City University of New York – Hunter College

Intro to Cyber Risk – Fall 2022

Syllabus

Course Information:

CSCI 39598-01: Intro to Cyber Risk (Section 1)

In-person, ThomHunter 502

Class Meets: Tuesdays 5:30 – 8:00 pm

Fall Term: August 25, 2022 – December 21, 2022

Office Hours: Please schedule individually

Contact Information:

Professor Jennifer Rothstein, Adjunct Lecturer

Department of Computer Science

jr5909@hunter.cuny.edu (for any communication or email assignments)

professorrothstein@gmail.com (for Google Doc sharing purposes)

917-596-0866 (text/call for emergencies)

Course Objectives & Learning Outcomes:

Introduction to Cyber Risk will teach students about the types of global cyber security threats our society faces, how we are defending against them and how we are preparing for the future. It is not a technical course focused on coding, programming or the mechanics behind a successful hack, but rather an analytical course which will introduce the most common categories of attacks; who is responsible for them and who; who the targets are and why; and what information is at risk.

Among the topics included are the deconstruction of the cyber attack chain, cyber risk management best practices, and relevant legal and regulatory implications. Students will apply interdisciplinary skills such as analysis, role-playing, and essay-writing to gain an understanding of the impact of cyber security, the practical implications of the damages and will study real-life incidents in real-time. Students will also become familiar with today's cyber leaders in both the private and public sector and will engage in group discussions as well as group projects to be better prepared to work in the collaborative environment the cyber security workforce requires. We will explore diversity in cyber security and consider ways to foster an inclusive and productive environment.

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

Define different types of cyber attacks/incidents/breaches

Identify the stakeholders and potential victims or affected parties before, during and after an incident

Develop an awareness of attacks in our everyday lives, track them and summarize them

Describe the potential damage from each type of attack

Present the major cyber attacks from the past decade and discuss predictions for 2022

Analyze an organization's cyber preparedness using industry-accepted standards

Understand basic regulations – both US and Global

Identify methodologies and actions for implementing best practices in cyber security

Discuss the benefits of cyber risk transfer and cyber insurance

Understand the role of law enforcement in the defense and investigation of cyber crimes

Develop an Incident Response Plan

Outline the life cycle of a ransomware attack

Present findings and recommendations to C-level executives as well as Board of Director
Consider a career in cyber security

Encourage the exchange of diverse perspectives and solutions for cyber security challenges

Appreciate the various cyber leaders from the public and private sector

Weekly Schedule of Topics to be Covered

Students are expected to come to class prepared and ready to participate in class discussions and group projects. The associated chapters and reading materials should be read ahead of time and every student will be asked to contribute actively in class. The schedule and reading materials are subject to change, but students will be notified with enough time in advance to prepare.

Each class will begin with a brief discussion of a cyber incident that took place during the previous week. Each student is encouraged to bring in an example of an attack they identified from the previous week and be prepared to share it with the class. Students will learn about the reliable sources in the news that track these events and will gain an appreciation for how much information is being circulated about cyber security on a daily basis.

Each class will also begin with a brief discussion of an alert issued by law enforcement to the public the previous week. These alerts may cover new threats, vulnerabilities, ransomware groups or litigation. Students will become familiar with the role different agencies and government have in in this sector, and how the public is informed in an actionable way.

READINGS

Accompanying each week in the syllabus is a list of readings. All of the books or links to publications or resources below are required reading and may be updated as important current events emerge. Any additional or substitute reading will be announced in class and on Blackboard.

SCHEDULE

We will have some guest speakers during the semester and dates will be confirmed during the semester.

Book (selections throughout the semester): Next Level Cyber Security by Sai Huda (available on Amazon)

Weekly Readings and Discussion Topics:

Week 1 (August 30th): First Class! (No reading due)

Discussion Topics:

- Introduction to the course – Interview with a Hacker
- Breach analysis
- Diversity & Inclusivity in cyber security
- BEC & Ransomware
- Cyber security in our interconnected world
- Incident v Breaches
- Leaders In Cyber Security
- War in Ukraine and its effect on ransomware attacks
- Role assignments & introductions

Reading:

https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

https://www.zdnet.com/article/microsoft-and-mcafee-headline-newly-formed-ransomware-task-force/

https://www.cisa.gov/uscert/ncas/tips/ST04-001

https://digitalguardian.com/blog/innovation-diversity-cybersecurity

https://www.uscybersecurity.net/history/

https://www.msn.com/en-us/money/news/a-diverse-cybersecurity-team-can-help-alleviate-the-talent-shortage/ar-AANie4U

https://www.cfr.org/blog/systemic-racism-cybersecurity-threat

https://news.microsoft.com/europe/features/why-we-need-more-diversity-in-cybersecurity/

Cyberwar_Data_Leaks.pdf (darkowl.com)

Week 2 (September 6th):

Discussion Topics:

