**Information Security Management**

**MASY1-GC 3220 | 100 | Fall 2024 | 09/04/2024 - 12/04/2024 | 3 Credits**

**Modality:** In-Person

**Course Site URL:** <https://brightspace.nyu.edu>

**General Course Information**

**Name/Title:** [Anthony Candeias](mailto:anthonycandeias@gmail.com), Adjunct Instructor

**NYU Email:** adc7@nyu.edu

**Class Meeting Schedule**: 09/04/2024 - 12/04/2024 |Wednesday | 6:20 PM - 8:55 PM

**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](https://www.nyu.edu/servicelink/KB0018507) 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](https://brightspace.nyu.edu/).

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.

**Generative AI Use**

**Welcome on Specific Projects**

Where noted, you are allowed to use generative AI tools for assignments or activities. However, assignments created with AI should not exceed 25% of the overall work, and you must identify the portions where you used AI tools, and describe how you used them. Note that you are responsible for all parts of an assignment; if an AI tool provides incorrect information, it is your responsibility to find and fix the error before submitting. Note too that overreliance on AI can hinder independent thinking and creativity (example from an NYU course).

Use of ChatGPT (or other similar tools that generate text) is allowed in this class for specific assignments only. When use of the tool is allowed, it will be explicitly noted in the assignment directions. If you utilize ChatGPT for any part of the assignment (from idea generation to text creation to text editing), you must properly cite ChatGPT. Violations can result in failure of the assignment or failure of the course and a notation on your transcript (example adapted from [University of Vermont](https://www.uvm.edu/wid/examples-ai-chatgpt-syllabi-statements)).

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](https://www.sps.nyu.edu/homepage/student-experience/policies-and-procedures.html) 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:

* Yuri Diogenes, Erdal Ozkaya, Cybersecurity – Attack and Defense Strategies – Second Edition Published 2019 - Pact Publishing. ISBN: 978-1-83882-779-3

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](https://www.sps.nyu.edu/homepage/student-experience/policies-and-procedures.html#Graduate1) 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.

**NYU SPS Graduate Grading Scale**

|  |  |  |  |
| --- | --- | --- | --- |
| **A** | 95-100 | 4.000 | **Exceptional:** Demonstrates exceptional mastery of all learning outcomes of the course and thorough and complete understanding of all concepts. |
| **A-** | 90-94 | 3.667 | **Excellent:** Demonstrates highly competent mastery of all learning outcomes of the course and strong understanding of all concepts. |
| **B+** | 87-89 | 3.333 | **Very Good; exceeds course standards:** Demonstrates mastery of all learning outcomes of the course and understanding of core concepts. |
| **B** | 83-86 | 3.000 | **Good; meets course standards:** Demonstrates mastery of some learning outcomes; understanding of some core concepts could be improved. |
| **B-** | 80-82 | 2.667 | **Somewhat Satisfactory;** meets some course standards and requires improvement: Demonstrates basic understanding of some learning outcomes; improved understanding of all core concepts is needed. |
| **C+** | 77-79 | 2.333 | **Less than Satisfactory; requires significant improvement:** Demonstrates partial understanding of all learning outcomes and core concepts; requires significant improvement. |
| **C** | 73-76 | 2.000 | **Unsatisfactory; requires substantial improvement:** Demonstrates partial understanding of some learning outcomes and core concepts; requires substantial improvement. |
| **C-** | 70-72 | 1.667 | **Unsatisfactory; requires extensive improvement:** Demonstrates poor understanding of all learning outcomes and core concepts; requires extensive improvement. |
| **F** | Below 70 |  | **Fail:** Demonstrates minimal to no understanding of all key learning outcomes and core concepts; work is unworthy of course credit towards the degree. |
| **P** |  |  | **Passing:** If a Pass/Fail grade is allowed, the choice of pass/fail must be made prior to the completion of the fifth week of the term. |

**Course Outline**

**Start/End Dates:** 09/04/2024 - 12/04/2024 | Wednesday

**Time:** 6:20 PM - 8:55 PM

**No Class Date(s):** N/A

**Special Notes:** N/A

**Session 1 - 9/4**

Topic: The Importance of Information Security

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:

* Reflect and share on an information security issue you, family or friends may have faced. Respond to two students comparing and contrasting your experience compared to theirs.

Assignment(s):

* Complete discussion post and respond to at least 2 students - Due on 9/11

Additional Recommended/Optional Resources:

* [Data Classification: How to Classify Your Company's Data and Be Better Prepared for a Data-driven Future](https://www.dasera.com/blog/data-classification-how-to-classify-your-companys-data-and-be-better-prepared-for-a-data-driven-future)

**Session 2 - 9/11**

Topic: How do we establish Compliance, Policies and Governance?

