Master of Science in Cybersecurity Risk and Strategy

NYU LAW NYU TANDON SCHOOL OF ENGINEERING

Information Systems Security Engineering and Management

Professor: M.J.Vaidya, mjv312@nyu.edu
Teaching Assistant: Anshita Lalwani, al5764@nyu.edu

COURSE OVERVIEW

This course presents a system and management view of information security: what it is, what drives the requirements for information security, how to integrate it into the systems-design process and life-cycle security management of information systems. A second goal is to cover basic federal policies on government information security and methodologies. Topics include information-security risk management, security policies, security in the systems-engineering process, laws related to information security and management of operational systems.

PREREQUISITES

This course will not be about the technologies of information security, but how those technologies are integrated into a system and managed. A broad (but not detailed) knowledge of information security technologies is assumed. A working understanding of common security threats and defensive technology from professional experience is sufficient.

LEARNING OBJECTIVES

By the end of this course students should be able to:

- Describe a management view of cybersecurity
- Enumerate and illustrate the general principles of risk analysis
- Explain fundamentals of business continuity management and how it can help address security incidents
- Analyse security components within organisational contest: identity and access management, data protection, security operations, etc.
- Create a plan for the third party risk assessments
- Apply this course knowledge to develop the system security strategy in practical cases

COURSE STRUCTURE

This course is conducted online, which means you do not have to be on campus to complete any portion of it. You will participate in the course using NYU Classes located at https://newclasses.nyu.edu.

Master of Science in Cybersecurity Risk and Strategy

NYU LAW NYU TANDON SCHOOL OF ENGINEERING

COURSE COMMUNICATION

WEEKLY VIRTUAL OFFICE HOURS

Professor normally will be available electronically to answer questions, resolve problems, and provide guidance Wednesday (6pm – 8pm EST), and other times as his schedule permits.

Please do not post questions to the weekly required discussion topic boards each week—they should only be used for the specific discussion questions. Please send course related email that is not of interest to the class to professor at mjv312@nyu.edu

TA Name - Anshita Lalwani
Availability – Tuesday – Saturday (5pm-8pm EST)
TA email –al5764@nyu.edu

RECOMMENDED READINGS

Textbooks: There is no textbook that covers even most of the material in this course in a complete manner. One book is useful for both the material in this course, and as valuable references for security professionals. Reading assignments will be made in each of these books, and other references will be found on the web.

Required: Whitman and Mattord, *Management of Information Security*, Sixth Edition, ISBN-13: 978-1337405713, ISBN-10: 133740571X, Cengage Learning, 2019.

- A good, general reference for risk analysis, policy, standard security management processes
- In my view, does not properly reflect the system view

Other References: Various web sites, etc. are listed on a per lecture basis.

STUDENT RESPONSIBILITIES

1. Course Organization: This course is an online course, with a new lecture available each week. Readings are checked via the weekly quizzes. Homework assignments and mandatory discussion topics are also posted at the same time. A team term project is also required. There are no examinations.
2. Term Project: The term project is carried out by teams of 3-4 students. Students work in their Capstone Groups and select projects within the guidelines presented in the lectures, but the instructor retains the right to approve projects. Final deliverable will be a 20-page executive summary presentation.
3. Each team should send the instructor email describing the proposed project briefly (by week 2). Project proposal (final version due week 3): It should include a Project Objective, Mission Statement, Outline, a High Level Approach, and What the Project expects to achieve. Initial draft of (by week 6) should be emailed to the instructor. This is for a very informal review and check that the project is off to a good start.
4. There is a mandatory project review in week 9, a final review the last week of class, and a final report due for each team's project on the week following the final presentation.

5. Homework: Homework is due eight days following the posting date. Extensions will be granted for holiday weeks, and for the first assignment which is due in two weeks (along with the second assignment).
6. Threaded Discussions: Participation at least ***twice*** in ***one*** mandatory, online discussion each week must be completed by the Saturday following the posting date. This is **a total of 2 posts per week**. Extensions will be granted for holiday weeks and the first week of the semester.
7. Reading Assignments and Webliography. Each week, there will be reading assignments that either supplement or provide the basis for parts of the lecture. You are responsible for the material in the reading assignments. In addition, the Webliography includes references with more depth or interesting examples related to the lecture. These are not all required reading, but it is recommended that you at least take a quick look at these references to become familiar with valuable resources for projects and for your careers. Readings from the webliography that are required will be given with the homework assignment each week; others are optional references or side interest articles.

GRADING POLICY

The course grade is based on the project (40%), homework (40%), discussion participation (15%) and reading/attendance (5%). The Grading scale will depend on instructor's rubrics for grading. The course follows the Program Academic Policy listed in the Student Handbook. If you are concerned about your performance during the semester contact me as soon as possible so I can help you to earn a better grade.

LEARNING TIME RUBRIC

Learning Time Element	Asynchronous* / Synchronous**	Time on Task for Students (weekly)	Notes
Lecture	Asynchronous	1.5 hours	Video format. Expect quizzes throughout the module.
Weekly Discussion Board	Asynchronous	0.5 hour	Students are expected to post initial response to weekly topic questions. See Interaction Policy.
Assessment (homework)	Asynchronous	1 hour	Students submit their assignment by [the end of the week]
Reading Assignment	Asynchronous	1 hour	Reading assigned textbook chapters and journal articles.
Webinars	Synchronous	1 hour	Weekly in a web conferencing software.
Group Project	Synchronous/Asynchronous	1 hour	Work [with group members] on the class project.

