JOHN JAY COLLEGE OF CRIMINAL JUSTICE
The City University of New York
524 W. 59th Street, New York, NY 10019

Syllabus

Professor

Chelsea Binns, PhD

Department

SFEM

Email

cbinns@jjay.cuny.edu

Phone

929-251-3670 (text)

Office Location

Virtual, Spring 2025

Office Hours

By appointment

on Zoom

SEC 107-99 Intro to Cybercrime

Course Description

This course delves into the complex world of cybercrime by exploring different types of cybercrime; the nature and extent of cybercrime; cybervictimization; criminological theories; the reasons why offenders commit cybercrime; cyberwitnesses' roles and reactions to cybercrime; the applicability of criminological theories to specific cybercrimes; and existing laws, policies, and measures and those needed to effectively control and combat cybercrime.

Course Meeting Schedule, Format and Organization

Online Asynchronous

Required Texts and Course Materials

Edwards, G. (2019). *Cybercrime Investigators Handbook*. Wiley Professional Development (P&T). (provided on Brightspace/John Jay Library online)

We will also be using additional materials, provided on Brightspace

Learning Outcomes

- Understand the scope and nature of cybercrime
- Describe typologies of cybercrime and the implications of cybercrime
- Identify the actors involved in cybercrime
- Identify causes and factors contributing to cybercrime
- Apply concepts to propose strategies reducing cybercrime

Course Technique

Each week, you will be reading the book Cybercrime Investigators Handbook, reading the chapter that's assigned on the syllabus and preparing answers to a series of questions provided on the syllabus and posting it on the discussion board. Throughout the course, we will also be conducting a case study.

For the final project, students will be writing a paper that is a minimum of 8 pages long, analyzing a cybercrime case study (students can chose their own case to analyze), covering the major points from the text and applying what was learned in the text, to the case study.

Participation and Attendance

In an online course, class attendance and participation are measured by your use of Brightspace to engage with the course material and your fellow classmates. It is very important to keep up with the weekly assignments. **Students are expected to log on regularly and to respond to all discussion boards within one week. Everything in the COURSE SCHEDULE below that says "POST ON BRIGHTSPACE" needs to be answered on the discussion board.** Discussion board weeks run from Monday to Sunday. Discussion board responses will be graded within two business days of the day they are due. Discussion boards that are submitted late may be accepted at a reduced grade, but they cannot be submitted more than one week after they are due. If students do not to log into Brightspace and do not participate in the discussion board, they may fail the course.

Course Tasks

- √ **Read Cybercrime Investigators Handbook**
- √ **Select a cybercrime case study and research it**
- √ **Select a case to investigate for your final paper**
- √ **Post responses to the questions provided on the Discussion Board**
- √ **Write your final paper, due May 15**

Course Assignment
For the final paper, you will be submitting an analysis of a cybercrime case - a recent, massive data breach. Please select one of these cases for your analysis:

- AT&T Data Breach, 2024
- Atlassian Data Breach, February 2024
- Change Healthcare Ransomware Attack, 2024
- Duolingo Data Breach, August 2024
- Financial Business and Consumer Solutions (FBCS) Data Breach, 2024
- National Public Data Breach, August 2024
- Reddit Data Breach, February 2024
- T-Mobile Data Breach, May 2024
- Toronto Public Library Data Breach, November 2024

The steps you will take to complete the paper are as follows.

First, you will investigate the **case that you select from the above list**. In doing so, you will conduct research on the internet, to include Lexis Nexis News (John Jay Library Website) and other news sources, such as Google News or the New York Times and Wall Street Journal websites (subscriptions provided for free from John Jay). You will consult these and other sources for information about these cases. Then, you will collect all of the relevant background information – including answers to the investigative essentials, "who, what, where, when, why and how."

Next, you will follow the methodology from the text in this course, creating and adding the sections below to your paper. Then, you will take each section and add the information that you learned by investigating this case. Some of the information may not be available, and you will need to use some creativity, adding your own ideas, thoughts or evaluation. In short, your paper should include the following information:

- √ **Cybercrime Offenses** – what was the offense in this case?
- √ **Motivations of the Attacker** – what was the motivation of the attackers in this case?
- √ **Determining that a Cybercrime is Being Committed** – how was the cybercrime caught?
- √ **Commencing a Cybercrime Investigation** – how would you get started in this case?
- √ **Initial Meeting with the Complainant** – who would you meet with and what would you ask them, if you were the investigator on the case?
- √ **Containing and Remediating the Cybersecurity Incident** – how would you contain and remediate? What did they do so far?
- √ **Challenges in Remediating the Cybersecurity Incident** – what are the challenges in this case?
- √ **Investigating the Cybercrime scene** – how you would investigate this case?
- √ **Open Source Evidence** – what kind of information could you get from open sources that would assist in solving this case?
- √ **The Dark Web** – what could you get from the dark web?
- √ **Interviewing Witnesses and Subjects** – who would you interview and what kind of questions would you ask them?
- √ **Review of Evidence** – what is the known evidence in this case and how would you evaluate it?

