University of Massachusetts Dartmouth
Charlton College of Business
MIS 381
Introduction to Cybersecurity

Instructor:	Shouhong Wang
Email:	swang@umassd.edu

100% Online

Course Description

Course Description:

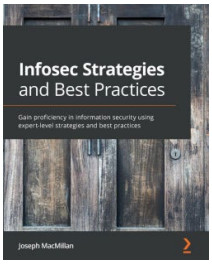
A comprehensive overview of cybersecurity issues and current best practices in several applicative domains. The course discusses emerging cybersecurity threats and available countermeasures with respect to the most recent information technologies, including access control, cryptography, and protection of wired and wireless networks and data systems. The course presents current trends and open problems in cybersecurity.

Prerequisite:

MIS 315 Information Systems, or permission.

Course Credits: 3 credits

Textbook:



Joseph MacMillan: Infosec Strategies and Best Practices, 2021, Packt, ISBN 9781800566354

(You may use the website of the ebook at a low price.)

https://www.packtpub.com/product/infosec-strategies-and-best practices/9781800566354

Course Objectives

Upon successful completion of the course, the student will

(1) understand fundamental cybersecurity principles;
(2) become familiar with practical security issues arising in a wide range of domains;
(3) understand the use of information techniques and tools to minimize security risks for organizations;
(4) be able to analyze and discuss cybersecurity related issues.

Competencies and Contact Hours

The student will be introduced to:

- Cybersecurity terms and concepts (2 hr)
- Cybersecurity categories (2 hr)
- Cybersecurity techniques (2 hr)
- Cybersecurity domains (2 hr)
- Computer networks (2 hr)
- Cybersecurity risk management (2 hr)

The student will understand:

- Access control (3 hr)
- Cybersecurity operations and administration (3 hr)
- Cybersecurity risk identification, monitoring, and analysis (3 hr)
- Cybersecurity incident response and recovery (3 hr)
- Cryptography (3 hr)
- Computer network security (3 hr)
- Systems and application security (3 hr)

The student will be able to:

- Analyze cybersecurity issues (6 hr)
- Develop cybersecurity plan for organizations (6 hr)

Communication Plan

Here are my expectations for electronic communication:

- Please use email ONLY (no voice mail on the phone) when the subject is of a personal and confidential matter. If your question is not a comment directed specifically at me, please post the question in the appropriate discussion board forum.
- I check my email daily Monday through Friday during my normal working hours. You can expect a reply from me via email within 24 hours during the work week.

You may get an email reply during the weekend, but that would be an exception not the rule.
- I will check the discussion forums daily during the work week, and make my own comments.
- It is your responsibility to meet the due times for all assignments and online tests. In an exceptional case (e.g., medical excuse) when you are unable to meet the due time, please send me an email as soon as you can to explain.

Time Considerations

Please remember that in a traditional 3 credit-house face-to-face course you would be coming to class for 3 hours and then spending an additional 3-6 hours (at least) outside of class on assignments and reading. In this 100% online course environment, you have the flexibility of self-paced learning; however, you must to commit the equivalent amount of time on your own, working on reading, thinking, and course reports in the same way as you would usually do in a face-to-face course.

Substantive Participation Should:

- Add value to the discussion and avoid simply repeating the materials of the textbook, agreeing with, or answering yes or no to peer's comments.
- Ask insightful questions.
- Answer other people's questions.
- Exemplify the point with real-life situations, when possible.
- Make comments that are relevant to the course contents and objectives.
- Use proper grammatical writing for discussions.

Ideas for Substantive Participation Include:

- Share an experience that is related to the discussion. Comment on other participants' experiences that are related to the course.
- Give insights gained from readings that were assigned for the week. If you need more information, ask the participants a question about the week's reading.
- Relate how you have applied what you have read, learned or discussed regarding the course to your personal and professional life.
- Share another resource such as web site, links, etc. that you have used to answer other participants' questions or as you explore the topics of the course, (as it is a violation of copyright law to copy the actual page).

Methods of Instruction

This is an online course. We will apply the flipped teaching approach to this course using the following methods.

(1) You read the textbook.
(2) You then participate in online class discussions and complete the assignments. You may share learning experiences with the instructor and other classmates.
(3) Upon the completion of reading and comprehension of the textbook, you conduct a course report.

The general requirements are:

(1) Students are required to complete assignments to understand the subjects.

(2) Each student must complete a course report in order to clearly understand the concepts covered in course, and apply them to a practical scene.

Evaluation and Grading Breakdown:

● Assignments – 64 points (8 assignments, 8 points for each)
● Course report – 36 points
- Documentation (10 points)
- Scope and significance (10 points)
- Analytical skills (16 points)

(* Detailed report requirements and rubrics are exhibited in a separate section.)

● To encourage students to exchange learning experiences, online discussion for each chapter/assignment and course report might receive extra up to 1 bonus point depending on the significance of contents of your post. Please read “Substantive Participation” above. 10 discussion sessions in total. Although the number of words is not a criterion for receiving extra points, a few words with little substantial contents might not receive credit. Excellent points beyond what we learned from the teaching materials and meaningful interaction are expected.

Grading Scale:

- 95 – 100 A+
- 90 – 94 A
- 85 - 89 A-
- 80 – 84 B+
- 75 – 79 B
- 70 – 74 B-
- 65 - 69 C+
- 60 – 64 C
- 57 – 59 C-
- 54 – 56 D+
- 52 – 53 D
- 50 – 51 D-

Policy on Late Assignments and Missing Assignments:
A late assignment is acceptable only when you have a legitimate reason. A missing assignment receives no credit.

Schedule

(Schedule is subject to change in accordance with the progress.)

The due time of assignments can be flexible based on your own learning pace, but should be done no later than a couple of days after the scheduled chapter.

Unit	Topic	Assignments
Chapter 1 ()	Chapter 1, Infosec and Risk Management	Start up
Chapter 2 ()	Chapter 2, Protecting the Security of Assets	Complete Chapter 1 assignment
Chapter 3 ()	Chapter 3, Designing Secure Information Systems	Complete Chapter 2 assignment
Chapter 4 ()	Chapter 4, Designing and Protecting Network Security	Complete Chapter 3 assignment **Course report proposal**
Chapter 5 ()	Chapter 5, Controlling Access and Managing Identity	Complete Chapter 4 assignment
Chapter 6 ()	Chapter 6, Designing and Managing Security Testing Processes	Complete Chapter 5 assignment
Chapter 7 ()	Chapter 7, Owning Security Operations	Complete Chapter 6 assignment Course report preparation
Chapter 8 ()	Chapter 8, Improving the Security of Software	Complete Chapter 7 assignment
	Complete all assignments	
Course Report	**Course report**	Course report due

As the semester progresses, this syllabus will be adjusted to accommodate any unforeseen circumstances, at the discretion of the instructor when needed.

Assignments

There are 8 assignments. Please complete your assignments online on schedule.

TBA

Report Requirements

The objective of the course report is to understand the concept of cybersecurity for organizations.

You choose one of the following two themes for your course report.

Theme-A (Recommended): ***A report of cybersecurity threats and countermeasures for an organization which you are familiar with.***

If you are working for an organization, or you are familiar with an organization, this theme is ideal for this course. The instructor encourages every student to choose this theme if it is feasible. You may not use sensitive or confidential information of the organization, even not the real name or any real figures of the organization, for this course report, but use your experiences and observations to make a business case to obtain deeper understanding of cybersecurity issues beyond the textbook and classroom.

Theme-B: ***This Introductory to Cybersecurity course are useful for your career.***

While Theme-A is the recommended theme for this course because it allows you to think about cybersecurity for the really world, you are allowed to choose Theme-B if you do not have work experience, and are not particularly familiar with any organization.

