USC Viterbi
School of Engineering
Information Technology Program

ITP 370: Information Security Management

Units: 3
Fall 2019
Tuesday, 6:00 – 8:50pm

Instructor: Michael Cassar
Class Location: KAP 138
Office: KAP 138
Office Hours: By Appointment Only
Contact Info: mcassar@usc.edu email only or Blackboard messenger
(Please place in email subject line: ITP 370)

Teacher's Assistant Contact: Joseph Blundell (Grader) and Stella Aghakian (Mentor)
TA contact: Blundell@usc.edu and Saghakia@usc.edu
TA Office Hours: By Appointment Only

IT Help: Viterbi Information Technology
Hours of Service: Monday-Friday 8AM – 9PM
Contact Info: Phone: 213-740-0517; Email: engrhelp@usc.edu

Program Mission: The goal of the Digital Forensics and Cyber Security program at USC is to develop the critical thinking, analytical reasoning, and technical writing skills that are necessary to effectively work in a junior level digital forensic or cyber security analyst role. This is accomplished through utilizing industry standard tools and techniques to investigate labs and cases based upon real-world investigations and intrusions. Students will study various areas of cyber investigations, including digital evidence gathering, reporting, examinations, and court presentations. Students will study cyber security tenants of risk analysis, remediation, as well as penetration testing and network security design.

Course Description

This course is designed to teach the fundamentals of security management. The course is not technical in nature, but relies on the student's previous understanding of security systems. The course instead looks at security from a managerial perspective with regards to security operations, risk management, and disaster recovery.

Learning Objectives

Upon completing this course, students will:

- Understand components of the security and risk management.
- Demonstrate understanding of the concepts of asset security.
- Design, implement, maintain a security engineered environment.
- Analyze components of risk in communications with network security.
- Develop a model for understanding identity and access management .
- Understand how to plan, perform, test, implement a security assessment and disaster recovery plan.
- Recognize the components of a security operations.

Prerequisite(s): ITP 125 From Hackers to CEOs: An Introduction to Information Security
Recommended: ITP 357 Enterprise Network Design

Course Notes

Course is letter graded, with any and all materials available on Blackboard (blackboard.usc.edu).

Technological Proficiency and Materials Required

It is assumed that the student has baseline technical knowledge (basic computer usage, basic internet usage). For any upper-division course (300-level and above), it is assumed that you have refined your technical abilities in ITP 125, including basic network design.
Materials: CISO COMPASS: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers Book by Todd Fitzgerald

Description and Assessment of Assignments

The assignments will be a combination of in-class and out-of-class laboratory exercises. They will typically involve some form of procedural work (we will provide instructions), with some reflection on the work performed including researching processes and procedures performed.

Grading Breakdown

The following percentage breakdown will be used in determining the grade for the course:

Lab Assignments/News	45%
Class Participation	10%
Midterm Exam	20%
Final Exam	25%
Total:	100%

Grading Scale

Course final grades will be determined using the following scale

A	93-100
A-	90-92
B+	87-89
B	83-86
B-	80-82
C+	77-79
C	73-76
C-	70-72
D+	67-69
D	63-66
D-	60-62
F	59 and below

Grading Policies

The lab assistants, graders, and instructors will do their best to return assignments graded to students within one week of the submission. Certain assignments that are longer in length, including exams, case reports, and final projects, may require more time.

The grading rubric is posted. There is no curve, and grades are based on performance in the class. While we understand the importance of grades and maintaining a high GPA, we cannot hand out high marks without justified performance in the class. Do not rely upon an expectation of a guaranteed minimum final grade in this class regardless of its impact on your overall GPA, financial situation, familial situation, or the fate of the galaxy.

The instructor is the ultimate authority over any grade for any assignment, exam or class.

University policy states that no extra credit may be afforded to individual students without the same opportunity made available to everyone in the class. Should there be extra credit in the class, it will be made available to the entire class. Do not ask the instructor for additional extra credit.

Grades will be posted on Blackboard and it is your responsibility to ensure that the grades online are accurate and to follow your progress in the class.

Contacting the Instructor, Lab Assistants or Graders

When emailing the lab assistants, graders or instructor, please be sure to include your full name, student ID, class name and number, and class section (day and time) in the email.

Emails sent to the lab assistants or graders will be responded to within two business days. The instructor will endeavor to respond to emails within two business days. Do not email anyone with the expectation of an immediate response within the hour. Please do not complain when we have not responded to your email ten minutes before the assignment deadline.

