**CRN**: 53209

**Course Dates**: January 15 - May 10, 2024

**Credits**: 3

**Prerequisites**: CS 124, or ECE 120, or IS 401, or instructor approval

**Meeting Time:** Lecture: Online. In-Person: Wednesdays 5:00-6:50pm, Location: Campus Instructional Facility (CIF), Room 0036

**Instructor**:Casey W. O’Brien, Assistant Director, Cyber Defense Education and Training, Information Trust Institute

**Office**: Coordinated Science Lab (CSL) 449

**Email**: cwobrien@illinois.edu

**Phone**: 217-265-7689

**Office Hours**: By appointment only

**Overview**

This 15-week, 3 credit survey course, also known as *Introduction to Cybersecurity*, introduces the learner to the current risks and threats to an organization’s users, systems, and data, combined with structured tactics, techniques, and procedures (TTPs) for addressing the safeguarding of these critical assets. The course also provides a foundation for those new to cybersecurity by delivering the broad-based knowledge and skills necessary to prepare students for further study in other specialized cybersecurity courses/fields/domains.

**Course Topics**

This course will provide an overview of core concepts that are part of the following topics:

* Module 1: Defining Cybersecurity
* Module 2: Threats, Attacks, and Vulnerabilities
* Module 3: Governance, Risk, and Compliance (GRC)
* Module 4: Identity and Access Management (IdAM)
* Module 5: Physical Security
* Module 6: Cryptography and Public Key Infrastructure (PKI)
* Module 7: Security Engineering
* Module 8: Security Testing
* Module 9: Security Operations

**Expected Course Outcomes**

Upon completion of this course, students will be able to:

* Understand the nature and consequences of vectors of disruption in cyber-social systems. Describe why information security is essential in today’s enterprise environments.
* Determine an example organization’s threat model.
* Identify the elements that make up an organizational security policy. Describe the measures needed to implement and enforce it.
* Recognize how an enterprise infrastructure is monitored.
* Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance.
* Identify common attacks and describe how to safeguard against them.
* Develop an information security program for a fictitious company, leveraging cybersecurity frameworks and standard operating procedures.
* Implement Asymmetric and Symmetric cryptography and hashing.
* Indicate how systems and services can be hardened.

**Learning Resources**

* All required material (e.g., narrated video lectures, readings, and labs) will be provided to students, as per the tentative schedule below.
* Campus resources (e.g., library, counseling, advising) provided as currently to online students.
* Lab Environment: The course leverages an online, hands-on lab environment. It is used to deliver the software and related tools/files, which are necessary components to not only completing the lab assignments, but also to help the learner develop their knowledge and skills.

**Assignments**

The course’s instructional content will be made available via **Canvas**, a web-based Learning Management System (LMS), that allows institutions to manage digital learning, educators to create and present online learning materials and assess student learning, and students to engage in courses and receive feedback about skill development and learning achievement. Course site:

**https://canvas.illinois.edu**

Each week’s Module may contain the following (not all weeks have the same assignments):

* Learning objectives for that week’s Module.
* A Checklist with that Module’s assignments.
* Discussion topic.
* Video(s).
* Required and supplemental (optional) reading material.
* Hands-on lab assignment(s).
* Extra credit assignment.
* Quiz.
* List of concepts.
* Links to supplemental materials.

**9 Quizzes (180 total points)**

Tech-related courses (and the related fields in general) are full of jargon and acronyms; you must learn this language if you are to be successful in this class, or the field in general. There is no shortcut around this. However, instead of memorizing and regurgitating facts that can be easily looked up, you will create the Module 1-9 quizzes. The quiz questions (10 total per Module) should be a combination of multiple-choice, true/false, and fill in the blank. These questions are to be generated from each Module’s list of concepts (at the end of each Module). You are allowed to use any resource at your disposal to create these questions. Each submitted quiz is 20 points each. See the Quiz Assignment in each Canvas Module for more on this.

**9 Discussions (180 total points)**

You will be required to participate in weekly, online discussions using the Discussions feature in Canvas.

Each “posting” helps you analyze one aspect of the methodological, theoretical, or disciplinary perspective based on that week’s topic, or a set of related core concepts, and respond to at least one others’ post. You are encouraged to use any resource at your disposal to complete these assignments. If you do use external resources (e.g., websites, textbooks, ChatGPT, etc.), be sure to cite your sources using the APA 7th edition format. Also, feel free to include curated media elements (e.g., videos, infographics, images, attached documents, etc.). Each post is 20 points each.

**Lab Assignments (TBD total points)**

The hands-on lab assignments are web-based and designed to reinforce the concepts covered in the reading material, as well as to help you develop your knowledge and skills. For more information, see *Module 0: Getting Started > Assignment: Purchasing & Redeeming Your Infosec Learning Platform Access Code* and *Assignment: Getting Started in the Infosec Learning Platform* in Canvas.

Lab assignment due dates are listed in each week’s Module. If you need additional time to complete a lab assignment, you must contact me by email prior to, or on the day the lab assignment is due. *Failure to contact me by the posted date will result in an automatic 20%-point deduction from that week’s lab assignment score*.

Extra credit assignments may be given during the semester. Students should do the extra credit, which is fun and designed to be challenging.

