Professor John Marks
Department of Sociology and Criminal Justice
Social Science Building
1000 Chastain Road
Kennesaw, GA 30144-5591
E-mail: GeorgiaView Vista
Office Hours: By Appointment
Technology and Cybercrime CRJU 4305/W01
Fall Semester 2012 (CRN# 81653)

Course Navigation

- Before you begin, please take a moment to familiarize yourself with this web-based course. The course is totally online in an asynchronous format. You can complete your course by navigating around the GeorgiaVIEW Vista CRJU 4305 homepage and reading the materials specified on it and through the material in the organizers on that page. We will utilize the 'assessment', 'discussion', 'mail', 'announcement', 'who's online', and 'my grade' tools which are all available to you on the menu at the top of the homepage. All requirements required for course completion are listed in the syllabus along with the due dates for the completion of the various requirements. If you have any questions whatsoever about how to access any of the course materials or assignments please contact me through Vista. You must check your email and the Vista course site at least three times per week for emails and announcements. Remember this is your classroom so please feel comfortable asking me any questions which you would ordinarily ask in class.

Contact Information

- It is requested that you use email in your Vista course to communicate with the instructor when you have questions about the class. PLEASE do not hesitate to ask questions. I try to check Vista email once per day and return your email within 48 hours or sooner, except on weekends and holidays.

Course Description

- This course provides an overview of cyber crime and computer-related crime issues facing the American criminal justice system, particularly law enforcement. The course looks at law enforcement's ability to respond and discusses law enforcement problems in dealing with computer crime. Students will learn about government response to cyber crime problems, especially from a law enforcement perspective. Future trends of cyber crime and computer-related crime will also be discussed.

Class Format

- An interactive online format will be used. You are expected to read the syllabus, the assignments in text or via the Internet, read and review chapter PowerPoint slides, complete two examinations (a Midterm and a Final), answer and respond to another classmates answers to10 questions posed by the Instructor, complete two cybercrime projects, and complete one syllabus quiz.

Class Requirements and Grading Policy

- Two examinations, mid-term and final
    - 200 points: 100 points each

- Discussion Postings for 10 questions
  - 100 points; 10 points each
- Interaction with other students' discussions by posting one response to each of the discussions
  - 80 points; 8 points per response
- CyberCrime Project 1
  - 100 points
- CyberCrime Project 2
  - 100 points
- Syllabus Quiz
  - 20 points

Score	Grade
540 – 600	A
480 – 539	B
420 – 479	C
360 – 419	D
Below 360	F

Course Due Dates

- This is a 16-week-long course that starts August 17th and ends December 11th, 2012. Each week covers one chapter and weekly activities. The due dates for each assignment in this class specified in the Grading Rubric and Submission Policy Table will be based on the date periods of this 16-week-long session showed in the course schedule at the end of this syllabus.

Requirement	Full Score	Where to Submit	What to Submit	Due Date	Late Posting or Submission
Syllabus Quiz	20 pts.	Assignment Dropbox	Word.doc File	August 21	5 pts. per day
Discussion	100 pts.	Discussion Board	Posting Online	5th Day	No credit.
Responses	80 pts.	Discussion Board	Posting Online	7th Day	No credit.
CC Project 1	100 pts.	Assignment Dropbox	Word.doc File	September 27th	10 pts. per day
CC Project 2	100 pts.	Assignment Dropbox	Word.doc File	November 15th	10 pts. per day
Mid-Term	100 pts.	Assignment Dropbox	Word.doc File	October 23rd	No credit.
Final	100 pts.	Assignment Dropbox	Word.doc File	December 11th	No credit.
TOTAL	600 pts.				

Note: The dates for each week period are shown in the second column of the course calendar table at the end of this course syllabus. Justification for this date specificity is that for each of the discussion questions, you and your classmates will have 2 days to respond to the main answers to the question. Grades in this course will not be curved. All the scores you earned from each assignment and the exams will be accumulatively added up at the end of the course. Moreover, it should be noted that chapter specific reading assignments made in this assignment schedule refer to readings in the required textbook entitled, *Understanding and Managing CyberCrime (*2006*)* by Samuel C. McQuade, III.

Make-Up Exam and Extra Credit Policies

- For the mid-term exam, you are expected to take the exam on the scheduled date. Students with a valid excuse (and hopefully with prior approval from the instructor) for missing the exam may make up for it. The make-up exam will be given at the end of the semester. Students who are eligible to make-up for an exam are responsible to contact the instructor to arrange for the make-up. <u>You cannot make-up for the final exam</u>. There is no make-up for the cybercrime projects and the online discussions. Under no circumstances will extra points be given in this course. If necessary, you must drop the course before the given deadline.

