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 safely. In fact, the White House has clearly and repeatedly identified cybersecurity as one of the most important challenges that we face as a nation.

Efficient and effective cybersecurity requires coordination among company executives, managers, IT staff, and regular employees, as well as the human resources, finance, purchasing, security, and legal departments. Cybersecurity begins with the thoughtful understanding of the risk to different components, and rapidly expands to include a myriad of technologies, people, and resources that must work together to be successful. It is often said, “the bad guys only have to get it right once, we [cybersecurity experts] have to be right 100% of the time.” By understanding the myriad components, in the context of recognized frameworks, leaders can guide organizations in accurately assessing risks, threats, vulnerabilities, and exposures, determining acceptable (and legal) defenses, minimizing the potential for incidents, and, when necessary, providing efficient and effective responses.

This course will provide students with a comprehensive knowledge and 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, case studies, and group students will be exposed to strategic cybersecurity concepts, high-level technical ideas, and gain a foundational understanding of cybersecurity issues in the business environment.

This is not a technical course. However, students should come prepared to learn technical concepts at a high level.

Pre-requisites:
There are no pre-requisites. Undergraduate students must be at least Juniors.

Office Hours
I do not have an office on campus. Therefore office hours are before and after class, in the classroom, as needed. If you need additional time or a different day, we will arrange something mutually convenient for us both, on campus or via telephone.

Grading:

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>20%</td>
<td>Class attendance and participation. Attendance is expected. If you know you’re going to be absent, notify me in advance. Participation is expected and includes participation in the lecture, group activities, and classroom exercises. University Medical Excuse Policy</td>
</tr>
<tr>
<td>15%</td>
<td>Homework assignments. A variety of homework assignments will be given throughout the semester. Completing these is vital to understanding and participating in the class. Assignments are due at the start of class. There is a 20</td>
</tr>
</tbody>
</table>
point penalty for late homework assignments.

| 20% | **Case Studies.** There will be 2 assigned case studies during the semester. Case Studies are due at the start of class. There is a 20 point penalty for late case studies. |
| 20% | **Midterm Exam.** The date of the midterm will be announced the first day of class. If a student provides adequate notification of a reasonable excuse to miss the midterm exam, a make-up exam may be administered at a time of the instructor's choosing. |
| 25% | **Capstone Exercise and Paper.** This will be a group-based table top exercise (TTX) requiring attendance during the last two classes and a presentation during the final exam period. There is no make-up period for the presentation. |

**Readings and Homework Assignments:**
All readings and assignments are subject to change due to ongoing events and will be posted on Blackboard. Reading material will be available through the Internet and does not require purchase of a book. In some cases, the readings may be made available on Blackboard for your convenience or the readings may consist of watching instructional videos.

All assignments are to be submitted via email to the Professor, before class starts, unless otherwise noted. Assignments should include, at a minimum, the student's name, date the assignment was given, class number, and complete answers to the all questions posed. Arial 11pt font, single-spaced text is preferred. Assignment grades are based on the student's thoroughness in answering the assigned questions and inclusion of class and reading content. Proper citations are required.

**Additional Readings:**
A list of additional, optional, sources of material will be provided on the first day of class.

**Incomplete Grades:**
For undergraduate students: [https://www.albany.edu/undergraduateeducation/grading.php](https://www.albany.edu/undergraduateeducation/grading.php).
For graduate students: Incomplete: A tentative grade given only when the student has nearly completed the course but due to circumstances beyond the student's control the work is not completed on schedule. The date for the completion of the work is specified by the instructor. The date stipulated will not be later than one month before the end of the session following that in which the Incomplete is received. The grade I is automatically changed to E or U unless work is completed as agreed between the student and the instructor. [https://www.albany.edu/graduatebulletin/requirements_degree.htm#graduate_grades](https://www.albany.edu/graduatebulletin/requirements_degree.htm#graduate_grades).

**Class Content:**
**Fundamentals**
- What is cybersecurity? What is the difference between cybersecurity and information technology?
- Why does it matter?

**Business and Data**
- What needs to be protected?
- Where does it come from and where does it go?
- Business impact analysis
- Networking basics
Actors, Threats, Vulnerabilities, and Exposures
- Who are we protecting our space from?
- What is the difference between a threat, vulnerability, and exposure?
- How do the actors, threats, vulnerabilities, and exposures change depending on the data?

Defensive Cybersecurity
- What can passive and active cyber defense do?
- How and when should data be secured?
- How secure is secure enough? How can you test for cybersecurity?
- Cybersecurity models, maturity concepts, access controls, and the sliding scale
- Planned responses

Protective Techniques
- Tools, devices, and technical details
- What is reasonable to implement in different environments?

Physical Security, the Supply Chain, & the Expansion of the Network
- How does cybersecurity integrate with physical security?
- Why does the supply chain matter and how can you deal with it?
- How are the Internet of Things (IoT), as-a-Service options, and Industrial Control Systems (ICS) changing cybersecurity?

Policies, Procedures, & Education
- What should policies and procedures cover?
- What is enforceable? How?
- What can/should employees be responsible for?
- How do you educate and train employees?

Offense & Incident Response
- What is offensive cybersecurity and what can it do for an organization?
- What is an incident? How do you respond? Who should respond?
- How do you recover afterwards?

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

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?

The Future
- What will be the major issues and technologies tomorrow?
- Are they emerging or disruptive?
- How do these changes effect the cybersecurity environment?
- Cybersecurity careers – own week if I have a 14th class

**Ethics & Privacy**
- What ethics apply when dealing with cybersecurity?
- What should you do with information you receive?
- When there an expectation of privacy?

**Students with Disabilities**
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 130, 518-442-5490, DRC@albany.edu). That office will provide the course instructor with verification of your disability, and will recommend appropriate 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. Further resources are available through the University Library’s [online system](#).

**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.

*Stacey A. Wright*
*January 2019*