CS 151-CTV
Addressing Cyber Threats and Vulnerabilities

Department of Computer Science, Tufts University — Spring 2025
Version 2025.2 – February 2025 (Updated dates)

Tuesdays and Thursdays, 10:30AM – 11:45AM

Instructor: Laurin Weissinger, laurin.weissinger@tufts.edu

Class Times:

- Tuesday 10:30AM – 11:45AM
- Thursday 10:30AM – 11:45AM

Office Hours: Tentatively: After class, Tuesday and Thursday; Happy to arrange other times with you!

Description and Objectives:

This class is about risks to computer and information systems as well as organizations and socio-technical systems, and, crucially, how to manage them.

Computer and information security can be understood as a discipline dealing with risk to computer and information systems and the data they process. This class will cover the analysis, assessment, understanding and management of risk and its components (threat, threat actor, vulnerability, impact, likelihood) from a technical perspective as well as a managerial one:

- Understanding the concepts of threat, threat actor, vulnerability, likelihood, and impact.
- Key technical and non-technical threats, vulnerabilities and risks:
- Hardware vulnerabilities (e.g. Spectre & Meltdown) and mitigations
- Software vulnerabilities (OWASP Top 10) and mitigations
- Network and Architecture vulnerabilities and mitigations
- Threats, vulnerabilities, and risks related to physical factors, human factors, and human-computer interaction
- The real world: where resources are limited and all the above factors interact
- Risk in an organizational context
- Quantitative and qualitative methodologies (e.g. FAIR, threat modeling) to collect data on, and understand, risk and its components.
- How to decide what (and how) to fix or address vulnerabilities, threats, and risks
- How to manage threats, vulnerabilities, and risks.
- How to deal with risks, e.g. how to mitigate technical issues.

Course Requirements:

- **Attendance and Reading** – Reading and tasks are assigned on a weekly basis. Most of the readings are available on Canvas but some you will have to access on the web.

  Attendance of both class sessions is highly recommended. Not only might you miss a lecture but also group tasks. Usually, sessions will NOT be recorded; however, some classes might be recorded due to absences, inclement weather, etc. in case everyone present consents to the recording.

  Absences: If you cannot attend a class, e.g. due to illness, please let me know as soon as possible.

- **Reflections** – **Most classes will have required reading or an alternative task attached – please check the class plan**. When there is reading for a given week and a reflection paper is scheduled on the course plan, summarize your findings, thoughts, and ideas by the stipulated deadline and upload to Canvas. Usually, that deadline is Monday 23:59 Eastern Time of that week. This allows me to consider your observations, questions, and ideas during the sessions. Expected length: 400-600 words. It will be graded as ✓+, ✓, ✓–, ✘ (A, A-, B+, I).

  Reflections are due:

  - **Wednesday, 1/22** – for week 2 reading
    graded only ✓+ (if submitted on time and in expected format), ✘). Please review comments!
  - Wednesday 1/22 – for week 3 reading
  - Monday 1/27 – for week 4 reading
  - Monday 2/3 – for week 5 reading
  - Monday 3/10 – for week 10 reading
  - Monday 3/31 – for week 12 reading

- **Take-home midterm** – Take-home exam covering the essentials of risk.

  Format: Canvas-administered take-home exam, duration two hours

  Deadline: End of Week 7

  Assessment: Percentage converted to Standard letter grades.

- **Take-home Final** – Take-home exam covering the essentials of risk.

  Format: Canvas-administered take-home exam, duration two hours

  Deadline: During Exam Week

  Assessment: Percentage converted to Standard letter grades.

- **Class Project (in groups)**

  Risk management is an active process that involves understanding technology, but also an organization, its risk profile, pertinent threats, threat actors, possible risk scenarios, their possible impact, and so on. When such understanding is achieved, choices have to be made, considering risks and the organization.

  To capture this process, this class will involve a multi-step project aiming to simulate such a process, tracking both the contents of the sessions as well as the steps involved in managing risk.

  This project will be broken down into multiple, separate pieces that must be submitted. The first submissions will be graded as ✓+, ✓, ✓–, ✘ (A, A-, B+, I), with the possibility to resubmit once and improve

the grade after a round of comments. This is to ensure that all groups can establish an appropriate basis for their later work.

The Presentation and Final Submission will be graded with standard letter grades and will not allow for re-submission. However, as many documents will be submitted during the class and receive feedback, all groups should be well prepared for these two submissions.

Submissions:

See the Class Schedule for exact dates!

1. Creating a fictional organization
   – Canvas Submission, 2/13 23:59. ✓+, ✓, ✓–, ✘
2. Establishing the organizational strategy and aims.
   – Canvas Submission, 2/21 23:59. ✓+, ✓, ✓–, ✘
3. Establishing the organization's risk context or profile
   – Canvas Submission, 3/7 23:59. ✓+, ✓, ✓–, ✘
4. Creating risk scenarios
   OR
   Threat modeling a key product or system
   – Canvas Submission, 3/28 23:59. ✓+, ✓, ✓–, ✘)
5. Creating a risk register and deciding what to tackle and how
   – Canvas Submission, 4/11 23:59. ✓+, ✓, ✓–, ✘
6. Presenting an overview of organization and how you are managing pertinent risk
   – Class Presentations 4/15 & 4/17, Standard Letter Grades
7. Final Submission of your approach to managing risk
   – Canvas Submission, 5/2 23:59. Standard Letter Grades

Grading

– Reading Reflections (20%)
– Mid-Term (20%)
– Final (20%)
– Risk Project (40%) – Presentation: 10%, Final Submission: 20%, Term submissions: 10%.

Class Schedule

A detailed class schedule including relevant deadlines and readings is available on Canvas and may be updated regularly. Always check Canvas for the latest version.