Course Syllabus

CS 3237

Human Dimension of Cybersecurity: People, Organizations, Societies

Fall 2026 | 3 Credits | Section A

Instructor Information

Instructors: Dr. Ryan Shandler Dr. Michael Bailey

Emails: rshandler@gatech.edu mbailey@gatech.edu

General Course Information

Description

This course examines the human dimension of cybersecurity as a core component of modern computing systems. Moving beyond purely technical defenses, students will analyze how human behavior shapes vulnerabilities, threat models, and security outcomes. The course introduces adversarial thinking as a foundational skill, enabling students to evaluate systems from the perspective of attackers and defenders alike. Through topics such as cognitive biases, trust, and decision-making under uncertainty, students will learn how human factors influence security failures, from phishing attacks and social engineering to insider threats and misuse of digital platforms.

Building on this foundation, the course situates individuals within broader cybersecurity ecosystems, including organizations, online communities, and state actors. Students will examine how different threat actors --- such as cybercriminal groups, ransomware organizations, and nation-states --- leverage human behavior to achieve their objectives. At the same time, the course explores how institutions design policies, governance frameworks, and technical controls to mitigate these risks. Case studies and challenge scenarios will expose students to real-world cybersecurity problems, including cybercrime, digital harassment, and cyberwarfare, emphasizing the interaction between technical systems and human actors.

Over the course of the semester, we will discuss theories and research associated with political science, behavioral economics, psychology, and international relations. There is no expectation that students possess background knowledge in these areas prior to the course.

Course Learning Outcomes

The course will introduce new tools and perspectives with which to understand attitudes, behaviors and choices in cyberspace. Students will recognize that combating cyberattacks requires an interdisciplinary approach combining computer science, social psychology, and behavioral science. These key cross-disciplinary concepts will help to explain vulnerabilities and resilience factors that impact users' experiences in cyberspace.

Upon successful completion of this course, students should be able to:

1. Apply adversarial thinking and threat modeling to analyze how human behavior introduces vulnerabilities into computing systems and cybersecurity environments.
2. Explain how cognitive biases, trust, and decision-making under uncertainty influence user behavior and can be exploited in cyberattacks such as phishing, social engineering, and ransomware campaigns.
3. Evaluate the motivations, capabilities, and strategies of different cyber threat actors—including cybercriminals, organizations, and nation-states—and how they leverage human factors in their operations.
4. Analyze real-world cybersecurity incidents by integrating technical, behavioral, and organizational perspectives to assess both vulnerabilities and potential mitigation strategies.
5. Communicate complex cybersecurity challenges and human-factor risks clearly and effectively to both technical and non-technical audiences.

Required Course Materials

There is no textbook for this course. All assigned readings will be available to download on Canvas or through the Georgia Tech Library.

Grading Policy:

Final grades in this course will be determined based on a combination of attendance and participation, quizzes, written work, and a final assessment. The weighting of each component is outlined below, allowing students to clearly track their progress throughout the semester.

<u>Assignments and Weighting:</u>

- Class Attendance and Participation – 15%
- End-of-Unit Quizzes (3 total) – 50%
- Reaction Paper – 15%
- Final Exam (Board Presentation) – 20%

This course follows the Georgia Tech grading scale of A–F with no plus/minus grades. A grade of C or higher is required to pass for students enrolled on a pass/fail basis.

Grading Scale:

Letter Grade	Score
A	90-100
B	80-89
C	70-79
D	60-69
F	59 and below

Final grades within 0.5 points of a letter grade threshold will be rounded up; scores below this threshold will not be rounded.

Description of Graded Components

a. **Class Attendance and Participation (15%)**
This course is conducted in person, and attendance will be taken at every class using PointSolutions. Students are expected to have the application installed on their devices. Students will receive full credit for attendance if they miss no more than three classes during the semester. Each additional absence will reduce the attendance grade by one-tenth of the total attendance score. Attendance and participation are essential components of the course, as in-class discussions and activities are central to engaging with the human dimensions of cybersecurity.

b. **End-of-Unit Quizzes (50%)**
Students will complete three quizzes throughout the semester, each designed to assess their understanding of course concepts, theories, and assigned readings. Each quiz will be administered during class time and will last 60 minutes. Quizzes are closed-book and completed using pen and paper.

