MET CS 684
Enterprise Cybersecurity Management
Online Course Syllabus

Instructor

Charles Pak, Ph.D., cpak4@bu.edu

Course Duration

Start: October 28, 2025
End: December 15, 2025

Course Credits

4 credits

Course Description

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.

Course Objectives

By successfully completing this course, you will be able to explain the following:

- 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.

Course Outline

Module 1: Information

- Security & Privacy Introduction
- Introduction to Information Security & Privacy
- Cyber Threats & Actors
- Law & Ethics

Module 2: Policy Framework

- The Policy Framework
- Policy Elements & 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

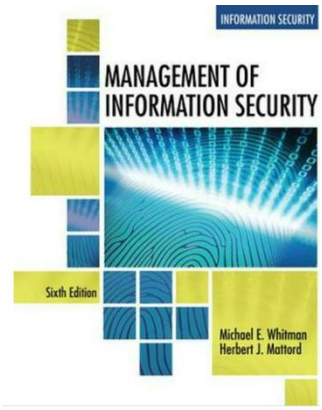
- Asset Classification
- Protected Personal Information
- Privacy Concerns and Considerations within Cloud Environments

Module 6: Incident Response & Disaster Recovery

- Incident Response Overview
- Disaster Recovery Planning

Course Resources

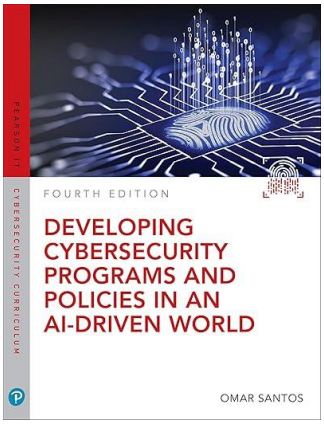
Required Books



Michael E. Whitman, Herbert J. Mattord
Management of Information Security, 6th Edition (2019).

ISBN-10: 133740571X
ISBN-13: 9781337405713

This book is available at a discounted price through the Barnes & Noble at BU's First Day® inclusive access program.



Omar Santos
Developing Cybersecurity Programs and Policies in an AI-Driven World (Pearson IT Cybersecurity Curriculum), 4th edition (2024).

ISBN-10: 0138074100
ISBN-13: 978-0138074104

This book is available at a discounted price through the Barnes & Noble at BU's First Day® inclusive access program.

Study Guide

Module 1 Study Guide and Deliverables (October 28 – November 3)

Topics:

- Information Security & Privacy introduction and overview
- Cyberattacks – methods and actors
- Understanding the changing threat landscape
- Law & Ethics

Readings:

- Whitman/Mattord, pp. 1-55, 78-104

Discussions:

- Discussion 1 posts due **Tuesday, November 4 at 6:00 AM ET**

Assignments:

- Assignment 1 due **Tuesday, November 4 at 6:00 AM ET**

Live Classroom:

- **Lecture: Tuesday, November 4 from 7:00 - 9:00 PM ET**

2 Study Guide and Deliverables (November 4 – November 10)

Topics:

- The Policy Framework
- Policy Elements and Hierarchy
- U.S. and International Standards Organizations

Readings:

- Whitman/Mattord, pp. 169-214
- Santos, pp. 2-34, 46-69, 80-118

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

Discussions:

- Discussion 2 posts due **Tuesday, November 11 at 6:00 AM ET**

Assignments:

- Assignment 2 due **Tuesday, November 11 at 6:00 AM ET**

Live Classroom:

- **Tuesday, November 11 from 7:00 - 9:00 PM ET**

Module 3 Study Guide and Deliverables (November 11 – November 17)

Topics:

- Planning the Security Program
- The Written Information Security Program (WISP)

Readings:

- Whitman/Mattord, pp. 123-164, 197-214

Recommended External Readings:

- 201 CMR 17.00 COMPLIANCE CHECKLIST

Discussions:

- Discussion 3 posts due **Tuesday, November 18 at 6:00 AM ET**

Assignments:

- Assignment 3 due **Tuesday, November 18 at 6:00 AM ET**

Live Classroom:

- **Tuesday, November 18 from 7:00 - 9:00 PM ET**

Module 4 Study Guide and Deliverables
(November 18 – November 24)

Topics:

- The Risk Assessment Process
- Assessing Risk Within the Organization

Readings:

- Whitman/Mattord, pp. 303-316, 365-406
- Santos, pp. 197-206

Recommended External Reading:

- Cybersecurity

Discussions:

- Discussion 4 posts due **Tuesday, November 25 at 6:00 AM ET**

Assignments:

- Assignment 4 due **Tuesday, November 25 at 6:00 AM ET**

Live Classroom:

- **Tuesday, November 25 from 7:00 - 9:00 PM ET**

Module 5 Study Guide and Deliverables
(November 25 – December 1)

Topics:

- Asset Classification
- Protected Personal Information (PII)
- Privacy Concerns and Considerations Within Cloud Environments

Readings:

- Whitman/Mattord, pp. 381-393
- Santos, pp. 556-588

Recommended External Readings:

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

Discussions:

- Discussion 5 posts due **Tuesday, December 2 at 6:00 AM ET**

Assignments:

- Assignment 5 due **Tuesday, December 2 at 6:00 AM ET**

Live Classroom:

- **Tuesday, December 2 from 7:00 - 9:00 PM ET**

Module 6 Study Guide and Deliverables
(December 2 – December 8)

Topics:

- Incident Response Overview
- Disaster Recovery Planning

- Privacy Breach Notifications
- Incident Response Planning

Readings:

- Whitman/Mattord, pp. 497-562
- Santos, pp. 474-504

Recommended External Readings:

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

Discussions:

- Discussion 6 posts due **Tuesday, December 9 at 6:00 AM ET**

Assignments:

- Research Paper due **Tuesday, December 9 at 6:00 AM ET**
- Assignment 6 due **Tuesday, December 9 by 6:00 AM ET**

Course Evaluation:

Please complete the course evaluation once you receive an email or Blackboard notification indicating the evaluation is open. Your feedback is important to MET, as it helps us make improvements to the program and the course for future students.

Live Classroom:

- **Tuesday, December 9 from 7:00 - 9:00 PM ET**

Final Exam Details

The Final Exam is a proctored exam available from **Wednesday, December 10 at 6:00 AM ET to Saturday, December 13 at 11:59 PM ET**. The Computer Science department requires that all final exams be administered using an online proctoring service that you will access via your course in Blackboard. In order to take the exam, you are required to have a working webcam and computer that meets the proctoring service system requirements. A detailed list of those requirements can be found on the How to Schedule page. Additional information regarding your proctored exam will be forthcoming from the Assessment Administrator. You will be responsible for scheduling your own appointment within the defined exam window.

The Final Exam will be **open book/open notes** and is accessible only during the final exam period. You may bring notes and other materials to the exam.

You can take the exam only once. The exam features **essay questions**.

Final Exam Duration: **3 hours**. There is a clock in the upper right corner of the screen keeping time for the exam.

Course Grading Information

Please check the **Study Guide** in the syllabus for Live Classroom dates and specific due dates for assignments and assessments.

Grading Policy

All students will be expected to demonstrate knowledge of IT Security Policies and Procedures. To obtain an exceptional grade you have to exceed expectations in your assignments, discussions and proctored final exam.

Grading Structure and Distribution

The grade for the course is determined by the following:

Overall Grading Percentages	
Assignments	40
Discussions	30
Proctored Final Exam	30
Total Possible	**100**

The next table shows the minimum points for each letter grade, which is a slightly augmented form of the registrar's system. To get a B+ for the course, for example, your course points should be at least 3.3. The only exception is that to obtain an A for the course, a score of 3.85 or more is required.

The following grade structure (the university's, with two refinements) will be applied for your assignments:

Letter Grade	100 pt. scale	4 pt. scale
A	95-100	3.85 - 4.0
A-	90-94	3.7 – 3.84
B+	86-89	3.3 – 3.69
B	82-85	3.0 – 3.29
B-	78-81	2.7 – 2.99
C+	74-77	2.3 – 2.69
C	70-73	2.0 – 2.29
C-	67-69	1.7 – 1.99
D	60-66	1.0 – 1.69
F	0-59	0.0 – 0.99

Assignments

Your homework assignments are an integral part of the learning process. You will receive feedback from your facilitator for each assignment. Please review the assignment rubric.