Questions regarding individual clarification or regrade must be made through email to both the grader and the instructor. When requesting a regrade, the instructor has the prerogative to alter a grade higher or lower based upon a review of the entire assignment. Be absolutely certain before requesting a regrade of any assignment or exam – if you are going to roll the dice, be certain of your gamble.

Questions about lab assignments should be submitted through the class discussion board this will have a faster response rate.

The instructor will post his/her regular office hours on blackboard. You may request a meeting with the instructor outside of normal office hours. Should you go to the instructor's office outside of normal office hours or outside of a scheduled meeting, do not expect the instructor to be able to meet with you. We do have other responsibilities outside of the class.

Lab Assignment Policies

The labs will be posted on Blackboard under the "Assignments" or "Labs" section. Each lab will include instructions, a due date, and a link for electronic submission. Labs must be submitted using this link. Do not email your assignments to the instructor, lab assistants, or graders. TurnItIn may be utilized for some assignments, and you must make sure that you have fully submitted the assignment (usually a two step process).

Unless otherwise noted, all lab assignments are due at the beginning of class the next class period, unless otherwise modified by Blackboard announcement and/or email from the instructor and/or Lab Assistants. Some assignments (typically longer in length) may have a due date on 11:59:59 PM on the Friday or Sunday of the following week or specificed in the assignment announcement. Do not expect a timely response from the lab assistants, graders, or instructors if emailed after normal business hours particularly on the date the assignment is due.

If you join the class after the semester has started, you will have two weeks from the date of enrollment to complete all assignments due before you joined the class unless a written extension is granted from the instructor, typically via email.

It is your responsibility to submit your assignments on or before the due date and verify it has been successfully submitted. Assignments turned in up to 24 hours late will have 25% of the total points deducted from the graded score. Assignments turned in between 24 and 48 hours late will have 50% of the total points deducted from the graded score. After two days, submissions will not be accepted and you will receive no credit for the assignment.

The lab assistants and graders are not authorized to grant an extension on any assignment. Any extensions must be requested of the instructor in writing and confirmed in writing. If you ask for an extension on the day the assignment is due, without expressing an emergency such as being kidnapped and taken to Mexico, it will probably not be granted.

Certain assignments will require a paper submission, and you may be asked to submit them to the main ITP office. There have been previous allegations of student rudeness to the ITP Staff. If the staff complains about you being rude, you will have 25% automatically deducted from your assignment. Don't be rude.

The instructor and lab assistants reserve the right to not answer certain questions about the lab assignment. This is normally due to the nature of the question being directly related to the learning objectives of the lab. You are encouraged to use online resources to further your understanding of the material to successfully answer questions related to the lab assignment (in other words, use your research skills).

All lab assignments have been tested by the instructor and/or lab assignments. Due to the nature of certain software packages and configurations in the lab, the assignments may or may not work as intended. You are encouraged to ask questions if something appears to not work correctly. However, there are certain instances where things are intended to not work correctly and the instructor and lab assistant will indicate as such. When in doubt, do a little research.

News Assignment

To promote class discussion, each student will be required to submit an article for class discussion starting week three. Articles shall be posted with a hyperlink to the article and a one-paragraph summary to the class Blackboard news discussion board for the appropriate week.
News stories should directly pertain to topics covered in this class.

- Post a link to the proper week on the Blackboard news board **no later than midnight the night before class**.
- Please submit a story that is no more than one week old.
- Please take care not to duplicate stories that have been submitted that week.
- If the story is behind a pay-wall or subscription-wall or requires a login, please submit a PDF copy along with the link.
- Be prepared to give a short two-minute summary of the article and any surrounding background details to start the discussion.
- Press releases including anything from prweb.com are not valid news content
- Make you you validate the veracity of your news story
    - Example: Content from TheHackerNews is frequently inaccurate
- Groups will be posted to Blackboard once enrollment has settled.
- Each proper posting is worth 3 points which is 12 points of your lab assignments grade

Quiz Policy:

There will be a short quiz at the end of every section completed (see Syllabus or Blackboard for exact dates). This quiz will cover material from labs and class lectures.

The questions on the quiz will be similar to the lab problems, but will not be identical to them. That is, they will not simply be the same problems you have already seen. You may be asked to combine ideas from class to solve a question that you have never seen before.

