Information Security Management

MASY1-GC 3220 | 102 | Spring 2024 | 01/24/2024 - 05/01/2024 | 3 Credits

Modality: In-Person

Course Site URL: https://brightspace.nyu.edu

General Course Information

Name/Title: Anthony Candeias, Adjunct Instructor
NYU Email: adc7@nyu.edu
Class Meeting Schedule: 01/24/2024 - 05/01/2024 | Wednesday | 06:20pm - 08:55pm
Class Location: TBD
Office Hours: By appointment, please email to make one.

Description

This course focuses on the importance of protecting data and information in today's digital world as related to strategy and policy, awareness, data classification, ownership and accountability, monitoring, and reporting. The course covers network components that comprise the environment, where the data are input, processed, and stored, and how the data travel through the Intranet, Extranet, and/or Internet. Upon completion of the course, students learn to assess the impact of data in the digital world, considering the steps that the Government, Corporations, and the Private Sector take to protect information assets. Students gain an understanding of the components that comprise network security and how each component provides protection. They become familiar with preventative and detective tools such as anti-malware, ACL, virus protection, cryptography, intrusion detection, audit logs, logical and physical controls and perform information risk assessments.

Prerequisites

1240 - Information Technology and Data Analytics

Learning Outcomes

At the conclusion of this course, students will be able to:
Apply the key principles of information security to the value of data and technologies in the digital world
Analyze different security frameworks used by Government, Corporations, and the Private Sector to protect digital asset
Design a digitally secure environment to protect business information assets
Justify how each digital security component provides protection from threats
Support the decision to select and use preventive, detective, and responsive security elements
Perform information security risk assessment to quantify and address high-risk occurrences

Communication Methods

Be sure to turn on your NYU Brightspace notifications and frequently check the “Announcements” section of the course site. This will be the primary method I use to communicate information critical to your success in the course. To contact me, send me an email. I will respond within 24 hours.

Credit students must use their NYU email to communicate. Non-degree students do not have NYU email addresses. Brightspace course mail supports student privacy and FERPA guidelines. The instructor will use the NYU email address to communicate with students. All email inquiries will be answered within 24 hours.

Structure | Method | Modality

This course is in-person and will meet once a week on Monday. NYU Brightspace is the learning management system we will use.

Active learning experiences and small group projects are key components of the course. Assignments, papers, and exams will be based on course materials (e.g., readings, videos), lectures, and class discussions. Course sessions will be conducted synchronously on NYU Zoom, which you can access from the course site in NYU Brightspace.

This course is Online and will meet once a week on Friday, with assignments, announcements, and emails being sent through Brightspace. Zoom is the remote instruction platform used at NYU. Students are expected to check email and/or Brightspace at least twice a week for announcements concerning assignments, class changes or cancellations, and other important information. The course will involve lectures/discussions/forum discussions as well as case studies. Two major papers/projects are required that will both be done on an individual basis.

Expectations

Learning Environment

You play an important role in creating and sustaining an intellectually rigorous and inclusive classroom culture. Respectful engagement, diverse thinking, and our lived experiences are central to this course and enrich our learning community.

Participation

You are integral to the learning experience in this class. Be prepared to actively contribute to class activities, group discussions, and work outside of class.

Assignments and Deadlines

- Students are expected to complete individual readings and complete independent assignments during the course.
- Frequent and high-quality participation and notes for the in class discussions is required
- Readings, individual papers, teamwork, and class discussions will be assigned and graded weekly.
- The final case project will be announced at the beginning of the course, and it will be due by the end of the last class.
    - The purpose of the project is to provide students with a hands-on experience with the intricacies, complexities, planning, meeting requirements, making presentation, and project reporting. Having completed the project, students are required to submit a final essay, and prepare a presentation, which includes a deck of the project and its expectations.

- All team members should contribute to the group projects. Submit a single paper (pdf or doc) for the team identifying which team member contributed to which part of the case. Include your team number, team members, and date, type each question and answers, and include in text and end references in the APA style. The team cases will be evaluated on both an individual and group level.
  - More details will be provided. All essays are to be written in the APA style.
- Please refer to the Course Outline below for Readings, Class Assignments, and Cases.
- Please review the Grading Policy below.

