CS684 A1 Enterprise Cybersecurity Management

Rev 1

Instructor: Pamela Campbell

Contact Information:

Office Location: Virtual Office

Office Hours via Zoom: email me and we will find a mutually agreeable time to meet

Office Phone: 978-884-1157

Wednesdays: 6:00 - 8:45 PM

The First Class will take place on September 4, 2024

DATES: Sept 4, 11, 18, 25, Oct 2, 9, 16, 23, 30, Nov 6, 13, 20 – NO CLASS NOV 27, Dec 4 Final Exam: Dec 18

Classroom: KCB Room 102 565 Comm Ave

E-Mail: pdc@bu.edu Pamela Campbell

Materials will be delivered using the 'Blackboard Learn' web site for this course which can be accessed at http://learn.bu.edu

Biography

Pamela Campbell is a lecturer at Boston University. She has been working and teaching in the area of Project Management, Education, and software development for 20 years in organizations such as MITRE, Synetics, and BEA Systems, Inc. While holding a Top Secret clearance she worked on a variety of government programs for the US and for Canada. She holds a Masters degree from Bentley College in Computer Information Systems and has designed and implemented systems that include large databases.

One of her most rewarding assignments was to manage the project to upgrade the Amver system (amver.com). Amver, sponsored by the United States Coast Guard, is a unique,

computer-based, and voluntary global ship reporting system used worldwide by search and rescue authorities to arrange for assistance to persons in distress at sea. Ms. Campbell has been teaching for Boston University for more than 15 years.

In addition to her lecturing, she is a consultant to Bridging Distances, for which she provides training services to software, healthcare, and engineering firms. Her latest focus has been on assisting companies with plans to return-to-the-office and with handling a mixture of remote and on-site employees.

Enterprise Cybersecurity Management

Course description

This course covers important topics that students need to understand in order to effectively manage a successful cybersecurity and privacy program, including governance, risk management, asset classification and incidence response. Students are first introduced to cybersecurity & privacy policy frameworks, governance, standards, and strategy. Risk tolerance is critical when building a cybersecurity and privacy program that supports business goals and strategies. Risk management fundamentals and assessment processes will be reviewed in depth including the methodology for identifying, quantifying, mitigating and controlling risks. Asset classification and the importance of protecting Intellectual Property (IP) will prepare students to understand and identify protection mechanisms needed to defend against malicious actors, including industry competitors and nation states. Incident Response programs will cover preparation and responses necessary to triage incidents and respond quickly to limit damage from malicious actors.

This course enables IT professionals to manage cybersecurity and privacy programs across industries. Students will be introduced to cybersecurity & privacy policy frameworks, governance, standards, and strategy. We will review and discuss methodologies for identifying, quantifying, mitigating, and controlling risks. Risk management fundamentals and assessment processes will be reviewed in depth to understand risk tolerance is critical when building a cybersecurity and privacy program that supports business goals and strategies.

Asset classification and the importance of protecting Intellectual Property (IP) will prepare students to understand and identify protection mechanisms needed to defend against malicious actors, including industry competitors and nation states. Incident Response programs will cover preparation and responses necessary to triage incidents and respond quickly to limit damage from malicious actors.

This course covers many important topics that students need to understand in order to effectively manage a successful cybersecurity and privacy program.

Learning Goals and Objectives and Outcomes

- The elements needed to effectively manage a cybersecurity and privacy program

- Risk management: identification, quantification, response, and control
- The importance of policy and governance within the cybersecurity and privacy program
- Asset classification and the value of Intellectual Property
- Security measures from Technology, Policy, and Practice; and Education, Training, and Awareness dimensions
- Incident Response process and the importance of postmortem reviews
- Why cybersecurity and privacy require alignment with business strategy and goals

Students will develop good documentation/technical writing skills, and through discussions, build communication skills.

All students must obtain a free Boston University computer account and email address as these are necessary both for essential electronics communications with students and to use the web sites for this and other courses at Boston University. Students are expected to check the 'Blackboard Learn' site for announcements and assignment changes, and to read their email **which will be addressed to their bu.edu email address**. Note that you can arrange for your bu.edu email to be forwarded to a different preferred email address via the university web site.