At the end, there should be a conclusion. In the conclusion, discuss what the author of our text might say about this case, what your thoughts about this case are, and how this crime could be prevented in the future.

The papers are due by the last day of class and should be submitted on Brightspace. No extensions are permitted.

Course Schedule

WEEK	MODULE	TOPIC	READINGS	POST ON BRIGHTSPACE
Jan 27	Intro	Chapter 1, Course Intro	Chapter 1	Welcome introduction

WEEK	MODULE	TOPIC	READINGS	POST ON BRIGHTSPACE
Feb 3	1	Cybercrime Offenses	Chapter 2	What are the cybercrimes discussed in this chapter and what are the top considerations for investigators when examining these cases? What are the main reasons the fraudster was able to perpetrate the crime described in the case study on page 26?
Feb 10	2	Motivations of the Attacker	Chapter 3	How can each type of cybercriminal be deterred, based on their individual motivations? Find an example of a cybercrime which demonstrates one or more of the listed motivations and be prepared to discuss it with the class. In one of the case studies in this chapter, you may notice a pattern, similar with the case study in the first chapter. What is that pattern and why is it concerning? What can be done to stop this from happening?

WEEK	MODULE	TOPIC	READINGS	POST ON BRIGHTSPACE
Feb 17	3	Determining that a Cybercrime is Being Committed	Chapter 4	What can be done to prevent each of the attack methodologies mentioned in Chapter 4? What went wrong in case study #1? How can this be prevented in the future? In case study #2, a specific technique was used by the perpetrator. What was that technique? Research that technique and be prepared to talk about how it's often used in cybercrimes. Find an example of another case in the media where this technique was used and share it with the class.
Feb 24	4	Conducting Cyber Case Study Research	Use the information that you have gathered so far, for your case study	Use the case that you selected for your case study final project to answer the following questions: What are the "investigative basics" in this case - the "Who, what, where, when, why and how?" [TIP:While you are conducting your research into this case, begin to think about how this could have been prevented. Write this up and add this to the beginning of your final paper.]
Mar 3	5	Commencing a Cybercrime Investigation	Chapter 5	The case study in this chapter highlights the risks of insiders. Research another case where a cybercrime was perpetrated by an insider and compare it to the case study provided in the text. In all cases, what weaknesses did the insider exploit? How could this crime have been prevented?

WEEK	MODULE	TOPIC	READINGS	POST ON BRIGHTSPACE
Mar 10	6	Initial Meeting with the Complainant	Chapter 7	*This chapter teaches you how to gather evidence in a cybercrime case.* Based on the information provided in this chapter, what seems to be the purpose of these initial meetings? Read the case study and review some of the questions provided by the author. What questions would be good to ask in this case? How could this incident have been prevented?
Mar 17	7	Containing and Remediating the Cybersecurity Incident	Chapter 8	In this chapter, the author discussed the NIST incident response framework which contains 5 pillars. Also, see the U.S. CERT Federal Incident Notification Requirements. What do you think the NIST would advise in the case that you are researching for your final project? Does it appear that NPD followed the notification requirements?
Mar 24	8	Challenges in Cybersecurity Incident Investigations	Chapter 9	How is a cybercrime scene different from a traditional crime scene? In the case study in this chapter, a challenge was described. What was that challenge, and how was it ultimately resolved? What was the type of cybercrime that was used in the case study and is this a common occurrence? How can we stop these cybercrimes from happening?

WEEK	MODULE	TOPIC	READINGS	POST ON BRIGHTSPACE
Mar 31	9	Investigating the Cybercrime scene	Chapter 10	Prepare a summary of the process that investigators go through when examining the crime scene in cybercrime cases. What type of evidence is collected? What's a general rule when it comes to evidence collection? What's especially important for the investigator to do with technology evidence?
Apr 7	10	Open Source Evidence	Chapter 14	What is open source investigations and what are some popular sources of information? Based on the information provided in the chapter, what seems to be the most important rules to follow when it comes to open source investigations? What's the single most important rule when it comes to search engines?
Apr 14	NO DISCUSSION BOARD DUE THIS WEEK~ SPRING BREAK			
Apr 21	11	The Dark Web	Chapter 15	What is the dark web? What can be obtained from the dark web that's useful for a cybercrime investigation? What's happening lately with AI and the dark web?

