Course Title: The Fundamentals of Cybersecurity  
Course Code: CS07  
Course Dates: March 31st - May 5th  
Instructor: Ahmed Banafa (Professor of Engineering, San Jose State University)

Course Summary:

The purpose of the course is to provide the student with an overview of the field of cybersecurity. In this course students will study the fundamentals of cybersecurity to understand how to identify and manage cyber threats. The course will help students assess and diminish vulnerabilities within an organization’s networks, systems, and data in order to protect the integrity, security, and confidentiality of the organization’s digital assets. General Cybersecurity Models, including CIA triad and the Parkerian Hexad Model, will be introduced, and legal, ethical, and professional issues in cybersecurity will be covered. Students will learn about cybersecurity hardware and software (firewalls, VPN, antivirus and anti-spyware, network monitoring tools) and will be introduced to intrusion detection and prevention systems, patch management, and incident response. The course includes a final project on designing and implementing a cybersecurity plan. Practical cases and real-world examples will be explored and discussed throughout the course. There are no prerequisites required.

*Please see course page for full description and additional details.

Grade Options and Requirements:

- No Grade Requested (NGR)
  - This is the default option. No work will be required; no credit will be received; no proof of attendance can be provided.
- Credit/No Credit (CR/NC)
  - Students must attend at least 80% of class sessions.
- Letter Grade (A, B, C, D, No Pass)
  - Students must attend at least 80% of class sessions and complete a piece of written work (to be discussed further in class).

*Please Note: If you require proof that you completed a Continuing Studies course for any reason (for example, employer reimbursement), you must choose either the Letter Grade or Credit/No Credit option. Courses taken for NGR will not appear on official transcripts or grade reports.
Tentative Weekly Outline:

Week 1 March 31st

Introduction and class policies
Introduction to Cybersecurity
Introduction to Risk Management
Case Study & Discussion (Sony)
Reading: Class Notes

Week 2 April 7th

General Cybersecurity Models
CIA triad, and the Parkerian Hexad Model
Case Study & Discussion (Target)
Reading: Class Notes

Week 3 April 14th

Legal, Ethical, and Professional Issues in Cybersecurity
Case Study & Discussion (Yahoo!)
Reading: Class Notes

Week 4 April 21st

Cybersecurity tools: hardware and software
Firewalls, VPN, Anti-Virus and spyware, and Network Monitoring tools
Case Study & Discussion (WannaCry)
Reading: Class Notes

Week 5 April 28th

Management of Cybersecurity Technology: Intrusion Detection
Prevention Systems, Patch Management and Incidents response.
Case Study & Discussion (Ukraine Power Grid)
Reading: Class Notes

Week 6 May 5th

Designing and implementing cybersecurity plans
Case Study & Discussions (Anthem)
Research Paper