John Marks
KSU Department of Sociology and Criminal Justice
Technology and Cybercrime CRJU 4305
Spring 2014

Introductory Course Note:
Kennesaw State University has switched to Desire2Learn. I hope that each of you will find it easier to navigate. There will very likely to be issues that each of us will encounter at the start of this semester. So, not panic or get upset if something goes wrong. Please be patient; we will work out any problems together, okay?

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 Desire2Learn 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 Desire2Learn. You must check your email and the Desire2Learn course site at least three times per week for emails and announcements.

Contact Information
I usually try to check email once per day and respond 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 (1) read the syllabus, (2) the assignments in text or via the Internet, (3) read and review chapter PowerPoint slides, (4) complete a Midterm and Final, (5) answer and respond to another classmates answers to 10 questions posed by the Instructor, (6) complete two cybercrime projects, and (7) complete one syllabus quiz.

Class Requirements and Grading Policy

- Midterm and Final
  - 200 points
- Discussion postings for 10 questions
  - 100 points; 10 points each
- Response posting for 10 questions
  - 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

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. You cannot make-up for the final exam. 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 Grade 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 in 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. Remember to post by the fifth class day of the week.

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. Remember to post by the seventh class day of the week.

Two CyberCrime Projects
You must complete two projects by following in the instructions in the Cybercrime Project organizer on the homepage; please submit each as a Word.doc file in the Dropbox.

Syllabus Quiz
You should click on the assessments tool and take the quiz on the syllabus no later than January 14th by 11:59 p.m. As mentioned previously, this course is condensed into an eight week period. 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.

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 the APA 6th Edition (both in-text citations and references).

Academic Integrity

All persons involved in academic dishonesty are subject to discipline in accordance with Kennesaw State University regulations and procedures.

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.

MODULE ONE

Module One Learning Outcomes

- Discuss how human behavior evolves in social and technological contexts
- Define high-tech crime constructs and terms and analyze the importance of these crime terms to better understand cybercrime and future crime labels
- 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
- List, describe, and differentiate the various types of abuse, attacks, and cybercrime
- Identify and compare different behavioral and social traits of abusers, attackers, and criminals
- Identify and compare different categories of abusers, attackers, and criminals

January 8 - 14 (Listed under Week 1)

- Become acquainted with the Desire2Learn 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.

January 15 - 22 (Listed under Week 2)

- Read Chapter 1 (McQuade, 2006) and accompanying PowerPoint slides.
- Week 2 Discussion: 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.
    - Your 250 word discussion post is due no later than 11:59 p.m. on January 20th
    - Your 100 word response is due no later than 11:59 p.m. on January 22nd

January 23 - 29 (Listed under Week 3)

- Read Chapter 2 (McQuade, 2006) and accompanying PowerPoint slides.
- Answer and respond to the discussion question: 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).
    - Your 250 word discussion post is due no later than 11:59 p.m. on January 27th
    - Your 100 word response is due no later than 11:59 p.m. on January 29th

January 30 – February 5 (Listed under Week 4)

- Read Chapter 3 (McQuade, 2006) and accompanying PowerPoint slides. .
- Answer and respond to the discussion question: 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?
    - Your 250 word discussion post is due no later than 11:59 p.m. on February 3rd
    - Your 100 word response is due no later than 11:59 p.m. on February 5th

February 6 - 12 (Listed under Week 5)

- Read Chapter 4 (McQuade, 2006) and accompanying PowerPoint slides.
- Answer and respond to the discussion question: 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.
    - Your 250 word discussion post is due no later than 11:59 p.m. on February 10th
    - Your 100 word response is due no later than 11:59 p.m. on February 12th

MODULE TWO

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.
- Explain the characteristics of cybercrime victims and analyze harms experienced by the victims of cybercrime
- Discuss and evaluate the accuracy and completeness of the various measures used to gather cybercrime statistics
- Assess the likelihood of potential cyber abuse within the agencies and design a safeguarding plan to protect it

February 13 - 19 (Listed under Week 6)

- Read Chapter 5 (McQuade, 2006) and accompanying PowerPoint slides.
- Answer and respond to the discussion question: Choose two of the four following theories, i.e., rational choice, social structure, social process and conflict, and describe how each one explains a hypothetical illegal computer activity. First, name your chosen theories and describe the hypothetical example.
    - Your 250 word discussion post is due no later than 11:59 p.m. on February 17th
    - Your 100 word response is due no later than 11:59 p.m. on February 19th

February 20 - 26 (Listed under Week 7)

- Read Chapter 6 (McQuade, 2006) and accompanying PowerPoint slides.
- Answer and respond to the discussion question: 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.
    - Your 250 word discussion post is due no later than 11:59 p.m. on February 24th
    - Your 100 word response is due no later than 11:59 p.m. on February 26th