Examinations

- There are two open-book examinations that will consist of objective and subjective measures of the course objectives with a value of 100 points on each exam. Each exam will cover chapters assigned before the exam. Questions are taken from your textbook, the Powerpoints and the Internet sites identified in the course outline and assignment schedule. Your score will be posted in your Gradebook with a maximum score of 100.

You will be given one attempt to complete each exam with a maximum of two hours each. To perform well on the exams, you need to read and study the text, posted chapter outlines, and required internet sites in detail before beginning them. All students are highly encouraged to study discussion questions given at the end of each chapter as those questions cover the same topics and in some cases will be the same or similar questions.

Discussion Question Postings

- All students must answer and discuss a response to ten discussion questions (10 points each: 7 points for the content and 3 points for including at least one relevant reference other than the textbook) posted on the discussion board by the professor. Each posting must (1) be a minimum of 250 words and may contain information from your text, accompanying materials, or assigned web sites; (2) include at least one additional outside reference; and (3) include both text citation (i.e., author's last name and year of the publication) and complete bibliographic information of all the references at the bottom of your posting. The references at the end of your posting must follow the APA style (including, the author's name, the name of the article, the name of the journal, the publication date, etc.) Citing only the website address is not considered a complete reference. Required content and format of your discussion may be found in the grading rubric for discussions found in the discussions organizer on the course homepage. To earn a high score, you must use formal English, proper punctuation, and proper spelling and grammar. ALL POSTINGS MUST BE DONE IN A RESPECTFUL AND ACADEMIC MANNER. THEY SHOULD BE IN FORMAL LANGUAGE WITH NO INTOLERENT, RUDE, ABUSIVE, OR OBSCENE LANGUAGE. VIOLATIONS OF THIS POLICY WILL RESULT IN ZERO POINT AND MAY BE REFERRED FOR DISCIPLINARY ACTION.

Responses to Other Students' Postings

- You must post one response per discussion question (8 points each). Each response should be at least 100 words or more. You should address how and why you agree or disagree with the response posted by your classmate. ALL POSTED COMMENTS MUST BE DONE RESPECTFULLY AND ACADEMICALLY WITH NO RUDE, ABUSIVE, OR OBSCENE LANGUAGE. VIOLATIONS OF THIS POLICY WILL RESULT IN ZERO POINT AND MAY BE REFERRED FOR DISCIPLINARY ACTION.

Two CyberCrime Projects

- Each of you must complete the two projects by following in the instructions in the Cybercrime Project organizer on the homepage. You are required to submit each project as a Word Document file (not WordPerfect or other formats) in the Assignment Dropbox.

Syllabus Quiz

- You should click on the assessments tool and take the quiz on the syllabus during the first week of the course. Please read the syllabus very carefully before taking the quiz. It is encouraged that you print out a copy of the syllabus and have it by you when taking the quiz.

Required Text

- *Understanding and Managing CyberCrime.* (2006) by Samuel C. McQuade, Ill. Allyn and Bacon Publishing. ISBN# 0-205-43973-X. Additionally, you are required to read appropriate, current criminal justice journal articles and internet material as assigned.

Learning Outcomes

- Identify and describe types of information systems and data that need protection
- Explain and analyze how abuse, attacks, and crimes committed with IT are accomplished
- Compare and contrast various theoretical and social perspectives used to explain cybercrime

- Discuss and analyze the impact the cybercriminals can create on cybercrime victims, society and economic, as well as predicting emerging and controversial cybercrime issues
- Apply cyber laws, regulations, and cybercrime-related legal concepts to explaining cybercrime activities
- Explain important steps law enforcement use to investigate cybercrime cases and bring the cases to trial
- Recognize security practices for protecting information systems and the steps IT professionals can take to improve the security measure within their organizations
- Analyze the potential effectiveness of the federal government's responses to addressing cybercrime and threat to critical information infrastructures

Writing Standards

- All written work will be graded on quality of writing as well as substantive content. The written paper must be pursuant to APA manual (especially the formats of the text citations and references). All written work must be formal usage and free from street terminology or office jargon, except when used in context and clearly and appropriately identified as non-standard usage. If you do not have such a style manual, you are strongly encouraged to obtain one or you can go to the following website (www.calstatela.edu/library/styleman.htm#apa).

