CEHC 242: Cybersecurity

Day/Time: Tuesdays/5:45 pm – 8:35 pm

Location: SS 256

Instructor: Daniel Domkowski

Lecturer/TA: Eric Reimer

Contact: dan.domkowski@gmail.com/ddomkowski@albany.edu, epreimer@albany.edu

Office Location and Hours: Tuesdays/4:30 pm – 5:30 pm and 8:35 pm – 9:35 pm

Course Information:

Course Description:
The purpose of this class is to provide students with a comprehensive introduction to cybersecurity, including an understanding of key issues like cyber-attack types, models of thinking about cyber threats, functions like network security and incident response, cyber-crime, cyber conflict, and the implications of cybersecurity for enterprises and individuals. While much has been made of “cyber war” and high profile cyber-attacks like STUXNET, there are actually a broad spectrum of cyber threats and cyber threat actors that present problems for organizations and policy makers. We will look at how government agencies, private sector firms, organizations of all kinds, and even individuals assess and respond to the changing cyber security landscape. We will examine how they assess the risks they face, how they manage those risks through security procedures and practices, and how they mitigate the impact of attacks that do happen on their systems.

The course begins with some background, looking at a history and technical explanation of how the Internet has essentially become a digital battleground. The course will then transition to an overview, based on the perspective of the “attackers,” of the many cyber security threats facing people, organizations, and systems today. These range from data breaches to computer crime, and from website defacements to cyber-attacks on critical infrastructure. The course will examine the various stages or elements of a computer network intrusion, as well as how such intrusions are investigated or mitigated, using an in-depth case study based on Cliff Stoll's account following a Soviet KGB attacker.
From there, the course will look at how various organizations, industries, and agencies (from both the Federal government but also from state and local governments) respond to cyber threats and to cyber incidents.

Finally the course will examine the many ways in which technology and policy converge. This section looks at numerous mechanisms through which organizations and societies use policy, law, regulation and other tools to thwart cyber threats. In order for the world to combat malicious attacks, policymakers and technologists will need to come together to attempt to make policies and laws that both protect individuals, data, and public safety, but also do not inhibit technical and economic progress; a balancing act between many tensions that is far from simple.

**Required Readings (books only):**


**Assessment:**

First, students will complete four short assignments in response to a list of discussion questions and major comments (1-2 pages, double-spaced, 11-point font, one inch margins) and which should address to some degree all the readings for recent sessions (i.e., some questions drawn from each of the readings). The reading response papers must be submitted to Blackboard by midnight of the due date.

Second, students will be given two exams (Midterm and Final, see Dates below) with an essay/short answer format.

Lastly, students will be expected to attend and participate in class discussions on topics and readings, in-class assignments, and by asking questions.

The response papers, exams, and class participation all serve the following purposes:

1. They ensure that students have completed and reflected upon the reading prior to discussion.
2. They give the instructor a sense of the student’s understanding of the material and its relation to the field.
3. The questions and comments will facilitate the discussion of the material.

**Course Learning Objectives:**

Upon completion of this course, you should be able to accomplish the following activities:

1. Conduct a comprehensive assessment of cyber risks, generate an analysis of options for mitigating cyber risks, select the most appropriate mitigating actions for cyber risk, develop contingency and crisis response plans, communicate the risk assessment to a variety of audiences, and evaluate risk management plans.
2. Review and understand the legal, regulatory, policy, and ethical issues related to securing cyberspace; identify and evaluate cybersecurity threats to organizations; and analyze the effectiveness of cybersecurity in an organization by performing vulnerability assessments, risk mitigation, auditing, certification and accreditation of information systems.

3. Demonstrate understanding of the ethical principles in general and the ability to recognize, articulate, and apply ethical principles in concrete situations related to cybersecurity.

**Prerequisites:** There are no prerequisites for this class. Although it is not required, we recommend that students currently enrolled in the undergraduate major in Emergency Preparedness, Homeland Security and Cybersecurity enroll in CEHC101 Introduction to Emergency Preparedness, Homeland Security and Cybersecurity before taking this class.