Revisions to this syllabus, schedule changes, new readings and assignments, and so forth, will be posted on the 'Blackboard Learn' web site as the course goes along, where you can download them. Additional materials will be posted to the site as needed, and as they become relevant.

Note: (If you plan to become a certified Project Management Professional this comment applies to you.) This course counts to PMP educational requirements and the project produced counts towards experience.

ASSIGNMENTS: See the Individual Assignments documents posted on Blackboard under "Assignments" for Detailed Homework Assignments and Discussion topics.

Course Outline

- **Readings** - Each module has textbook readings. There are additional materials online. Your professor may suggest additional readings during the running of the course.
- **Discussion** – **Discussions will be conducted in class**. Reading will be assigned in advance. Discussion topics and assigned readings are found under "Assignments" on Blackboard.
- **Assignments** - There are assignments that are due throughout the course. – Look in Assignments on the website for detailed instructions.

Module 1: Introduction and Information

- Security and Privacy Introduction
- Introduction to Information Security and Privacy

- Cyber threat and actors
- Law and Ethics

Module 2: Policy Framework
- The Policy Framework
- Policy elements and hierarchy
- U.S. and international standards organizations

Module 3: Developing the Security Program
- Planning the Security Program
- The Written Information Security Program (WISP)

Module 4: Risk Management
- The Risk Assessment Process
- Assessing Risk within the organization

Module 5: Asset Management & Information Classification
- Asset Classification
- Protected Personal Information
- Privacy concerns and considerations within cloud environments

Module 6: Incident Response and Disaster Recovery
- Incident Response Overview
- Disaster Recovery Planning

Class Schedule

Class sessions are 6:00 – 8:45 PM

THIS IS A FACE-TO-FACE CLASS AND ATTENDANCE WILL BE PART OF YOUR PARTICIPATION GRADE

LECTURE SCHEDULE: This is a 'provisional' schedule and is subject to change as the course progresses and evolves.

HOMEWORK: See the Assignments doc on Blackboard for Detailed Homework Assignments instructions**.** Assignments are to be submitted through Blackboard.

Assignments are to be completed in **12 pt font, single spaced**. See the last pages of this Syllabus for examples of how to cite various sources, including AI sources such as CHATgpt.

******** There is a policy document posted on Blackboard that describes the inclusion of AI sources as part of homework assignments for this class ********

DISCUSSIONS: See the Discussion document on Blackboard under Assignments for topics and detailed instructions**.** Discussions will be held in class.

CURRENT SECURITY EVENTS: Each student should bring to EACH class a security-related current event to be shared for discussion purposes.

Session 1. **Sep 4** – **Module 1 *Intro and Info*, Study Guide and Deliverables**

- **Readings:** *Whitman/Mattord*: pp 1-55, 78-104
- **Discussions: Discussion 1 will be in class, Sept 11**
- **Assignments: Assignment 1 due - Sept 18 by 5:00 PM on Blackboard**

Session 2. **Sep 11** - **Module 1 Continued**

- **Discussions: Discussion 1 in class, Sept 11**
- **Current Security Events:** Each student should bring to EACH class a security-related current event to be shared for discussion purposes
- **Assignments: Assignment 1 due - Sept 18 by 5:00 PM**

Session 3. **Sep 18** – **Module 2 *Policy Framework* Study Guide and Deliverables**

- **Readings:** *Whitman/Mattord*: pp 169 - 214 *Santos*: pp 2-21, 32-53, 64-82
- **Current Security Events:** Each student should bring to EACH class a security-related current event to be shared for discussion purposes
- **Discussions: Discussion 2 will be in class, Sept 25**
- **Assignments: Assignment 2 due - Oct 2 by 5:00 PM**

Recommended External Readings:

- NIST information security framework
- NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management
- American National Standards Institute, ANSI
- International Organization for Standardization, ISO

Session 4. Sep 25 – **Module 2 Continued**

- **Assignments: Assignment 2 due - Oct 2 by 5:00 PM**

Session 5. **Oct 2 –– Module 3 *Developing the Security Program***
Study Guide and Deliverables