Criteria	**C or lower**	**B- (2.7-2.99)**	**B (3.00-3.29)**	**B+ (3.30-3.69)**	**A- (3.7-3/84**	**A (3.85-4.00)**
Thoroughness & Coverage	Hardly covers any of the major relevant issues.	Covers some of the major relevant issues	Reasonable coverage of the major relevant areas.	Good coverage of the major relevant areas.	Thorough coverage of almost all of the major relevant areas.	Exceptionally thorough coverage of all major relevant issues.
Depth, Understanding, & Insight	Lack of understanding, or lack of insight into material.	Some understand of material.	Good overall understanding of material.	Very good overall understanding of material.	Very good overall understanding of material, with some real depth.	Excellent, deep understanding of material and its interrelationships.

Criteria	C or lower	B- (2.7-2.99)	B (3.00-3.29)	B+ (3.30-3.69)	A- (3.7-3/84	A (3.85-4.00)
Relevance & Significance	Focus is off topic or on insubstantial or secondary issues.	Some of the content is meaningful and on topic.	Most of the content is reasonably meaningful and on topic.	All content is reasonably meaningful and on-topic.	All content is meaningful and relevant to the case.	All content is exceptionally relevant and meaningful.
Persuasiveness & Clarity	Disorganized or hard to understand presentation.	Some parts of the presentation are disorganized or hard to understand.	Generally organized and clear.	Organized and persuasive presentation of ideas.	Very clear, organized, and persuasive presentation of ideas.	Exceptionally clear, organized, and persuasive presentation of ideas.
Creativity & Innovativeness	Little significant or reasonably backed creative or innovative points-of-view or ideas.	Few creative and innovative ideas or points-of-view that are reasonable and are backed by some analysis.	Good, and fairly creative ideas or points-of-view that are perceptive and are backed by good analysis.	Very good, creative, and innovative ideas or points-of-view that are perceptive.	Very good, creative, and innovative ideas or points-of-view that are perceptive and are backed by strong analysis.	Outstanding, creative, and innovative ideas or points-of-view that are perceptive and are backed by very strong analysis.
Utilization of Source Materials	No useful references, or weak references with incorrect details or applicability.	Some use of source material and/or some details or applicability is incorrect.	References indicate research.	Good references applied usefully.	References indicate strong research used well.	References indicate exceptional researched used persuasively.

Discussions

Graded Discussions - you will participate in discussions that will be graded using the A = 4.0, B = 3.0, etc. scale described above. Each week's discussions are to concern only the online notes or the textbook readings. The post subject should be the relevant section, e.g, "5.9 **Real-Life Security Procedures"**

Graded discussion periods are held Day 1 of each module until 6:00 AM ET on Day 1 of the following module. You're certainly welcome to continue a discussion past the grading period, but that additional posted material will not affect your discussion grade. The discussion grading rubric below is the guide we use to evaluate your discussion contributions.

Criteria	Description
Relevance	This criterion is designed to keep you focused. It concerns the degree to which your postings are relevant to the week's material. Meaningful questions about material in the notes or the book may qualify also. (This should be an easy way for you to keep your discussion grade in reasonable territory.)
Degree of substance	This assesses the management or technical content of your posts, taken as a whole. This is most commonly achieved by putting the content of the notes or books in your own words or by giving examples that you have come across. Meaningful questions about material in the notes or the book may qualify also. Normally, interactive posts with no management or technical content will not count against you here (e.g., we encourage you to let a fellow student know that you found a post interesting or useful).
Usefulness of your week's contributions for the rest of your group	This evaluates how useful to your fellow students the totality of your comments and questions are in the context of each week's specified focus. "A" work will result from a significant set of comments and questions that are very useful to you and to the class. This criterion encourages you to be *participatory* (e.g., by responding to good questions or points posed by others). You should have an *even rate* of substantive postings throughout the week. (Contributions posted only at the end of the week are far less useful to your classmates.) If your posts are *long*, they are less likely to be read by others, and this *reduces their usefulness*. This is the only criterion affected by quantity. For example, if you make no posts, they can't be called useful.

