Authorization Agreement (SSAA) and practice using tools and templates used to create a SSAA
    f. Examine the NIST Special Publication 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems". Compare the NIST SP 800-37 methodology to the DITSCAP and DIACAP processes and identify the differences
5. Introduction to Trusted Networks: In this topic, you will be introduced to the fundamental concepts of building trusted networks and the Public Key Infrastructure.
    a. Define the need to develop trusted networks
    b. Identify the function of both authentication and identification
    c. Examine the components of a Public Key Infrastructure (PKI)
    d. Indentify the applications of PKI
6. Cryptography and Data Security: In this topic, you will be introduced to the concepts of cryptography and its function in data security. You will examine how cryptography has evolved, encryption and decryption systems, private key and public key algorithms, and key lengths.
    a. Describe the history of cryptography
    b. Describe the function of math in cryptography
    c. Describe the process of private key cryptography
    d. Describe the process of public key cryptography
    e. Identify the function of message authentication
7. Law and Legislation: In this topic, you will be introduced to the common laws and pertinent legislation regarding information security, computing, and network technologies. You will be exposed to laws and legislation, and although the concepts in this topic are global, every state and/or country has different laws and regulations; those in this topic are primarily from the United States regarding security, computers, and network technologies.
    a. Examine the concepts of intellectual properties
    b. Identify the primary categories of law
    c. Examine the process of handling evidence for a trail
    d. Examine computer-related laws and legislation

8. Biometrics – Who You Are: In this topic, you will examine the process of biometrics, their accuracy, and their application. You will determine the characteristics of common biometrics, and examine methods of compromising biometric systems.
    a. Describe the core concepts of biometrics
    b. Examine the accuracy of biometrics
    c. Identify applications of biometrics
    d. Implement and examine fingerprint scanning
    e. Examine facial scanning
    f. Implement and examine iris and retinal scanning
    g. Implement and examine vocal scanning
    h. Examine uncommon biometrics
    i. Examine methods of compromising biometrics
9. Strong Authentication: In this topic, you will learn about strong authentication. You will step through examples of authentication solutions, such as tokens and biometrics.
    a. Describe strong authentication
    b. Examine authentication tokens
    c. Implement an authentication token system
    d. Examine smart cards
10. Digital Certificates: In this topic, you will examine various ways we establish our identity in the real world, examine an important document recognized internationally, review various tamper-proofing methods and mechanisms for such documents, and look at the electronic equivalents for such documents.
    a. Examine the various ways that identities are established in the world
    b. Examine the role of an authority that thoroughly examines applications and then issues some form of identity document, such as a certificate
    c. Examine issues surrounding the protection of the sanctity of a Certificate Authority
    d. Distinguish between the purposes of certificates issued in the physical world versus the digital world
    e. Examine key standards specified for digital certificates
    f. Examine the X.509 authentication standard as defined by the ITU and the information contained in an X.509 certificate
    g. Perform a case study of one of the leading Certification Authorities
11. Digital Signatures: In this topic, you will work with message digest and symmetric-key encryption algorithms to define the structure of digital signatures.
    a. Compare digital signatures with real world signatures
    b. Examine the features of digital signatures and their requirements for use in e-commerce
    c. Describe how digital signatures function
    d. Examine the various types and emerging standards for digital signatures
    e. Examine the digital signature applications and protocols used

Course Outline:

1. Risk Analysis
2. Security Policies
3. Business Continuity Planning
4. Common Criteria
5. Certification and Accreditation
6. Biometrics
7. Strong Authentication

Learning/Instructional Methods:

Lectures	Discussions
PowerPoint Presentations	Term Papers
Lab and Reading Assignments	

Performance Evaluation:

Midterm and Final Exams	Weekly written assignments
Term Paper	Discussion participation
Quizzes	

Suggested Text(s): Please refer to syllabus

Origination date: March 2012

Revisions: