Georgia Institute of Technology

Course Syllabus: Information Security Strategies and Policies

(PUBP/CS/MGT 6725)

Fall 2019 Section OCY	MS in Cybersecurity, School of Public Policy, IAC
Delivery: 100% Web-Based, Asynchronous	Canvas & edX for Content Delivery
Dates: August 19 – December 8, 2019	

General Course Information

Description

This is a required core course for all tracks in the Online MS in Cybersecurity. This course introduces students to the policy and management aspects of cybersecurity. It is divided into four modules. The first involves basic concepts and definitions regarding policy, governance, and threats; the second deals with cybersecurity management and policy at the organizational level; the third deals with cybersecurity public policy at the national level; the fourth deals with cyber conflict, policy and diplomacy at the transnational level. The course situates cybersecurity in the overall Internet ecosystem.

Pre- and/or Co-Requisites

Students will be expected to have a basic understanding of computers and data networking and will learn some technical material regarding internet protocols, vulnerabilities, exploits and incident response, but the primary focus of the course is on the public policy, management and international relations aspects of cybersecurity. The course does not require programming skills, although they can be useful in some assignments. Students should be able to blend and integrate economic, technical and political modes of analysis. This course is best taken in conjunction with CS 6035 (Introduction to Information Security) for an introduction to the more technical aspects of cybersecurity.

Course Goals and Learning Outcomes

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

1. Recognize the different governance structures used to promote cybersecurity
2. Identify key cybersecurity policy frameworks and standards (e.g., NIST framework)
3. Write a cybersecurity policy for an organization
4. Analyze and assess the effects of existing and proposed cybersecurity laws and regulations
5. Identify the geopolitical dimension of cyber conflict
6. Recognize the intersections of cybersecurity governance with the governance, standards and operations of the Internet

Course Materials

Due to the dynamic nature of our subject matter, no single book exists that meets all course requirements. Each topical area has one or two required readings, which are listed in the course schedule under the “Readings” column. All required readings are available as pdfs or via the Georgia Tech library. Doing the readings is very important and forms a significant portion of your grade. Quizzes assess your comprehension of the readings. Additional recommended or supplemental materials may be posted in the Canvas site in response to relevant ongoing events in cybersecurity.

Georgia Institute of Technology

Course Syllabus: Information Security Strategies and Policies (PUBP/CS/MGT 6725)

Course Website and Other Classroom Management Tools

This class will use Canvas and edX to deliver course materials to online students. ALL course materials and activities will take place on these two platforms. In order to login to Canvas and edX…

Assignment Distribution and Grading Scale

Here is a list of the assignments and activities required in the course. Grading is not "curved;" students will be graded based on how well they have met the requirements of the assignment and accomplished specific learning objectives. With the exception of quizzes, most assignments will have a rubric associated with them so that students can see what criteria are used for grading and what weight is given to them.

Assignment	Release Date	Due Date	Weight
Go Phish (team assignment) Assignment #1	September 2	September 17	15%
Developing an organizational policy (team assignment) Assignment #2	September 18	October 9	25%
Legislative challenge Assignment #3	October 10	October 31	20%
Term paper applying diamond model (individual) Assignment #4	November 4	December 8	25%
Quizzes on lectures and readings (7 total)	Semi-weekly	Semi-weekly	15%

Assignment Submission and Due Dates

All assignments will be due at the times listed above. These times are specified in UTC and are subject to minor changes so please check Canvas. To convert from UTC to your local time zone, use a Time Zone Converter. Each assignment will have a separate entry in Canvas that explains in more detail what is expected and what criteria are used to grade it. The weighting of the different assignments in determining your final grade is clear from the table above. Most assignments will be finalized by the student uploading a file in the relevant assignment place in Canvas. Do not send assignments directly to the professors or TA's via email. All assignments must be submitted within Canvas, otherwise they cannot be graded properly and do not count towards the grade. If there are technical issues, please notify the help desk, as well as each professor immediately. Assignments should be graded with feedback within one week of when learners turn it in.

