MIS 5206 – Protection of Information Assets (3 Credit Hours)

Fall 2021

Instructor

David Lanter
Office: Speakman 209C and online via Zoom
Office Hours: Thursday 10am – 11am and by appointment
Email: *David.Lanter@temple.edu*
e-profile: *http://community.mis.temple.edu/dlanter/*

Class Format: In-Person

Class Meetings: Thursdays 11:15AM – 1:45 PM

Where: In-class: 1810 Liacouras Walk, Room 420

Website: *https://community.mis.temple.edu/mis5206sec001fall2021/*

Canvas: *https://templeu.instructure.com/courses/98275*

Course Description

In this course you will learn key concepts and components necessary for protecting the confidentiality, integrity and availability (CIA) of information assets. You will gain an understanding of the importance and key techniques for managing the security of information assets including logical, physical, and environmental security along with disaster recovery and business continuity.

The first half of the course, leading up to the mid-term exam, will focus on Information Security Risk Identification and Management. The second half of the class will cover the details of security threats and the mitigation strategies used to manage risk.

Course Objectives

1. Gain an overview of information security vulnerabilities and threats
2. Learn how information security risks are identified, classified and prioritized
3. Develop an understanding of how information security risks are managed, mitigated and controlled
4. Gain experience working as part of team, developing and delivering a professional presentation
5. Gain insight into certification exams and improve your test taking skills

Textbook and Readings

Textbook	Computer and Information Security Handbook - Third Edition, 2017, John R. Vacca, Elsevier, Inc. ISBN: 978-0-12-803843-7 Available online at O'Reily for Higher Education via Temple University Libraries
ISACA	ISACA Reading 1: ISACA Risk IT Framework
	ISACA Reading 2: "Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans"
	ISACA Reading 3: "What Every IT Auditor Should Know About Backup and Recovery",
SANS	SANS Reading 1: "The Importance of Security Awareness Training"
	SANS Reading 2: "Making Security Awareness Work for You"
	SANS Reading 3: "Implementing Robust Physical Security"
	SANS Reading 4: "An Overview of Cryptographic Hash Functions and Their Uses"
	SANS Reading 5: "The Risks Involved With Open and Closed Public Key Infrastructure"
	SANS Reading 6: "Assessing Vendor Application Security A Practical Way to Begin"
	SANS Reading 7: "Application Development Technology and Tools: Vulnerabilities and threat management with secure programming practices, a defense in-depth approach"
FIPS	FIPS Reading 1: "Standards for Security Categorization of Federal Information and Information Systems"
NIST	NIST Reading 1: "Framework for Improving Critical Infrastructure Cybersecurity"
	NIST Reading 2: "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"
FGDC	FGDC Reading 1: "Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns"
Harvard Business Publishing (HBP)	2 case studies and 1 reading are available in the course pack for purchase from HBP: https://hbsp.harvard.edu/import/853285 Case Study 1: "Snowfall and a Stolen Laptop" Case Study 2: "Autopsy of a Data Breach: The Target Case" HBR Reading 1: "The Myth of Secure Computing (HBR OnPoint Enhanced Edition)"
Misc.	Case Study 3: "A Hospital Catches the "Millennium Bug"

Schedule:

Unit	Assignment Topics	Date
1	Introduction to MIS5206 Understanding an Organization's Risk Environment	Aug. 26
2	Case Study 1: *Snowfall and a stolen laptop* Data Classification Process and Models	Sept. 2
3	Risk Evaluation	Sept. 9
	Class will not be held on September 16th	*Sept. 16*
4	Case Study 2: *Autopsy of a Data Breach: The Target Case*	Sept. 23
5	Creating a Security Aware Organization	Sept. 30
6	Physical and Environmental Security	Oct. 7
7	**Midterm Exam**	Oct. 8-10
8	Case Study 3: *A Hospital Catches the "Millennium Bug"*	Oct. 14
9	Business Continuity and Disaster Recovery Planning	Oct. 21
10	Network Security	Oct. 28
11	Cryptography, Public Key Encryption and Digital Signatures	Nov. 4
12	Identity Management and Access Control	Nov.11
13	Computer Application Security Team Project Presentations	Nov. 18
14	Review Team Project Presentations	Dec.2
15	**Final Exam**	Dec. 9

Assignments

The readings, questions, and case study assignments will bring the real world into class discussion while illustrating fundamental concepts.

