

Texas Cybersecurity Clinic
Applied Cybersecurity Foundations Course
I 320 – Spring 2025 – 28170

Contact Info

Professor Francesca Lockhart

francesca.lockhart@austin.utexas.edu

Office hours: Monday 12:30-2:00 PM, Thursday 10:30-12:00 PM [by appointment only](#)

Class Meetings

Tuesdays and Thursdays from 12:30-2:00 PM in GDC 6.202

Class Overview

The Texas Cybersecurity Clinic is a two-semester sequence that first equips students with the technical and business skills of an entry-level cybersecurity analyst (semester 1) and then partners them in (supervised) teams with a Texas-based small business, public sector organization, or nonprofit to render pro bono cybersecurity services (semester 2). During the first semester, students will learn key cybersecurity defense concepts and skills, such as risk assessment, network configuration and security, access controls, responding to a cyberattack, business planning, and penetration testing. Students will also learn how to form an effective cybersecurity consulting team and communicate with organization leaders and employees about essential cybersecurity controls and functions. By the conclusion of this course, students will be prepared to work within their assigned teams to assess, design, and render a cybersecurity improvement project plan for their assigned clinic client organization next semester.

Learning Objectives

Students will:

- Learn how to assess, prioritize, and mitigate cyber risks to small organizations through readings, lectures, case studies, and simulated exercises on access and authorization controls, vulnerability management, secure configuration of networking assets, cyber incident response, and other tools and concepts commonly utilized to protect under-resourced organizations
- Understand how to project plan and communicate cybersecurity risks and solutions with organization and business leaders with no prior cybersecurity knowledge or experience
- Prepare to provide supervised hands-on cybersecurity services on a day-to-day basis to a small business, public sector organization, or nonprofit in Texas during the second semester clinic course

Grading and Assessment Methods

This course will use plus/minus grades.

Assignments submitted on Canvas (12 total) will cumulatively account for **55% of your grade**.

- The first ten assignments will be weighted equally and graded on a pass/fail basis based on completion to make up **25% of your overall grade**. Several of the first ten assignments have two assignment options (A or B). For these assignments, you may choose to complete either option A or B based on your interests and goals for growth in the field.
- Assignments #11 and #12 are the final class project and will each count for **15% of your overall grade (30% total)**. These assignments will be graded out of 100 according to the provided guidelines and rubric available on Canvas. These assignments will be due the night before and presented on the last class day, **April 24th**.

- Please note that assignments are listed below according to the dates they become available in Canvas. It is your responsibility to note the due date for each assignment and submit via Canvas on or prior to that date. Concerns about meeting the below deadlines will be considered, but only if they are communicated to the instructor **before** the assignment due date/time, not after.

There will be a midterm exam on **Thursday, February 22nd** consisting of 60 multiple-choice questions to be completed on Canvas during a class session. The midterm exam will account for **30% of your grade**.

As stated in the Cybersecurity Clinic Student Code of Conduct, regular and punctual attendance is required for you to be a successful cyber clinic team member. Therefore, class attendance and participation will count for **15% of your grade**.

Assigned Materials

Please do the readings before the assigned class date and come to class prepared to discuss and apply them. As there were no formal prerequisites for this course, the readings will cover basic cybersecurity concepts and give you the theoretical background you need to be successful on the midterm and especially in the applied clinical component of semester two.

- Assigned textbook:
 - *CompTIA Security+ Study Guide Exam SY0-701* by Mike Chapple and David Seidl: Provided in eBook format at no cost to you, courtesy of the Strauss Center. See email sent to your preferred email address or course Canvas site for your personal link to download.
- Assigned online materials:
 - [Google Cybersecurity Professional Certificate](#): Provided at no cost to you via Coursera, courtesy of Google.org.
 - Access the certificate via the email sent to your preferred email address or by using this link: <https://coursera.org/programs/texas-cyber-clinic-spring-2025-0vgxl>
 - [Tryhackme.com](#): Create a free account to complete assigned labs for Assignment 9B.
- Optional/recommended materials for additional or continuing education:
 - [Professor Messer's CompTIA SY0-701 Security+ Training Course Videos](#)
 - [AI and Cybersecurity Readings Portal](#): A collection of essential cybersecurity and AI readings compiled by Virtual Routes
 - Should you seek to attain the [CompTIA Security+](#) credential following completion of this course, please let me know so we can discuss other study and financial resources.