- **Readings:** *Whitman/Mattord*: pp 123-164, 197-214
- **Current Security Events:** Each student should bring to EACH class a security-related current event to be shared for discussion purposes

- **Discussions: Discussion 3 will be in class, Oct 9**
- **Assignments: Assignment 3 due - Oct 16 by 5:00 PM**

Recommended External Readings:

- 201 CMR 17.00 COMPLIANCE CHECKLIST

Session 6. **Oct 9 Module 3 Continued**

- **Current Security Events:** Each student should bring to EACH class a security-related current event to be shared for discussion purposes
- **Discussions: Discussion 3 will be in class, Oct 9**
- **Assignments: Assignment 3 due - Oct 16 by 5:00 PM**

Session 7. **Oct 16** – **Module 4 *Risk Management* Study Guide and Deliverables**

- **Readings**: *Santos*: pp 105–112 *Whitman/Mattord*: pp 303-316, 365-406
- **Current Security Events:** Each student should bring to EACH class a security-related current event to be shared for discussion purposes
- **Discussions: Discussion 4 will be in class, Oct 23**
- **Assignments: Assignment 4 due Oct 30 by 5:00 PM**

Recommended External Readings:

- Cybersecurity

Session 8. **Oct 23** – **Module 4 Continued**

- **Current Security Events:** Each student should bring to EACH class a security-related current event to be shared for discussion purposes
- **Discussions: Discussion 4 will be in class, Oct 23**
- **Assignments: Assignment 4 due Oct 30 by 5:00 PM**.

Session 9. **Oct 30** - **Module 5 *Asset Management & Info Classification***
Study Guide and Deliverables

- **Readings**: *Santos*: pp 442-470 *Whitman/Mattord*: pp 381-393
- **Current Security Events:** Each student should bring to EACH class a security-related current event to be shared for discussion purposes
- **Discussions**: **Discussion 5 will be in class, Nov 6**
- **Assignments: Assignment 5 due Nov 13 by 5:00 PM**

Recommended External Readings:

- Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories
- Specification for Asset Identification 1.1

Session 10. **Nov 6** – **Module 5 Continued**

- **Current Security Events:** Each student should bring to EACH class a security-related current event to be shared for discussion purposes
- **Discussions**: **Discussion 5 will be in class, Nov 6**
- **Assignments: Assignment 5 due Nov 13 by 5:00 PM**

Session 11. **Nov 13** – **Module 6 *Incident Response and Disaster Recovery***
Study Guide and Deliverables

- **Readings:** *Whitman/Mattord*: pp 497-562
- **Current Security Events:** Each student should bring to EACH class a security-related current event to be shared for discussion purposes
- **Discussions: Discussion 6 will be in class, Nov 29**
- **Assignments: Assignment 6 due Dec 4 by 5:00 PM**

Recommended External Readings:

- Cybersecurity
- Introduction to Information Security
- Incident Management
- Business Continuity Plan
- Crisis Communications Plan
- IT Disaster Recovery Plan
- CRR Supplemental Resource Guide

Session 12. **Nov 20** – **Module 6 Continued**

- **Canadian Pacific RR Case Study** (.pdf online)
- **Current Security Events:** Each student should bring to EACH class a security-related current event to be shared for discussion purposes
- **Discussions: Discussion 6 will be in class, Dec 4**
- **Assignments: Assignment 6 due Dec 4 by 5:00 PM**

Nov 27 – NO CLASS – Thanksgiving Break

Session 13. Dec 4 – **Module 6 Continued, Review for final exam**

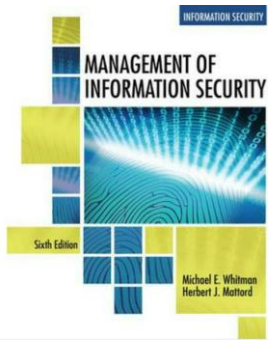
- **Assignments: Assignment 6 due Dec 4 by 5:00 PM**