February 27 – March 5 (Listed under Week 8)

- Read Chapter 7 (McQuade, 2006) and accompanying PowerPoint slides.
- Answer and respond to the discussion question: Discuss major challenges and potential pitfalls associated with protecting the information infrastructure of any organization from cyber abusers.
    - Your 250 word discussion post is due no later than 11:59 p.m. on March 3rd
    - Your 100 word response is due no later than 11:59 p.m. on March 5th

March 6 - 12 (Listed under Week 9)

- Study for Midterm Exam

March 13 - 19 (Listed under Week 10)

- Midterm Exam

MODULE THREE

Module Three Learning Outcomes

- Explain the rationale and reach of cyber laws and regulations and how they are created and administered
- Recognize key federal cybercrime laws and information security regulations and apply them to illegal cyber behavior and activity
- 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
- Discuss security practices for protecting information systems and steps IT professionals can take to improve the security measures within their organizations
- 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

March 20 - 26 (Listed under Week 11)

- Read Chapter 8 (McQuade, 2006) and accompanying PowerPoint slides.
- Answer and respond to the discussion question: Discuss the genesis of the USA PATRIOT Act, and how it has affected American life; provide examples of impact on the online community and law enforcement.
    - Your 250 word discussion post is due no later than 11:59 p.m. on March 24th
    - Your 100 word response is due no later than 11:59 p.m. on March 26th

March 27 – April 7 (Listed under Week 12)

- Read Chapter 9 (McQuade, 2006) and accompanying PowerPoint slides.
- Answer and respond to the discussion question: Discuss the relationship between types of evidence, chain of custody, and computer forensics in investigating and prosecuting cybercrime.
    - Your 250 word discussion post is due no later than 11:59 p.m. on April 5th
    - Your 100 word response is due no later than 11:59 p.m. on April 7th

April 8 - 14 (Listed under Week 13)

- Read Chapter 10 (McQuade, 2006) and accompanying PowerPoint slides.
    - Your 250 word discussion post is due no later than 11:59 p.m. on April 12th
    - Your 100 word response is due no later than 11:59 p.m. on April 14th

April 15 - 21 (Listed under Week 14)

- Read Chapter 11 (McQuade, 2006) and accompanying PowerPoint slides.
- Answer and respond to the discussion question: Assume you are an IT professional tasked with designing 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.
    - Your 250 word discussion post is due no later than 11:59 p.m. on April 19th
    - Your 100 word response is due no later than 11:59 p.m. on April 21st

April 22 - 28 (Listed under Week 15)

- Study For Final

April 29 – May 5 (Listed under <u>Week 16)</u>

- Final Exam
-

Spring 2014 CLASS CALENDAR

Dates	Learning Modules	Reading Assignments	Notes
January 8 - 14	Introduction to class	Syllabus and all the documents posted on Desire2Learn	(1) Surf Desire2Learn course homepage (2) Read Syllabus (3) Syllabus Quiz due on January 14th.
January 15 - 22	Module 1	Chapter 1	Discuss/Respond Week 2's question
January 23 - 29		Chapter 2	Discuss/Respond Week 3's question
January 30 – February 5		Chapter 3	Discuss/Respond Week 4's question
February 6 - 12		Chapter 4	Discuss/Respond Week 5's question
February 13 - 19	Module 2	Chapter 5	Discuss/Respond Week 6's question
February 20 - 26		Chapter 6	Discuss/Respond Week 7's question
February 27 – March 5		Chapter 7	Discuss/Respond Week 8's question
March 6 - 12	Study for Midterm CyberCrime Project 1 due March 6th		
March 13 - 19	Midterm Exam		
March 20 - 26	Module 3	Chapter 8	Discuss/Respond Week 11's question
March 27 – April 7		Chapter 9	Discuss/Respond Week 12's question
April 8 - 14		Chapter 10	Discuss/Respond Week 13's question
April 15 - 21		Chapter 11	Discuss/Respond Week 14's question
April 22 - 28	Study for Final CyberCrime Project 2 due April 22nd		
April 29 – May 5	Final Exam		

SUBMISSION POLICY TABLE

Requirement	Full Score	Where to Submit	What to Submit	Due Date	Late Posting or Submission
Syllabus Quiz	20 pts.	Assignment Dropbox	Word.doc	Jan 14th	No Credit
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	Mar 6th	25 pts. Per Day
Mid-Term	100 pts.	Assignment Dropbox	Word.doc	Mar 19th	No Credit
CC Project 2	100 pts.	Assignment Dropbox	Word.doc	April 22nd	25 pts. Per Day
Final	100 pts.	Assignment Dropbox	Word.doc	May 5th	No Credit
TOTAL	600 pts.				