STATE UNIVERSITY OF NEW YORK
COLLEGE OF TECHNOLOGY
CANTON, NEW YORK

MASTER SYLLABUS

CYBR250 – Information Security

Created by: Kambiz Ghazinour

SCHOOL OF SCIENCE, HEALTH & CRIMINAL JUSTICE
FALL 2020

A. **TITLE**: Information Security

B. **COURSE NUMBER:** CYBR250

C. **CREDIT HOURS:** 3

- 3 hours of lecture per week
- Course length: 15 weeks

D. **WRITING INTENSIVE COURSE**: No

E. **GER CATEGORY:** None

F. **SEMESTER(S) OFFERED:** Fall

G. **COURSE DESCRIPTION:** An introduction to various technical and administrative aspects of Information Security and Assurance. Students are exposed to the spectrum of Information Security activities, methods, methodologies, and procedures. Coverage include inspection and protection of information assets, detection of and reaction to threats to information assets, and examination of pre- and post-incident procedures, technical and managerial responses and an overview of Information Security planning and staffing functions.

H. **PRE-REQUISITES/CO-REQUISITES:**

a. Pre-requisite(s): CYBR 165 Survey of Cybersecurity or CITA 220 Data Communications and Network Technology
b. Co-requisite(s): none
c. Pre- or co-requisite(s): none

I. **STUDENT LEARNING OUTCOMES:**

By the end of this course, the student will be able to:

Course Student Learning Outcome [SLO]	***PSLO***	***ISLO***
a. Specify information assets	3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5
b. Specify threats to information assets	3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5
c. Define an Information Security strategy and architecture	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	5
d. Exhibit an approach to plan for and respond to intruders in an information system	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	5
e. Describe legal and public relations	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and	5

implications of security and privacy issues	complete all work in compliance with relevant policies, practices, processes, and procedures	
f. Demonstrate a disaster recovery plan for recovery of information and assets after an incident.	2. Interpret, produce, and present work-related documents and information effectively and accurately. 5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	5

J. APPLIED LEARNING COMPONENT: **Yes**__X___ **No**_____

- Computer Lab Classroom

K. TEXTS: Computer Security: Principles and Practice, 3rd Edition By: Stallings, William and Brown, Lawrie Pearson Education Inc. (publishing as Prentice Hall), 2015, ISBN 978-0-13-377392-7

L. REFERENCES: Various online resource such as SUNY Canton Library Books24x7 ITPro Book Database, Blackboard slides. All Power Point presentations are created by myself, Dr. Ghazinour, and are intended for use in this course.

M. EQUIPMENT: Computer lab classroom

N. GRADING METHOD: A-F

O. SUGGESTED MEASUREMENT CRITERIA/METHODS:

- Participation
- Discussions
- Assignments
- Tests

P. DETAILED COURSE OUTLINE:

- Introduction to Information Security
  - Computer Security Concepts
  - Threats, Attacks, and Assets
  - Security Functional Requirements
  - Fundamental Security Design Principles
  - Attack Surfaces and Attack Trees
  - Computer Security Strategy
- Cryptographic Tools
  - Confidentiality with Symmetric Encryption
  - Message Authentication and Hash Functions
  - Public-Key Encryption
  - Digital Signatures and Key Management
  - Random and Pseudorandom Numbers
  - Practical Application: Encryption of Stored Data
- User Authentication
  - Electronic User Authentication Principles
  - Password-Based Authentication
  - Token-Based Authentication
  - Biometric Authentication
  - Remote User Authentication
  - Security Issues for User Authentication
  - Practical Application: An Iris Biometric System
  - Case Study: Security Problems for ATM Systems
- Access Control
  - Access Control Principles
  - Subjects, Objects, and Access Rights
  - Discretionary Access Control
  - Example: UNIX File Access Control
  - Role-Based Access Control
  - Attribute-Based Access Control
  - Identity, Credential, and Access Management
  - Trust Frameworks
  - Case Study: RBAC System for a Bank
- Database and Cloud Security
  - The Need for Database Security
  - Database Management Systems
  - Relational Databases
  - SQL Injection Attacks
  - Database Access Control
  - Inference
  - Database Encryption
  - Cloud Computing
  - Cloud Security Risks and Countermeasures
  - Data Protection in the Cloud
  - Cloud Security as a Service
- Malicious Software
  - Types of Malicious Software
  - Advanced Persistent Threat
  - Propagation – Infected Content - Viruses
  - Propagation – Vulnerability Exploit - Worms
  - Propagation – Social Engineering – SPAM E-Mail, Trojans

