This syllabus is subject to change as the semester progresses to accommodate instructional and/or student needs.

Instructor: Nir Kshetri, Ph D
Phone: 334-4530
Office hours: M1-2 PM
Office location: 368 BRYAN

Email: nbkshetr@uncg.edu

Required Text
None.

Catalog Description
Examines cyber-threats facing organizations and individuals and analyzes mechanisms to strengthen cybersecurity. Introduces tools, policies, concepts, safeguards, guidelines, risk management, actions, training, best practices, assurance and technologies to enhance cybersecurity

Student Learning Outcomes:
At the completion of the course, the students will be able to:

1) Identify cybersecurity related threats facing individuals, organizations and government agencies
2) Analyze the impacts of cybercrimes on business and management
3) Analyze workplace, human resources and top management issues in cybercrime and cybersecurity
4) Evaluate cybersecurity related issues in international offshoring/outsourcing
5) Evaluate the economic factors affecting cybercrimes and cyberattacks and their variations across the world
6) Assess the economic factors affecting individuals’ and organizations’ cybersecurity measures and their variations across the world
7) Demonstrate an understanding of the effects of cultural factors on cybercrime and cyberattack patterns and their variations across the world
8) **Demonstrate** an understanding of the effects of cultural factors on cybersecurity measures and their variations across the world

9) **Assess** political, legal and law enforcement systems affecting cybercrimes and cyberattacks and their variations across the world

10) **Assess** the cross-national differences in political and legal factors affecting cybersecurity

11) **Analyze** the ethical underpinning that guides practices of hackers and cybercriminals from various cultures

12) **Demonstrate** an understanding of recent regulatory developments related to cybersecurity in major world economies

13) **Analyze** the regulatory compliance issues related to cybersecurity in key industry sectors in the U.S.

14) **Demonstrate** an understanding of industry standards and certification issues related to cybersecurity.

15) **Evaluate** the functioning of international cybersecurity related institutions and organizations

16) **Demonstrate** an understanding of cyberwarfare and cyberterrorism related issues in the global context

**Teaching Methods and Assignments for Achieving Learning Outcomes:**

This online course requires you to participate in online discussion, take quizzes and exams online, doing assignments and analyzing cases. A tentative outline of activities is provided in this syllabus.

Topics covered include:

1. Definitions and concepts related to cybercrime and cybersecurity
2. Impacts of cybercrimes on business and management
3. Workplace, human resources and top management issues in cybercrime and cybersecurity
4. Cybersecurity divide.
5. Economics of cybercrime and cybersecurity and variation across world economies
6. Formal and informal institutional factors affecting cybercrime and cybersecurity.
8. Variations in cybercrimes originating in and affecting different regions and economies across the world
9. The governance of the cyberspace and cybersecurity issues
10. Cybersecurity related issues in offshoring/outsourcing.
11. Social, cultural, ethical, legal and political perspectives of cybersecurity.
12. Recent regulatory developments related to cybersecurity in major world economies.
13. Regulatory compliance issues related to cybersecurity in key industry sectors
15. International variation in cybersecurity issues.
16. International cybersecurity related institutions and organizations.
17. Cyberwarfare and cyberterrorism related issues.

**Online Attendance, Participation and Contribution (200 points)**

Canvas is an important component of this course. You are expected to login regularly and post to the discussion topics (at least TEN posts are required, each post is required to be at least two
paragraph long, sample posts are available in Canvas). The purpose of online discussions is to supplement the materials covered in the course. Your posts enhance not only your own learning but also that of your fellow students. However, please feel free to post anything that contributes to our learning of International Business.

Two of the posts are required to be on the forum “Online video contribution”. Your posts on this forum are required to be mainly based on free video(s) available online (e.g., YouTube) to help learn understand some concepts related to cybersecurity. Ideal videos are 5-15 minutes long. It is a good idea to connect/combine information in the video with information from other sources. As an example of a post, see the following item I have posted on this forum: Global cybercrime industry and cloud security (Nir Kshetri).