Quizzes

Quizzes become available for a week before they are due and also have a due date, but your answers are recorded and graded as you enter them. They remain available for three days past the due date – after that they become unavailable. If you fail to take a quiz before it disappears you lose the points. Quizzes are individual assignments – they are intended to provide an incentive to study the readings and strengthen your recall and understanding of the reading and lecture material. We strongly discourage students from helping other individuals to answer the quiz questions.

Late assignments, Missed Quizzes, Re-scheduling

The major assignments are due before midnight on the due date. There is a very simple policy governing late assignments: for every day it is late, you lose two percentage points off what your score would have been. This policy will be applied regardless of the reason for your lateness; it doesn't matter whether you just forgot, your day job intervened, you had family problems, etc. The only special circumstances that will be accommodated are those that literally incapacitate the student for a significant period of time, such as injury and hospitalization, floods, hurricanes, power outages for several days, etc. Please do not waste the instructors' time asking for extensions for any other reasons.

Peer evaluations

Near the end of the semester students will fill out a peer evaluation form to assess how each group member contributed to the group projects. This allows group members to praise their peer for their contribution, to identify "free riders" who did not contribute, or to identify and explain problems with group coordination or behavior that affected the quality or timeliness of the project.

Grading Scale

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

A	90-100%
B	80-89%
C	70-79%
D	60-69%
F	0-59%

Technology Requirements and Skills

To participate in this class, you need the following computer hardware and software:

- Broadband Internet connection
- Laptop or desktop computer with a **minimum** of a 2 GHz processor and 2 GB of RAM
- Windows for PC computers or Mac iOS for Apple computers.
- Complete Microsoft Office Suite or comparable applications and ability to use Adobe PDF software (install, download, open and convert)
- Mozilla Firefox, Chrome and/or Safari browsers

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 the professor use the following guidelines:

- Include a descriptive title for the subject field that includes 1) the name of course 2) the issue.
- List the steps or describe the circumstance that preceded the technical issue or error. Include the exact wording of the error message.
- When possible, include a screenshot(s) demonstrating the technical issue or error message.
- Also include what you have done to try to remedy the issue (rebooting, trying a different browser, etc.).

Communication Policy

Email personal concerns, including grading questions, to the professor privately using the Canvas platform’s messaging. Do NOT submit posts of a personal nature to the discussion board.

Email will be checked at least twice per day Monday through Friday. On Saturday, email is checked once per day. During the week, I will respond to all emails within 24 hours; on weekends and holidays, allow up to 48 hours. If there are special circumstances that will delay my response, I will make an announcement to the class.

Student Forum/Q&A discussion boards will be checked twice per day Monday through Friday; Saturday, these discussion boards will be checked once per day.

Virtual office hours will be held using the Bluejeans. I will hold Virtual Office Hours every [day, time], as well as special office hours for dedicated topics, such as a large, upcoming assignment. Special topic hours will be announced in advance. I am also happy to schedule one-on-one office hours in person, via... For questions related to technology, please contact:...

Online Student Conduct and Netiquette

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:

Read first, Write later. Read the ENTIRE set of posts/comments on a discussion board before posting your reply, in order to prevent repeating commentary or asking questions that have already been answered.

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.

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.

Consider the privacy of others. Ask permission prior to giving out a classmate's email address or other personally identifiable information.

Keep attachments small. Avoid gigantic files; if it is necessary to send pictures, minimize the size.

No inappropriate material. Do not forward virus warnings, chain letters, jokes, porn, etc. to classmates or instructors. 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 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 http://www.catalog.gatech.edu/rules/18/.

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.

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 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 students. See the GT catalogue for an articulation of some basic expectation that you can have of me and that I have of you. In the end, respect for knowledge, hard work, and cordial interactions will help build the environment we seek. 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 the Canvas announcement tool and/edX bulk email and or the class Piazza discussion forum. It is the responsibility of students to stay current.