1. **Readings:** Below is the reading schedule you are responsible for completing. Complete each reading and answer reading discussion questions posted to the class website before the first class:

Unit	Readings
1	• Vacca Chapter 1 "Information Security in the Modern Enterprise" • Vacca Chapter 2 " Building a Secure Organization" • NIST Reading 1: "Framework for Improving Critical Infrastructure Cybersecurity" • ISACA Risk IT Framework, pp. 1-42
2	• Case Study 1: *"Snowfall and a Stolen Laptop"* • Vacca Chapter 24 "Information Security Essentials for IT Managers: Protecting Mission-Critical Systems" • FIPS Reading 1: "Standards for Security Categorization of Federal Information and Information Systems" • FGDC Reading 1: "Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns" • NIST Reading 2: "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"

3	• Vacca Chapter 25 "Security Management Systems" • Vacca Chapter 34 "Risk Management" • ISACA Reading 1: "Risk IT Framework" pp. 47-96
4	• Case Study 2: *"Autopsy of a Data Breach: The Target Case"*
5	• Vacca Chapter 27 (online) "Information Technology Security Management" • Vacca Chapter 33 "Security Education, Training and Awareness" • SANS Reading 1: **"**The Importance of Security Awareness Training" • SANS Reading 2: "Making Security Awareness Work for You"
6	• HBR Reading 1: "The Myth of Security Computing" • Vacca Chapter 69 "Physical Security Essentials" • SANS Reading 3: "Implementing Robust Physical Security"
8	• Case Study 2: "*A Hospital Catches the "Millennium Bug"*
9	• Vacca Chapter 61 (online) "SAN Security"Vacca • Chapter 62 "Storage Area Networking Security Devices" • Vacca Chapter 36 "Disaster Recovery" • Vacca Chapter 37 "Disaster Recovery Plans for Small and Medium businesses" • ISACA Reading 2: "Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans" • ISACA Reading 3: "What Every IT Auditor Should Know About Backup and Recovery"
10	• Vacca Chapter 8 "Guarding Against Network Intrusions" • Vacca Chapter 13 "Internet Security" • Vacca Chapter 14 "The Botnet Problem" • Vacca Chapter 15 "Intranet Security" • Vacca Chapter 16 (online) "Local Area Network Security" • Vacca Chapter 72 "Intrusion Prevention and Detection Systems"
11	• Vacca Chapter 46 (online) "Data Encryption" • Vacca Chapter 47 "Satellite Encryption" • Vacca Chapter 48 "Public Key Infrastructure" • Vacca Chapter 51 "Instant-Messaging Security" • SANS Reading 4: "An Overview of Cryptographic Hash Functions and Their Uses" • SANS Reading 5: "The Risks Involved with Open and Closed Public Key Infrastructure"
12	• Vacca Chapter 71 "Online Identity and User Management Services" • Vacca Chapter 52 "Online Privacy" • Vacca Chapter 53 "Privacy-Enhancing Technologies" • Vacca Chapter 59 "Identity Theft – First Part" • Vacca Chapter 59 "Identity Theft – Second Part"
13	• SANS Reading 6: "Assessing Vendor Application Security A Practical Way to Begin" • SANS Reading 7: "Application Development Technology and Tools: Vulnerabilities and threat management with secure programming practices, a defense in-depth approach"

2. **Answer Questions:** Questions for each week's top will be available on the class website, under "WEEKLY DISCUSSIONS". You are expected to post your answer to each question on the class website blog by the **Sunday 11:59 PM** of the week of the class. To do so, click "Leave a Comment". Provide a thoughtful but brief (paragraph or two) analysis as your answer to each question. ***Late and missing submissions of answers will result in lost credit for the assignment.***

   Post your answers to the assignments, and come to class prepared to discuss all of your answers in-detail.

   Case Studies: Case study analysis will be conducted in three phases:

   i. Individual preparation and writeup is done as homework assignment questions you answer that will prepare you to contribute in group discussion meetings. It will prepare you to learn from what others say. To fully benefit from the interchange of ideas about a case's problem, however, you must possess a good understanding of the facts of the case and have your own ideas. Studying the case, doing your homework and answering the questions readies you to react to what others say. This is how we learn.

      Answer assigned questions in a way that demonstrates the depth of your understanding of the security and auditing concerns represented by the case.

      Post your answers to the questions as a PDF document to Canvas **by Tuesday at 11:59 PM of the week the Case will be covered**.