The last day for posting on the discussion is July 27, 2017. Please note that I will strictly follow this deadline. Please copy all your posts in ONE word document and email me by July 28, 2017. Make sure that each post has the date you posted on the Canvas.

Any item posted on these forums (your original post as well as your comments/responses to the posts of others participants) will count as a post.

Your posts are evaluated using the following criteria:

a) Have you done additional research and included source(s) of your information? You need to include each reference in its complete form, not just the link.
b) Have you connected your discussion with materials from your textbook or those discussed in the class?
c) Have you connected your posts with the current business related events (some of them)?
d) Do your posts refer to other course participants’ posts (some of them)?
e) Are your posts uniformly distributed throughout the session?
f) Are they sufficient long (that is, at least 2 paragraphs)?
g) Are they insightful and provide the reader with new ideas?

Quizzes (75 points)

There will be THREE quizzes. Please inform the instructor as soon as possible if you have a technical problem to complete a quiz/exam on Canvas.

Exam 1 (125 points)

More details about this exam will be available on Canvas. Please inform the instructor as soon as possible if you have a technical problem to complete a quiz/exam on Canvas.

Exam 2 (125 points)

More details will be available on Canvas. Please inform the instructor as soon as possible if you have a technical problem to complete a quiz/exam on Canvas.
Exam 3 (250 points)

Details will be announced in Canvas. Please inform the instructor as soon as possible if you have a technical problem to complete a quiz/exam on Canvas.

Assignments (225 points)

Assignment 1 (100 points)

Case Analysis of “Alibaba and the 2,236 cyber thieves”. More details will be available on Canvas.

Assignment 2 (125 points)

In Assignment 2, you are required write a paper on the following topic:

The roles of cryptocurrencies such as bitcoin in the growth of cyber-extortion involving ransomware.

Your paper is expected to cover the following:

a) Recent growth in ransomware and cyber-extortion with some examples
b) Why cyber-extortionists demand that ransom be paid by cryptocurrencies such as bitcoin
c) What types of victims are likely to comply with cyber-extortionists demand to pay ransom with bitcoin?
d) Assume that you are the CEO of a bank. All of your bank’s files have been encrypted by cybercriminals. You received an email from the cybercriminals that they will decrypt the files if you pay $30,000 by bitcoins. How would you respond? Why

Your analysis is expected to be about 1,600 words in length excluding the references. Please cite all the sources of your information.

Evaluation and Grading:

Points possible for the various evaluation components are summarized below:

<table>
<thead>
<tr>
<th>Component</th>
<th>Points possible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Attendance, Participation and Contribution</td>
<td>200</td>
</tr>
<tr>
<td>Exam 1</td>
<td>125</td>
</tr>
<tr>
<td>Exam 2</td>
<td>125</td>
</tr>
<tr>
<td>Exam 3</td>
<td>250</td>
</tr>
<tr>
<td>Three Quizzes</td>
<td>75</td>
</tr>
<tr>
<td>Assignment 1</td>
<td>100</td>
</tr>
</tbody>
</table>
Scoring System for the Final Grade

The following scoring system will be used for the final grade.

<table>
<thead>
<tr>
<th>Score</th>
<th>Grade</th>
<th>Score</th>
<th>Grade</th>
<th>Score</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>965-1000</td>
<td>A+</td>
<td>790 – 844</td>
<td>B</td>
<td>630 – 669</td>
<td>C-</td>
</tr>
<tr>
<td>945 - 964</td>
<td>A</td>
<td>750 – 789</td>
<td>B-</td>
<td>590 – 629</td>
<td>D+</td>
</tr>
<tr>
<td>910 – 944</td>
<td>A-</td>
<td>710 – 749</td>
<td>C+</td>
<td>550 – 589</td>
<td>D</td>
</tr>
<tr>
<td>845 – 909</td>
<td>B+</td>
<td>670 – 709</td>
<td>C</td>
<td>0 – 549</td>
<td>F</td>
</tr>
</tbody>
</table>

The following criteria will apply to the grading of assignments

A: Work that demonstrates not only a clear understanding of the material under study, but also a superior ability to utilize that material in the assignment. All criteria are met. The student’s work goes beyond the task and contains additional, unexpected or outstanding features.