- Cyber attack chain
- Cyber roles and careers
- Critical infrastructure
- PHI & PII
- Brief history of cyber security and cyber risk
- Privacy Matters

Reading:

Huda, Chapters 1&2 (focus on pages 16-17), Chapters 3- 4

Critical Infrastructure Sectors | CISA

https://cybersecurityventures.com/50-cybersecurity-titles-that-every-job-seeker-should-know-about/

White House Pushes to Fill 700,000 Cybersecurity Jobs in U.S. (ampproject.org)

https://www.uscybersecurity.net/history/

https://www.hhs.gov/answers/hipaa/what-is-phi/index.html

https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

https://www.nysenate.gov/legislation/laws/GBS/899-AA

https://blog.didomi.io/en/privacy-made-positive

https://www.apple.com/customer-letter/

https://www.apple.com/customer-letter/answers/

Week 3 (September 13th):

Discussion Topics:

- Cyber definitions
- CVEs
- Case studies: Solar Winds, Kronos, Log4J, I LOVE YOU virus
- Review for quiz

Reading:

https://niccs.us-cert.gov/about-niccs/glossary#A

https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/

https://www.msspalert.com/cybersecurity-breaches-and-attacks/kaseya-rmm-cyberattack-warning/

https://gizmodo.com/kaseya-is-making-its-customers-sign-non-disclosure-agre-1847356517

https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html

https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html

https://www.cyberscoop.com/fireeye-mandia-face-the-nation-solarwinds/

https://www.cnn.com/2021/12/16/tech/kronos-ransomware-attack/index.html

https://thestack.technology/kronos-ransomware-attack-ukg-kronos-private-cloud/

https://www.cybersecuritydive.com/news/kronos-ransomware-attack-lawsuits/620184/

https://www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/

How Russia Used SolarWinds To Hack Microsoft, Intel, Pentagon, Other Networks : NPR

Microsoft Autopatch arrives to make Windows Patch Tuesday a breeze | ZDNET (ampproject.org)

Week 4 (September 20th): Quiz in class

Discussion Topics

- Cyber Attacks in Hollywood
- Threat attack maps
- TTPs
- Historic cyber attacks

Reading:

Huda, (cont'd) Chapters 1&2 (focus on pages 16-17), Chapters 3- 4

https://www.imperva.com/cyber-threat-attack-map/

https://www.cisa.gov/tlp

Traffic Light Protocol (TLP) (first.org)

Next Two Weeks – No Class: Reading - https://www.acq.osd.mil/cmmc/about-us.html

Week 5 (September 27th): No Class

Week 6 (October 4th): No Class

Week 7 (October 11th):

Discussion Topics

- Historic cyber attacks
- Trends
- Attribution

Reading:

https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/

Huda, (cont'd) Chapters 1&2 (focus on pages 16-17), Chapters 3- 4

Cybersecurity's Greatest Showman On Earth: Kevin Mitnick (cybersecurityventures.com)

Week 8 (October 18th):

Discussion Topics

- Ransomware
  - Attacks
  - Gangs

Reading:

https://www.willistowerswatson.com/en-US/Insights/2021/08/hacking-back?utm_source=slipcase&utm_medium=affiliate&utm_campaign=slipcase

North Korean ransom gang undercuts competitors by charging low fees | Cybernews

Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022 (ampproject.org)

Florida's New Ransomware and Cybersecurity Requirements/Restrictions | Privacy & Data Security Law Journal

Ransomware gang now lets you search their stolen data (ampproject.org)

https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed

https://www.cbsnews.com/colorado/news/jbs-cyberattack-meat-supplier-fbi-

https://techcrunch.com/2022/08/12/state-conti-ransomware-intelligence/attributes-revil-ransomware-operation-russia-greeley/

Week 9 (October 25th): **Assignment 1 in class**

Discussion Topics

- Silk Road

Reading:

https://www.wired.com/2015/05/silk-road-untold-story/ (Part 1 & 2)

Week 10 (November 1st):

Discussion Topics

- NIST – Introduction to Standards and Framework
- CIS – Critical Security Controls

Reading:

https://www.nist.gov/cyberframework

https://www.cisecurity.org/controls/ (Please download and read the controls)

Huda, Chapter 12

Week 11 (November 8th): Midterm in class

Discussion Topics

- Regulations – HIPAA, GDPR. FERPA, DFS, CCPA, NY Shield Act
- Litigation

Reading:

https://gdpr.eu/what-is-gdpr/

https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (look over list)

https://studentprivacy.ed.gov/?src=fpco

https://www.dfs.ny.gov/system/files/documents/2019/01/cyber_memo_12212018.pdf

https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf

https://oag.ca.gov/privacy/ccpa

https://lewisbrisbois.com/privacy/US

Week 12 (November 15th):

Discussion Topics

- Cyber Insurance
  - Types of coverage
  - Underwriting applications
  - Pre-breach services

