

# Georgia Institute of Technology

## Course Syllabus: Enterprise Cybersecurity Management

### Instructor Information

<b>Professor</b> Jerry Perullo	<b>Email:</b> perullo at gatech dot edu <b>LinkedIn</b> (student connections welcome and encouraged): <a href="https://www.linkedin.com/in/perullo/">https://www.linkedin.com/in/perullo/</a>
<b>Instructor Office Hours</b> on request	<b>Teaching Assistants and Office Hours</b> see Canvas

### General Course Information

#### Description

This course is intended for students with an interest in designing and leading cybersecurity organizations or operating in functions that need to work closely with security teams. Beginning with a focus on strategy and guiding principles, the course then moves into organizational structure and specific roles and duties required to address the cybersecurity needs of different organizations. Core concepts of risk management are introduced and used to frame modules on cyber risk management and oversight. Finally, cyber risk governance is studied with a focus on both internal oversight structures and Board-level interaction.

#### Pre- &/or Co-Requisites

None

#### Course Level Objectives

Upon successful completion of the course, you will be able to:

1. Identify the key components of an Enterprise Cybersecurity Strategy.
2. Identify Threat Objectives and map recent cybersecurity events to the corresponding adversary objective.
3. Propose an organizational model for an information security department.
4. Describe the core components of a Cybersecurity Incident Response Procedure (CIRP).
5. Summarize key aspects of a cybersecurity architecture strategy.
6. Identify the core components of a Risk Assessment Management Procedure (RAMP).
7. Recognize the components of prevailing cybersecurity legislation and regulation.
8. Identify key methodologies and outcomes for successful application security assessment and red team testing.
9. Propose an internal governance structure for an enterprise security program.
10. Identify the top goals and outcomes for Board-level cybersecurity oversight.

#### Format

This course may be offered via the online masters (OMS) program or on-campus in person.

### **OMS specific Considerations**

OMS sections of this course use pre-recorded video lectures professionally recorded in Fall 2022. Occasional written or recorded supplemental material is included in the course to clarify or extend the original topics or add references to current events. Further, an interactive chat is used to facilitate ongoing discussions of current events and application of the course material.

### **In-person specific Considerations**

In-person sections of this course are delivered via live in-person lectures on the Georgia Tech campus. In-person classes include an undergraduate section with the same material and expectations with the exception of case studies, which are only required for students in the graduate-level section. Where unavoidable circumstances prohibit an in-person class, a lecture may be delivered via a live or recorded online video format. Further, efforts will be made to record in-person lectures for later review and studying, but this will be on a best-effort basis and should not be relied upon.

### **Course Text**

There are no required works to purchase for this course. All required learning materials will be linked in the modules or freely available.

## **Course Requirements, Assignments & Grading**

### **Assignment Distribution and Grading Scale**

<b>Discussion</b>	10%
<b>Exams (3 total)</b>	45% (15% each)
<b>Final Exam</b>	25%
<b>Assignments (2 Case Studies)</b> **Masters/OMS sections only - undergraduate students scale other graded components to 100%	20% (10% each)

### **Grading Scale**

Your final grade will be assigned the highest letter grade according to the following scale:

- A >=90%
- B >=80%
- C >=70%
- D >=60%
- F

Grades will not be rounded up (e.g., 89.999 = B).

## Description of Graded Components

### Participation:

You are expected to demonstrate class participation in each of the 4 class modules. You may do so by submitting evidence of which of the following way/s you participated **for each module**:

- A brief but meaningful submission or comment within the module discussion in Canvas or module channel in Slack. Sincerity is prized over length - even a single sentence reply is completely adequate if expressing a thought that is on-topic.

#### Examples:

Module 1: Slack: "I found the reading excerpt highly relevant, as I received a phishing attempt via my GT email last week that addressed me as "<USER>" - demonstrating it was completely opportunistic and untargeted.

Module 2: Slack: "See the attached screenshot of my contribution in the Module 1 Slack discussion"

Module 3: Slack: "The following link goes to my discussion thread in the Module 3 Slack discussion: <https://link>"

- Listing a date and topic where you attended during an in-person lecture or panel discussion related to the module and contributed a meaningful question or comment.