B: Work that demonstrates a good understanding of the material under study, and utilizes the material well in the assignment. The student meets the assignment criteria, with few errors or omissions.

C: Work that fails to demonstrate a basic or technical understanding of the material under study, and fails to use relevant material in the assignment. Work may not address one or more criteria or may not accomplish what was asked.

F: Work that is incomplete, inappropriate and/or shows little or no comprehension of the material under study.

TENTATIVE COURSE SCHEDULE

<table>
<thead>
<tr>
<th>Week</th>
<th>Detail</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 1 (8/15-20) | **Part 1: Mechanisms and growth of cybercrimes and the current state of cybersecurity**  
- Reading #01: Growth of Cybercrimes and the Current State of Cybersecurity | • Handout/readings in Canvas |
| 2 (8/21-27) |  
- Reading #02: The Simple Economics of Cybercrimes  
- Reading #03: Positive Externality, Increasing Returns and the Rise in Cybercrimes | • Handout/readings in Canvas |
| 3 (8/28-9/3) | **Part 2: Strategic and organizational issues associated with cybersecurity**  
- Reading #04: Cybersecurity as a key element of corporate strategy: The development of deployment of resources  
- Reading #05: The Economics of Click Fraud | • Quiz 1 online. This quiz will open on 8/28 at 5 PM and will be available for 48 hours.  
• Handout/readings in Canvas |
<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Topic</th>
<th>Readings</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>(9/4-10)</td>
<td><strong>Part 3: CS issues associated with new ICTs and systems</strong></td>
<td>Reading #06: Privacy and Security Aspects of Social Media: Institutional and Technological Environment</td>
<td>Handout/readings in Canvas</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Exam 1 online. This exam will open on 9/4 at 5 PM and will be available for 48 hours.</td>
</tr>
<tr>
<td>6</td>
<td>(9/18-24)</td>
<td></td>
<td>Reading #08: Big data's impact on privacy, security and consumer welfare</td>
<td>Handout/readings in Canvas</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Quiz 2 online. This quiz will open on 9/18 at 5 PM and will be available for 48 hours.</td>
</tr>
<tr>
<td>7</td>
<td>(9/25-10/1)</td>
<td></td>
<td>Reading #09: Cybersecurity and Privacy Issues Facing Smart Cities and the Internet of Things</td>
<td>Handout/readings in Canvas</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reading #10: Can Blockchain Strengthen IoT?</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>(10/2-8)</td>
<td><strong>Part 4: Political, legal, social, cultural, and ethical issues in cybercrime and cybersecurity</strong></td>
<td>Reading #11: Pattern of Global Cyber War and Crime: A Conceptual Framework</td>
<td>Handout/readings in Canvas</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Assignment 1 due: 10/2/2017. Please submit before 11:59 PM.</td>
</tr>
<tr>
<td>10</td>
<td>(10/16-22)</td>
<td></td>
<td>Reading #13: Recent U.S. cybersecurity policy initiatives: Challenges and implications</td>
<td>Handout/readings in Canvas</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Exam 2 online. This exam will open on 10/16 at 5 PM and will be available for 48 hours.</td>
</tr>
<tr>
<td>11</td>
<td>(10/23-29)</td>
<td></td>
<td>Reading #14: EU and US Cybersecurity Strategies: Impacts on Businesses and Consumers</td>
<td>Handout/readings in Canvas</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reading #15: Cloud Computing and EU Data Privacy Regulations</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>(10/30-11/5)</td>
<td></td>
<td>Reading #16: China's Data Privacy Regulations: A Tricky Trade-Off between ICT's Productive Utilization and Cyber-Control.</td>
<td>Handout/readings in Canvas</td>
</tr>
<tr>
<td>13</td>
<td>(11/6-12)</td>
<td></td>
<td>Reading #17: Cyber-victimization and Cybersecurity in China</td>
<td>Handout/readings in Canvas</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reading #18: Cyber-threats and cybersecurity challenges: A cross-cultural perspective</td>
<td></td>
</tr>
</tbody>
</table>
### Part 5: Cyber-warfare
- Reading #19: Information and communications technologies, strategic asymmetry and national security
- Handout/readings in Canvas
- Quiz 3 will open on 11/13/2017 at 5 PM. Each quiz will be available for 48 hours