      Format: Your analysis should be single-spaced pages using 11-point Times New Roman font with one-inch margins, and the entire document should be limited to 3 pages (including a diagram if appropriate for answering the question.) Do not prepare a separate cover page, instead put your name, the class section number (e.g. MIS5206.001), and the case name in the top-left corner of the header. Add page numbers in the footer of the document. Your assignment should be saved as a PDF formatted file to Canvas, your PDF file should be named Case2-YourName.pdf

   ii. Group discussions are informal sessions of give and take. Come to class with your own ideas and leave with better understanding. By pooling your insights with the group you advance your own analysis. Discussions within small groups is also helpful for those uncomfortable talking in large classes to express their views and gain feedback.

   iii. Class discussion advances learning from the case, but does not necessarily solve the case. Rather it helps develop your understanding why you need to gain more knowledge and learn concepts that provide the basis of your intellectual toolkit you develop in class and apply in practice.

Below is the schedule for the Case Studies:

Unit	Case Studies
2	Case Study 1: *Snowfall and a stolen laptop*
4	Case Study 2: *Autopsy of a Data Breach: The Target Case*
8	Case Study 3: *A Hospital Catches the "Millennium Bug"*

Participation

Your participation in class discussions is critical. Evaluation is based on you consistently demonstrating your thoughtful engagement with the material. Assessment is based on what you contribute. The frequency and quality of your contributions are equally important.

Each week, in addition to posting your answers to weekly assignments of reading questions, you are also expected to participate through written postings to the class blog:

1. **Comments on other student's answers and comments to weekly reading discussion questions.** Read the answers of others to the discussion questions and contribute at least three (3) substantive posts. Include your thoughtful comments as you participate in the discussion of the answers to questions with your classmates. The posting of the comments is due by **Tuesday @ 11:59 PM**.

2. **"In the News" articles.** Research a current events article relevant to information security. Identify the article, write a summary of the article, and post a link to it at the end of your summary. Be prepared to discuss the article you found in class about a current event in the Information Security arena. An ideal article would be tied thematically to the topic of the week. However, any article you find interesting and would like to share is welcome. The deadline for posting is **Tuesday @ 11:59 PM**.

Team Projects Presentation

Students will be organized into project teams. The teams will receive instruction on the project's topic early in the semester and are responsible for working with the instructor throughout the semester to clarify their understanding of the project's scope and gain feedback to refine and improve their presentation and deliverables.

During Weeks 13 and 14 teams will present their final project. Each will have a total time of 15 minutes to present, following by 10 minutes for questions and answers. The teams not presenting will be responsible for asking questions of the presenting project teams.

Exams

There will be two exams given during the semester. The Midterm and Final exams combine to count towards 25% of each student's final grade. A missed exam can only be made up in the case of documented and verifiable extreme emergency situation. No make-up is possible for the Final Exam. Both midterm and final exams will consist of CISA and CISSP style multiple-choice questions. You will have a fixed time (e.g. 150 minutes) to complete the exam. The exams will be taken online in Canvas during the regular class time.

Below is the exam schedule:

Date	Exam
Oct. 7	Midterm
Dec. 9	Final

Quizzes

At the end of a certain classes I will provide you with a test taking tip followed by a practice quiz consisting of multiple-choice questions modeled after the content of the CISA and CISSP certification exams. Quizzes are for practice only. They will not count towards your final grade. The goals for the quizzes are twofold:

1) Help you become familiar with technical information security areas requiring additional study and attention
2) Help you gain skills that improve your test taking abilities

Weekly Cycle

As outlined above in the **Assignments and Participation** sections, much of your learning will occur as you prepare for and participate in discussions about course content. To facilitate learning course material, we will discuss course material on the class blog in between classes. Each week this discussion will follow this cycle:

When	Actor	Task	Type
Thursday	Instructor	Post reading questions	
Sunday 11:59 PM	Student	Post answers to reading questions	Assignment
Tuesday 11:59 PM	Student	Upload answers to case study questions to Canvas	Assignment
Tuesday 11:59 PM	Student	Post 3 comments to others' answers	Participation
Tuesday 11:59 PM	Student	Post "In the News" article	Participation
Thursday	All of Us	Class meeting	Participation
Thursday	Instructor	Post Wrap-up notes	

Evaluation and Grading

Item	Weight
Assignments	25%
Participation	25%
Team Project	25%
Exams	25%
	100%

Grading Scale			
94 – 100	A	73 – 76	C
90 – 93	A-	70 – 72	C-
87 – 89	B+	67 – 69	D+
83 – 86	B	63 – 66	D
80 – 82	B-	60 – 62	D-
77 – 79	C+	Below 60	F

Grading Criteria

The following criteria are used for evaluating assignments. You can roughly translate a letter grade as the midpoint in the scale (for example, an A- equates to a 91.5).

