SYLLABUS

L589: Cybersecurity Risk Management Capstone
&
B655: Information Privacy and Cybersecurity Management Practicum

Indiana University
Spring 2021
Professor Scott Shackelford

The course is run according to the terms in the syllabus, which is intended to let students know what they can expect and what is expected of them in the course. Students who remain in the course are presumed to understand and accept the terms in the syllabus; those who object should drop the course.

HOW TO CONTACT PROFESSOR SHACKELFORD

Office: CG2000 (Kelley School of Business), Office #206 (Ostrom Workshop, 513 Park Ave.),
Email: sjshacke@indiana.edu
Office Phone: (812) 856-6728
Mobile: (812) 369-1612

OFFICE HOURS

Mondays, 11:00AM-12:00PM. You do not need an appointment to come in during office hours. If these hours aren't convenient for you, I'll be glad to meet with you at another mutually convenient time. To set up an appointment, see me before or after class or contact me by email or phone.

SYLLABUS QUICK REFERENCE

COURSE DESCRIPTION & LEARNING OUTCOMES

Enhancing cybersecurity and protecting privacy are critical issues impacting all of us, and are forces increasingly shaping the competitiveness of firms and the security of governments. This course takes an interdisciplinary, global, and hands-on approach to introduce students to the practice of privacy and cybersecurity law and policy. Specifically, this course focuses on the management of information privacy and security within organizations. While it includes key legal issues in these fields—including U.S. and international cyber law and policy—it is more concerned with the challenges of addressing those issues effectively within public- and private-sector institutions. Those challenges include, for example, managing compliance across multinational organizations, best practices for mitigating cyber risk, communicating effectively with executive leadership, motivating employees while managing insider threats, responding to data breaches and government investigations, and thinking strategically about how best to conduct cybersecurity due diligence in a given transaction or venture. Ultimately, we will analyze regulatory solutions as part of a larger universe of reforms needed to enhance cybersecurity and safeguard both intellectual property and civil rights, while applying the skills you have gained throughout your academic program for a real-world client.

The primary aim of the course is to provide students with a better understanding of how privacy and cybersecurity law and policy is applied in United States, but put in a global perspective. To do this, the course is broken into two primary components. The first component takes the form of a deep dive into a handful of important, current privacy and security controversies in the United States and Europe as a vehicle for examining broad, crosscutting themes. To that end, the first component of the course will be taught primarily through case studies and interaction with current senior privacy and security officers within industry and government. It is designed to help prepare students for employment as privacy and security officers, for jobs as attorneys advising these people, and for any position that requires working within large organizations. The second component of this course takes the form of the capstone project for an actual client for which students will be broken into teams to undertake a cybersecurity assessment. The learning outcomes for this course are listed below, and are mapped on to the Cybersecurity Program Learning Goals that may be found in Appendix C.

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

1. Understand the processes and mechanisms by which privacy and cybersecurity laws are made, amended, interpreted, and most importantly applied in the United States and beyond (4);
2. Identify significant concepts related to both privacy and cybersecurity risk management of interest to managers and policymakers (1, 2);
3. Increase your awareness and sensitivity to the legal, ethical, and business implications of cybersecurity and privacy decisions, as well as the contours and implications of cybersecurity market failures (5);

4. Strengthen your critical thinking, logical reasoning, and problem-solving skills through applied service-learning (3);
5. Develop the confidence necessary to work collaboratively on an interdisciplinary cybersecurity and privacy project, and be a more robust contributor to the marketplace, our civil society, and the common good (2, 6).

TIME COMMITMENT

This three-credit course is designed to integrate lessons learned throughout the M.S. in Cybersecurity Risk Management program through applied service-learning work with a real-world client. As such, this course requires significant time and effort. It is designed to challenge students to adopt the work ethic necessary to excel in future academic and professional settings. To help facilitate that purpose, you can expect that I will do my best to: present subject matter that is mentally challenging as clearly as possible and by using frequent examples, be fair and impartial in dealing with students, create an environment in which you should feel free to ask questions and express opinions, assign grades that reflect your ability to apply what you have learned, and hopefully leave you wanting to learn more about cybersecurity risk management.

A reasonable approximation of the breakdown in terms of time required to succeed in this course is as follows. First, students are expected to participate in each live session during which we will discuss case studies in cybersecurity risk management as well as interact with thought leaders at the front lines of this field, including a range of prominent Chief Information Officers and Chief Privacy Officers. Second, students will work individually and in small teams to complete short research projects and simulations, in particular the National Security Council Cybersecurity Simulation discussed below. Third, throughout the term students will be working in groups with a real-world client on a cybersecurity capstone project, also discussed below. These projects require in-depth interactions with both the instructor, in groups, and with the client outside of normal class time, and as such should comprise approximately sixty percent of the total required time in this course.

ASSIGNED MATERIALS

Canvas/Internet (C/I): Materials to be downloaded from Canvas or a website
Harvard Business (HBR): HBR Cases
Handouts (HO): Handouts occasionally distributed in class

All information for the course will be posted on the course website on Canvas (https://canvas.iu.edu/lms-prd/app), which students should regularly check.

ASSESSMENT

Course performance will be assessed as follows:

Capstone Report & Presentation (100 points): Although it is important to have a basic grounding in the academic debates surrounding both privacy and cybersecurity law and policy, it is equally imperative to gain a better understanding for how some of the issues we will be discussing impact organizations in the real world. Toward that end, we have the unique opportunity of partnering with a real-world client to undertake a cybersecurity assessment. Details will be discussed in class during our first week.

Participation (50 points): To measure students' comprehension of the concepts and their proficiency at applying them, students will undertake periodic assessments along with several projects designed to help further our client's goals focusing on privacy and cybersecurity awareness-raising activities. Further, students will be asked to prep a 'hot topics' discussion of their choosing in Unit Three.

National Security Council (NSC) Cybersecurity Simulation (50 points): In order to better understand how federal agencies work together and with the private sector to mitigate cyber risks facing U.S. stakeholders, students will role play as principals on the National Security Council in a simulation designed by the Council on Foreign Relations. This is also an opportunity to integrate lessons across the curriculum in an effort to strategize about cybersecurity risk management at the highest policy levels.

UN Security Council (NSC) Cybersecurity Simulation (50 points): In order to better understand how the international community can meet the challenge of mitigating cyber risks, students will role play as members of the UN Security Council in a simulation designed by the Council on Foreign Relations. This is also an opportunity to integrate lessons across the curriculum in an effort to strategize about cybersecurity risk management at the highest policy levels.

	Total Available Points:	
Consulting Project:	100	40%
Participation:	50	20%
NSC Simulation	50	20%
UNSC Simulation	50	20%
TOTAL:	**250**	100%

GRADING SCALE

The grading scale for the course is as follows:

Score	Grade	Score	Grade	Score	Grade	Score	Grade
97.50-100	A+	87.50-89.49	B+	77.50-79.49	C+	67.50-69.49	D+
91.50-97.49	A	81.50-87.49	B	71.50-77.49	C	61.50-67.49	D
89.50-91.49	A-	79.50-81.49	B-	69.50-71.49	C-	59.50-61.49	D-

***Please note that I rarely curve to arrive at final grades**, and I will not deviate from the grading scale unless necessary to achieve an appropriate grade distribution for the class. Such a departure will only raise, not lower, students' grades.*

****I reserve the right to create extra credit opportunities**, but do not guarantee that there will be extra credit opportunities in the course.*

MAKEUP POLICY

To be fair to students who are struggling with documentable, life-altering events beyond their control, I will entertain requests to make up an assignment if you meet ***all 3 of these conditions***:

> **(1)** You have a very **compelling emergency** that will cause you to miss the assessment;
>
> **(2)** You provide **written and dated evidence** that proves the compelling emergency, such as a note from a physician stating that you were too ill to attend class on the day of the assessment or a dated obituary notice that mentions you by name' and
>
> **(3)** You **contact me** by email, phone, or in person and secure my permission to take a makeup **before** you miss the assessment.

The burden of proof is on you to provide adequate evidence of the compelling emergency. You must provide your evidence prior to taking the makeup and I reserve the right to revoke my permission to provide a makeup if your evidence does not demonstrate the claimed emergency or if it is not provided in what is, in my judgment, a timely manner.

The following are examples of compelling emergencies:

- Hospitalization or illness that is severe enough for you to seek medical attention
- Death in your immediate family
- Military deployment
- Jury duty or other mandatory court proceeding that cannot be rescheduled

APPEALS OF GRADED WORK

Appeals of graded work must be submitted in writing within one week of the date on which the graded work is returned to you. You may do this by email, phone, or in person.

ATTENDANCE

Attendance is required in this class, and it is factored into the participation grade. It will provide the opportunity for you to get to know your classmates and the course material. If you do miss class, it is your responsibility to find out from your classmates what occurred in class.

READING ASSIGNMENTS

I expect you to have completed the assigned reading BEFORE class. Background materials are not required but are beneficial for students wanting a better grounding in a particular area.