See the discussion of the grading policy for the percentage of your grade that will come from your quizzes. It is your responsibility to submit your in-class or take home quizzes on or before the due date and verify it has been successfully submitted. Quizzes turned in up to 24 hours late will have 25% of the total points deducted from the graded score. Late submissions will not be accepted and you will receive no credit for the assignment. If you have a learning disability for which you should receive extra time on quizzes, you must inform me of this by the first week of class. You also should make arrangements with me to view your documentation card issued by the office of student support.

Exam Policies

Please review the schedule of classes for the Final Exam schedule. Should you have a scheduling conflict with the final exam, you must contact the instructor and coordinate an alternative time by the end of Week three. Any requests made after Week 3 are not guaranteed to be accommodated.

Per USC policy, Final Exams must be scheduled during the assigned final examination schedule. It is your responsibility to arrange your travel after the scheduled date of the final exam.

All students are required to participate in the final exam and/or project. Failure to take the final exam and/or submit a final project will result in an automatic failure in the class.

No make-up exams (except for documented medical or family emergencies) will be offered nor will there be any changes made to the Final Exam schedule. Missing your alarm is not an emergency. A documented medical event (car accident with documentation), family emergency (death in the family), or alien abduction can be considered emergencies.

Writing Skills

A significant portion of the cyber security and digital forensics curriculum involves communicating what was discovered by writing professional quality reports. These reports are held to standards that are expected by professionals in industry who are writing reports for clients, attorneys, judges and juries. It is expected that the reports will be written with correct spelling, grammar and language nuances of the American English language. A component of each report grade will be based on writing style, grammar and word choice. These reports must be accessible to technical and non-technical readers alike.

If you are not a native English speaker and writer, it is recommended that you visit the USC American Language Institute (http://ali.usc.edu/) for resources to assist you in this course and your professional careers. Writing assistance is also available from the Dornsife Writing Center (https://dornsife.usc.edu/writingcenter/). You do not need to be a Dornsife student to take advantage of the services from the Writing Center. Additional writing assistance is also available from the Viterbi Writing Center in the form of Writing Consultations (http://viterbi.usc.edu/students/undergrad/varc/writing-consultations.htm). In accordance with University standards, plagiarism of any type will not be tolerated.

Attendance Policy

You are expected to be in class, on time, and distraction free. As this class meets twice a week and as it is lecture and lab any student who misses more than four classes is in danger of failing the course. Please see the instructor immediately if you have missed at least two class meetings.

This is a lab-based class. Certain class sections will be lecture, lab, or a combination of lecture and lab. Attendance is vital to success in the class, and punctuality is vital to success in your professional careers. The lab assistants will be taking attendance for every class meeting. If you anticipate missing a class due to an event, please email the lab assistants and instructor prior to the start of class. If you are sick, we want you to get better and not infect your fellow classmates – please email the lab assistants and instructor. Should you miss a class with a lab assignment, contact the lab assistants to determine available times to come to the lab and finish your assignment.

Additional University policies follow the course schedule.

Information Security Management
ITP 370

Course Outline - Fall 2019

Note: Schedule or Guest Lecturer subject to change

Week 1 (August 27) – Introduction & Defining the Cybersecurity Challenge

- Introduction to Cyber Security and Careers
- Types of Areas in Cyber Security
- Pathway of Cyber Security
- Where does Information Security Management Fit?

Guest Speaker:

eSENTIRE

Week 2 (September 3) – Security and Risk Management

- Understand and apply concepts of confidentiality, integrity and availability
- Evaluate and apply security governance principles
- Determine compliance requirements
- Understand legal and regulatory issues that pertain to information security in a global context
- Understand, adhere to, and promote professional ethics
- Develop, document, and implement security policy, standards, procedures, and guidelines

Week 3 (September 10) – Security and Risk Management Cont.

- Identify, analyze, and prioritize Business Continuity (BC) requirements
- Contribute to and enforce personnel security policies and procedures
- Understand and apply risk management concepts
- Understand and apply threat modeling concepts and methodologies
- Apply risk-based management concepts to the supply chain
- Establish and maintain a security awareness, education, and training program

Week 4 (September 17) – Asset Security

- Identify and classify information and assets
- Determine and maintain information and asset ownership
- Protect privacy
- Ensure appropriate asset retention
- Determine data security controls
- Establish information and asset handling requirements

Week 5 (September 24) - Security Architecture and Engineering*

- Implement and manage engineering processes using secure design principles
- Understand the fundamental concepts of security models
- Select controls based upon systems security requirements

Guest Speaker:

Week 6 (October 1) – Security Architecture and Engineering Cont.

- Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
- Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
- Assess and mitigate vulnerabilities in web-based systems
- Assess and mitigate vulnerabilities in mobile systems
- Assess and mitigate vulnerabilities in embedded devices

Week 7 (October 8) – Security Architecture and Engineering Cont.

- Apply cryptography
- Apply security principles to site and facility design
- Implement site and facility security controls

Midterm Review

Week 8 (October 15) – Midterm & Communication and Network Security

- Implement secure design principles in network architectures
- Secure network components
- Implement secure communication channels according to design

Week 9 (October 22) – Identity and Access Management (IAM)

- Control physical and logical access to assets
- Manage identification and authentication of people, devices, and services
- Integrate identity as a third-party service
- Implement and manage authorization mechanisms
- Manage the identity and access provisioning lifecycle

Week 10 (October 29) – Security Assessment and Testing

- Design and validate assessment, test, and audit strategies
- Conduct security control testing
- Collect security process data (e.g., technical and administrative)
- Analyze test output and generate report
- Conduct or facilitate security audits

Week 11 (November 5) – Security Operations

- Understand and support investigations
- Understand requirements for investigation types
- Conduct logging and monitoring activities
- Securely provisioning resources

Week 12 (November 12) – Security Operations Cont.

- Understand and apply foundational security operations concepts
- Apply resource protection techniques
- Conduct incident management
- Operate and maintain detective and preventative measures
- Implement and support patch and vulnerability management

Week 13 (November 19) – Security Operations Cont.*

- Understand and participate in change management processes
- Implement recovery strategies
- Implement Disaster Recovery (DR) processes
- Test Disaster Recovery Plans (DRP)

Guest Speaker:

Week 14 (November 26) – Security Operations Cont.

- Participate in Business Continuity (BC) planning and exercises
- Implement and manage physical security
- Address personnel safety and security concerns

Week 15 (December 3) – Final Review

Week 16 (December 17) – Final Exam

Statement on Academic Conduct and Support Systems

Academic Conduct:
Plagiarism – presenting someone else's ideas as your own, either verbatim or recast in your own words – is a serious academic offense with serious consequences that can include expulsion. Please familiarize yourself with the discussion of plagiarism in *SCampus* in Part B, Section 11, "Behavior Violating University Standards" policy.usc.edu/scampus-part-b. Other forms of academic dishonesty are equally unacceptable. See additional information in *SCampus* and university policies on scientific misconduct, http://policy.usc.edu/scientific-misconduct.

Support Systems:
Student Counseling Services (SCS) – (213) 740-7711 – 24/7 on call
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention. engemannshc.usc.edu/counseling

National Suicide Prevention Lifeline – 1 (800) 273-8255
Provides free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week. www.suicidepreventionlifeline.org

Relationship and Sexual Violence Prevention Services (RSVP) – (213) 740-4900 – 24/7 on call
Free and confidential therapy services, workshops, and training for situations related to gender-based harm. engemannshc.usc.edu/rsvp

Sexual Assault Resource Center
For more information about how to get help or help a survivor, rights, reporting options, and additional resources, visit the website: sarc.usc.edu

Office of Equity and Diversity (OED)/Title IX Compliance – (213) 740-5086
Works with faculty, staff, visitors, applicants, and students around issues of protected class. equity.usc.edu

Bias Assessment Response and Support
Incidents of bias, hate crimes and microaggressions need to be reported allowing for appropriate investigation and response. studentaffairs.usc.edu/bias-assessment-response-support

The Office of Disability Services and Programs
Provides certification for students with disabilities and helps arrange relevant accommodations. dsp.usc.edu

Student Support and Advocacy – (213) 821-4710
Assists students and families in resolving complex issues adversely affecting their success as a student EX: personal, financial, and academic. studentaffairs.usc.edu/ssa

Diversity at USC
Information on events, programs and training, the Diversity Task Force (including representatives for each school), chronology, participation, and various resources for students. diversity.usc.edu

USC Emergency Information
Provides safety and other updates, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible. emergency.usc.edu

USC Department of Public Safety – UPC: (213) 740-4321 – HSC: (323) 442-1000 – 24-hour emergency or to report a crime.
Provides overall safety to USC community. dps.usc.edu