Course Technology Use

We will utilize multiple technologies to achieve the course goals. I expect you to use technology in ways that enhance the learning environment for all students. All class sessions require use of Zoom. All class sessions require use of technology (e.g., laptop, computer lab) for learning purposes.

Feedback and Viewing Grades

I will provide timely meaningful feedback on all your work via our course site in NYU Brightspace. You can access your grades on the course site Gradebook.

Attendance

I expect you to attend all class sessions. Attendance will be taken into consideration when determining your final grade.

Refer to the SPS Policies and Procedures page for additional information about attendance.

Excused absences are granted in cases of documented serious illness, family emergency, religious observance, or civic obligation. In the case of religious observance or civic obligation, this should be reported in advance. Unexcused absences from sessions may have a negative impact on a student's final grade. Students are responsible for assignments given during any absence.
Each unexcused absence or being late may result in a student's grade being lowered by a fraction of a grade. A student who has three unexcused absences may earn a Fail grade.

Students who join the course during add/drop are responsible for ensuring that they identify what assignments and preparatory work they have missed and complete and submit those per the syllabus.

Textbooks and Course Materials

Students can purchase these items through the NYU Bookstore.
Required:

- Cybersecurity – Attack and Defense Strategies: Improve your security posture to mitigate risks and prevent attackers from infiltrating your system, 3rd Edition 3rd Edition ISBN: 978-1803248776

Recommended:

- Peter L. Bernstein, Against the Gods the Remarkable Story of Risk, John Wiley & Sons, Inc.; ISBN: 0471295639, Published: 1998
- (ISC)2 CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL- CISSP Copyright 2018 John Wiley & Sons Inc. ISBN 978-1-119-47593-4
- Recommended for those interested in achieving a Certification.

Grading | Assessment

Your grade in this course is based on your performance on multiple activities and assignments. Since all graded assignments are related directly to course objectives and learning outcomes, failure to complete any assignment will result in an unsatisfactory course grade. All written assignments are to be completed using APA format and must be typed and double-spaced. Grammar, punctuation, and spelling will be considered in grading. Please carefully proofread your written assignments before submitting them for a grade. I will update the grades on the course site each time a grading session has been completed— typically three (3) days following the completion of an activity.

DESCRIPTION	**PERCENTAGE**
4 Group Presentations (20% Group grade & 20% Individual grade)	40%
Primary Posts in the Forum	10%
Subsequent Posts in the Forum	10%
Participation	10%
Final Group Presentation (15% group grade & 15% individual grade)	30%
TOTAL POSSIBLE	100%

See the “Grades” section of Academic Policies for the complete grading policy, including the letter grade conversion, and the criteria for a grade of incomplete, taking a course on a pass/fail basis, and withdrawing from a course.

Course Outline

Start/End Dates: 01/24/2024 - 05/01/2024 | Wednesday
Time: 06:20pm - 08:55pm
No Class Date(s): Wednesday - 3/20/2024
Special Notes: Spring Break 03/18/24 - 03/24/24

Session 1 - 1/24

Topic: Security Posture
Description: What is data, and why should it be protected?

- The importance of data and why organizations must focus on protecting it
- How to begin by performing a data classification exercise
- Data Classification Types

Assigned Readings:

- Read: Chapter 1 - Cybersecurity - Attack and Defense Strategies

Discussion:

- Select an industry you work for or desire to work in. What information would be the most important to protect specifically for that industry?

Assignment(s):

- Complete discussion post and respond to at least 2 students - Due on 1/31

Additional Recommended/Optional Resources:

- Data Classification: How to Classify Your Company's Data and Be Better Prepared for a Data-driven Future

Session 2 - 1/31
Topic: Incident Response Process
Description: Reasons to have an IR Process

- Create an Incident response process
- Incident Response Life Cycle

Assigned Readings:

- Read: Chapter 2 - Cybersecurity - Attack and Defense Strategies
- Incident Response Plan 101

Discussion:

- How does the incident response impact the business? Why does this make a positive impact on the organization?