Criteria	Grade
The assignment consistently exceeds expectations. It demonstrates originality of thought and creativity throughout. Beyond completing all of the required elements, new concepts and ideas are detailed that transcend general discussions along similar topic areas. There are no mechanical, grammatical, or organization issues that detract from the ideas.	A- or A
The assignment consistently meets expectations. It contains all the information prescribed for the assignment and demonstrates a command of the subject matter. There is sufficient detail to cover the subject completely but not too much as to be distracting. There may be some procedural issues, such as grammar or organizational challenges, but these do not significantly detract from the intended assignment goals.	B-, B, B+
The assignment fails to consistently meet expectations. That is, the assignment is complete but contains problems that detract from the intended goals. These issues may be relating to content detail, be grammatical, or be a general lack of clarity. Other problems might include not fully following assignment directions.	C-, C, C+
The assignment constantly fails to meet expectations. It is incomplete or in some other way consistently fails to demonstrate a firm grasp of the assigned material.	Below C-

Late Assignment Policy

An assignment is considered late if it is turned in after the assignment deadlines stated above. No late assignments will be accepted without penalty unless arrangements for validated unusual or unforeseen situations have been made.

- The exercise assignments will be assessed **a 50% penalty** if they are late. No credit is given for late participation assignments including required posts of comments and In the News articles.
- You must submit all assignments, even if no credit is given. **If you skip an assignment, an additional 10 points will be subtracted from your final grade in the course.**
- Plan ahead and backup your work. ***Equipment failure is not an acceptable reason for turning in an assignment late.***

University Policies

TEMPLE AND COVID-19

Temple University's motto is Perseverance Conquers, and we will meet the challenges of the COVID pandemic with flexibility and resilience. The university has made plans for multiple eventualities. Working together as a community to deliver a meaningful learning experience is a responsibility we all share: we're in this together so we can be together.

PROTOCOL: Use of Face Masks or Cloth Face Coverings.

The full university protocol for the use of masks or cloth face coverings can be found at this link:
https://tuportal5.temple.edu/html/TEMPLE/apps/WSTF/TUP/Files/protocol-mask-face-covering.pdf

The use of face coverings is an important component to reducing the spread of COVID-19. Face coverings must be worn by all students, faculty, and staff in all classrooms, public and shared spaces on campus, and in areas where physical distancing of six feet or more cannot be observed. Physical distancing of six feet or more should be maintained as much as possible in all university building spaces and outdoors. All students in the classroom should wear face coverings for the entire class. There will be distribution points around campus for students, employees and visitors who need a face mask or covering.

For individuals unable to wear face coverings due to a health condition or disability* , face shields may be used as an alternative. Such individuals should be extra cautious about maintaining physical distancing and observing all other hygiene protocols. In addition to face coverings, other public health precautions must be observed by the whole community, including frequent, thorough hand washing, physical distancing, the implementation of regular cleaning and disinfecting procedures, and encouraging or requiring students and staff to stay home when they are sick.

* Students who require accommodation should contact Disability Resources and Services (215-204-1280).

Attendance and Your Health

To achieve course learning goals, students must attend and participate in classes, according to your instructors' requirements. However, if you feel unwell or if you are under quarantine or in isolation because you have been exposed to the virus or tested positive for it, you should not come to campus or attend in-person classes or activities. It is the student's responsibility to contact their instructors to create a plan for participation and engagement in the course as soon as they are able to do so, and to make a plan to complete all assignments in a timely fashion, when illness delays their completion.

Video Recording and Sharing Policy

Any recordings permitted in this class can only be used for the student's personal educational use. Students are not permitted to copy, publish, or redistribute audio or video recordings of any portion of the class session to individuals who are not students in the course or academic program without the express permission of the faculty member and of any students who are recorded. Distribution without permission may be a violation of educational privacy law, known as FERPA as well as certain copyright laws. Any recordings

made by the instructor or university of this course are the property of Temple University. Any unauthorized redistribution of video content is subject to review by the Dean's office, and the University Disciplinary Committee. Penalties can include receiving an F in the course and possible expulsion from the university. This includes but is not limited to: assignment video submissions, faculty recorded lectures or reviews, class meetings (live or recorded), breakout session meetings, and more.