**Grading:**
This course is A-E graded and the grades are determined based on the following criteria:
Writing Assignments: 10% each/40% total
Midterm Exam (10/18): 20%
Final Exam (12/20): 25%
Participation: 15%

**Collaboration:** Please refer to the course Blackboard site for all Announcements, Assignments, Readings, Grades, etc.

**Lecture and Reading Schedule:**

<table>
<thead>
<tr>
<th>Session</th>
<th>Subject</th>
<th>Topics</th>
<th>Readings</th>
</tr>
</thead>
</table>
| 1 1/24  | The Internet and Security | - Introduction to data networks and computer systems  
- Why are these systems vulnerable?  
- What does an attack mean?  
- The KGB, the Computer, and Me.  
https://www.youtube.com/watch?v=EcKxaq1FTac  
| 2 1/31  | Network Intrusions, Cyber Attacks, and Securing Data | - What is a network intrusion?  
- What are the elements of a network intrusion?  
- What steps can network administrators take to respond to such an intrusion?  
- The KGB, the Computer, and Me.  
https://www.youtube.com/watch?v=EcKxaq1FTac  
<table>
<thead>
<tr>
<th>Week</th>
<th>Assignment/Due Date</th>
<th>Topic</th>
<th>Subtopics</th>
<th>References</th>
</tr>
</thead>
</table>
| 3 2/7| Assignment 1 Due    | Who are Attackers and their Targets? | - Evolution of attackers  
- The kill chain model of intrusion  
- Hacker groups/hacktivist  
- Organized crime  
- Nation-states | - Mandiant. (2013) APT1: Exposing One of China’s Cyber Espionage Units.  
| 4 2/14| Assignment 1 Due | Vulnerabilities and Attack Vectors – Part I | - Web-based vulnerabilities and attacks  
| 5 2/21| Vulnerabilities and Attack Vectors – Part II | - Malware  
| 6 2/28| Individual and Data Security | - Data collection  
- Identity theft  
| 7 3/7| MIDTERM EXAM | Detection/Defense | - Tactics and behaviors  
- Products and best practices  
| 8 3/21| Assignment 2 Due | Cybersecurity and Government | - National security concerns around cybersecurity  
- Agencies and division of labor  
<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
<th>Key Points</th>
<th>References</th>
</tr>
</thead>
</table>
| 9 3/28 | Enterprise Cybersecurity and the Move to the Cloud | - Enterprise-scale attacks, defense, and incident response  
- Economics of cybersecurity at an enterprise level  
- Cloud Computing: SaaS, PaaS, and IaaS  
- CSA's Treacherous 12 Cloud Computing Threats  
| 10 4/4 | Cybersecurity, Infrastructure, and Cyber-Physical Systems | - SCADA/ICS  
- Criticality and Critical Infrastructure  
| 11 4/18 | Cyber Crime and Law | - Cyber Criminals  
| 12 4/25 | Policy and Management Part I | - Policy, plans, programs  
- Compliance  
- Security Frameworks  
| 13 5/2 | Policy and Management continued | - The NIST framework continued | - NIST Special Publication 800-53 |
| 14 5/9 | Future of Cybersecurity | - Internet of Things (IoT)  

**5/16**  
**FINAL EXAM**  
5:45 - 7:45 pm
Policies:

Attendance and Participation Policy: At the college level of education, the expectation is that students will attend every class session and actively participate in class every discussion each week. I expect students to have read and thought about the material assigned for that week. If language or some other barrier inhibits you from participating actively, you should meet with the instructor during the first two weeks of class to devise a solution. Attendance is not participation. Students missing a class session without prior approval of the instructor (or documentation of an emergency medical situation) will be penalized. UAlbany’s medial excuse policy can be reviewed at: http://www.albany.edu/health_center/medicalexcelse.shtml.

Disability Policy: Reasonable accommodations will be provided for students with documented physical, sensory, systemic, cognitive, learning and psychiatric disabilities. If you believe you have a disability requiring accommodation in this class, please notify the Director of the Disability Resource Center (Campus Center 137, 442-5490). That office will provide the course instructor with verification of your disability, and will recommend appropriate accommodations.

Academic Dishonesty Policy: Students are expected to comply with the University at Albany’s Community Rights and Responsibilities. An incident of unethical conduct (e.g. cheating, plagiarism) or classroom disruption will result in a Fail and referral to the appropriate Departmental and University Committees. More information on academic integrity is available at the following website: http://www.albany.edu/undergraduate_bulletin/regulations.html. Students will be asked to sign a statement of honor, promising to act with academic integrity.

Grade Complaint Policy: Students that feel their exams have been graded incorrectly should follow a three-step procedure. First, the student should carefully read the exam or assignment and identify the precise problem with the grading. Second, the student must send a written appeal explaining why their answer was appropriate to the instructor. Third, the instructor will meet with the student to discuss the appeal and resolve the conflict.