Standard Course Outline
IS 656 Information Systems Security and Assurance

I. General Information

- Course number: IS 656
- Title: Information Systems Security and Assurance
- Units: 3
- Prerequisites: Graduate standing
- Course Coordinator: Spiro Samonas
- SCO Prepared by: Spiro Samonas
- Date prepared/revised: Aug 24, 2016

II. Catalog Description

Managerial and technical aspects of cybersecurity. Principles and best practices of security governance and management. Network security and cryptography. Incident response and computer forensics. Ethical hacking. Individual project. Letter grade only (A-F).

III. Course Objectives, Student Learning Outcomes, Evaluation Instruments, and Instructional Strategies for Skill Development

OUTLINE OF SUBJECT MATTER and COURSE OBJECTIVES

Over the last decade alone, we have witnessed an enormous amount of cybersecurity breaches that have made the headlines. Motivated insiders and/or outsiders have been particularly successful at criminal acts such as stealing information, defrauding enterprises or engaging in acts of industrial espionage using computers. Cybersecurity breaches are a major threat to the global economy and can have a devastating financial impact on the victim. As organizations are nowadays exposed to more information security attacks than ever before, adequate measures need to be put in place to ensure the security and systemic integrity of an enterprise.

This course discusses the most important recent developments in cybersecurity. Adopting an interdisciplinary approach that draws on fields such as Information Systems, Computer Science, Psychology, Criminology and Accounting, the course provides a detailed overview of cybersecurity threats and vulnerabilities, potential compromises and related protection mechanisms. Topics include the security of communications, networks and infrastructure, IT audit and compliance, best practices in security policy formulation, the use of computer forensics for the detection and prevention of cybercrime in business, and security problem solving in the context of incident response.

MEASURABLE OUTCOME

Students who pass IS 656 must demonstrate the following;

- demonstrate an understanding of various kinds of cyberattacks and malicious threats, including external attacks, network intrusion, viruses, Trojan Horses and worms.
- ability to evaluate the financial and managerial impact of cybersecurity in a business environment.
- recognize the social and organizational aspects of designing, deploying and managing defensive measures, and technical solutions in cybersecurity.
- understand how cryptography and steganography works through hands-on exercises.
- examine incident response methodologies and best practices through real industry cases.
- perform ethical hacking tasks (for instance, footprinting, SQL injection, network scanning, etc.), as well as computer forensic investigations in a lab environment to understand how security vulnerabilities work.

LEARNING OBJECTIVES

The primary learning objective of this course is to develop a conceptual framework and the analytic skills to understand the variety of management, technology, and funding issues related to constructing a viable business model. The specific learning objectives of this course are as follows:

- **Critical Thinking Skills**: Students will be able to demonstrate conceptual learning, critical thinking, and problem-solving skills. More specifically, students will be able to:
  - Research and systematically examine cases of known cybersecurity breaches in business, and critically evaluate potential solutions.
  - Identify and address cybersecurity risks and vulnerabilities by developing defensible recommendations based on the relevant facts, and effectively communicating these recommendations both orally (e.g., presentations, class discussion) and in writing.
- **Interpersonal, Leadership, and Team Skills**: Students will be able to demonstrate interpersonal and leadership skills for working in a dynamic and diverse world, both independently and in a team environment. More specifically, students will be able to:
  - Manage an individual project and deliver a written report and a formal presentation in front of their peers.
- **Ethics**: Students will be able to demonstrate awareness and knowledge of social responsibility, ethical leadership, and citizenship issues in the local, regional and world communities. More specifically, students will be able to:
  - Demonstrate understanding of the ethical and social aspects of security governance and management.
- **Business Functions Skills**: Students will be able to demonstrate understanding of all business functions, practices and related theories and be able to integrate this functional knowledge in order to address business problems. More specifically, students will be able to:

- Recognize the technical, managerial, economic, ethical and organizational challenges that cybersecurity poses to modern enterprises.

- **Quantitative & Technical Skills**: Students will possess quantitative and technological skills enabling them to analyze, interpret, and communicate business data effectively and to improve business performance. More specifically, students will be able to:
  - Practice elementary coding for security in Python.
  - Develop an appreciation for the detective and preventive value of computer forensics through the use of relevant forensic and ethical hacking tools in Kali Linux.
  - Examine recent developments in cryptography in a lab setting.

