California State University, Long Beach
College of Business

Standard Course Outline
IS 360 Introduction to Cybersecurity in Business

I. General Information

- Course number: IS 360
- Title: Introduction to Cybersecurity in Business
- Units: 3
- Prerequisites: None
- Course Coordinator: Dr. Spiro Samonas
- SCO Prepared by: Dr. Spiro Samonas
- Date prepared/revised: 3/10/2018

II. Catalog Description

Foundation and business applications of cybersecurity. Principles and methodologies of risk assessment and management. Assurance and internal control. Security operations and administration. Introduction to cybersecurity attacks, threats and vulnerabilities. Regulatory and organizational compliance. Individual project. Letter grade only (A-F).

III. Curriculum Justification(s)

In real-time systems, global operations, and the e-business environment, the security of hardware, software, data, processes and people, is of paramount importance. Estimates of the size of the digital crime market range widely from the low hundreds of billions of dollars to over a trillion dollars. Personally Identifiable Information, such as name, social security number, date and place of birth, and mother's maiden name are easily available on the Dark Web for a handful of dollars. Cybersecurity is an inter-disciplinary field that encompasses the protection of information as well as human assets. In this challenging environment, students need to gain a sound understanding of the complex and interdisciplinary nature of cybersecurity, and evaluate the socio-technical impact of security and privacy on business.

This is an introductory course that provides an overview of the fundamental concepts and operations of cybersecurity in a business context, while laying emphasis on information assurance. Information assurance is the practice of ensuring the confidentiality, integrity and availability of information systems. This involves the identification, prioritization, and management of risks that are pertinent to the creation, processing, storage, transmission, and use of information. Information assurance also involves corporate governance issues such as privacy, regulatory compliance, information technology audits, business continuity, and disaster recovery. The course draws relevant knowledge from Information Systems, Computer Science, Psychology, and Criminology.

IV. CBA Undergraduate Program Learning Goals:

General Learning Goals

- **Critical Thinking**: Students will be able to demonstrate conceptual learning, critical thinking, and problem-solving skills. Students will be able to:
- Research and systematically examine cases of known cybersecurity breaches in business, develop defensible recommendations based on the relevant facts, and effectively communicate these recommendations both orally (e.g., presentations, class discussion) and in writing.
- **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. Students will be able to:
    - Demonstrate understanding of the ethical and social aspects of security governance and management.
- **Interpersonal, Leadership & 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. Students will be able to:
    - Manage an individual project and deliver a written report and a formal presentation in front of their class peers.

Management-Specific Learning Goals

- **Business Functions**: 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 business.
- **Quantitative & Technical Skills**: Students will possess quantitative and technological skills enabling them to analyze, interpret, and communicate business data effectively and to improve business operations. Students will be able to:
    - Identify and assess different types of security risks using quantitative techniques.

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

OBJECTIVE 1: Develop a sound understanding of risk assessment and management.

- ***MEASURABLE OUTCOME***: After taking this course, students will be able to assess and prioritize security risks using quantitative methodologies.
- ***EVALUATION INSTRUMENTS***: Class assignments will vary by instructor, but typical assignments include written assignments based on case studies, and in-class essay exams.
- ***INSTRUCTIONAL STRATEGIES FOR SKILL DEVELOPMENT***: A written assignment rubric evaluating the ability of students to identify and assess the impact of cybersecurity risks will be used. Performance expectations and standards will be discussed in class before and after any written assignments.

OBJECTIVE 2: Examine cybersecurity threats and vulnerabilities and suggest relevant safeguards.

- ***MEASURABLE OUTCOME***: After taking this course, students will be able to identify organizational assets, threats and vulnerabilities, and select appropriate technical and organizational safeguards.
- ***EVALUATION INSTRUMENTS***: Specific assignments will vary by instructor, but typical assignments include written assignments based on case studies, and in-class essay exams.
- ***INSTRUCTIONAL STRATEGIES FOR SKILL DEVELOPMENT***: A written assignment rubric evaluating the ability of students to identify organizational assets, threats and vulnerabilities will be used. Performance expectations and standards will be discussed in class before and after any written assignments.

OBJECTIVE 3: Develop an appreciation for the role of security operations and administration

- ***MEASURABLE OUTCOME***: After taking this course, students will be able to develop a security policy based on the templates provided by the world renowned SANS Institute, as well as a disaster recovery plan.
- ***EVALUATION INSTRUMENTS***: Specific assignments will vary by instructor, but typical assignments include written assignments based on case studies, and in-class essay exams.
- ***INSTRUCTIONAL STRATEGIES FOR SKILL DEVELOPMENT***: A written assignment rubric evaluating the ability of students to develop appropriate security policies and disaster recovery plans will be used. Performance expectations and standards will be discussed in class before and after any written assignments.

