Course Summary and Objectives
Over the past two decades cyber crime has undergone a series of radical shifts, from being the purview of computer nerds to any crime involving computers, to the current definition which often focuses on computer network intrusions. Cyber crime currently involves a range of 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.

A comparable shift is ongoing within organizations, as they struggle to adapt to the changing dynamics of cyber crime. In the early 2000’s cyber crime was the purview of information technology (IT) employees and solved through the use of antivirus software and reimaging computers. Today, preventing, mitigating and responding to cyber crime incidents requires coordination among 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. Law enforcement and public safety personnel, including intelligence analysts, risk analysts, and public managers, must find ways to aid targeted organizations and support victims within the constraints of law enforcement and homeland security functions ill-equipped to handle digital innovations.

By understanding the myriad cyber threats and actor motivations, leaders can guide organizations in accurately accessing threats, risks, and vulnerabilities, to minimize the potential for incidents and, when necessary, provide more thoughtful responses.

This course will examine cyber crime from different angles to introduce students to today's actors, motivations, TTPs, and mitigation techniques, while providing insight into the impact of cyber crime on victim organizations and employees. A variety of case studies will be used to study how TTPs are applied, and aid students in understanding attack consequences, responding agency abilities, and the various protection, mitigation, and remediation measures. The objective of the course is to provide students with a foundation for understanding the cyber threat intelligence so they can lead their organization in the prevention, mitigation, and remediation of cyber attack. Students attending this course should be familiar with the structure of the Internet and willing to learn technical information. This will not be a technical course, but will require students to understand technical information at a high-level.

Grading:

<table>
<thead>
<tr>
<th>Graduate Level</th>
<th>Undergrad Level</th>
<th>Class attendance and participation. Attendance is expected. More than 2 absences will result in a deduction in your Attendance and Participation grade. 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.</th>
<th>Homework assignments. A variety of homework assignments will be given throughout the semester. Completing these is vital to understanding and participating in the class.</th>
<th>Case Studies.</th>
</tr>
</thead>
<tbody>
<tr>
<td>20%</td>
<td>15%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20%</td>
<td>20%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30%</td>
<td>30%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Grad students – 5 assigned case studies of 3 pages each. Undergrad students – 4 assigned case studies of 2 pages each.

20% 25%

**Case Analysis Term Paper.**
Grad students – 6-8 pages; 1 page proposal due at 3rd class; Paper due 2nd to last class.
Undergrad students – 4-6 pages; 1 page proposal due at 3rd class; Paper due 2nd to last class.

10% 10%

**Case Analysis Presentation**
Grad students – a 7-minute presentation of their case study, from the viewpoint of the victim company.
Undergrad students – a 5-minute presentation of their case study, from the viewpoint of the victim company

---

**Class Content, Readings, and Homework Assignments:**
*All readings and homework assignments are subject to change due to ongoing events and reports.*

**1st Class - Class introduction**
- What is cyber crime? What is not cyber crime?
- What can’t anyone agree on anything about cyber crime?
- What is cyber threat intelligence?
- How do we conceptualize cyber crime?
  - .

**2nd Class - TTPs**
- How does understanding TTPs help an organization before they are attacked?
- What are the common TTPs and vectors?

**3rd Class – Monetizing Cyber Crime**
- Where is the money in the different TTPs?
- Who are the actors responsible for the majority of US financially-motivated compromises?
- Which TTPs do they prefer?

**4th Class – Hacktivism**
- Who are the hacktivists? What motivates them?
- When is hacktivism wrong? When is it right?

**5th Class – Nation-state actors and Red Teams**
- Who conducts CNE and for what purposes?
- Which actors pose the greatest threat toward US organizations?

**6th Class – Insiders**
- What types of insiders pose cyber threats?
- What cyber threats do they pose?

**7th Class – The “security” in “cybersecurity”**
- How do you protect data?
- What agencies work cyber crime matters?
- How can physical security affect cybersecurity?
- Is anything truly anonymous?
Why is the ability to conduct anonymous activity over the Internet good? Bad?

8th Class – Critical Infrastructure and Key Resources (CIKR), Industrial Control Systems (ICS), and Internet of Things (IoT)
- How does cyber activity affect CIKR? ICS? IoT?
- Should cyber infrastructure be CIKR?
- What are the challenges in cyber regulations and how can they be overcome?

9th Class – Disruptive and emerging technology
- What are disruptive and emerging technologies?
- What roles will disruptive and emerging technologies play in defining the business landscape in the next 1-3 years? 3-10 years?
- How does cyber crime prediction reporting differ from those in other fields?

10th Class - Biases, mindsets, assumptions, and uncertainty
- How do our biases, mindsets, and assumptions affect our responses?
- How do the biases, mindsets, and assumptions of malicious actors affect their activity?
- Why do cybersecurity reports vary so greatly? Can we use the uncertainty in cybersecurity to our advantage?

11th Class –Cyber Ethics
- What ethics apply when dealing with malicious cyber actors?
- Is back-tracking/back-hacking ethical?
- What are the ethics of victim notification?

12th Class – Capstone exercise
- Students, in small groups, will participate in a capstone table top exercise. Each group will work together to apply what they have learned during the class to a real-life scenario, culminating in a group paper describing how their fictitious company would respond to the threat.

13th Class – Individual Case Study Presentations and Final Discussions