#### Examples:

Module 4: In-class: "On April 20 at the panel on Board presentations I submitted a question about how practices differ in healthcare versus manufacturing to the speakers"

## Examinations

Examinations are open-book/open-note and online. While examinations are timed, a more flexible window is provided in which that timer can be started. While online and class resources can be used, no other humans may be consulted during an exam. Exam material should not be discussed in class discussion forums until all grades have been released.

### Taking this course on Pass/Fail:

You may take this course on a pass/fail basis subject to Institute guidelines and restrictions. A passing mark will require the equivalent grade of a 60/100 or better.

Reference: <https://catalog.gatech.edu/policies/grading-gpa/pass-fail-system-rules/>

### Timing Policy

- The Modules follow a logical sequence that includes knowledge-building and experience-building.
- Assignments should be completed by their due dates.

- While in-person sections will have the pace of material dictated by lectures, OMS students can choose their own sequence and pace. The Canvas calendar will suggest course pacing based on what has worked best in in-person sections.

### **Grading and Feedback**

Instructors will aim to have exams graded within one week and case studies within two weeks of submission.

### **Case Study Rubric**

The following rubric will be applied when grading case studies:

- Poorly articulated, weakly supported, or missing specific deliverable: **-1 to -4 points per item**
- Violating the word length requirement (excluding references): **-5 points total**
- Grammatical errors: **-1 to -5 points total**
- Incorrect application of class concepts: **-1 to -5 points total**
- Exceptional organization, clarity, and accuracy that allows the reader to quickly grasp the context, conclusions, and subject-matter: **+1 to +5 points**

## **Technology Requirements and Skills**

### **Computer Hardware and Software**

- High-speed Internet connection
- Laptop or desktop computer with a **minimum** of a 2 GHz processor and 2 GB of RAM
- Mozilla Firefox, Chrome and/or Safari browsers

### **Technology Skills**

Reports may be submitted as text, Microsoft Word, or pdf files.

### **Canvas**

This class will use Canvas to deliver course materials to online students. To login to Canvas visit [canvas.gatech.edu](https://canvas.gatech.edu).

### **Technology Help Guidelines**

**30-Minute Rule:** When you encounter struggles with technology, give yourself 30 minutes to 'figure it out.' If you cannot, then post a message to the discussion board; your peers may have suggestions to assist you. You are also directed to contact the Helpdesk 24/7.

When posting or sending email requesting help with technology issues, whether to the Helpdesk, message board, or me use the following guidelines:

- Include a descriptive title for the subject field that includes 1) the name of course 2) the issue. Do NOT just simply type "Help" into the subject field or leave it blank.

- List the steps or describe the circumstance that preceded the technical issue or error. Include the exact wording of the error message.
- When possible, always include a screenshot(s) demonstrating the technical issue or error message.
- Also include what you have already tried to remedy the issue (rebooting, trying a different browser, etc.).

## Course Policies, Expectations & Guidelines

### Attendance and/or Participation

- **OMS**  
This is an asynchronous course. Students are expected to watch all lectures. Students are also required to participate in discussions, as detailed in the assignments section.
- **In-person**  
Lectures are delivered synchronously, and attendance will dramatically improve the likelihood of success in the class.

### Extensions, Late Assignments, & Re-Scheduled/Missed Exams

- The window for submission assignments will remain open for three days after the due date.
- 0.5 points (out of 100) will be deducted for each hour a submission is late
- Exceptions to turn in assignments or exams after the three-day late period (or within it for no penalty) will be given for official Institute approved absences. Approval must be issued by the Registrar's office via the process documented at:  
<https://registrar.gatech.edu/info/forms-list-absences>

### 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. See [Student-Faculty Expectations](#) for an articulation of 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.

### Subject to Change Statement

The syllabus and course schedule may be subject to change. Changes will be communicated via email and/or Canvas announcements . It is the responsibility of students to check email messages and course announcements to stay current in their online courses.

### Communication Policy

- Please use professional etiquette when communicating with your professors, your TAs, and your peers.
- Do NOT submit posts of a personal nature to the discussion board.

- Teaching Assistants will hold office hours, generally via Zoom.
- For questions related to technology, please contact: [Digital Learning Support](#).