Course report proposal:

Each student must submit a typed course report proposal by the deadline. The proposal should not be longer than 1 page typed - 1.5 spaced. It describes the idea of course report so that the instructor can provide feedback. The approved proposal, along with the instructor's comments (no grading), will be returned to the student with comments a day later.

Course report:

Although the number of pages is not an assessment criterion, the course report is worth 27% and needs sufficient materials. The report text is typically about 10 pages

(excluding appendices and other support material), 1.5 spaced (exclusive of the title page, diagrams, and appendices). The text must be typed.

Guidelines for major contents of report are given as follows.

Theme-A:

(1) Title page

- Title of the course report
- Student name

(2) Text

- Introduction (company's background – no confidential information)
- Overview of the information system (computer network, data system, computer devices, users, and business process) of the organization related to cybersecurity
- Overview of cybersecurity policies and procedures of the organization
- Issues of cybersecurity in the organization
- Analysis of the issues and recommendations to improve cybersecurity for the organization.

(3) Appendices, if any

Theme-B:

The contents of a course report with this theme could be diversified. Topics could include the following.

- The most exciting part of this course that encourages you to learn more about it in the future.
- Research into 3 interesting issues / topics related to cybersecurity beyond what you have learned from the textbook and assignments.

To make good contents, you may conduct research work to search the literature and the Internet (ABI/INFORM Global in the Library online databases http://library.umassd.edu/find/articles-databases , Google Scholar, and other web sites) to generate good findings and support your career plan.

A guideline for the organization of report with this theme is given as follows.

(1) Title page

- Title of the course report
- Student name

(2) Text
● Introduction (overview of your topics)
● Report body
(The structure depends on your topics of your report, but you must organize the report body in sections.)
- First section
. . . .
- Last section
● Conclusion
● References if any (such as web sites, other articles…)

Format of Citations and References

1. For papers in journals and magazines:

Citation in text:

Data mining can be beneficial for the knowledge management by sharing common understanding of the context of business intelligence among the data miners (Wang and Wang, 2008).

Reference:

Wang, H. and Wang, S., A knowledge management approach to data mining process for business intelligence, *Industrial Management & Data Systems*, 108(5), 2008, 622-634.

2. For Web sites:

Citation in text:

Since the Internet became the e-commerce media, online auctions are virtually adopted for all kinds of commodities ranging from low-price books to expensive real estate (eBay, 2021).

Reference:

eBay (2021). eBay Home Page, <http://www.ebay.com>, [accessed April 8, 2021].

Rubrics

Rubrics for Course Report

	Learning Outcomes of Course Report	Performance Poor Excellent 0 100
Scope and Significance (25%)	° Clearly defined objectives of the report ° Excellent report scope/scale	
Analytical Skills (60%)	° Excellent understanding and analysis of cybersecurity issues ° Excellent understanding of cybersecurity techniques ° Excellent recommendations/suggestions/conclusion	
Written Documentation (15%)	° Excellent documentation organization ° Complete support materials	

Attendance Policy

Attendance:
This is a pure online course. The quality and frequency of class discussions are counted as the attendance.

Center for Access and Success

In accordance with University policy, if you have a documented disability and require accommodations to obtain equal access in this course, please meet with the instructor at the beginning of the semester and provide the appropriate paperwork from the Center for Access and Success. The necessary paperwork is obtained when you bring proper documentation to the Center.

University Academic Policies

The policies regarding incompletes, student conduct, plagiarism and academic integrity, and others are available in the student handbook on the University website - umassd.edu.

- Information on Incompletes
- Student Behavior
- Student Academic Integrity
- Definition of Credit Hour
- Course Withdrawal
- Grade Appeal
- Attendance Policy

- Academic Calendar
- Title IX and Sexual Assault/Harassment

Academic and Technical Support

Tutoring
If you have difficulty with the coursework, please reach out to me or contact the Academic Resource Center.

Technical Help
- 24/7 email, live chat, and phone support for myCourses is available at the myCourses support portal.
- Do you need help with other UMass Dartmouth technologies? Please contact CITS.