EVALUATION INSTRUMENT

Specific assignments will vary by instructor, but typical assignments include hands-on tasks, projects, and presentations.

INSTRUCTIONAL STRATEGIES:

The instruction should include lectures, cases analyses, and hand-on exercises.

The instruction should cover the planning and deployment of security controls and safeguards.

IV. Methods of Instruction

A. INSTRUCTION MODE.

☒ Traditional ☐ Hybrid ☐ Local Online ☐ Distance Education

B. CLASSROOM ACTIVITIES.

i. Demonstration and computer lab

ii. Presentations and discussions

C. EXTENT AND NATURE OF TECHNOLOGY USE

Extensive usage of computers

V. Information about Textbooks/Readings

- Whitman, M. E., and Herbert, J. M. (2017) "*Management of Information Security, 5th Edition with MindTap*", Cengage Learning.
- Luttgens, J., Pepe, M., & Mandia, K. (2014) "*Incident Response & Computer Forensics*", McGraw Hill Professional.
- Ciampa, M. (2015) "CompTIA Security+ Guide to Network Security Fundamentals, 5th Edition", Cengage Learning ISBN-13: 9781305093911.
- Whitman, M. E., & Mattord, H. J. (2014) "*Hands-on Information Security Lab Manual, 4th Edition*". Cengage Learning.

VI. Instructional Policies Requirements

Instructor's syllabi must contain explicit statements regarding their own policies with regard to plagiarism, withdrawal, absences, etc., which should be consistent with the University policies published in the CSULB Catalog. It is expected that every course will follow University policies on Attendance (PS 01-01), Course Syllabi (PS 04-05), and Final Course Grades, Grading Procedures, and Final Assessments (PS 12-03). If some or all sections of the course are to be taught, in part or entirely, by distance learning, the course must follow the provisions of Academic Technology and the Mode of Instruction (PS 03-11).[1] Instructors should refer to the current CSULB Catalog and to the Academic Senate website for campus guidelines and policy statements as they develop their individual course policies.

All sections of the course will have a syllabus that includes the information required by the syllabi policy adopted by the Academic Senate. Instructors will include information on how students may make up work for excused absences. When class participation is a required part of the course, syllabi will include information on how participation is assessed.

VII. Course Assessment and Grading (Optional but highly recommended for core courses)

A. Assessment Criteria

Homework

Students will complete individual homework profiling their competence in various subject matters.

Projects

Instructors are strongly encouraged to assign comprehensive course project that requires problem solving and uses software tools to conduct real-world data analysis.

---

[1] The university policies listed are active as of 2015-2016 but may be subject to change in the future. For the most up-to-date policies, refer to the Academic Senate website's Policy Statements.

Individual student will complete a real world project involving an organization.

B. Required Statement

In compliance with university policy: Final grades will be based on at least three, and preferably four or more, demonstrations of competence. In no case will the grade on any class tests count for more than one-third of the course grade.

C. Attendance, Withdrawal, Late Assignments

Students are expected to attend courses and turn in assignments on time. Specific attendance and late assignment policies are up to each individual instructor's discretion. The withdrawal policy is the same as that of the university.

VIII. Disabilities

Students with disabilities are responsible for notifying their instructor as early as possible of their needs for an accommodation of a verified disability. A student with a disability is urged to consult with Disabled Student Services as soon as possible in order to identify possible accommodations to enhance academic success.

IX. Assistive Technology

In compliance with Accessibility and Faculty Responsibility for the Selection of Instructional Materials (PS 08-11), instructors are responsible for ensuring that their syllabi and instructional materials are accessible to all students.

X. Bibliography (Optional)

XI. Consistency of SCO Standards across Sections

XII. Additional Resources for Development of Syllabi

- University policy Course Syllabi and Standard Course Outlines (PS 11-07)
- Academic Technology (ATS) Accessible Syllabus Template
- Faculty Center for Professional Development (FCPD) Sample Syllabus Template