ACADEMIC INTEGRITY

Unless I expressly authorize you to work with another student on any assignment or extra credit project, discussing anything about the assignment or project other than the required format and due date is academic dishonesty. Students are subject to both IU's general and school-specific Academic Regulations.

ADMINISTRATIVE MATTERS

A. Students with Disabilities

Any student with a disability requiring reasonable accommodation should inform me by email within the first two weeks of class so that we can make the necessary accommodation(s). You also must provide to me a completed copy of the "Testing / Classroom Modifications" form from the Office of Disability Services.

B. Religious Holidays

Any student who has a religious conflict with an assignment or is otherwise unable to participate in the class for religious reasons must inform me by email within the first two weeks of class so that we can make alternative arrangements. Forms are available at http://www.indiana.edu/~vpfaa/holidays.shtml.

PROJECTED COURSE CALENDAR & ASSIGNED READINGS

C/I = Document or case to be downloaded from Canvas or a website
HBR = Harvard Business Review
HO = Handout distributed in class

** The following projected calendar is only a draft and is subject to change. The instructor will communicate any revisions to the students as early as possible prior to the session in question, but last-minute alterations may be unavoidable due to travel issues and other logistical concerns arising from our guest speakers.*

*** The first live session will take place from 7:30-8:45pm EST on **Monday, Feb. 22.** The class will find a convenient meeting time following this meeting, including over the Tuesday lunch honor or in the morning.*

Date	Topic	Reading Assignments	Deliverables
Session #1 M Feb. 22	Welcome & Orientation to the Course	**C/I**: Review the syllabus	
Session #2 M Mar. 1	Launch of Capstone Projects & Sim Prep	**C/I**: NSC Cyber Clash with China Case Prep & Student Guide	*Consulting Project Choices Due
UNIT 1: CASE STUDIES & SIMULATIONS IN CYBERSECURITY RISK MANAGEMENT			
Session #3 M Mar. 8	Equifax & Just the Fax mini case	**HBR**: Equifax **C/I**: Just the Fax mini case Background: **C/I**: Breach podcast (Season 2)	*Group Contracts Due
Session #4 M Mar. 15	National Security Council Simulation	**C/I**: NSC Simulation	
Session #5	UN Security Council	**C/I**: UNSC Simulation	*Progress Report Due to Instructor

M Mar. 22	Simulation		
UNIT 2: CYBERSECURITY POLICYMAKING: INSIGHTS FROM THE CYBERSPACE SOLARIUM COMMISSION (CSC)			
Mid-Semester Course Evaluation *Your opportunity to anonymously evaluate the course*			
Session #6 M Mar. 29	CSC Overview	• Congressional Research Service (CRS), *The Cyberspace Solarium Commission: Illuminating Options for Layered Deterrence*, March 20, 2020 (link). This CRS document provides a primer on the CSC. • CSC report, March 11, 2020 (link to report; link to executive summary). Students should review the 22-page executive summary and skim appendix A, roll-up of recommendations (p. 123); and appendix B, legislative proposals (p. 127).	
Session #7 M Apr. 5	CSC Policy Recommendations	• Justin Katz, "Senators: Biden picks Anne Neuberger to lead SolarWinds response," February 11, 2021, *FCW*. (Link) • Kara Swisher, "Does the U.S. Need a Cyberdefense Czar?" *The New York Times*, February 10, 2021. (Link) • Andrew Grotto, "How to Make the National Cyber Director Position Work," January 15, 2021, *Lawfare*. (Link) • CSC (YouTube video), "Congressman Langevin's Special Order Speech on the National Cyber Director Act," December 8, 2020. (Link). • Philip Reitinger, "Establishing a National Cyber Director Would Be a Mistake," July 17, 2020, *Lawfare*. (Link)	
Session #8 M Apr. 12	CSC Hot Topics: Cyber Risk Insurance & Supply Chain Security	• CSC report, March 11, 2020 (link to report; link to executive summary). Students should review pages 78-83 focusing on cyber insurance and pages 76-77 on liability for final goods assemblers. • Brad Noe, *What to Know About Cyber Insurance*, Forbes (Nov. 27, 2019), https://www.forbes.com/sites/forbestechcouncil/2019/11/27/what-to-know-about-cyber-insurance/#d99e9e916a34. • "A Quiet Panic Is Growing in U.S. Boardrooms Over Huawei Ban" (*Bloomberg*, June 10)	*Rough Draft Due to Team and Instructor