### Part 6: Integrative cases cybercrime organizations’ operations and firms’ and industry’s cybersecurity measures
- Reading #20: Banking on Availability
- Reading #21: Cybercrimes in the Former Soviet Union and Central and Eastern Europe: Current Status and Key Drivers
- Handout/readings in Canvas

### Academic Integrity Policy:
Students are expected to adhere to the Academic Integrity Policy on all assignments and tests. The syllabus will provide a link to the complete description of the Academic Integrity Policy as found in the UNCG Graduate Bulletin. [http://academicintegrity.uncg.edu/complete/](http://academicintegrity.uncg.edu/complete/)

**ATTENDANCE POLICY:** You are required to logon the Canvas at least once a week.

### Final Examination:
There will be no final proctored examination.

### Additional Requirements:

**Late Work Penalty**
Assignments may not be submitted late. Exceptions will be granted only in rare circumstances and be evaluated on a case-by-case basis.

**Expectations of Students**

Students in the Bryan School are also expected to adhere to the Student Code of Conduct. Further details may be found at http://academicintegrity.uncg.edu/complete/ and http://studentconduct.uncg.edu/policy/code/. The Bryan School has additional expectations and guidelines for students to follow which can be found at http://www.uncg.edu/bae/faculty_student_guidelines.pdf.

**Expectations of Faculty**

The Bryan School expects its faculty to conform to all existing UNCG codes and policies. These are found at http://provost.uncg.edu/faculty/h_section4.asp In addition, the Bryan School has expectations and guidelines for faculty to follow which can be found at http://www.uncg.edu/bae/faculty_student_guidelines.pdf.
Instructor Information

Nir Kshetri is Professor at Bryan School of Business and Economics, The University of North Carolina-Greensboro and a research fellow at Research Institute for Economics & Business Administration - Kobe University. Nir is the author of seven books. His 2014 book Global Entrepreneurship: Environment and Strategy (Routledge: New York) was selected as an Outstanding Academic Title by Choice Magazine. Nir has also published about 110 articles in various journals. Nir participated as lead discussant at the Peer Review meeting of the UN’s Information Economy Report 2013 and Information Economy Report 2015.

Nir was the winner of 2016 Bryan School Senior Research Excellence Award. He is a two-time winner of the Bryan School Teaching Excellence Award (2012 and 2008). Nir’s recent research related awards include Best Academic Paper Award at The Business and Entrepreneurship in Africa Conference (May 2013) and best paper award at the 5th International Conference on Information Systems and Economic Intelligence (2012). A 2012 study ranked him # 2 in terms of the number of articles published in Journal of International Management over a 13-year period (1998-2010). Nir received Emerald Literati Network Award for Excellence in 2013 and 2010. He is a two time winner of the Pacific Telecommunication Council’s Meheroo Jussawalla Research Paper Prize (2010 and 2008). Nir has been recognized by Business Week as a "prominent faculty" in 2013, 2014 and 2015.

Nir has travelled to about 100 countries. He has taught classes or presented research papers (over 165) at various national and international meetings/conference in Azerbaijan, Argentina, Belgium, Canada, Chile, China, Colombia, Croatia, Czech Republic, Denmark, Dominican Republic, Ecuador, Estonia, France, Germany, Greece, Guatemala, India, Indonesia, Italy, Japan, Lithuania, Macao, Malaysia, Mexico, Mongolia, Morocco, Myanmar, Nepal, New Zealand, Oman, Peru, Portugal, Rwanda, Romania, Serbia, Sri Lanka, South Africa, South Korea, Singapore, Sri Lanka, Sweden, Switzerland, Thailand, Taiwan, the Philippines, the U.K., the U.S., Tunisia, Turkey, Uganda and Vietnam. Nir has been interviewed and/or quoted in over 150 TV channels, magazines and newspapers.