WEEK	MODULE	TOPIC	READINGS	POST ON BRIGHTSPACE
Apr 28	12	Interviewing Witnesses and Subjects	Chapter 16	What does the author say is the most important thing to do during an interview? What is an important strategic advantage the investigator can use during the interview? Who is the best person to conduct the interview? When does the author think you should interview a suspect? What are some ways you can prepare for your safety during the interview?
May 5	13	Review of Evidence	Chapter 17	What does the author say is important when it comes to an evidence report? Discuss the process of preparing the report, highlighting the critical areas discussed in the chapter.
May 12	14	Producing Evidence for Court	Chapter 18	What does the author say is true of all evidence? What is considered to be the best evidence in a cybercrime case? How do you make sure to avoid hearsay?
Extra credit	Module 15	CASE STUDY SUMMARY		Discuss the major points of your paper. What are your 3 main points? What fascinated you the most about the case study that you conducted? What weaknesses did it expose? What can be done in the future to prevent this type of cybercrime?
May 15				Final Writing Assignment Due

Grading

Grading Breakdown	# points for assignment	% of total grade
Participation (attendance & class discussion)	5 points per discussion response	50%
Final Project/Paper	50	50%

TOTAL	100 points	100%

Final Grade Scale

Grade		Grade	% of points
A	93.0 - 100%	C	73.0 - 77.0%
A-	90.0% - 92.9%	C-	70.0 – 72.9%
B+	87.1 – 89.9%	D+	67.1 – 69.9%
B	83.0 - 87.0%	D	63.0 - 67.0%
B-	80.0 - 82.9	D-	60.0 – 62.9%
C+	77.1 – 79.9	F	Below 60%

Final Paper Grading Rubric

Category	Key Criteria
Case Comprehension	Accurately identifies key issues and relevant details from the cases. Demonstrates a thorough understanding of the context and background information.
Analysis and Critical Thinking	Provides a well-structured analysis of the case, considering multiple perspectives. Applies relevant theoretical frameworks and concepts to explain the situation. Identifies potential causes and consequences of the problem.
Argumentation and Evidence	Supports claims with clear and relevant evidence from the case study. Uses logical reasoning and clear explanation to justify conclusions.
Recommendations	Presents feasible and well-reasoned recommendations based on the analysis. Considers potential implications and limitations of proposed solutions.
Writing Quality	Clear and concise writing style with proper grammar and mechanics. Well-organized structure with logical flow of ideas. Proper citation format.

Grading Scale

Grade	Description
A	Demonstrates a comprehensive understanding of the case and course readings, insightful analysis, strong arguments supported by evidence, and a clear, cohesive writing style.

B	Shows a good grasp of the case issues, provides solid analysis with relevant concepts, and presents arguments with adequate evidence.
C	Identifies key issues but may lack depth in analysis, with arguments that are not fully supported and writing that could be improved.
D	Shows limited understanding of the case, lacks critical analysis, and presents weak arguments with insufficient evidence.
F	Shows no effort/did not hand in a paper.

Discussion Board Grading Rubric

None (F): Student does not participate in the discussion board.

Low (B-, C): Student doesn't maintain a regular online presence (defined as logging on and participating at least once per week), student does not do the readings and/or respond to the posts of other students, student responds at times, but makes only general comments that do not contribute to the discussion.

Medium (B+, B): Student maintains a regular online presence (defined as logging on and participating at least once per week), student reads and responds to the posts of at least 2 other students regularly and makes comments that indicate they have read the assigned text.

High (A, A-): Student maintains a regular online presence (defined as logging on and participating at least once per week), students reads all posts and responds to the posts of several other students (2 or more) and makes comments that are insightful and give pertinent information from the course readings and also demonstrate a mastery of those readings, by relating it to postings, and drive the discussion and take it in new directions (offer new information and address prior questions with specific comments and information)

POLICIES & RESOURCES

Americans with Disabilities Act (ADA) – CUNY Accommodations Policy

CUNY'S Policy on Religious Accommodations

CUNY's Equal Opportunity and Non-Discrimination Policy

CUNY Policy on Academic Integrity

John Jay's Artificial Intelligence (AI) responsible use guidelines

Extra Credit Work

As an extra credit, students are offered the opportunity to do an additional discussion board post. Please see the post in the Course Schedule and answer the questions in Blackboard if you are interested in receiving this credit, worth 5 points.

Incomplete Grade Policy

INC policy

Graduate INC policy

The Alan Siegel Writing Center

The Alan Siegel Writing Center offers, free for all current students, support and assistance to enhance your writing skills through workshops and individual instruction. You can schedule their services online, by clicking here.