**Principles and Practices of Cybersecurity**  
RPAD 545

**Course Summary and Objectives**  
Cybersecurity threats are global, persistent, and sophisticated. They touch almost every aspect of our lives and securing technology is fundamental to our ability to work and play. In fact, the White House has clearly and repeatedly identified cybersecurity as one of the most important challenges that we face as a nation. And we do face it as a nation.

Efficient and effective cybersecurity begins at the design level for every protocol and piece of software, continues through the supply chain, to deployment, and the destruction of old equipment. It requires coordination among company executives, managers, IT staff, and regular employees, as well as the human resources, finance, purchasing, security, and legal departments. Every employee, third-party providers, and the supply chain all have to work together to make cybersecurity a success. By understanding the myriad components, leaders can guide organizations in accurately accessing threats, risks, and vulnerabilities, to determine acceptable risks, minimize the potential for incidents, and, when necessary, provide thoughtful responses.

This course will provide students with a comprehensive understanding of the principles and practices of cybersecurity. Starting from the ground up, the class will examine cybersecurity from different angles to introduce students to and provide insight into the way cybersecurity can impact organizations and employees. Students will be exposed to today's key concepts and issues through lectures, discussions, and case studies in this continual developing domain.

This is not a technical course, but will require students to learn technical concepts.

**Grading:**

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>20%</td>
<td><strong>Class attendance and participation.</strong> 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.</td>
</tr>
<tr>
<td>15%</td>
<td><strong>Homework assignments.</strong> 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><strong>Case Studies.</strong> 5 assigned case studies of 4 pages each.</td>
</tr>
<tr>
<td>25%</td>
<td><strong>Capstone Exercise and Paper.</strong> 6-8 pages; group assignment.</td>
</tr>
<tr>
<td>15%</td>
<td><strong>Midterm Exam</strong></td>
</tr>
</tbody>
</table>

**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.
1st Class - Fundamentals
- What is cybersecurity? What is the difference between “cyber” and information technology?
- What are we protecting?
- Who are we protecting it from?
- NIST, Critical Security Controls, CIA triad, device and network basics, actors, computers/networking/Internet 101

2nd Class – Threats, Vulnerabilities, and Exposures
- What is the difference between a threat, vulnerability, and exposure?
- What are common cybersecurity risks and how do we protect against them?
- TTPs, CVEs, patching and patch management, intro to actors, defensive and active security

3rd Class – Cyber Threat Actors
- Who are the current cyber threat actors?
- What are their motivations, skills, capabilities, and targets?

4th Class – Defensive Cybersecurity
- What can passive and active cyber defense do for an organization?
- How do you implement each?
- Access control, identity management, backups, antivirus, anti-spam, IDS/IPS, firewalls, proxy servers

5th Class – Active Cybersecurity & Incident Response
- What is active cybersecurity and what can it do for an organization?
- How do you implement it?
- How can you test for cybersecurity?
- What is an incident? How do you respond? Who should respond?
- Vulnerability assessments, pen testing, auditing, takedowns, actor tracking, striking back, Forensics, reimaging, sandboxing, out of the box solutions, evasion techniques

6th Class – MidTerm Exam and Policies, Procedures, & Education
- MidTerm Exam
- What should policies and procedures cover?
- What is enforceable?
- How do you educate and train employees?
- Continuity of Operations Plans, BYOD, cloud, IOT, remote employees, data ownership, data retention, law enforcement cooperation, travel, etc.

7th Class – Physical Security & the Expansion of the Network
- MidTerm Exam Review
- 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?
- Physical security of systems and networks, hot and cold sites, mobile devices and BYOD, cloud computing, IoT, wearables, drones, bitcoins

8th Class – Securing and Hiding Data
- How and when should data be secured?
• How secure is secure?
• Data evaluation and risk ranking, cryptography, hashing, encryption, steganography, best practices vs. recommendations vs. standards, wireless security algorithms

9th Class - Information Sharing & Cyber Threat Intelligence
• What information is useful to share? Who should be sharing it? With whom?
• How do you make cyber threat intelligence actionable?
• Indicators of compromise, STIX/TAXII, strategic/operational/technical intelligence, automating information sharing

10th Class – Cybersecurity in Government
• Who is responsible for security, standards, assets, response?
• Is the ‘big brother’ approach the right approach?
• Should information be shared? If so, to whom?
• DHS, FBI, USSS, NSA, NCCIC, US-CERT/ICS-CERT, NCJTF, NIST, Congress, GAO, Fusion Centers, ISACs, ISAOs, critical infrastructure, state and local law enforcement

11th Class – Ethics & Privacy
• What ethics apply when dealing with cybersecurity?
• What should you do with information you receive?
• When there an expectation of privacy?

12th Class – Capstone Table Top Exercise – Responding to an Incident

13th Class – The Future
• What will be the major issues tomorrow?
• How do these changes effect the cybersecurity environment?
• Biometrics, two-factor authentication, the demise of antivirus and passwords, large data, supply chains and third-party providers, lack of trained cybersecurity professionals, government involvement, critical infrastructure, cyber warfare