*Asynchronous learning is defined as any non-real time student learning, such as recorded lecture, podcast, interactive module, articles, websites, etc. This also includes any student-to-student or faculty-to-student communication that may happen with an asynchronous tool, such as discussion board, chatroom, e-mail, text, etc.
**Synchronous learning is defined as any real-time student-to-student and/or faculty-to-student learning, such as a live webinar session or other video/audio communication service.

COURSE INTERACTIONS

Announcements -
Announcements will be posted on NYU Classes on a regular basis. You can locate all class announcements under the *Announcements* tab of our class. Be sure to check the class announcements regularly as they will contain important information about class assignments and other class matters.

Email –
You are encouraged to post your questions about the course in the Forums discussions on NYU Classes. This is an open forum in which you and your classmates are encouraged to answer each other's questions. But, if you need to contact me directly, please email me at mjv312@nyu.edu, CC the course TA at al5764@nyu.edu. You can expect a response within 48 hours.

Weekly Discussion Forums –
Discussion forums are an excellent way for you to engage with the course material and with your peers. Each module will have an accompanying discussion board question posted in the *Forums* tab. You are expected to read the discussion boards and engage in thoughtful discussions. I will read all discussion posts and provide content clarification and feedback when necessary.

Weekly Virtual Meetings –
Once a week, we will hold a virtual class meeting through the *Meetings* tool on NYU Classes. This weekly meeting is an opportunity for you to ask questions and gain clarification about the course content from myself and your peers. You are highly encouraged to attend these meetings. I understand that not all students will be available to attend these virtual meetings. Due to this fact, the meetings will be recorded so you can watch them when you are available.

Netiquette –
When participating in an online class it is important to interact with your peers in an appropriate manner. Always use professional language (no netspeak) in your discussion board posts and emails. Please be respectful of your classmates at all times even if you disagree with their ideas.

Interaction Policy

You are required to be an active online learner in this course and expected to participate in the Active Learning Modules, weekly discussion boards, weekly virtual meetings, etc.

Moses Center Statement of Disability:
If you are student with a disability who is requesting accommodations, please contact New York University's Moses Center for Students with Disabilities (CSD) at 212-998-4980 or mosescsd@nyu.edu. You must be registered with CSD to receive accommodations. Information about CSD can be found at www.nyu.edu/csd. It is located at 726 Broadway on the 2nd floor.

Master of Science in
Cybersecurity Risk and Strategy

NYU LAW NYU TANDON SCHOOL OF ENGINEERING

COURSE OUTLINE

The project team plans to produce one self-contained active module for each topic. Approximate length to complete each lesson will vary. As long as this approximate length is clearly indicated to students before they begin each lesson, this should have no impact on the efficacy of instruction. Students will need to complete the lessons in the following order:

1. **Introduction**
   - Fundamentals of information security management - course overview and expectations.
   - Term project approach goals, teaming, and expectations.
   - Weekly discussion topic and assignment.
   - ISM & Law

2. **IS program, policy management, and security governance. Information security program**
   - Security policy management.
   - Security governance.

3. **Business priorities, secure development, and training & awareness**
   - Business priorities and information security risks.
   - Integrating security into software development process.
   - Security training and awareness.

4. **Cyber threats and information security risks**
   - Cyber Threats, including motivation, trends, and threat monitoring
   - General principles of risk analysis

5. **IT risk analysis, risk management, and security risk metrics**
   - Major steps of risk analysis (probability, impact, prioritization, etc.).
   - Approaches to managing risks (reduction, mitigation transfer, and acceptance).
   - Managing risk with metrics.

6. **Identity and access management (IAM)**
   - What is it? Identity and access management approach.
   - IAM service components (manage access, enforce access, report access)
   - IAM reference architecture and strategy

7. **Data protection**
   - Identifying critical assets / data classification (data elements, PII, process)
   - Data loss prevention (data in motion, data at rest, and data at endpoint)
   - Data privacy (privacy laws, data flow, data inventory, integrated framework)

8. **Incident response planning and business continuity**

- Security incident response planning (prepare, identify, assess, contain, investigate, resolve, learn).
- Business Continuity Planning: making sure the organization can continue functioning after a security incident.

9. **Term Project Preliminary Gate Review**
   - Each team will present their preliminary (high level) project approach for instructor feedback and guidance.

10. **Third party risk management**
    - Third party risk management.
    - Third party risk assessment.

11. **Security monitoring**
    - Security monitoring overview and how it can help manage risk.
    - Overview of security monitoring data, logging requirements, and monitoring tools.

12. **Cloud security models (SaaS, PaaS, IaaS)**
    - Cloud security concerns and risks.
    - Which applications and data can be migrated to the Cloud?
    - Impact to traditional security management.

13. **Mobile security, outsourcing, auditing**
    - Approaches to securing mobile devices
    - Emerging challenges, including Bring your own device (BYOD)
    - Overview of managed security services.
    - Evaluation and assurance and information security audits.

14. **Term Project Final Gate Review**: each team will present their final (detailed) project design for class discussion and instructor feedback. Final deliverable will be a 20-page executive summary presentation.

    - This review is essentially an outline of the project final report.
    - Complete Term Project Report is due during the week following the final project presentation.

Total Lessons: 14