MIS 5206 – Protection of Information Assets
May 2019

Instructor

David Lanter
Email: David.Lanter@temple.edu
e-profile: *http://community.mis.temple.edu/dlanter/*

Class Website: http://community.mis.temple.edu/bnaisum18/category/welcome/

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 the nature 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
	Vacca, Chapter 16 (online) "Local Area Network Security"
	Vacca, Chapter 27 (online) "Information Technology Security Management"
	Vacca, Chapter 46 "Data Encryption"
	Vacca, Chapter 59 (online) "Identity Theft – First Part"
	Vacca, Chapter 59 (online) "Identity Theft – Second Part"
	Vacca, Chapter 61 (online) "SAN Security"
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"
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/626138 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 of class topics:

Unit #	Assignment Topics	Date
0a	Webinar – Introduction to MIS5206	
0b	Understanding an Organization's Risk Environment	
1a	Case Study 1: *Snowfall and a stolen laptop*	May 27
1b	Data Classification Process and Models	May 27
1c	Risk Evaluation	May 27
2a	Case Study 2: *Autopsy of a Data Breach: The Target Case*	May 28
2b	Creating a Security Aware Organization	May 28
2c	Physical and Environmental Security	May 28
3a	**Exam 1 - Midterm**	May 29
3b	Case Study 3: *A Hospital Catches the "Millennium Bug"*	May 29
3c	Business Continuity and Disaster Recovery Planning	May 29
4a	Team Project Assignment	May 30
4b	Network Security	May 30
4c	Cryptography, Public Key Encryption and Digital Signatures	May 30
5a	Identity Management and Access Control	May 31
5b	Computer Application Security	May 31
5c	Review	May 31
	Exam 2 - Final	June 3

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
0b	• 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
1a	• Case Study 1: "Snowfall and a Stolen Laptop"
1b	• 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
1c	• Vacca Chapter 25 "Security Management Systems"

	• Vacca Chapter 34 "Risk Management" • ISACA Reading 1: "Risk IT Framework" pp. 47-96
2a	• Case Study 2: ""Autopsy of a Data Breach: The Target Case"
2b	• 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"
2c	• HBR Reading 1: "The Myth of Security Computing" • Vacca Chapter 69 "Physical Security Essentials" • SANS Reading 3: "Implementing Robust Physical Security"
3b	• Case Study 3: "A Hospital Catches the "Millennium Bug"
3c	• 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"
4b	• 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"
4c	• 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"
5a	• 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"
5b	• 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 topical unit are available on the class website, under "QUESTIONS ABOUT THE READINGS AND CASE STUDIES. Post your answer to each of the questions as you work through the readings with the goal of completion before first day of class June 11. To do so, click "Leave a Comment". Provide a paragraph or two of thoughtful analysis as your answer to each question. ***Late 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 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.
   ii. Group discussions are informal sessions of give and take. Come 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 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
1a	Case Study 1: *Snowfall and a stolen laptop*
2a	Case Study 2: *Autopsy of a Data Breach: The Target Case*
3b	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.

Team Projects Presentation

During Unit #4a students will be organized into project teams. Each team will receive a topic, and will follow up by developing a presentation covering the assigned topic. Afterwards, each team will have a total time of 15 minutes to present, following by questions and answer (Q&A) session.

Exams

There will be two exams given during the semester. Together these exams are weighted 25% of each student's final grade.

Below is the exam schedule:

Unit #	Exam
3a	Midterm Exam
June 3	Final Exam

Both exams will consist of multiple-choice questions. You will have a fixed time (e.g. 40 minutes) to complete the exam. The Midterm Exam will occur during Unit #3a and the Final Exam will occur after the last class.

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.

Quizzes

At the end of many class units 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 certification exam. Quizzes are for practice only. They will not count towards your final grade. You will be given time to answer the quiz, and then we will go over the answers to the quiz. The goals for the quizzes are twofold: 1) help you become familiar with technical information security areas requiring additional study and attention, and 2) help you gain skills that improve your test taking abilities.

Evaluation and Grading

Item	Weight
Assignments	25%
Participation	25%
Team Project Presentation	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	B-, B, B+

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.	
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 20% penalty** each day they are late. No credit is given for assignments turned in over five calendar days past the due date.
- 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.***

Citation Guidelines

If you use text, figures, and data in reports that were created by others you must identify the source and clearly differentiate your work from the material that you are referencing. If you fail to do so you are plagiarizing. There are many different acceptable formats that you can use to cite the work of others (see some of the resources below). The formats are not as important as the intent. You must clearly show the reader what is your work and what is a reference to someone else's work.

Plagiarism and Academic Dishonesty

All work done for this course: examinations, homework exercises, blog posts, oral and written presentations — is expected to be the individual effort of the student presenting the work.

Plagiarism and academic dishonesty can take many forms. The most obvious is copying from another student's exam, but the following are also forms of this:

- Copying material directly, word-for-word, from a source (including the Internet)
- Using material from a source without a proper citation
- Turning in an assignment from a previous semester as if it were your own
- Having someone else complete your homework or project and submitting it as if it were your own

- Using material from another student's assignment in your own assignment

Plagiarism and cheating are serious offenses, and behavior like this will not be tolerated. In cases of cheating, both parties will be held equally responsible, i.e. both the student who shares the work and the student who copies the work. Penalties for such actions are given at my discretion, and can range from a failing grade for the individual assignment, to a failing grade for the entire course, to expulsion from the program.

Student and Faculty Academic Rights and Responsibilities

The University has adopted a policy on Student and Faculty Academic Rights and Responsibilities (Policy # 03.70.02).

Additional Information

Availability of Instructor	▪ Please feel free to contact me via e-mail with any issues related to this class. I will also be available at the end of each session. Please note that these discussions are to address questions/concerns but are NOT for helping students catch up on content they missed because they were absent. Note: I will respond promptly when contacted during the week ▪ I am available to meet personally with you: ✓ Immediately before or after class ✓ During class breaks
Attendance Policy	▪ Class discussion is intended to be an integral part of the course. Therefore, full attendance is expected by every student. ▪ If you are absent from class, speak with your classmates to catch up on what you have missed.
Class Etiquette	▪ Please be respectful of the class environment. ▪ Class starts promptly at the start time. Arrive on time and stay until the end of class. ▪ Turn off and put away cell phones, pagers and alarms during class. ▪ Limit the use of electronic devices (e.g., laptop, tablet computer) to class-related usage such as looking up terms and taking notes. Restrict the use of an Internet connection (e.g., checking email, Internet browsing, sending instant messages) to before class, during class breaks, or after class. ▪ Refrain from personal discussions during class. Please leave the room if you need to speak to another student for more than a few words. If a student cannot refrain from engaging in private conversation and this becomes a pattern, the students will be asked to leave the classroom to allow the remainder of the students to work. ▪ During class time speak to the entire class (or breakout group) and let each person "take their turn." ▪ Be fully present and remain present for the entirety of each class meeting.