Description: Governance risk and Compliance

* This process includes developing clear policies, implementing effective controls, and continuously monitoring and auditing to ensure adherence and address any areas of non-compliance.

Assigned Readings:

* Read: Chapter 10 - Cybersecurity - Attack and Defense Strategies

Discussion:

* Research a business you work for or desire to work for, Identify all the cybersecurity compliance requirements the business would need to abide by. Respond to two students comparing and contrasting your experience compared to theirs.

Assignment(s):

* Complete discussion post and respond to at least 2 students - Due on 9/18
* Group Project - Create a PowerPoint presentation, research a business which has been violated in cybersecurity or privacy compliance or regulation. - Due on 9/18

Additional Recommended/Optional Resources:

* [How to Create a Cybersecurity Incident Response Plan](https://hyperproof.io/resource/cybersecurity-incident-response-plan/)
* [How to Make and Implement a Successful Incident Response Plan](https://www.securitymetrics.com/learn/how-to-make-and-implement-successful-incident-response-plan)
* [Building Your Own IR Process Based on NIST Guidelines](https://www.cynet.com/incident-response/nist-incident-response/)

**Session 3 – 9/18**

Topic: How do we establish Compliance, Policies and Governance? (Continued)

Description: Governance risk and Compliance

* This process includes developing clear policies, implementing effective controls, and continuously monitoring and auditing to ensure adherence and address any areas of non-compliance.

Assigned Readings:

* Read: Chapter 10 - Cybersecurity - Attack and Defense Strategies

**Session 4 – 9/25**

Topic: How does Enterprise Risk interact with Cybersecurity risk?

Description: Understanding how incorporate cybersecurity programs into the overall Enterprise Risk Strategy

* Key Stakeholders involved
* Strategies to implement this

Assigned Readings:

* Read: Chapter 3 - Cybersecurity - Attack and Defense Strategies
* [4 Areas of Cyber Risk That Boards Need to Address](https://hbr.org/2023/06/4-areas-of-cyber-risk-that-boards-need-to-address)

Discussion:

* How does a publicly traded company and board of directors address the risks presented by cybersecurity?

**Session 5 – 10/2**

Topic: Where does legal and Cybersecurity Intersect?

Description: Strategies for understanding the legal repercussions of cybersecurity practices

* What laws should cybersecurity professionals be aware of?

Assigned Readings:

* Read: Chapter 6 - Cybersecurity - Attack and Defense Strategies
* [SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures](https://www.sec.gov/newsroom/press-releases/2023-227)

Discussion:

* Research SEC Charges against the SolarWinds CISO, explore the complexities of the charges brought against the CISO and how this sets a precedent for handing future cybersecurity incidents.

Assignment(s):

* Complete discussion post and respond to at least 2 students - Due on 10/9

**Session 6 – 10/9**

Topic: How did cyberspace become a domain of war?

Description: What was the first act of cyberwar?

* What are cyber weapons and how were they used?

Assigned Readings:

* Read: Chapter 7 & 8 - Cybersecurity - Attack and Defense Strategies

Assignment(s):

Group Project - Create a PowerPoint presentation, research a cyber act of war which was used in an international conflict. - Due on 10/16

Additional Recommended/Optional Resources:

* [**Russian State Hackers Take Minutes to Move Laterally**](https://www.infosecurity-magazine.com/news/russian-state-hackers-take-minutes-1/)

**Session 7 – 10/16**

Topic: How did cyberspace become a domain of war? (Continued)

Description: What was the first act of cyberwar?

* What are cyber weapons and how were they used?

Assigned Readings:

* Read: Chapter 7 & 8 - Cybersecurity - Attack and Defense Strategies

Additional Recommended/Optional Resources:

* [**Russian State Hackers Take Minutes to Move Laterally**](https://www.infosecurity-magazine.com/news/russian-state-hackers-take-minutes-1/)

**Session 8 – 10/23**

Topic: How do we build a framework to respond to threats?

Description: Detection capabilities for identifying threats

* Intrusion detection systems vs Intrusion prevention system

Assigned Readings:

* Read: Chapter 10-11 - Cybersecurity - Attack and Defense Strategies

Discussion:

* Research the common security tools which 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 11/3

Additional Recommended/Optional Resources:

* [**What is a WAF?**](https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/)
* [**Amazon GuardDuty vs Inspector: which one should you use?**](https://cloudkatha.com/amazon-guardduty-vs-inspector-which-one-should-you-use/)
* [**Google Security Command Center**](https://cloud.google.com/blog/products/identity-security/how-zebra-technologies-uses-security-command-center)
* [**Microsoft Azure Security Center**](https://www.techtarget.com/searchcloudcomputing/definition/Microsoft-Azure-Security-Center)

**Session 9 – 10/30**

Topic: Emerging Internet of Things Threats

Description: Introduction to threat intelligence

* Open-source tools for threat intelligence
* Leveraging threat intelligence to investigate suspicious activity

Assigned Readings:

* Read: Chapter 7 - Cybersecurity - Attack and Defense Strategies

Discussion:

* Research a threat from an internet of things device which has impacted you personally? Has there been any devices you use that has experienced any security or privacy breaches?

