Course Summary and Objectives

Over the past two decades cybersecurity has transitioned from being the purview of computer nerds and information technology (IT) departments to requiring special knowledge, skills, and abilities. Similarly, cybercrime has undergone a series of radical shifts from any crime involving computers to the current definition which often focuses on computer network intrusions. Cybercrime currently involves a range tactics, techniques, and procedures (TTP) from the introduction of malware into networks through varying delivery mechanisms, to distributed denial of service (DDoS) and Structured Query Language (SQL) injection (SQLi) attacks. Motivations run the gamut from financial gain to notoriety, social activism, espionage, and revenge.

Preventing, mitigating, and responding to cyber incidents requires a thorough understanding of the risk equation, encompassing both the threats and the vulnerabilities. Company executives, managers, and communication liaisons, as well as the human resources, IT, finance, security, and legal departments, many of whom have limited experience with or understanding of incidents, are often involved in the response. By understanding the myriad cyber threats and motivations, leaders can guide organizations in accurately determining risks, minimize the potential for incidents, and, when necessary, provide more thoughtful responses to incidents.

This course will examine cybersecurity risk from the threat side of the risk equation. Students will be introduced to the different types of threats, with a special focus on today's actors, motivations, and TTPs, while gaining insight into the impact of cybercrime on victim organizations and employees. A variety of case studies will be used to study threats to organizations, why TTPs are chosen, and attack consequences. As a course in the Intelligence field, students will receive an introduction into intelligence analysis and receive a variety of tools to aid them in understanding the foundation of cyber threat intelligence (CTI).

Students attending this course should be familiar with the structure of the Internet and willing to learn technical information. This is not a technical course but the course will require students to understand technical information at a high-level.

Students with Disabilities
Reasonable accommodations will be provided for students with documented physical, sensory, systemic, medical, cognitive, learning and mental health (psychiatric) disabilities. If you believe you have a disability requiring accommodation in this class, please notify the Disability Resource Center (518-442-5490; drc@albany.edu). Upon verification and after the registration process is complete, the DRC will provide you with a letter that informs the course instructor that you are a student with a disability registered with the DRC and list the recommended reasonable accommodations.

Academic Integrity:
It is every student's responsibility to become familiar with the Standards of Academic Integrity at the University. Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity.
Plagiarism: Presenting as one's own work the work of another person (for example, the words, ideas, information, data, evidence, organizing principles, or style of presentation of someone else). Plagiarism includes paraphrasing or summarizing without acknowledgment, submission of another student's work as one's own, the purchase of prepared research or completed papers or projects, and the unacknowledged use of research sources gathered by someone else. Failure to indicate accurately the extent and precise nature of one's reliance on other sources is also a form of plagiarism. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly, or creative indebtedness, and the consequences for violating University regulations.

Grading:

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Component</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>20%</td>
<td>Class Attendance and Participation.</td>
<td>Attendance is expected. If you know you’re going to be absent, notify the professor. Participation is expected and includes both participation in lecture and in group activities and exercises. <a href="#">University Medical Excuse Policy</a></td>
</tr>
<tr>
<td>25%</td>
<td>Homework Assignments.</td>
<td>A variety of homework assignments will be given throughout the semester. Completing these is vital to understanding and participating in the class.</td>
</tr>
<tr>
<td>25%</td>
<td>Case Studies.</td>
<td>Three assigned case studies.</td>
</tr>
<tr>
<td>20%</td>
<td>Case Analysis Term Paper.</td>
<td>1-page proposal due at 3rd class; paper due 2nd to last class.</td>
</tr>
<tr>
<td></td>
<td>• Grad students – 6-8 pages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Undergrad students – 4-6 pages</td>
<td></td>
</tr>
<tr>
<td>10%</td>
<td>Case Analysis Presentation</td>
<td>• Grad students – a 7-minute presentation of their case study</td>
</tr>
<tr>
<td></td>
<td>• Undergrad students – a 5-minute presentation of their case study</td>
<td></td>
</tr>
</tbody>
</table>

Office Hours
Office hours are before and after class and by appointment.

Class Content, Readings, and Homework Assignments:
All readings and homework assignments are subject to change due to ongoing events and reports and will be posted on Blackboard.

Class Schedule:
1st Class - Class introduction
• What is cybersecurity? Cybercrime?
• Cyber risk equation
• What are the types of cyber threats? Why do they matter?
• What is intelligence analysis? What is CTI? How do they compare?
• Standards, practices, and models in CTI

2nd Class – Biases, Mindsets, and Assumptions
• What are our biases, mindsets, and assumptions? How do they affect our responses?
• Words of Estimative Probability
• What tools can we use to prevent, be aware of, or offset them?

3rd Class – TTPs and Terminology
• What are the common TTPs and vectors?
• How does understanding TTPs help an organization?
• Other terminology
• Quadrant analysis

4th Class – Cybercriminals and Monetizing Cybercrime
• How do you monetize the different TTPs?
• Who are the actors responsible for the majority of US financially-motivated compromises?
• Who is most at risk? Why? From which TTPs?
• Key Assumptions Check

5th Class – Hacktivism
• Who are hacktivists? What motivates them?
• When is hacktivism wrong? When is it right?
• Who is most at risk? Why? From which TTPs?
• Quality of Information Check

6th Class – Insiders
• What is the threat?
• What insiders pose cyber threats? Why?
• Who is most at risk? Why? From which TTPs?
• Brainstorming

7th Class – Terrorists
• What is the threat?
• Who are the actors behind the threat?
• Who is most at risk? Why? From which TTPs?
• What is critical infrastructure?
• High-impact/low-probability analysis (black swan events)

8th Class – Nation-State Actors: Russia and China
• What is the threat?
• Who are the actors behind the Russian and Chinese nation-state threat?
• What do they want?
• Who is most at risk? Why? From which TTPs?
• Red teaming/Mirror imaging

9th Class – Nation-State Actors: Iran and North Korea
• What is the threat?
• Who are the actors behind the Iranian and North Korean nation-state threat?
• What do they want?
• Who is most at risk? Why? From which TTPs?
• Signposts of Change

10th Class – Criminals and Cybercriminals – Everyone else (4/16)
• Which criminals are using cyber TTPs? Which TTPs? For what purpose?
• Which cybercriminals are motivated by something not already discussed?
• “What if?” Analysis

11th Class – Intelligence Challenges and Failures
• What makes intelligence analysis and CTI so difficult?
When does it go wrong?
What can you do about it?
Analysis of Competing Hypothesis (ACH)

12th Class – CTI in the Government
- Which agencies are responsible for CTI for the U.S. government?
- What do they produce?
- What do they do with what they produce?
- How can you make CTI actionable?

13th Class - Ethics, and Ramifications
- What ethics apply when dealing with malicious cyber actors?
- Is back-tracking/back-hacking ethical?
- What are the ethics of victim notification?
- What happens after your decision?

Final Exam period – Individual Case Study Presentations