### **Online Student Conduct and (N)etiquette**

Communicating appropriately in the online classroom can be challenging. In order to minimize this challenge, it is important to remember several points of “**internet etiquette**” that will smooth communication for both students and instructors:

1. *Avoid language that may come across as strong or offensive.* Language can be easily misinterpreted in written electronic communication. Review email and discussion board posts BEFORE submitting. Humor and sarcasm may be easily misinterpreted by your reader(s). Try to be as matter of fact and professional as possible.
2. *Follow the language rules of the Internet.* Do not write using all capital letters, because it will appear as shouting. Also, the use of emoticons can be helpful when used to convey nonverbal feelings.
3. *Consider the privacy of others.* Ask permission prior to giving out a classmate's email address or other information.
4. *Keep attachments small.* If it is necessary to send pictures, change the size to an acceptable 250kb or less.
5. *No inappropriate material.* Do not forward virus warnings, chain letters, jokes, etc. to classmates or instructors. The sharing of pornographic material is forbidden.

**NOTE:** *The instructor reserves the right to remove posts that are not collegial in nature and/or do not meet the Online Student Conduct and Etiquette guidelines listed above.*

### **University Use of Electronic Email**

A university-assigned student e-mail account is the official university means of communication with all students at Georgia Institute of Technology. Students are responsible for all information sent to them via their university-assigned e-mail account. If a student chooses to forward information in their university e-mail account, he or she is responsible for all information, including attachments, sent to any other e-mail account. To stay current with university information, students are expected to check their official university e-mail account and other electronic communications on a frequent and consistent basis. Recognizing that some communications may be time-critical, the university recommends that electronic communications be checked minimally twice a week.

### **Plagiarism & 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. All students enrolled at Georgia Tech, and all its campuses, are to perform their academic work according to standards set by faculty members, departments, schools and colleges of the university; and cheating and plagiarism constitute fraudulent misrepresentation for which no credit can be given and for which appropriate sanctions are warranted

and will be applied. For information on Georgia Tech's Academic Honor Code, please visit <http://www.catalog.gatech.edu/policies/honor-code/> or [Academic Honor Code](#).

Any student suspected of cheating or plagiarizing 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.

### Use of Artificial Intelligence (AI) and Generative Pre-trained Transformers (GPT)

AI GPTs can be useful as virtual discussion partners and research partners while studying or proofing writing, but they should not be used to generate substantive content expected to be created by the students. If a GPT is employed in the preparation of a written submission, it should be accompanied by a brief written section (not counting toward any word count requirement) explaining the strategy and prompts used to engage with the GPT and demonstrating student subject matter comprehension, along with commentary on efficacy of the program and adaptations that had to be made to content. GPTs are known to produce vague equivocating output that can be easy to spot in a course with such specificity to the material. Submissions of this nature are likely to score poorly whether they are written by a GPT or not. Further, University plagiarism detection software now includes capabilities to detect AI and GPT usage. While these systems are not foolproof, high scores from them will alert the Professor and TAs to study a submission more carefully for insincere content. As a rule, do not submit any content you are not prepared and willing to defend in detail.

### Accommodations for Students with Disabilities

If you are a student with learning needs that require special accommodation, contact the Office of Disability Services at (404)894-2563 or <http://disabilityservices.gatech.edu/>, 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 to set up a time to discuss your learning needs.

## Topical Outline

	Topic	Reading (expected before class)
Module 1: Strategy		
Topic 1	Strategy Composition	NIST Cybersecurity Framework (CSF) 2.0 <a href="https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf">https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf</a> <b>Mandatory:</b> Sections 1&2, Appendix A <b>Optional:</b> The rest