Each quiz consists of three components:

- Multiple-choice questions assessing key concepts and theories.
- Short-answer questions requiring explanation and interpretation.
- Free-response questions that ask students to apply course concepts to analyze a cybersecurity case study.

The three quizzes collectively account for 50% of the final grade, with each quiz contributing an equal share. A practice quiz will be conducted prior to the first graded quiz to familiarize students with the format; this practice quiz will not count toward the final grade.

c. **Reaction Paper (15%)**
Students will complete one reaction paper during the semester analyzing a recent cybersecurity incident reported in the news. The paper will require students to apply theories and concepts from the course to interpret the incident and its broader implications. The paper should be approximately three pages in length and follow the provided template. This assignment is designed to develop students' ability to connect theoretical frameworks to real-world cybersecurity events.

d. **Final Exam: Board Presentation (20%)**
During the final exam period, students will complete a capstone assessment in the form of a simulated board presentation. In this exercise, students will assume the role of a cybersecurity executive presenting to a board of directors. Students will be expected to respond to questions about the organization's cybersecurity posture, defend threat modeling decisions, explain responses to a recent cyber incident, and recommend future investments in cybersecurity. In advance of the assessment, students will receive a detailed briefing dossier describing the organization, its threat environment, and its cybersecurity history. Additional details regarding expectations and format will be provided during the semester.

Course Policies

Attendance and/or Participation

This course will be conducted as in-person course. You are expected to attend all classes unless you have a compelling reason. Note that all medical absences should be dealt with by submitting an approved medical certificate to the Office of Student Life.

There may be occasional virtual lectures in lieu of in-person classes interspersed throughout the semester. Class announcements and information will be posted to email and Canvas. Lecture slides will be uploaded to Canvas. Lectures will not be recorded.

For each class there will be one article that is marked as required readings. Students are expected to read these articles in advance of each lecture. Successful students will refer to the weekly readings in the quizzes and reaction papers.

Academic Integrity

Georgia Tech aims to cultivate a community based on trust, academic integrity, and honor. Students are expected to act according to the highest ethical standards. Review Georgia Tech's Honor Code and the student Code of Conduct.

Any student suspected of cheating or plagiarism on a quiz, exam, or assignment will be reported to the Office of Student Integrity, who will investigate the incident and identify the appropriate penalty for violations.

Core IMPACTS

Core IMPACTS is the University System of Georgia's General Education curriculum. If you are teaching a course that counts towards Core IMPACTS, you should include a syllabus statement about the Core area and associated career competencies. This resource developed by the Center for Excellence in Teaching and Learning and Online Education at Georgia State University includes template syllabus statements for each of the Core IMPACTS areas that you may adapt for your course.

Accommodations for Students with Disabilities

If you are a student with learning needs that require special accommodation, contact the Office of Disability Services (404-894-2563) as soon as possible to make an appointment to discuss your special needs and to obtain an accommodations letter. Please also e-mail me as soon as possible in order to set up a time to discuss your learning needs.

Student-Faculty Expectations Agreement

At Georgia Tech, we believe that it is important to strive for an atmosphere of mutual respect, acknowledgement, and responsibility between faculty members and the student body. The Student-Faculty Expectations articulate some basic expectations that you can have of me and that I have of you. In the end, simple respect for knowledge, hard work, and cordial interactions will help build the environment we seek. Therefore, I encourage you to remain committed to the ideals of Georgia Tech while in this class.

Pre- &/or Co-Requisites

CS 1301 (or equivalent) is a prerequisite for this course.

Campus Resources for Students

Student Well-Being:

At Georgia Tech, we are concerned about your overall physical, social, and mental well-being. A comprehensive list of wellness related resources has been compiled and maintained by the Office of the Vice President for Student Engagement and Well-being (student-resource-guide (gatech.edu)