Accommodations

The university is committed to creating an accessible and inclusive learning environment consistent with university policy and federal and state law. Please let me know if you experience any barriers to learning so I can work with you to ensure you have equal opportunity to participate fully in this course. If you are a student with a disability, or think you may have a disability, and need accommodations please contact Disability & Access (D&A). Please refer to the D&A website for more information: <http://diversity.utexas.edu/disability>. If you are already registered with D&A, please deliver your Accommodation Letter to me as early as possible in the semester so we can discuss your approved accommodations and needs in this course.

Course Sequence, Readings, and Assignments

Subject to change at instructor's discretion. Updates will be announced in class and new versions of the syllabus will be located on the [course Canvas site](#).

Week 1

Tuesday, January 14: Syllabus Review and Clinic Policies

- **Assignment 1 (due Monday, January 20 by 11:59pm CST):** Turn in signed Code of Conduct via Canvas Assignment #1. Additionally, complete the Student Pre-Engagement Questionnaire via Canvas Quizzes.

Thursday, January 16: Foundational Cyber Policies and Agencies

- Readings (Also available to read on Canvas):
 - [PPD 41](#)
 - [EO 14028 Fact Sheet](#)
 - [National Cyber Strategy Overview](#)
 - [NSM-22 Fact Sheet](#)

Week 2

Tuesday, January 21: Cyber Attacks, Threat Actors, and Methods: The Threat to Target-Rich, Resource-Poor Organizations

- Readings:
 - Textbook chapter 2: “Exploring Cybersecurity Threats” section
 - [Lifting the world out of cybersecurity poverty](#)
- **Assignment 2A (due Monday, January 27 by 11:59pm CST):** Pick one of the following three articles ([Dallas Cyber Attack](#), [North Texas Municipal Water Authority Cyber Attack](#), [UT Health East Texas Cyber Attack](#) – also available to read on Canvas) and identify the following items for your selected case study. Submit paragraphs (2-3 sentences) describing the following via Canvas Assignment #2, and note that you may need to do some additional research:
 - Threat actor (or your best guess, if unknown)
 - Likely motivation
 - Attack type
 - Attack vector (or your best guess, if unknown)
 - Recommended mitigation to prevent this attack in the future

OR

- **Assignment 2B (due Monday, January 27 by 11:59pm CST):** Pick one of the following three articles ([Dallas Cyber Attack](#), [North Texas Municipal Water Authority Cyber Attack](#), [UT Health East Texas Cyber Attack](#) – also available to read on Canvas) and identify the following items for your selected case study. Prepare to verbally brief a summary of the case study and the following items for 1-2 minutes during class on Monday, September 9. Submit which article you chose via Canvas Assignment #2 to help Professor Lockhart prepare the briefing order.
 - Threat actor (or your best guess, if unknown)
 - Likely motivation
 - Attack type
 - Attack vector (or your best guess, if unknown)
 - Recommended mitigation to prevent this attack in the future

Thursday, January 23: Inventory Assets and Assess Risks

- Readings:

- Textbook chapter 17: “Analyzing Risk,” “Managing Risk,” and “Risk Tracking” sections
- [Global Cyber Alliance \(GCA\) Small Business Toolkit - Step 1](#)
- **Assignment 3 (due Friday, January 31 by 11:59pm CST):** Complete [Module 1 of the “Assets, Threats, and Vulnerabilities” course](#) from the Google Cybersecurity Professional Certificate; submit screenshot(s) showing completion via Canvas Assignment #3.

Week 3

Tuesday, January 28: Manage Authentication and Authorization

- Readings:
 - Textbook chapter 4
 - Textbook chapter 8: “Authentication methods” section through end
- **Assignment 4A (due Wednesday, February 5 by 11:59pm CST):** Complete the “[Authentication, authorization, and accounting](#)” section within Module 2 of the “Assets, Threats, and Vulnerabilities” course from the Google Cybersecurity Professional Certificate; submit a screenshot showing completion via Canvas Assignment #4.

OR

- **Assignment 4B (due Wednesday, February 5 by 11:59pm CST):** Use the [2FA Directory](#) to implement 2FA on five of your personal accounts that did not previously have it enabled. Submit the names of the five websites/platforms and what type of 2FA you enabled on each via Canvas Assignment #4.