VI. Outline of Subject Matter

The topic outline for the course is the following. Subject matter and sequence of topics may vary by instructor.

1. Overview of Information Assurance and Cybersecurity
2. Risk Assessment and Management
3. Business Continuity and Disaster Recovery
4. Information Technology Auditing and Control
5. Security Operations and Administration
6. Incident Response
7. Overview of Networks and Telecommunications in Business
8. Cryptography
9. Cybersecurity Attacks, Threats, and Vulnerabilities
10. Compliance: Law and Ethics
11. Optional additional topics include:
12. Digital Crime, Computer Forensics, Privacy and the Dark Web

VII. Methods of Instruction

INSTRUCTION MODE

As per the University policies Academic Technology and the Mode of Instruction (PS 03-11) and Course Syllabi and Standard Course Outlines (PS 11-07) that pertain to modes of instruction, this course is authorized to use the traditional mode of instruction that involves face-to-face class sessions.

CLASSROOM ACTIVITIES

The course has four main components: (1) lecture and readings, (2) case analyses, (3) homework assignments, and (4) an individual project. Students are required to actively participate in in-class discussions, work individually and in groups, and build interpersonal, communication, and presentation skills. Student will be evaluated using case reports, assignments, oral presentations, an individual project, and three exams. For both written and oral tasks, the instructor's feedback will be provided to students regularly to support their continuous improvement.

EXTENT AND NATURE OF TECHNOLOGY USE.

Instructors will assign homework and in-class assignments involving the use of hardware and software, as well as projects on managing cybersecurity.

VIII. Information about Textbooks/Readings

The following is a short list of textbooks that are suggested for this course. Instructors may assign one or more of these and/or include other relevant texts/readings. Instructors may be asked to justify the use of old textbooks, if updated texts are available:

- Kim, D., & Solomon, M. G. (2016). *"Fundamentals of information systems security, 3rd Edition"*. Jones & Bartlett Learning.
- Whitman, M. E., and Herbert, J. M. (2017) "*Management of Information Security, 5th Edition with MindTap*", Cengage Learning.

IX. Instructional Policies Requirements

Every course should comply with the relevant Academic Senate Policy Statements. Instructional policies should be consistent with the course description outlined in Sections II and III, and should serve the course objectives listed in section IV of this SCO. Specific attendance and late assignment policies are up to the discretion of each instructor, as long as these policies follow the Academic Senate Policy Statements. The same applies if some or all sections of the course are to be taught, in part or entirely, by distance learning in the future.

Students are expected to abide with the following policies that are outlined in the CSULB Catalog:

- The Standards for Student Conduct
- Academic Integrity Regarding Cheating and Plagiarism
- The withdrawal policy

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

DESCRIPTION OF ASSESSMENT

The suggested workload and grading for this course is as follows:

Assignment Description	% of Course Grade
Project	15%
In-class Assignments and Homework	25%
Mid-term Exam 1	20%
Mid-term Exam 2	20%
Final Exam	20%
Total:	100%

GRADING POLICIES AND PROCEDURES

Grading policies, procedures, and the percentage of the course grade associated with each assessment must be explicit on each instructor's syllabus and must be consistent with University policy on Final Course Grades, Grading Procedures, and Final Assessments (PS 12-03). Instructors must develop scoring guidelines for assessments, which must be made available to students. The final course grade will be based on a descriptive scale such as the following:

Percentage	Letter Grade	Description of Grade
90-100%	A	Mastery of the relevant course standards.
80-89%	B	Above average proficiency of the relevant course standards.
70-79%	C	Satisfactory proficiency of the relevant course standards.
60-69%	D	Partial proficiency of the relevant course standards.
Below 60%	F	Little or no proficiency of the relevant course standards.

XI. Disabilities

The Bob Murphy Access Center (BMAC) provides certification for students with disabilities and helps arrange relevant accommodations. Any student requesting academic accommodations based on a disability is strongly encouraged to register with Disabled Student Services (BMAC) each semester. A letter of verification for approved accommodations can be obtained from BMAC. Please be sure to

provide your instructor with BMAC verification of accommodations as early in the semester as possible. The phone number for BMAC is (562) 985 5401. The email address is: bmac@csulb.edu.

XII. 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.

XIII. Consistency of SCO Standards across Sections

All future syllabi will conform to the SCO. The course coordinator should review the SCO and offer advice and/or materials to faculty member new to teaching the course. The course coordinator may offer or require regular review of instructors' course materials as well as anonymous samples of student work.

XIV. Additional Resources for Development of Syllabi

- Academic Senate Policy 11-07: Course Syllabi and Standard Course Outlines
- College of Business Accessible Syllabus Template
- Faculty Center Course and Syllabus Design