UNIT 3: HOT TOPICS IN CYBERSECURITY RISK MANAGEMENT			
Session #9 M Apr. 19	Machine Learning & AI Governance	**C/I**: *Machine Learning for Policymakers*, HARVARD, https://www.belfercenter.org/sites/default/files/files/publication/MachineLearningforPolicymakers.pdf.	
Session #10 M Apr. 26	Cybersecurity & the C-Suite & Quantum Computing	**C/I**: Bill Sweeney, *Cybersecurity Is Every Executive's Job*, HARVARD BUSINESS REVIEW (Sept. 13, 2016), https://hbr.org/2016/09/cybersecurity-is-every-executives-job **C/I**: Dorothy Denning, *Is Quantum Computing a Cybersecurity Threat?*, AMERICAN SCIENTIST (2019), https://www.americanscientist.org/article/is-quantum-computing-a-cybersecurity-threat.	
Session #11 M May 3	5G & the Internet of Things	***C/I***: *Have You Updated Your Toaster?*, HASTINGS LAW JOURNAL (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3208018.	*Final Report Due
Session #12 M May 10	Final Capstone Presentations		
***POTENTIAL TRIP TO ESTONIA (MAY 25-29)**			

APPENDIX A: WHO'S PROFESSOR SHACKELFORD?

Professor Shackelford serves on the faculty of Indiana University where he is Cybersecurity Program Chair along with being the Executive Director of the Ostrom Workshop. He is also an Affiliated Scholar at both the Harvard Kennedy School's Belfer Center for Science and International Affairs and Stanford's Center for Internet and Society, as well as a Senior Fellow at the Center for Applied Cybersecurity Research, and a Term Member at the Council on Foreign Relations. Professor Shackelford has written more than 100 articles, book chapters, essays, and op-eds for diverse outlets ranging from the *University of Illinois Law Review* and the *American Business Law Journal* to the *Christian Science Monitor*, *Huffington Post*, *Slate*, the *Conversation*, and the *San Francisco Chronicle*. Similarly, Professor Shackelford's research has been covered by diverse outlets, including *Politico*, NPR, *Marketplace*, *Forbes*, *Time*, *Associated Press*, *Forensics Magazine*, *Law360*, *Indy Star*, *Washington Post*, and the *LA Times*. He is also the author of *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace* (Cambridge University Press, 2014). Both Professor Shackelford's academic work and teaching have been recognized with numerous awards, including a Harvard University Research Fellowship, a Stanford University Hoover Institution National Fellowship, a Notre Dame Institute for Advanced Study Distinguished Fellowship, the 2014 Indiana University Outstanding Junior Faculty Award, and the 2015 Elinor Ostrom Award.

APPENDIX B: USEFUL CYBERSECURITY & PRIVACY WEBSITES

- IU-Bloomington Cybersecurity Program
- Ostrom Workshop Program on Cybersecurity and Internet Governance
- State of Indiana CISO Blog, http://www.in.gov/iot/cisoblog.htm

- IU Cybersecurity, https://cybersecurity.iu.edu/
- Cybersecurity: White House, http://www.whitehouse.gov/cybersecurity
- Stanford Cybersecurity, http://cisac.stanford.edu/research/2956/
- Center for Strategic and International Studies Cybersecurity Page, http://csis.org/category/topics/technology/cybersecurity
- International Association for Privacy Professionals, https://iapp.org/
- Politico Cybersecurity, http://www.politico.com/cybersecurity
- Cyber Wire, https://thecyberwire.com/

APPENDIX C: CYBERSECURITY M.S. LEARNING GOALS

Goal 1: Technical Cybersecurity

Demonstrate a basic understanding of the technical aspects of cybersecurity. Articulate the drivers and types of cyber conflict and describe the technical cybersecurity best practices that public- and private-sector actors are developing to help mitigate the multifaceted cyber threat

Goal 2: Integrated Cybersecurity Risk Management

Apply IT Risk Management basics—including risk prioritization strategies, approaches to project risk management, and drafting incident and disaster recovery plans—to an array of business situations within the cybersecurity context.

Goal 3: Critical Thinking and Communication

Apply critical thinking skills to develop evidence-based cybersecurity recommendations and effectively communicate them to non-technical professionals.

Goal 4: Global Cybersecurity Law and Policy

Understand the mechanisms by which cyber laws and policies are made, changed, interpreted, and applied—and how disputes get resolved—in the United States and other leading economies.

Goal 5: Ethics, Information Privacy, and Internet Governance

Gain awareness of important related areas to cybersecurity risk management, especially ethics and privacy, as well as Internet governance.

Goal 6: Teamwork and Collaboration

Demonstrate effective teamwork and collaboration skills and the ability to work with clients professionally.