Proctored Final Exam

There will be a proctored Final Exam in this course. The type and nature of questions in the final exam will be very similar to your quiz questions.

Expectations

Many learning activities require sharing your assignments and opinions with you classmates. For example, you may be given a set of criteria on the basis of which to evaluate other classmates' assignments, and asked to submit the results to your facilitator by a specified day of

the week. It is, therefore, very important that you, as well as your classmates, submit your assignments on a timely basis. Timely submission by all will result in each of you being able to evaluate each other's assignments.

Delays

If, for any reason, you are unable to meet any assignment deadline, contact your Course Facilitator. All assignments must be completed. Extensions may be granted under mitigating circumstances.

Policy for the Use of Generative AI

Students should learn how to use AI text generators and other AI-based assistive resources (collectively, AI tools) to enhance rather than damage their developing abilities as writers, coders, communicators, and thinkers.

When using Generative AI in coursework, students shall:

1. Give credit to AI tools whenever used, even if only to generate ideas rather than usable text or illustrations.
2. When using AI tools on assignments, add an appendix showing (a) the entire exchange, highlighting the most relevant sections; (b) a description of precisely which AI tools were used (e.g. ChatGPT private subscription version or DALL-E free version), (c) an explanation of how the AI tools were used (e.g. to generate ideas, turns of phrase, elements of text, long stretches of text, lines of argument, pieces of evidence, maps of conceptual territory, illustrations of key concepts, etc.); (d) an account of why AI tools were used (e.g. to save time, to surmount writer's block, to stimulate thinking, to handle mounting stress, to clarify prose, to translate text, to experiment for fun, etc.).
3. Not use AI tools during in-class examinations, or assignments, unless explicitly permitted and instructed.
4. Employ AI detection tools and originality checks prior to submission, ensuring that their submitted work is not mistakenly flagged.
5. Use AI tools wisely and intelligently, aiming to deepen understanding of subject matter and to support learning.

For more details, please see the Generative AI Assistance (GAIA) policy.

Important Message on Final Exams

Dear Boston University Computer Science Online Student,

As part of our ongoing efforts to maintain the high academic standard of all Boston University programs, including our online MSCIS degree program, the Computer Science Department at Boston University's Metropolitan College requires that each of the online courses includes a proctored final examination.

By requiring proctored finals, we are ensuring the excellence and fairness of our program. The final exam is administered online.

Specific information regarding final-exam scheduling will be provided approximately two weeks into the course. This early notification is being given so that you will have enough time to plan for where you will take the final exam.

I know that you recognize the value of your Boston University degree and that you will support the efforts of the University to maintain the highest standards in our online degree program.

Thank you very much for your support with this important issue.

Regards,

Professor Lou Chitkushev, Ph.D.
Associate Dean for Academic Affairs
Boston University Metropolitan College

Academic Conduct Policy

Academic Integrity: Plagiarism is the passing off of another's words or ideas as your own, and it is a serious academic offense. Plagiarism and cheating also defeat the purpose of getting an education. Plagiarism and cheating cases will be handled in accordance with the disciplinary procedures described in the College of Arts and Sciences Academic Conduct Code. You are expected to know and abide by the code, which can be read online: Academic Conduct Code. Penalties range from failing an assignment or course (first offense) to suspension or expulsion from BU. If in doubt, cite your source. If you have any questions about academic integrity, please ask your instructor.

Incidents of academic misconduct will be reported to the Academic Conduct Committee (ACC). The ACC may suspend/expel students found guilty of misconduct.

Disability and Access Services

In accordance with University policy, every effort will be made to accommodate students with respect to speech, hearing, vision, or other disabilities. Any student who may need an accommodation for a documented disability should contact Disability and Access Services at 617-353-3658 or at access@bu.edu for review and approval of accommodation requests.

Once a student receives their accommodation letter, they must send it to their instructor and/or facilitator each semester. They must also send a copy to their Faculty & Student Support Administrator, who may need to update the course settings to ensure accommodations are in place. Accommodations cannot be implemented if the student does not send their letter.