Dec 11 – NO CLASS – Study period

Dec 18 – Final Exam

Course Resources

Required Books

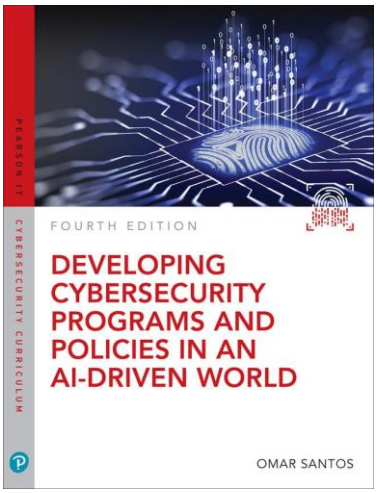


Michael E. Whitman, Herbert J. Mattord

Management of Information Security, 6th Edition (2019)

ISBN-10: 133740571X

ISBN-13: 9781337405713



Omar Santos

Developing Cybersecurity Programs and Policies 4th Edition (2024)

PAPERBACK

by Santos, Omar (9780138074104) - 4TH 24

ISBN-10 – 0138074100

ISBN-13 - 978-0138074104

These books can be purchased from Barnes and Noble at Boston University.

Grading Structure

All students will be expected to demonstrate knowledge of IT Security Policies and Procedures and relevant techniques. To obtain an exceptional grade you have to exceed expectations in your projects and weekly assignments.

Accommodation of Special Needs

In accordance with University policy, we make every effort to accommodate unique and special needs of students with respect to speech, hearing, vision, seating, or other disabilities. Please notify Disability Support Services as soon as possible of requested accommodations.

Grading Structure, Distribution and Grading Criteria

The course consists of homework assignments, participation in discussions, and a final exam, weighted as follows:

Assignments:	**40%**
Participation and Discussions:	**30%**

Students are expected to attend class and to participate in discussions and exercises. Each student is to bring a current event item regarding security to be shared for discussion.

Final Exam:	**30%**

There is a Rubric (grading criteria) posted online that describes the specifics of grading for all assignments, showing what is required to achieve a high grade.

Expectations

Homework are to be submitted at the deadline via Blackboard.

This is a graduate course and you are expected to produce quality materials.

Students are expected to attend all classes. If you will be absent, notify your professor as soon as you know you will miss class. More than one absence may impact your grade, especially as participation is a large portion of the grade.

Deadline Expectations

Due dates must be respected for assignments. It is unfair to other students to allow extensions for some. Issues that interfere with coursework such as work travel, home demands and vacations can all be anticipated. These pressures face everyone and are not sufficient reason for extensions to be offered. Extensions can only be granted under truly extenuating circumstances. Contact your instructor as soon as you think you will miss a deadline.

Security Reference links:

http://www.securitystrategy101.com

This site provides the basic of InfoSec as well as useful links

https://www.fireeye.com/current-threats/threat-intelligence-reports.html

Cyber Threat Intelligence Reports

http://www.ponemon.org/
Ponemon Institute conducts independent research on privacy, data protection and information security policy.

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/index.html
U.S. Department of Health & Human Services - enforcement data.

http://www.isaca.org/
The Information Systems and Control Association and Foundation. The guidelines and framework for the Control Objectives for Information Technology (COBIT) can be downloaded from this website

http://www.isc2.org/
The International Information Systems Security Certification Consortium.

http://www.cert.org
The website of the Computer Emergency Response Team at Carnegie Mellon University, USA.

http://www.attrition.org/
A web site for the collection, dissemination and distribution of information about computer security.

http://cve.mitre.org/
A web site with a database of standardized names for Common Vulnerabilities and Exposures in information systems.

http://www.htcn.org/
The High Tech Crimes Network – a somewhat complex home page leads into valuable information, training and testing facilities, conferences and technology issues.

http://www.csoonline.com/
CSO provides news, analysis and research on a broad range of security and risk management topics.

https://www.ic3.gov/default.aspx
Federal Bureau of Investigation – Internet Crime Complaint Center (IC3)

Grading Standards

Grade inflation is not in the best interests of BU students or the reputation of the institution. I have a responsibility to differentiate the performance of my students, and to reward with high grades only those who do exceptionally well. A Grade of 'A' or 'A minus' will be limited only to those students truly distinguishing themselves in the course. The Academic Policy Committee of Metropolitan College recommends the following guidelines for distinguishing grades.