Assignment(s):

- Complete discussion post and respond to at least 2 students - Due on 2/7
- Group Project - Create a PowerPoint presentation outlining an IR plan, select a business or industry, and outline an incident response plan. - Due on 2/7
    - Provide an overview of what **unique** incident response aspects for the business.
    - What documents need to be created?
    - Who are the key stakeholders involved in the incident response process?
    - What training is required to educate staff across the organization?

Additional Recommended/Optional Resources:

- How to Create a Cybersecurity Incident Response Plan
- How to Make and Implement a Successful Incident Response Plan
- Building Your Own IR Process Based on NIST Guidelines

Session 3 - 2/7
Topic: Incident Response Process (Continued)
Description: Reasons to have an IR Process

- Implementing an incident response plan
- Case Studies of Implementation Approaches

Assigned Readings:

- Read: Chapter 2 - Cybersecurity - Attack and Defense Strategies
- Incident Response Plan 101

Assignment(s):

- Identify the unique lessons learned from the case studies presented - Due 2/14

Session 4 – 2/14
Topic: Understanding the Cybersecurity Kill Chain, Reconnaissance & Compromising the System

Description: Diving deep into the tools that attackers will use to breach your organization

- Access and privilege escalation
- Exfiltration

Understanding how attackers go from start to finish in the attack lifecycle

- External and Internal reconnaissance
- Analyzing current trends

Assigned Readings:

- Read: Chapters 3 - 5 - Cybersecurity - Attack and Defense Strategies
- OSINT: How to find information on anyone
- Cyber Kill Chain® | Lockheed Martin
- Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

Discussion:

- How can the Cybersecurity Kill chain be used to mature the incident response process?

Assignment(s):

- Complete discussion post and respond to at least 2 students - Due on 2/21
- Group Project - Create a PowerPoint presentation researching a CVE (Common Vulnerabilities and Exposures) released in the last 2 years. - Due on 2/21
  - How was the CVE discovered?
  - How does the CVE work?
  - How would this impact an organization?

Session 5 – 2/21
Topic: Understanding the Cybersecurity Kill Chain, Reconnaissance & Compromising the System (Continued)

Description: Diving deep into the tools that attackers will use to breach your organization

- Access and privilege escalation
- Exfiltration

Understanding how attackers go from start to finish in the attack lifecycle

- External and Internal reconnaissance
- Analyzing current trends

Assigned Readings:

- Read: Chapters 3 - 5 - Cybersecurity - Attack and Defense Strategies
- OSINT: How to find information on anyone
- Cyber Kill Chain® | Lockheed Martin
- Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

Assignment(s):

- Identify the unique lessons learned from the case studies presented - Due 2/28

Session 6 – 2/28

Topic: Chasing a User's Identity

Description: Strategies for compromising a user's identity

- Hacking a user's identity
- Analyzing current trends

Assigned Readings:

- Read: Chapter 6 - Cybersecurity - Attack and Defense Strategies

Discussion:

- Research the strategies businesses impose to protect identities and use Google, Facebook, and Apple as examples to understand how they protect their customers' accounts.

Assignment(s):

- Complete discussion post and respond to at least 2 students - Due on 3/6

Additional Recommended/Optional Resources:

- It's a great day to secure your Apple and iCloud accounts

Session 7 – 3/6

Topic: Lateral Movement & Privilege Escalation

Description: Performing lateral movement & privilege escalation

- Infiltration
- Avoiding alerts

Assigned Readings:

- Read: Chapters 7 & 8 - Cybersecurity - Attack and Defense Strategies

Discussion:

- Research the strategies to limit lateral movement. What techniques can be implemented on the configuration of systems? What additional technology can be implemented to prevent this exploit method?

Assignment(s):

- Complete discussion post and respond to at least 2 students - Due on 3/13

Additional Recommended/Optional Resources:

- **Russian State Hackers Take Minutes to Move Laterally**

Session 8 – 3/13
Topic: Network Security, Investigating an Incident & Threat Intelligence
Description: Investigation techniques for actual incidents & threat intelligence

- Open-source tools for threat intelligence
- Leveraging threat intelligence to investigate suspicious activity
- Intrusion detection systems vs Intrusion prevention system

Assigned Readings:

- Read: Chapters 10-13 - Cybersecurity - Attack and Defense Strategies

Discussion:

- Research two industries and compare how the threat intelligence programs might be different. For example, how much threat intelligence is other than an airline program compared to a bank threat intelligence program?