    - Payload – System Corruption
    - Payload – Attack Agent – Zombie, Bots
    - Payload – Information Theft – Keyloggers, Phishing, Spyware
    - Payload – Stealthing – Backdoors, Rootkits
    - Countermeasures
- Denial-of-Service Attacks
    - Denial-of-Service Attacks
    - Flooding Attacks
    - Distributed Denial-of-Service Attacks
    - Application-Based Bandwidth Attacks
    - Reflector and Amplifier Attacks
    - Defenses Against Denial-of-Service Attacks
    - Responding to a Denial-of-Service Attack
- Intrusion Detection
    - Intruders
    - Intrusion Detection
    - Analysis Approaches
    - Host-Based Intrusion Detection
    - Network-Based Intrusion Detection
    - Distributed or Hybrid Intrusion Detection
    - Intrusion Detection Exchange Format
    - Honeypots
    - Example System: Snort
- Firewalls and Intrusion Prevention Systems
    - The Need for Firewalls
    - Firewall Characteristics and Access Policy
    - Types of Firewalls
    - Firewall Basing
    - Firewall Location and Configurations
    - Intrusion Prevention Systems
    - Example: Unified Threat Management Products
- Buffer Overflow
    - Stack Overflows
    - Defending Against Buffer Overflows
    - Other Forms of Overflow Attacks
- Software Security
    - Software Security Issues
    - Handling Program Input
    - Writing Safe Program Code
    - Interacting with the Operating System and Other Programs
    - Handling Program Input
- Operating System Security
    - Introduction to Operating System Security
    - System Security Planning
    - Operating Systems Hardening
    - Application Security
    - Security Maintenance
    - Linux/UNIX Security
    - Windows Security
    - Virtualization Security
- Trusted Computing and Multilevel Security
    - The Bell-LaPadula Model for Computer Security
    - Other Formal Models for Computer Security
    - The Concept of Trusted Systems

    - Application of Multilevel Security
    - Trusted Computing and the Trusted Platform Module
    - Common Criteria for Information Technology Security Evaluation
    - Assurance and Evaluation
- IT Security Management and Risk Assessment
    - IT Security Management
    - Organizational Context and Security Policy
    - Security Risk Assessment
    - Detailed Security Risk Analysis
    - Case Study: Silver Star Mines
- IT Security Controls, Plans and Procedures
    - IT Security Management Implementation
    - Security Controls or Safeguards
    - IT Security Plan
    - Implementation of Controls
    - Monitoring Risks
    - Case Study: Silver Star Mines
- Physical and Infrastructure Security
    - Overview
    - Physical Security Threats
    - Physical Security Prevention and Mitigation Measures
    - Recovery from Physical Security Breaches
    - Example: A Corporate Physical Security Policy
    - Integration of Physical and Logical Security
- Human Resources Security
    - Security Awareness, Training, and Education
    - Employment Practices and Policies
    - E-Mail and Internet Use Policies
    - Computer Security Incident Response Teams
- Security Auditing
    - Security Auditing Architecture
    - The Security Audit Trail
    - Implementing the Logging Function
    - Audit Trail Analysis
    - Example: An Integrated Approach
- Legal and Ethical Aspects
    - Cybercrime and Computer Crime
    - Intellectual Property
    - Privacy
    - Ethical Issues
- Internet Security Protocols and Standards
    - Secure Email and S/MIME
    - DomainKeys Identified Mail
    - Secure Sockets Layer (SSL) and Transport Layer Security (TLS)
    - HTTPS
    - IPv4 and IPv6 Security
- Internet Authentication Applications
    - Kerberos
    - X.509
    - Public-Key Infrastructure
    - Federated Identity Management

Q. LABORATORY OUTLINE: N/A