Principles and Practices of Cybersecurity  
CEHC/RPAD 445/545

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 assessing risks, and vulnerabilities, determining acceptable risks, minimizing the potential for incidents, and, when necessary, providing 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. Through lectures, discussions, and case studies students will be exposed to strategic cybersecurity concepts and gain a foundational understanding of how cybersecurity issues work within the business environment.

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

Grading:

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

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

4th Class – Data
- What needs to be protected?
- Where does it come from and where does it go?

5th Class – Securing and Hiding Data
- How and when should data be secured?
- How secure is secure enough?

6th Class – Defensive Cybersecurity
- What can passive and active cyber defense do for an organization?
- How do you implement each?

7th 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?

8th Class – Physical Security & the Expansion of the Network
- How does cybersecurity integrate with physical security?
- How is the expansion into the Internet of Things (IoT) and Industrial Control Systems (ICS) changing cybersecurity?
- What can/should employees be responsible for?

9th Class – Policies, Procedures, & Education
- What should policies and procedures cover?
- What is enforceable? How?
- How do you educate and train employees?

10th Class – Midterm Exam and Government
- Midterm Exam
- Who in the government works on cyber matters and what are they responsible for?
- Who is responsible for using the information?
- Is the ‘big brother’ approach to cybersecurity the right approach?

11th – Information Sharing & Cyber Threat Intelligence
- Midterm Exam Review
- What information is useful to share?
• Who should be sharing it? With whom?
• How do you make cyber threat intelligence actionable?
• How do you automate information sharing?

12th Class – Ethics & Privacy
• What ethics apply when dealing with cybersecurity?
• What should you do with information you receive?
• When there an expectation of privacy?

13th Class – The Future
• What will be the major issues and technologies tomorrow?
• Are they emerging or disruptive?
• How do these changes effect the cybersecurity environment?

14th Class – Capstone Table Top Exercise – Responding to an Incident

Final Class – Capstone Table Top Exercise Presentation