Thursday, January 30: Identify and Patch Vulnerabilities

- Readings:
 - “[Flaws in the System](#)” section and “[Approaches to vulnerability scanning](#)” reading within Module 3 of the “Assets, Threats, and Vulnerabilities” course from the Google Cybersecurity Professional Certificate
 - Textbook chapter 5: “Vulnerability Management” and “Vulnerability Life Cycle” sections

Week 4

Tuesday, February 4: Automatic Updates and Encryption

- Readings:
 - Textbook chapter 7: “Goals of Cryptography” section through “Cryptographic Attacks” section

Thursday, February 6: Endpoint and Mobile Security

- Readings:
 - Textbook chapter 3
 - Textbook chapter 11: “Endpoint Security Tools” subsection within “Protecting Endpoints”
 - Textbook chapter 13: “Managing Secure Mobile Devices” section
- **Assignment 5A (due Wednesday, February 12 by 11:59pm CST):** Play the Financial Times [Ransomware Negotiation](#) simulation and submit a screenshot showing completion via Canvas Assignment #5.

OR

- **Assignment 5B (due Wednesday, February 12 by 11:59pm CST):** Complete the “[Encryption Methods](#)” section within Module 2 of the “Assets, Threats, and Vulnerabilities” course from the

Google Cybersecurity Professional Certificate; submit a screenshot showing completion via Canvas Assignment #4.

Week 5

Tuesday, February 11: Network and Wireless Security

- Readings:
 - Textbook chapter 12: beginning through “Virtual Private Networks and Remote Access” section; “Secure Protocols” section
 - Textbook chapter 13: “Building Secure Wireless Networks” section
- **Assignment 6 (due Monday, February 17 by 11:59pm CST):** Complete [Modules 1 and 2](#) of the “Connect and Protect: Networks and Network Security” course from the Google Cybersecurity Professional Certificate; submit screenshot(s) showing completion via Canvas Assignment #6.

Thursday, February 13: Network Security Devices; Email Security

- Readings:
 - Textbook chapter 12: “Network Appliances and Security Tools” section through “Network Security, Services, and Management” section
 - “[Network Hardening](#)” section within Module 4 of “Connect and Protect: Networks and Network Security” course from the Google Cybersecurity Professional Certificate
 - [DMARC, SPF, and DKIM explainer](#)
- **Assignment 7 (due Friday, February 21 by 11:59pm CST):** From the Google Cybersecurity Professional Certificate:
 - Complete [Module 3](#) of the “Play It Safe: Manage Security Risks” course
 - Complete [Module 2](#) and [Module 4](#) of the “Sound the Alarm: Detection and Response” course
 - Submit screenshot(s) showing completion via Canvas Assignment #7.

Week 6

Tuesday, February 18: Cloud Security

- Readings:
 - Textbook Chapter 10

Thursday, February 20: Cyber Threat Intelligence and Pentesting

- Readings:
 - Textbook chapter 2, “Threat Data and Intelligence” section
 - Textbook chapter 5, “Penetration Testing” section
 - “[Attacker Mindset](#)” section within Module 3 of the “Assets, Threats, and Vulnerabilities” course from the Google Cybersecurity Professional Certificate
 - “[Securing Linux](#)” section within Module 4 of the “Connect and Protect: Networks and Network Security” course from the Google Cybersecurity Professional Certificate

Week 7

Tuesday, February 25: Midterm Review Session

Thursday, February 27: Midterm Exam: 60 question multiple choice completed through Canvas in class; open note and book.

- Receive midterm participation grade preview – this is not factored into your final grade, but is simply intended to show you where I assess your grade at should you continue at your current participation and attendance levels.

Week 8

Tuesday, March 4: AI in Cybersecurity

- Readings:
 - [“Envisioning Cyber Futures with AI”](#) from Aspen Digital
 - Textbook chapter 6: “Automation and Orchestration” section
 - **Optional:** [“Secure, Empower, Advance: How AI Can Reverse the Defender’s Dilemma”](#) from Google

Thursday, March 6: Organizational Security Policies and Plans

- Readings:
 - [“Best practices for effective documentation”](#) section within Module 3 of “Sound the Alarm: Detection and Response” course from the Google Cybersecurity Professional Certificate
 - Textbook chapter 16: “Understanding Policy Documents”, “Personnel Management”, and “Third-Party Risk Management” sections
- **Assignment 8 (due Wednesday, March 12 by 11:59pm CST):** Utilize the provided “Assignment 8 – Nonprofit Profile” to fill out the “Assignment 8 – Sample Information Security Policy Template” for the fictional nonprofit. Note that in addition to filling in the highlighted portions of the template correctly, you may add or remove sections from the template. Submit the completed information security policy for the nonprofit via Canvas Assignment #8.