Academic Integrity

- It is the philosophy of Kennesaw State University that each student is responsible for following the Student Code of Conduct, and students should read the Code in their Catalog pertaining to all aspects of academic integrity, especially the provisions regarding plagiarism and academic dishonesty. Academic dishonesty is a completely unacceptable mode of conduct and will not be tolerated in any form. All persons involved in academic dishonesty will be disciplined in accordance with University regulations and procedures. Discipline may include suspension from the University or other resolutions as required by the University Judiciary Program. Academic dishonesty includes but is not limited to cheating, plagiarism, collusion, the submission for credit of any work or materials that are attributable in whole or in part to another person, taking an examination for another person, or any act designed to give unfair advantage to a student.

Netiquette

- Please express all posted comments in formal English without street jargon or employment related jargon that will not be understood by all students. Avoid being critical of your fellow classmates and focus your responses to the content of what they posted. Do not make emotional outbursts on the discussion page and always remember that anything you post will be retained as you post it for a long time and can be referred to exactly as you post it in the future.

COURSE CALENDAR AND ASSIGNMENT SCHEDULE

Week 1

- Become acquainted with the GeorgiaVIEW Vista homepage.
- Go over all the materials and information given in this course.
- Read the course syllabus in detail.
- Complete the syllabus quiz by the due date.

MODULE ONE

Learning Outcomes

- Discuss how human behavior evolves in social and technological contexts (assessed by Week 2's discussion question)

- Define high-tech crime constructs and terms and analyze the importance of these crime terms to better understand cybercrime and future crime labels (assessed by Week 2's discussion question)
- Apply the critical infrastructure protection concepts and the information assurance ideas to explaining the need for securing information and data in justice and security management (assessed by Week 3's discussion question)
- List, describe, and differentiate the various types of abuse, attacks, and cybercrime (assessed by Week 4's discussion question and the cybercrime project)
- Identify and compare different behavioral and social traits of abusers, attackers, and criminals (assessed by Week 5's discussion question)
- Identify and compare different categories of abusers, attackers, and criminals (assessed by Week 5's discussion question)

Week 2

- Read Chapter 1 in the text and accompanying PowerPoint slides.
- Answer and respond to the discussion question (remember that your discussion should be 250 words and your response to another posting should be at least 100 words): Distinguish between computer crime, computer-related crime, and cybercrime. Can these crime terms be permanently defined and completely understood? Why or why not? Provide two examples of computer-related deviancy and briefly explain hypothetical circumstances for each example.

Week 3

- Read Chapter 2 in the text and accompanying PowerPoint slides.
- Answer and respond to the discussion question (remember that your discussion should be 250 words and your response to another posting should be at least 100 words): Explain the fundamental difference between CI and CII. Provide example of a hypothetical attack on each and possible damage or harm that could result. Also discuss possible interfacility and systems effects and consequences (i.e., how an attack on either CI or CII could affect the other).

Week 4

- Read Chapter 3 in the text and accompanying PowerPoint slides.
- Answer and respond to the discussion question (remember that your discussion should be 250 words and your response to another posting should be at least 100 words): In recent years there has been a dramatic increase in the number of worms, viruses, and Trojans released on the Internet. Why do you think this has occurred? Which attack is the most difficult one to defend and why?

Week 5

- Read Chapter 4 in the text and accompanying PowerPoint slides.
- Answer and respond to the discussion question (remember that your discussion should be 250 words and your response to another posting should be at least 100 words): Differentiate between social engineering tactics and the adversarial SKRAM model and provide appropriate examples for each. Based on 12 categories of IT abusers, select one of these abusers and provide a hypothetical situation that such an abuser can cause great harm to the criminal justice system if he/she could successfully employ the social engineering tactic.

MODULE TWO

Learning Outcomes

- Discuss and compare theoretical and social perspectives used to explain why people commit cyber abuse and crime, including classical and choice theory, trait theory, social process theory, social structure theory, conflict theory, and integrated and technological theories. (assessed by Week 6's discussion question and the cybercrime project)

- Explain the characteristics of cybercrime victims and analyze harms experienced by the victims of cybercrime (assessed by Week 7's discussion question and the cybercrime project)
- Discuss and evaluate the accuracy and completeness of the various measures used to gather cybercrime statistics. (assessed by Week 7's discussion question)
- Assess the likelihood of potential cyber abuse within the agencies and design a safeguarding plan to protect it (assessed by Week 8's discussion question)

Week 6

- Read Chapter 5 in the text and accompanying PowerPoint slides.
- Answer and respond to the discussion question (remember that your discussion should be 250 words and your response to another posting should be at least 100 words): Choose two of the four following theories, i.e., rational choice, social structure, social process or conflict, and explain how each one explains a single illegal computer activity – of your own choosing.