Reading:

https://thestack.technology/lloyds-cyber-insurance-exclusions-state-backed-systemic-risk/

https://woodruffsawyer.com/cyber-liability/cyber-101-liability-insurance/

https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyber-cover-guide.pdf

https://www.eqgroup.com/Pdf/Chubb/CHUBB-Cyber-Privacy-Insurance-Application.pdf

https://axaxl.com/-/media/axaxl/files/pdfs/insurance/pre-breach-services.pdf

Week 13 (November 22nd):

Discussion Topics

- Cyber insurance (cont’d)
- Scoping calls & Table Top Exercises (TTX)

Week 14 (November 29th): **Assignment 2 in class**

Discussion Topics

- Blockchain & Bitcoin
- NFPs

Reading:

Russia is banning crypto payments - Protocol (ampproject.org)

https://bitcoin.org/bitcoin.pdf

https://www.forbes.com/advisor/investing/cryptocurrency/nft-non-fungible-token/

Week 15 (December 6th):

Discussion Topics

- Threat intel
- Third party and supply chain risk

Reading:

https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html

Week 16 (December 13th):

Discussion Topics

- Predictions for the future and for the Board of Directors
- Enactment of a breach
- Review for final

Reading:

https://www.cfr.org/report/confronting-reality-in-cyberspace

https://www.solarium.gov/

Week 17 (December 20th) Final Exam Due

Grading Policy –

- 10% - 1 quiz
- 20% - Discussion Forum:
  - At least 10 posts in the Discussion Forums and 2 of those 10 posts must be in response to another student's post to create a dialogue
- 20% - Midterm
- 20% - 2 Assignments (each assignment is 10%)

- 20% - Final Exam
- 10% - Participation, in-class group work, attendance

Communication

Preferred method to contact instructor for urgent / non-urgent matters: email

Secondary method to contact instructor for urgent/non – urgent matters: text/call

Response time to outreach for urgent/non-urgent matters – same day

Academic Integrity/Honesty Policy

Hunter College regards acts of academic dishonesty (e.g., plagiarism, cheating on examinations, obtaining unfair advantage, and falsification of records and official documents) as serious offenses against the values of intellectual honesty. The College is committed to enforcing the CUNY Policy on Academic Integrity and will pursue cases of academic dishonesty according to the Hunter College Academic Integrity Procedures.

ADA Policy

In compliance with the American Disability Act of 1990 (ADA) and with Section 504 of the Rehabilitation Act of 1973, Hunter College is committed to ensuring educational parity and accommodations for all students with documented disabilities and/or medical conditions. It is recommended that all students with documented disabilities (Emotional, Medical, Physical, and/or Learning) consult the Office of AccessABILITY, located in Room E1214B, to secure necessary academic accommodations. For further information and assistance, please call: (212) 772- 4857 or (212) 650-3230.

Hunter College Policy on Sexual Misconduct

In compliance with the CUNY Policy on Sexual Misconduct, Hunter College reaffirms the prohibition of any sexual misconduct, which includes sexual violence, sexual harassment, and gender-based harassment retaliation against students, employees, or visitors, as well as certain intimate relationships. Students who have experienced any form of sexual violence on or off campus (including CUNY-sponsored trips and events) are entitled to the rights outlined in the Bill of Rights for Hunter College.

a. Sexual Violence: Students are strongly encouraged to immediately report the incident by calling 911, contacting NYPD Special Victims Division Hotline (646-610-7272) or their local police precinct, or contacting the College's Public Safety Office (212-772-4444).

b. All Other Forms of Sexual Misconduct: Students are also encouraged to contact the College's Title IX Campus Coordinator, Dean John Rose (jtrose@hunter.cuny.edu or 212-650-3262) or Colleen Barry (colleen.barry@hunter.cuny.edu or 212-772-4534) and seek complimentary services through the Counseling and Wellness Services Office, Hunter East 1123.

CUNY Policy on Sexual Misconduct Link:
http://www.cuny.edu/about/administration/offices/la/Policy-on-SexualMisconduct-12-1-14-with-links.pdf

Diversity & Inclusivity Policy

It is critical in every learning environment to create not only a spirit of tolerance, but a strong feeling of support, encouragement and celebration amongst students and faculty who are come to the course with distinct backgrounds, ethnicity, race, religion, sexual orientation, sexuality, disability, age, socioeconomic status, nationality, gender identity and culture. Everyone is welcome equally, and it is my intent to conduct this course with equality in mind and respect for each other's differences. I will require the same of all students, and in the event something is said or done in this classroom that causes discomfort or offense, please let me know immediately, as it will always be treated with the attention it deserves. Please do approach any concerns with the assumption that there was no intent to cause any harm or negative feelings and with an open mind toward prompt resolution.

Syllabus Change Policy

Any changes to the syllabus (assignments or scheduling) will be provided with enough advance notice depending on the change. Changes will be announced on Blackboard as well as through email and during class if appropriate.