Topic 2	Threat Objectives	What are they after? A threat-based approach to cybersecurity risk management <a href="https://www.linkedin.com/pulse/what-after-threat-based-approach-cybersecurity-risk-jerry-perullo/">https://www.linkedin.com/pulse/what-after-threat-based-approach-cybersecurity-risk-jerry-perullo/</a>
Topic 3	Departmental Organization	Three Lines Model <a href="https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf">https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf</a> Cybersecurity in the Three Lines model <a href="https://www.linkedin.com/pulse/cybersecurity-three-lines-model-jerry-perullo/">https://www.linkedin.com/pulse/cybersecurity-three-lines-model-jerry-perullo/</a>
Topic 4	Talent Management	Bad CISO Archetypes <a href="https://www.linkedin.com/pulse/draft/AgHntK4Etj6fGgAAAX5F4o6db9_kM4aEIA-LI3bPveZAmL423wB7hCUFg_F4egU0cvmu7Zo">https://www.linkedin.com/pulse/draft/AgHntK4Etj6fGgAAAX5F4o6db9_kM4aEIA-LI3bPveZAmL423wB7hCUFg_F4egU0cvmu7Zo</a>
Topic 5	Cyber Threat Intelligence	
Module 2: Cybersecurity Operations		
Topic 6	Architecture and Automation	Log4J and egress LinkedIn post and discussion <a href="https://www.linkedin.com/posts/perullo_adversarial-cybersecurity-reality-activity-6875174587668148224-QI4C">https://www.linkedin.com/posts/perullo_adversarial-cybersecurity-reality-activity-6875174587668148224-QI4C</a>
Topic 7	Cyber Incident Response Procedures (CIRP)	Value of the True Positive <a href="https://www.linkedin.com/pulse/value-true-positive-jerry-perullo/">https://www.linkedin.com/pulse/value-true-positive-jerry-perullo/</a>
Topic 8	CIRP Examples	SEC Charges Intercontinental Exchange and Nine Affiliates Including the New York Stock Exchange With Failing to Inform the Commission of a Cyber Intrusion <a href="https://www.sec.gov/newsroom/press-releases/2024-63">https://www.sec.gov/newsroom/press-releases/2024-63</a> ; and <a href="https://www.sec.gov/files/litigation/admin/2024/34-100206.pdf">https://www.sec.gov/files/litigation/admin/2024/34-100206.pdf</a>
Module 3: Security Assurance		
Topic 9	GRC - Risk Register Management	
Topic 10	GRC – Compliance and Corporate Policy	



Topic 11	GRC - Reporting and Metrics	Briefing Your Board on Cybersecurity part 3/3: Board Committees - Metrics and Materials <a href="https://www.linkedin.com/pulse/briefing-your-board-cybersecurity-part-33-committees-jerry-perullo/">https://www.linkedin.com/pulse/briefing-your-board-cybersecurity-part-33-committees-jerry-perullo/</a>
Topic 12	Application Security	Measuring Your Application Security Program & Empowering Dev Leads - Jerry Perullo <a href="https://www.youtube.com/watch?v=ZyfsoeJ0Mrk">https://www.youtube.com/watch?v=ZyfsoeJ0Mrk</a> It's not the MFA, it's the OTP! <a href="https://www.linkedin.com/pulse/its-2fa-1tp-jerry-perullo/">https://www.linkedin.com/pulse/its-2fa-1tp-jerry-perullo/</a>
Topic 13	Red Teaming	
Module 4: Governance		
Topic 14	Internal Cyber Governance	CyberGov Charter & Handbook <a href="https://www.linkedin.com/pulse/draft/AgG0kNHppjbleAAAAX5F8CcXj1N-WzroddM2AaHbYAnaqxTn59iEL-J2Szd7yxXysvg5xCk">https://www.linkedin.com/pulse/draft/AgG0kNHppjbleAAAAX5F8CcXj1N-WzroddM2AaHbYAnaqxTn59iEL-J2Szd7yxXysvg5xCk</a>
Topic 15	External/Board Cyber Governance	Briefing Your Board on Cybersecurity Part 1/3: Corporate Governance 101 for Security Professionals <a href="https://www.linkedin.com/pulse/briefing-your-board-cybersecurity-part-13-corporate-101-jerry-perullo/">https://www.linkedin.com/pulse/briefing-your-board-cybersecurity-part-13-corporate-101-jerry-perullo/</a> Briefing Your Board on Cybersecurity part 2/3: Full Board Meetings <a href="https://www.linkedin.com/pulse/briefing-your-board-cybersecurity-part-23-full-meetings-jerry-perullo/">https://www.linkedin.com/pulse/briefing-your-board-cybersecurity-part-23-full-meetings-jerry-perullo/</a> Cybersecurity for Investor Relations and Corporate Governance <a href="https://www.linkedin.com/pulse/cybersecurity-investor-relations-corporate-governance-jerry-perullo/">https://www.linkedin.com/pulse/cybersecurity-investor-relations-corporate-governance-jerry-perullo/</a>