Course Schedule

Module 1: The Basics

Week/Dates	Topic	Deliverables	Readings
Week 1 **Aug 19-25**	**Topic 1: Cyberspace and the societal "layers,"** Lessons 1 – 2	Engage with discussion question 1	Institutional Landscape of Cybersecurity, by Kuerbis and Badii (2017)
Week 2 **Aug 26-Sept 1**	**Topic 2: Cybersecurity governance,** Lessons 1 – 4	Quiz 1 on readings and lessons	Economics of Cybersecurity, by Asghari, van Eeten and Bauer (2016)
Week 3 **Sept 2-8**	**Topic 3: Concepts and Vocabulary,** Lessons 1 – 3	Go Phish assignment begins Engage with discussion question 2	The Diamond Model of Intrusion Analysis, by S. Caltagirone et al (2013)

Module 2: Cybersecurity in the Organization

Week/Dates	Topic	Deliverables	Readings

Week 4 **Sept 9-15**	**Topic 4: Understanding the risks,** Lessons 1 – 3	Quiz 2 on readings and lectures	Ross Anderson, Chris Barton et al. Measuring the Changing Cost of Cybercrime. *Workshop on the Economics of Information Security*, 2019 Examining the cost and causes of cyber incidents, by S. Romanosky (2016).
Week 5 **Sept 16-22**	**Topic 5: Organizational security policies** Lessons 1 – 4	Go Phish assignment due Begin Assignment 2	Measuring Risk: Computer Security Metrics, Automation and Learning, by R. Slayton. *(*2015)
Week 6 **Sept 23-29**	**Topic 5: Organizational security policies,** Lessons 5 – 7	Quiz 3 on readings and lessons.	NIST Cybersecurity Framework, pp. 24 – 45 Link to NIST Cybersecurity Framework
Week 7 **Sept 30-Oct 6**	**Topic 6: Industry self-regulatory efforts,** Lessons 1 – 6		Berkowsky, J.A. and Hayajneh, T., Security issues with certificate authorities. (2018). T. Chung et al, A Longitudinal, End-to-End View of the DNSSEC Ecosystem (2017). Asghari, et al, Post-Mortem of a Zombie: Conficker Cleanup After Six Years (2015).

Module 3: Cybersecurity policy at the national level

Week/Dates	Topic	Deliverables	Readings
Week 8 **Oct 7-13**	Topic 7: US laws and policies, Lessons 1 – 6	Quiz 4 on readings and lectures Assignment 2 due Begin Assignment 3 Legislative Challenge	Survey of US Laws
Week 9 **Oct 14-20**	Topic 8: Protecting government networks, Lessons 1 – 2	Legislative Challenge Part 1: Discussion and debate	Harknett and Stever, The New Policy World of Cybersecurity (2011)
Week 10 **Oct 21-27**	Discussion and debate of proposed legislation	Quiz 5 on readings and lectures Legislative Challenge Part 2: Deadline for amendments Oct 27	
Week 11 **Oct 28-Nov 3**	Topic 9: Critical infrastructure	Final votes due on legislative challenge	Securing North American critical infrastructure: by Shackelford et al (2016)

Module 4: Cybersecurity and International Relations

Week/Dates	Topic	Deliverables	Readings

Week 12 **Nov 4-10**	Topic 10: Cyberspace and inter-state conflict Topic 10, Lessons 1 – 5	Quiz 6 on readings and lectures Begin Final Term Paper (due Dec 8)	Buchanan, Chapter 1 in The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations (2017). US Cyber Command, "Achieve and Maintain Cyberspace Superiority"
Week 13 **Nov 11-17**	Topic 11: International Norms and Treaties Topic 11, Lessons 1 – 3		What the Cloud Act means for privacy pros, by Peter Swire and Jennifer Daskal, (2018) https://iapp.org/news/a/what-the-cloud-act-means-for-privacy-pros/
Week 14 **Nov 18-24**	Topic 12: Global Internet Governance Topic 12, Lessons 1 – 5	Quiz 7 on readings and lectures	Sovereignty in Cyberspace: Governance for a non-territorial domain, by Milton Mueller
Week 15 **Nov 25-Dec 5**		Engage with discussion question 3 (TBD)	Holiday break Nov 27-28 (Thanksgiving)
Week 16 **Dec 8**		Final paper due	