Assignment(s):

- Complete discussion post and respond to at least 2 students - Due on 3/27
- Group Project - Create a PowerPoint presentation around Cloud Security strategy. - Due on 3/27
- Research a cybersecurity incident that has occurred to an enterprise through a cloud vulnerability.
    - Provide an overview of the event and how it was remediated
    - How was the business impacted?
    - Provide a recommendation for cloud security best practices

Additional Recommended/Optional Resources:

- **What is a WAF?**
- **Amazon GuardDuty vs Inspector: which one should you use?**
- **Google Security Command Center**
- **Microsoft Azure Security Center**

Session 9 – 3/27
Topic: Network Security, Investigating an Incident & Threat Intelligence (Continued)

Description: Investigation techniques for actual incidents & threat intelligence

    - Case studies to understand cloud security failures and implementations

Assigned Readings:

- Read: Chapters 12 & 13 - Cybersecurity - Attack and Defense Strategies

Discussion:

- Research the standard security tools that would be deployed to protect cloud workloads. Identify the top 3 tools you would recommend your organization to implement to protect systems from attackers.

Assignment(s):

- Complete discussion post and respond to at least 2 students - Due on 4/3

Additional Recommended/Optional Resources:

- **4 Simple Steps for an Effective Threat Intelligence Program**

Session 10 – 4/3

- Topic: AI Security and Ethical Concerns
- Description: AI Security Overview
    - Ethical Considerations in AI
    - Intersection of Security and Ethics

Discussion:

- In this discussion, please choose an industry you currently work in or aspire to work in. Identify a specific AI use case within that industry where AI technology could be leveraged to enhance business operations or innovation. Additionally, highlight potential security issues associated with implementing AI in that use case. Discuss how addressing these security concerns is crucial for ensuring the successful integration of AI while maintaining data integrity and user trust. Engage with your peers by providing insights and reflections on their chosen industries and AI use cases.

Assignment(s):

- Complete discussion post and respond to at least 2 students - Due on 4/10

Session 11 – 4/10

Topic: Security Policy

Description: Reviewing your security policy

    - Policy enforcement
    - Monitoring for compliance

Assigned Readings:

- Read: Chapter 9 - Cybersecurity - Attack and Defense Strategies

Discussion:

- How do you create security awareness in an organization? What type of campaigns would you launch in an organization to make people aware of the risks the business face?

Assignment(s):

- Complete discussion post and respond to at least 2 students - Due on 4/17
- Group Project - Create a PowerPoint presentation around the Security Policy strategy. - Due on 4/17
  - What policies are the **UNIQUE** required for the business?
  - What is contained in those policies?
  - What is unique in your policies based on your industry?

Additional Recommended/Optional Resources:

- **Security Awareness Campaigns in Your Company**
- **How to create an effective security policy: 6 tips**

Session 12 – 4/17
Topic: Security Policy (Continued)
Description: Reviewing your security policy

- Practical implementation of security policies
- Case Studies of Implementation

Assigned Readings:

- Read: Chapter 9 - Cybersecurity - Attack and Defense Strategies

Session 13 – 4/24
Topic: Risk Management & Legal Considerations
Description: Creating a risk management strategy

- Analysis of policies and procedures
- Reporting and remediation tracking

Assigned Readings:

- Read: Chapter 15 - Cybersecurity - Attack and Defense Strategies

Discussion: Select an industry you work for or desire to work in. How do you prioritize risk discovered in the organization? What are the criteria used to make the determination?

Assignment(s):

- Complete discussion post and respond to at least 2 students - Due on 5/1
- **Final Project** - Due on 5/1

Additional Recommended/Optional Resources:

- Managing Risks: A New Framework

Session 14 – 5/1
Topic: Final Project Presentation
Description: In this session, you will present your final project. Additionally, you will learn from their presentations as each student explains their research.