A, A-	20%
B+, B, B-	80%
Other	As merited

While there are strict policies for grades at MET, I do NOT impose a grading curve.

You can expect to be challenged in this course, and excellent, high-quality work will be rewarded with an 'A'. If everyone submits high quality work, then everyone will get an 'A'. An 'A' grade requires high quality excellence in all aspects of the course: homework, class discussions, final project and exams.

6. Academic Conduct Policy

The academic conduct policy is summarized below. Cheating and plagiarism will not be tolerated in any Metropolitan College course. They will result in no credit for the assignment or examination and may lead to disciplinary actions. Please take the time to review the Student Academic Conduct Code:

For the full text of the academic conduct code, please go to:
http://www.bu.edu/met/metropolitan_college_people/student/resources/conduct/code.html

Academy Conduct Policy

For the full text of the academic conduct code, please go to http://www.bu.edu/met/metropolitan_college_people/student/resources/conduct/code.html

A Definition of Plagiarism

"The academic counterpart of the bank embezzler and of the manufacturer who mislabels products is the plagiarist: the student or scholar who leads readers to believe that what they are reading is the original work of the writer when it is not. If it could be assumed that the distinction between plagiarism and honest use of sources is perfectly clear in everyone's mind, there would be no need for the explanation that follows; merely the warning with which this definition concludes would be enough. But it is apparent that sometimes people of goodwill draw the suspicion of guilt upon themselves (and, indeed, are guilty) simply because they are not aware of the illegitimacy of certain kinds of "borrowing" and of the procedures for correct identification of materials other than those gained through independent research and reflection."

"The spectrum is a wide one. At one end there is a word-for-word copying of another's writing without enclosing the copied passage in quotation marks and identifying it in a footnote, both of which are necessary. (This includes, of course, the copying of all or any part of another student's paper.) It hardly seems possible that anyone of college age or more could do that without clear intent to deceive. At the other end there is the almost casual slipping in of a particularly apt term which one has come across in reading and which so aptly expresses one's opinion that one is tempted to make it personal property.

Between these poles there are degrees and degrees, but they may be roughly placed in two groups. Close to outright and blatant deceit-but more the result, perhaps, of laziness than of bad intent-is the patching together of random jottings made in the course of reading, generally without careful identification of their source, and then woven into the text, so that the result is a mosaic of other people's ideas and words, the writer's sole contribution being the cement to hold the pieces together. Indicative of more effort and, for that reason, somewhat closer to honest, though still dishonest, is the paraphrase, and abbreviated (and often skillfully prepared) restatement of someone else's analysis or conclusion, without acknowledgment that another person's text has been the basis for the recapitulation."

{The two paragraphs above are from H. Martin and R. Ohmann, The Logic and Rhetoric of Exposition, Revised Edition. Copyright 1963, Holt, Rinehart & Wins

BOSTON UNIVERSITY

GUIDELINE FOR ALL PAPERS SUBMITTED TO DEPARTMENT COURSES

1. ORIGINAL ARTICLES ONLY

Submission of a paper to the department represents a certification on the part of the author(s) that the paper is an original work. **Ideas of others either indirect or quoted must be referenced.**

2. MANUSCRIPT STYLE

References, citations and general style of manuscripts for this Journal must follow the APA style (Please refer to the latest edition of the *Publication Manual* of the American Psychological Association for style questions.

[For homework assignments – which are not being submitted for publication – the title page, table of contents, and abstract can be omitted.]

References should be double-spaced and placed in alphabetical order. Each reference must be fully described, showing date of publication clearly. **Links to website are not acceptable as a substitute.**

Examples of References *to Periodicals:*

Journal article: One author

Levitt, T. (1983). The globalization of markets *Harvard Business Review,* 61(3), 92-102.