Week 9

Tuesday, March 11: Data Privacy; Governance, Risk, and Compliance

- Readings:
 - [“Information privacy: Regulations and compliance”](#) section within Module 2 of the “Assets, Threats, and Vulnerabilities” course from the Google Cybersecurity Professional Certificate
 - Textbook chapter 16, “Complying with Laws and Regulations” section
- **Assignment 9 (due Monday, March 24 by 11:59pm CST):** Turn in signed Texas Cybersecurity Clinic Data Guidance Policy via Canvas Assignment #9.

Thursday, March 13: Recognizing Cyber Threats

- Readings:
 - Textbook chapter 12: “Network Attacks” section
 - Textbook chapter 14: “Incident Response” section

Week 10

No Class – Spring Break

Week 11

Tuesday, March 25: Incident Response and Recovery

- Readings:
 - Textbook chapter 14: “Incident Response Data and Tools” section through end

- **Assignment 10 (due Monday, March 31 by 11:59pm CST):** Within the Google Cybersecurity Professional Certificate:
 - Complete “[The incident response lifecycle](#)” and “[Incident response operations](#)” sections within Module 1 of “Sound the Alarm: Detection and Response” course;
 - Complete “[Response and recovery](#)” and “[Post-incident actions](#)” sections within Module 3 of “Sound the Alarm: Detection and Response” course;
 - Submit screenshot(s) showing completion via Canvas Assignment #10.

Thursday, March 27: Selecting and Categorizing Controls

- Readings:
 - Textbook chapter 1: “Implementing Security Controls” section
 - [Recommending Security Tools](#)
 - Trusted CI Framework 16 Musts One Pager (Canvas)

Week 12

Tuesday, April 1: Creating a Cybersecurity Project Plan

- **Receive team assignments in class and via Canvas**
- Readings:
 - BBB Business Profile (Canvas)
 - BBB Project Plan and Presentation Rubric (Canvas)
- **Assignment 11 (due Wednesday, April 23 by 11:59pm CST):** Within your group, any 3 students should work together to create a 10-minute presentation identifying the top 5 risks your group identified and proposed controls to mitigate these risks for Ballot’s Bowwow Box. Prepare to present in class on Monday, December 9th, followed by 5 minutes Q&A. Only one team member needs to submit the presentation on behalf of your group via Canvas Assignment #11.
 - Include at a minimum the sections outlined in the presentation template provided on Canvas, including but not limited to:
 - Executive summary
 - Risk matrix showing top 5 risks
 - Suggested controls to address risks, including estimated cost
 - Who within your group is assigned to implement each control
 - Who within the company will need to assist with install/configuration/long-term management of each control
 - Timeline/schedule for implementation

AND

- **Assignment 12 (due Wednesday, April 23 by 11:59pm CST):** Within your group, the remaining (other 3) students not developing the presentation for Assignment #11 should create a written report summarizing your group’s project plan for improving the cybersecurity of Ballot’s Bowwow Box. Only one team member needs to submit on behalf of your group via Canvas Assignment #12.
 - Include at a minimum the sections outlined in the report template provided on Canvas, including but not limited to:
 - Executive summary
 - Asset inventory
 - Risk assessment methodology and results (including a risk matrix showing all identified risks, not just the top 5)
 - Suggested controls to address risks, including control type, goal, and estimated cost
 - Who within your group is assigned to implement each control
 - Who within the company will need to assist with install/configuration/long-term management of each control

- Timeline/schedule for implementation
- Refer to the BBB Project Plan and Presentation Rubric provided on Canvas for grading. Groups will be graded holistically based on the scores assigned to both the presentation and the written report.

Thursday, April 3: How to Fact-Find and Communicate with Organizational Leaders

- Readings:
 - [Why Your Audience Should Care—and Act](#)
 - [How To Teach Adults](#)
 - Textbook chapter 16: “Security Awareness and Training” section

Week 13

Tuesday, April 8: Ballot’s Bowwow Box: Asset Inventory, Risk Assessment

Thursday, April 10: Ballot’s Bowwow Box: Research Controls for Risks

Week 14

Tuesday, April 15: Ballot’s Bowwow Box: Suggest Controls for Risks

Thursday, April 17: Ballot’s Bowwow Box: Task Assignments and Timeline

Week 15

Tuesday, April 22: Ballot’s Bowwow Box: Presentation and Report Work Day

Thursday, April 24: Final Project Presentations (Guests: Industry Expert Mentors)

- **Optional, but very strongly encouraged:** Stay after class for snacks and formally meeting/mingling with your assigned Industry Expert Mentors!