

COURSE OUTLINE

CMSY-145

Internet Security and Risk Management

3 Semester Hours

HOWARD COMMUNITY COLLEGE

Description

Students will learn about ways of protecting an ebusiness against unique risks and exposures, will explore insurance coverages (and their exclusions) that are specific to electronic business, and steps business managers should take to manage risks. This course examines ways in which technological advances in computer and operating systems have placed data, as a tangible asset, at risk. This course is an overview of internet security and risk management issues. It is not designed to train students to be security experts or to implement security systems. Prerequisite: CMSY-126 and CMSY-139 or CMSY-129. (3 hours weekly)

Overall Course Objectives

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

1. Describe general risks of doing online business and recommended protective measures.
2. Describe insurance contracts and coverages that protect ecommerce ventures.
3. Set up a digital signature online and demonstrate the ability to use it in email messages to the instructor and other classmates.
4. Outline symmetric and public key cryptographic techniques.
5. Describe how message digests work.
6. Explain application of public key algorithms.
7. Define system and network security.
8. List principal internet security protocols and how they work.
9. Define a Virtual Private Network, including its features, components, and deployment.
10. Identify the appropriate payment protocols for a variety of instances.
11. Identify the appropriate PKI recommendation for a variety of instances.
12. Understand exclusions in various insurance coverages that do not provide coverage for ecommerce exposures.
13. Analyze security risks in a fictitious company and make recommendations to reduce risk.

Major Topics

I. **Risks of Internet Exposure**

Fraud through misappropriation of funds
Disruption of service
Theft of confidential corporate information
Negative public image and loss of consumer confidence
Hackers
Copyright infringement
Trademark infringement
Trade secrets
Exposure to risk by employees
Stolen identity
Invasion of privacy
Use and abuse of metatags
Exposures for credit card fraud

II. Insurance Contracts, Coverages, and Exceptions

Insuring agreement - promises/operations and products/completed operations
Contractual liability
Advertising liability
Personal injury
Exclusions: contractual, damage to property, personal and advertising injury
Professional liability
Commercial umbrellas and commerce protection policies
Business income loss
PR expenses
Interruption of service liability
Electronic publishing liability
Defense expenses
Investigation expenses
Protecting intellectual property

III. Security and Cryptography

Symmetric and public key encryption

IV. Public Key Infrastructure (PKI)

Digital certificates
Digital signatures
Public key infrastructures

V. Network and Application Security

Security Protocols
Application and Messaging Security
Virtual Private Networks

VI. Consumer Payment Protocols

Consumer to Business Commerce - payment system requirements
 Privacy, authentication, integrity, nonrepudiability
 Microtransactions
 Certification Authorities and classes of certificates
 SET Protocols - protection of payment made over the internet
 Digital wallets
 SSL
 Online Payments
 Digital cash (anonymous cash and micropayments, smart cards), electronic checks, online credit cards, Joint Electronic Payments Initiative
Business to Business Commerce - EDI

Course Requirements

Grading/exams: Grading procedures will be determined by the individual faculty member but will include: quizzes and written papers for a fictitious company described by the instructor. One paper will be a security risk analysis report, and one will be a report outlining a plan for cryptography and payment protocols.

Other Course Information

To be successful in this course, students must spend a significant amount of time on coursework outside of class.