Journal article: Multiple authors

Kaynak, E. & Kothan, V. (1984) Export behavior of small and medium-sized manufacturers Some policy guidelines for international marketers. *Management International Review,* 24(2) June, 61-69

Magazine article

Tinnin, D. B. (1981, November 16). The heady success of Holland's Heineken. *Fortune,* pp. 158-164

Newspaper article

The opportunity for world brands. (1984, June 3) *The* New *York Times,* p 6E

Website

Rasmussen, C. (2021, October 12). *Icy 'glue' may control pace of Antarctic ice-shelf breakup*. National Aeronautics and Space Administration. https://www.nasa.gov/feature/jpl/icy-glue-may-control-pace-of-antarctic-ice-shelf-breakup

Monograph

Franco, L G (1979). *A* survey *of* the *impact of manufactured exports from industrializing countries in Asia and Latin America* (Monograph). *Changing International Realities,* 6.

Examples of References* to *Books:

Reference to an entire book

Kaynak, E (1986) *Marketing and economic development* New York: Praeger Publishers Inc.

Book with a corporate author

Committee for Economic Development (1981) "*Transnational corporations and developing Countries"* New York. Author.

Edited book

Kaynak, E (Ed). (1986). *International Business in the Middle East,* Berlin, New York: Walter de Gruyter.

Book with no author or editor

"Marketing opportunities in Japan" (1978) London Dentsu Incorporated

Article or chapter in an edited book

Bucklin, L. P (1 986) "Improving food retailing in less developed countries" In E Kaynak (Ed), World Food Marketing Systems (pp. 73-81) London. Butterworth Scientific Publishers

Proceedings of Meetings and Symposia

Published proceedings, published contributions to a symposium

Lee K H. (1981) "From production orientation to marketing orientation - Hong Kong in the international trade setting" In D. B, Yeaman(Ed.), *Developing* global strategies (pp. 753-766) Conference held at the University of Navarra, Barcelona, Spain, 2 (December 17-19)

Unpublished paper presented at a meeting

Kaynak, E (1988). *Strategic and organizational Issues in tourist* services Paper presented at Second International Tourism Advertising Conference, Portoroz, Yugoslavia.

Doctoral Dissertations/Masters Theses

Unpublished doctoral dissertation Czinkota, M F. (1980) "An analysis of export development strategies in selected U S. industries" Dissertation Abstracts International. (University Microfilms No. 80-15, 865)

HOW TO REFERENCE THE USE OF AI such as CHATgpt IN HOMEWORK ASSIGNMENTS:

OpenAI. (2023, January 17). [ChatGPT response to a prompt about three prominent themes in Emily Dickinson's
poetry]. https://chat.openai.com/.....

If the text that ChatGPT generates is *not* retrievable or sharable, then it falls into the **"personal communication"** category, where you cite with an in-text only citation.

Example:

"(OpenAI, personal communication, January 16, 2023)."

This technology is new and we are all learning about generative AI resources and how to ethically use them. Consider making the ChatGPT conversation retrievable by including the text as an **appendix** or as online supplemental material. If you do so, then readers may be referred to the appendix or the online supplemental material (where the ChatGPT response may be contextualized) when the ChatGPT conversation is cited. It would be good practice to describe, in the narrative or a note, the prompt that generated the specific ChatGPT response. This too will help inform the understanding of the technology and its outputs.

3. MANUSCRIPT PREPARATION

Margins: leave at least a one-inch margin on all four sides
Paper: use clean white, 8-1/2" x 11" bond paper.
Cover page [not required for homework assignments]: This should provide full authorship, along with authors' academic degrees, professional titles, affiliations and addresses (mail, fax, and e-mail)
Title page [not required for homework assignments]: This should provide only the title of the manuscript, and abstract of about 100 words, and 3-10 words for index purposes.

4. SPELLING, GRAMMAR, AND PUNCTUATION

You are responsible for preparing manuscript copy which is clearly written in acceptable scholarly language (English with no errors of spelling, grammar, or punctuation). Verify the accuracy of arithmetic calculations, statistics, numerical data, text citations, and references as well as avoiding the following common errors:

- dangling modifiers
- misplaced modifiers
- unclear antecedents
- incorrect or inconsistent abbreviations

5. INCONSISTENCIES MUST BE AVOIDED

Be sure you are *consistent* in your use of abbreviations, terminology, and in citing references. Only use abbreviations after the abbreviation has been explained. For example, define the acronym "The North American Free Trade Agreement (NAFTA)" in the appropriate part of the document, and .later in the text, it is acceptable to use "It was found that NAFTA