Assignment(s):

- **Final Project**
    - **Research a cybersecurity event that has a geo-political impact.** The event selected should have at least a national impact if not a global impact. Provide an overview of the event that occurred and the impact it had on the region. The research should include the following sections in the research paper as well as the presentation.
        - **Setting the stage** - A high-level overview of what led to the events
        - **What happened?** - A timeline of the events that occurred should be clearly outlined
        - **What was the holistic impact?** - Several perspectives should be included in the research
            - Political
            - Financial & Economical
            - Social
            - Technology
            - Legal
        - **What was the outcome?** - What changed after the events? Who was negatively impacted by the event?

    - Once a topic is selected one member of the team should post a new thread in the “Group Project” with the client and team members.
        - This is to ensure no duplicate topics are selected.
    - Teams will need to produce 2 items a **Research paper and PowerPoint.**
        - As per NYU Policy, the documents should make clear which student was responsible for each part. Each student should play a part in each of the tasks - Research paper, PowerPoint, and presentation -
        - Every member will need to speak during the presentation.
    - The research paper should be in-depth into the theory of the information security incident, the failure of security controls, and recommendations to remediate the information security issues.
        - The length of the research paper should be 10 pages minimum double-spaced, in MLA format.
    - PowerPoint slides should summarize all the major points in the research paper into a 15-minute presentation.

NOTES:

The syllabus may be modified to better meet the needs of students and to achieve the learning outcomes.

The School of Professional Studies (SPS) and its faculty celebrate and are committed to inclusion, diversity, belonging, equity, and accessibility (IDBEA), and seek to embody the IDBEA values. The School of Professional Studies (SPS), its faculty, staff, and students are committed to creating a mutually respectful and safe environment (*from the SPS IDBEA Committee*).

NYU | SCHOOL OF PROFESSIONAL STUDIES

New York University School of Professional Studies Policies

1. Policies - You are responsible for reading, understanding, and complying with University Policies and Guidelines, NYU SPS Policies and Procedures, and Student Affairs and Reporting.

2. Learning/Academic Accommodations - New York University is committed to providing equal educational opportunity and participation for students who disclose their dis/ability to the Moses Center for Student Accessibility. If you are interested in applying for academic accommodations, contact the Moses Center as early as possible in the semester. If you already receive accommodations through the Moses Center, request your accommodation letters through the Moses Center Portal as soon as possible (mosescsa@nyu.edu | 212-998-4980).

3. Health and Wellness - To access the University's extensive health and mental health resources, contact the NYU Wellness Exchange. You can call its private hotline (212-443-9999), available 24 hours a day, seven days a week, to reach out to a professional who can help to address day-to-day challenges as well as other health-related concerns.

4. Student Support Resources - There are a range of resources at SPS and NYU to support your learning and professional growth. For a complete list of resources and services available to SPS students, visit the NYU SPS Office of Student Affairs site.

5. Religious Observance - As a nonsectarian, inclusive institution, NYU policy permits members of any religious group to absent themselves from classes without penalty when required for compliance with their religious obligations. Refer to the University Calendar Policy on Religious Holidays for the complete policy.

6. Academic Integrity and Plagiarism - You are expected to be honest and ethical in all academic work. Moreover, you are expected to demonstrate how what you have learned incorporates an understanding of the research and expertise of scholars and other appropriate experts; and thus, recognizing others' published work or teachings—whether that of authors, lecturers, or one's peers—is a required practice in all academic projects.

Plagiarism involves borrowing or using information from other sources without proper and full credit. You are subject to disciplinary actions for the following offenses which include but are not limited to cheating, plagiarism, forgery or unauthorized use of documents, and false form of identification

Turnitin, an originality detection service in NYU Brightspace, may be used in this course to check your work for plagiarism.

Read more about academic integrity policies at the NYU School of Professional Studies on the Academic Policies for NYU SPS Students page.

7. Use of Third-Party Tools - During this class, you may be required to use non-NYU apps/platforms/software as a part of course studies, and thus, will be required to agree to the “Terms of Use” (TOU) associated with such apps/platforms/software.

These services may require you to create an account, but you can use a pseudonym (which may not identify you to the public community, but which may still identify you by IP address to the company and companies with whom it shares data).

You should carefully read those terms of use regarding the impact on your privacy rights and intellectual property rights. If you have any questions regarding those terms of use or the impact on the class, you are encouraged to ask the instructor prior to the add/drop deadline.