**Grading Summary**

Grades are assigned based on the grading policy stated in this syllabus, as follows:

|  |  |  |
| --- | --- | --- |
| **Assignments** | **Points Possible for Each Activity** | **Total Points Possible** |
| **Quizzes** | **20 points each (x9)** | **180** |
| **Discussions** | **20 points each (x9)** | **180** |
| **Lab Assignments** | **25 points each (x TBD)** | **TBD** |
| **Extra Credit** | **TBD** | **TBD** |
|  | **Total >>** | **TBD** |

**Grading Policy**

A+ = 100 - 96%

A = 95 - 93%

A- = 92 - 90%

B+ = 89 - 87%

B = 86 - 83%

B- = 82 - 80%

C+ = 79 - 77%

C = 76 - 73%

C- = 72 - 70%

D+ = 69 - 67%

D = 66 - 63%

D- = 62 - 60%

F = Below 60%

**Course Policies**

* Late assignments: 20% penalty per week.
* Attendance: In person synchronous classes.
* ChatGPT Usage Policy:
* You may not type a question into ChatGPT, exactly copy and paste its response, and turn it in as your own work.
* You can use Grammarly on any ChatGPT output once you rephrase the answer in your own words.
* You must cite any information that comes from ChatGPT in APA 7th edition. To cite ChatGPT in the APA 7th edition style, you will need to provide a reference for the source of the information you are citing. Here is an example of how you might cite:
	+ OpenAI. (n.d.). ChatGPT. Retrieved from https://openai.com/blog/chatgpt.
* If you are citing specific information or ideas from ChatGPT in the text of your assignment, you will need to provide an in-text citation. Here is an example of how you might do this:
	+ “According to OpenAI (n.d.), ChatGPT is a large language model that can generate human-like text when provided with a prompt.” Note that in APA style, you should include the author's name (in this case, OpenAI) and the year of publication if it is available. If the year is not available, you can use the abbreviation "n.d." (no date) to indicate that the year is not known.
* It is also important to provide a full reference for the source in your reference list at the end of any assignments. This will allow your readers to locate the source and verify the information you have cited. For example, References: OpenAI. (n.d.). ChatGPT. Retrieved from https://openai.com/blog/chatgpt.

**Contacting the Instructor**

The best way for students to reach the instructor is via email, who will typically respond to student emails within 24-48 hours.

**Equal Opportunity and Access**

To obtain disability-related academic adjustments and/or auxiliary aids, students with disabilities must contact the course instructor and the Disability Resources and Educational Services (DRES) as soon as possible. To contact DRES you may visit 1207 S. Oak St., Champaign, call 217-333-4603 (V/TDD), or e-mail **disability@uiuc.edu**.

To ensure that disability-related concerns are properly addressed from the beginning, students with disabilities who require assistance to participate in this class are asked to see the instructor as soon as possible.

If you need accommodations for any sort of disability, please contact the instructor.

**Wellness**

Significant stress, mood changes, excessive worry, substance/alcohol misuse or interferences in eating or sleep can have an impact on academic performance, social development, and emotional wellbeing. The University of Illinois offers a variety of confidential services including individual and group counseling, crisis intervention, psychiatric services, and specialized screenings which are covered through the Student Health Fee. If you or someone you know experiences any of the above mental health concerns above, it is strongly encouraged to contact or visit any of the University’s resources provided below. Getting help is a smart and courageous thing to do – for yourself and for those who care about you.

* Counseling Center (217) 333-3704
* McKinley Health Center (217) 333-2700
* National Suicide Prevention Lifeline (800) 273-8255
* Rosecrance Crisis Line (217) 359-4141 (available 24/7, 365 days a year)
* Anonymous Suicide Incident Referral Form: [**http://www.counselingcenter.illinois.edu/counseling/counseling-center-policies/suicide-intervention-policy**](http://www.counselingcenter.illinois.edu/counseling/counseling-center-policies/suicide-intervention-policy).

**Academic Integrity**

The Illinois Student Code should also be considered as a part of this syllabus. You should pay particular attention to Article 1, Part 4: Academic Integrity. Read the Code at the following URL: [**https://studentcode.illinois.edu**](https://studentcode.illinois.edu/).

Academic dishonesty will result in a failing grade. Every student is expected to review and abide by the Academic Integrity Policy: [**https://studentcode.illinois.edu**](https://studentcode.illinois.edu/). Please note, you are responsible for reading this policy. Ignorance is not an excuse for any academic dishonesty.

# Emergency Planning

Plan for emergency situations by reviewing the important material found at [**https://police.illinois.edu/em**](https://police.illinois.edu/em). The more prepared you are, the safer you will be.

**Tentative Schedule** (subject to change)

| **Weeks** | **Modules** | **Due Dates** |
| --- | --- | --- |
| 1-2: Jan. 15-28 | - **Module 0**: Getting Started- **Module 1**: Defining Cybersecurity | Jan. 28 |
| 3-4: Jan. 29 - Feb. 11 | - **Module 2:** Threats, Attacks, and Vulnerabilities | Feb. 11 |
| 5: Feb. 12-18 | - **Module 3:** Governance, Risk, and Compliance (GRC) | Feb. 18 |
| 6: Feb. 19-25 | - **Module 4:** Identity and Access Management (IdAM)  | Feb. 25 |
| 7: Feb. 26 - Mar. 3 | - **Module 5:** Physical Security | Mar. 3 |
| 8: Mar. 4-8 | - **Module 6:** Cryptography & Public Key Infrastructure (PKI) | Apr. 7 |
| 9: Mar. 9-17 | **NO CLASS: SPRING BREAK** |
| 10-12: Mar. 18 - Apr. 7 | - **Module 6:** Cryptography & Public Key Infrastructure (PKI) | Apr. 7 |
| 13: Apr. 8-14 | - **Module 7:** Security Engineering | Apr. 14 |
| 14: Apr. 15-21 | - **Module 8:** Security Testing | Apr. 21 |
| 15: Apr. 22 - May 1 | - **Module 9**: Security Operations | May 1 |
| May 2 | **NO CLASS: READING DAY** |
| May 3-10 | **FINALS WEEK** |
| May 11 | **GRADES DUE BY 2PM** |