Assignment(s):

* Complete discussion post and respond to at least 2 students - Due on 11/6

Additional Recommended/Optional Resources:

* [**4 Simple Steps for an Effective Threat Intelligence Program**](https://www.rapid7.com/blog/post/2021/10/15/4-simple-steps-for-an-effective-threat-intelligence-program/)

**Session 10 – 11/6**

Topic: AI and ML Threats

Description: How does new advancement of Machine Learning or Artificial Intelligence impact the cybersecurity space

Assigned Readings:

* [Preparing for the Next AI Frontier: Leveraging AI Compute Security to Counter Threats in Edge Devices](https://www.rstreet.org/commentary/preparing-for-the-next-ai-frontier-leveraging-ai-compute-security-to-counter-threats-in-edge-devices/)

Assignment(s):

* Assignment(s):
  + Group Project - Create a PowerPoint presentation, research emerging threats and how artificial intelligence could impact the security of a technology stack used by a business. - Due on 11/13

**Session 11 – 11/17**

Topic: AI and ML Threats (Continued)

Description: How does new advancement of Machine Learning or Artificial Intelligence impact the cybersecurity space

Assigned Readings:

* [Preparing for the Next AI Frontier: Leveraging AI Compute Security to Counter Threats in Edge Devices](https://www.rstreet.org/commentary/preparing-for-the-next-ai-frontier-leveraging-ai-compute-security-to-counter-threats-in-edge-devices/)

Assignment(s):

* Assignment(s):
  + Group Project - Create a PowerPoint presentation, research emerging threats and how artificial intelligence could impact the security of a technology stack used by a business. - Due on 11/13

**Session 12 – 11/20**

Topic: User and Network Threats

Description: Exploring how users pose a threat to a business in the same way the systems used to generate and manage profits

Assigned Readings:

* Read: Chapter 8,9,11 - Cybersecurity - Attack and Defense Strategies

Discussion: Create a strategy to raise employee awareness about the cybersecurity threats they may encounter in a business setting.

Assignment(s):

* Complete discussion post and respond to at least 2 students - Due on 11/20

**Session 13 – 11/27**

Topic: App Sec, Web, Mobile and Cloud Threats

Description: Explore the most technical aspects of cyber security and understand how vulnerabilities in applications can be introduced into applications being developed.

Assigned Readings:

* Read: Chapter 16 - Cybersecurity - Attack and Defense Strategies

Assignment(s):

* **Final Project** - Due on 12/4

Additional Recommended/Optional Resources:

* [The Ultimate Guide to Windows Event Logging](https://www.sumologic.com/blog/windows-event-logging/)
* [What is AWS CloudTrail logs?](https://www.sumologic.com/blog/what-is-aws-cloudtrail/)
* [Understanding the Apache Access Log: View, Locate and Analyze](https://www.sumologic.com/blog/apache-access-log/)
* [Linux Logs Explained](https://www.plesk.com/blog/featured/linux-logs-explained/)
* [A beginner’s guide to SQL Server transaction logs](https://www.sqlshack.com/beginners-guide-sql-server-transaction-logs/)

**Session 14 – 12/4**

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?** - A number of 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*](https://www.sps.nyu.edu/homepage/about-us/idbea/about-idbea.html)).

**New York University School of Professional Studies Policies**

1. Policies - You are responsible for reading, understanding, and complying with [University Policies and Guidelines](http://www.nyu.edu/about/policies-guidelines-compliance.html), [NYU SPS Policies and Procedures](http://sps.nyu.edu/academics/academic-policies-and-procedures.html), and [Student Affairs and Reporting](https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/student-services.html).

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](https://www.nyu.edu/students/communities-and-groups/student-accessibility.html). If you are interested in applying for academic accommodations, contact the [Moses Center](https://www.nyu.edu/students/communities-and-groups/student-accessibility/academic.html) 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](https://www.nyu.edu/students/communities-and-groups/student-accessibility.html) as soon as possible ([mosescsa@nyu.edu](mailto: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](https://www.nyu.edu/students/health-and-wellness/wellness-exchange.html). 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](https://www.sps.nyu.edu/homepage/student-experience/resources-and-services.html).

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](https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/university-calendar-policy-on-religious-holidays.html) 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](https://www.nyu.edu/servicelink/KB0018471), 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](https://www.sps.nyu.edu/homepage/student-experience/policies-and-procedures.html) 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.