Week 7

- Read Chapter 6 in the text and accompanying PowerPoint slides.
- Answer and respond to the discussion question (remember that your discussion should be 250 words and your response to another posting should be at least 100 words): Locate IT-enabled computer or cybercrime statistics for any state. (You may try the website of your local and state police agencies, or you can visit the Bureau of Justice Statistics at http://www.ojp.usdoj.gov/bjs). Describe characteristics of victims of cybercrime, cost and harm of the crime, and types of cyber abuse.

Week 8

- Read Chapter 7 in the text and accompanying PowerPoint slides.
- Answer and respond to the discussion question (remember that your discussion should be 250 words and your response to another posting should be at least 100 words): Discuss major challenges and potential pitfalls associated with protecting the information infrastructure of any organization from cyber abusers.

Week 9

- Midterm Review

Week 10

- Midterm Exam

MODULE THREE

Learning Outcomes

- Explain the rationale and reach of cyber laws and regulations and how they are created and administered (assessed by Week 11's discussion question)
- Recognize key federal cybercrime laws and information security regulations and apply them to illegal cyber behavior and activity (assessed by Week 11's discussion question)
- Discuss the collaborative roles of public enforcement and private security in the investigating and prosecuting processes associated with legal issues, crime scene processing, and evidence management (assessed by Week 12's discussion question)
- Discuss security practices for protecting information systems and steps IT professionals can take to improve the security measures within their organizations (assessed by Week 14's discussion question and the cybercrime project)
- Identify some of the current efforts by the federal government to addressing cybercrime and threats to information security and assess the practicality of these endeavors for success (assessed by Week 14's discussion question and the cybercrime project)

Week 11

- Read Chapter 8 in the text and accompanying PowerPoint slides.
- Answer and respond to the discussion question (remember that your discussion should be about 250 words and your response to another posting should be about 100 words):

Discuss the USA PATRIOT Act and how subsequent legislative amendments dictate how law enforcement polices the online community.

Week 12

- Read Chapter 9 in the text and accompanying PowerPoint slides.
- Answer and respond to the discussion question (remember that your discussion should be 250 words and your response to another posting should be at least 100 words): Discuss the relationship between types of evidence, chain of custody, and computer forensics in investigating and prosecuting cybercrime.

Week 13

- Read Chapter 10 in the text and accompanying PowerPoint slides.

Week 14

- Read Chapter 11 in the text and accompanying PowerPoint slides.
- Answer and respond to the discussion question (remember that your discussion should be 250 words and your response to another posting should be at least 100 words): Assume you are an IT professional who needs to design an information security plan for the organization. Discuss key elements that must be included for your plan to succeed – provide supporting information to strengthen your points.

Week 15

- Final Exam Review

Week 16

- Final Exam

Course Schedule for All Class Activities

Periods	Dates	Learning Modules	Reading Assignments	Notes
Week 1	Aug. 17th - 23rd	Introduction to class	Syllabus and all the documents posted on Vista	(1) Surf Georgiaview Vista course homepage (2) Read Syllabus (3) Syllabus Quiz due on August 23rd
Week 2	Aug. 24th - 30th	Module 1	Chapter 1	Discuss Week 2's question
Week 3	Aug. 31st - Sept. 6th	Module 1	Chapter 2	Discuss Week 3's question
Week 4	Sept. 7th - 13th	Module 1	Chapter 3	Discuss Week 4's question
Week 5	Sept. 14th - 20th	Module 1	Chapter 4	Discuss Week 5's question
Week 6	Sept. 21st - 27th	Module 2	Chapter 5	Discuss Week 6's question
CyberCrime Project 1 is due on September 27th				
Week 7	Sept. 28th - Oct. 4th	Module 2	Chapter 6	Discuss Week 7's question
Week 8	Oct. 5th - 11th	Module 2	Chapter 7	Discuss Week 8's question
Week 9	Oct. 12th - 18th	Mid-term Review - No Class Activities (study guide given)		
Week 10	Oct. 19th - 25th	Midterm Exam starts 00:00 (Oct. 19th) and ends 11:59 (Oct. 25th)		
Week 11	Oct. 26th - Nov. 1st	Module 3	Chapter 8	Discuss Week 11's question
Week 12	Nov. 2nd - 8th	Module 3	Chapter 9	Discuss Week 12's question
Week 13	Nov. 9th - 15th	Module 3	Chapter 10	
CyberCrime Project 2 is due on November 15th				
Week 14	Nov. 16th - 26th	Module 3	Chapter 11	Discuss Week 14's question
Week 15	Nov. 27th - Dec. 3rd	Final Review - No Class Activities (study guide given)		
Week 16	Dec. 4th - 11th	Final Exam starts 00:00 (Dec. 4th) and ends 11:59 (Dec. 11th)		

Important Dates:

October 12: Last day to withdraw without academic penalty

December 3: Last day of class