Code of Conduct Statement for Online Classes Online Behavior
Students are expected to be respectful of one another and the instructor in online discussions. The goal is to foster a safe learning environment where students feel comfortable in discussing concepts and in applying them in class. If for any reason your behavior is viewed as disruptive to the class, you will be asked to leave and you will be marked absent from that class. Please read the university policy concerning disruptive behavior:

> ***The disruptive student is one who persistently makes inordinate demands for time and attention from faculty and staff, habitually interferes with the learning environment by disruptive verbal or behavioral expressions, verbally threatens or abuses college personnel, willfully damages college property, misuses drugs or alcohol on college premises, or physically threatens or assaults others. The result is the disruption of academic, administrative, social, or recreational activities on campus.***

Online Classroom Etiquette

The expectation is that students attending online courses will behave in the same manner as if they were in a live classroom. Be courteous and professional in your location, attire and behavior. Specifically, your location should reflect a clean and professional appearance - not a bedroom, crowded conference room, loud restaurant/bar, etc. Your attire should mirror what you might wear to a live classroom. We expect that students will not disrupt class through visuals or verbal outbursts, such as but not limited to, conversations with other people in the room, engaging in inappropriate behavior while you are in class or distracting the class in any other way. In addition, students should refrain from doing something in their online class that they would not do in a live classroom. which includes eating large meals, drinking alcohol, vaping, getting up often and leaving the online class (not staying at their computer). You should arrive on time and leave when the class is over. If there is an emergency of some kind, notify your faculty member via email or the chat function in Zoom.

Student and Faculty Academic Rights & Responsibilities

Freedom to teach and freedom to learn are inseparable facets of academic freedom. The University has a policy on Student and Faculty Academic Rights and Responsibilities (Policy #03.70.02) which can be accessed at policies.temple.edu.

Inclement Weather Policy

Please be advised that while Temple University campuses may close for inclement weather, online courses are not on-campus and therefore are still expected to meet. Your instructor will contact you regarding any adjustments needed in the event of a power outage or severe circumstances. Should you have any questions, please contact the professor.

Academic Honesty

Learning is both an individual and a cooperative undertaking. Asking for and giving help freely in all *appropriate* setting helps you to learn. **You should represent only your own work as your own.** *Personal integrity* is the basis for intellectual and academic integrity. Academic integrity is the basis for academic freedom and the University's position of influence and trust in our society. University and school rules and standards define and prohibit "academic misconduct" by all members of the academic community including students. You are asked and expected to be familiar with these standards and to abide by them. A link to Temple's Policy on Academic Dishonesty can be found at the following link: https://grad.temple.edu/resources/policies-procedures

Disability Statement

Any student who has a need for accommodations based on the impact of a documented disability or medical condition should contact Disability Resources and Services (DRS) in 100 Ritter Annex (drs@temple.edu; 215-204-1280) to request accommodations and learn more about the resources available to you. If you have a DRS accommodation letter to share with me, or you would like to discuss your accommodations, please contact me as soon as practical. I will work with you and with DRS to coordinate reasonable accommodations for all students with documented disabilities. All discussions related to your accommodations will be confidential.

Temple University's Technology Usage Policy

This site includes information on unauthorized access, disclosure of passwords, and sharing of accounts. https://secretary.temple.edu/sites/secretary/files/policies/04.71.11.pdf

Limited resources are available for students who do not have the technology they need for class. Students with educational technology needs, including no computer or camera or insufficient Wifi-access, should submit a Student Technology Assistance Application located in TUPortal and linked from the Dean of Students Support and Resources webpage. The university will endeavor to meet needs, such as with a long-term loan of a laptop or Mifi device, a refurbished computer, or subsidized internet access. Internet Essentials from Comcast provides the option to purchase a computer for $150 and high-speed Internet service for $9.95 a month, plus tax. The Emergency Broadband Benefit (EBB) is available to purchase Xfinity, Verizon, T-Mobile, and other internet services. Qualified households can receive a temporary monthly credit of up to $50/month toward their Internet service and leased Internet equipment until the program's funding runs out.

On-campus computer labs have resumed normal operations and are available for student use.