53:623:343:90 Emerging IT Topics: Cyber Security and Risk Management

Spring 2023

Mark Wehrle MBA, CISA

Contact Information	**Phone:** 215-554-4239 **e-mail:** Mark.Wehrle@rutgers.edu
Class Meetings:	Virtual
Office Hours:	Meetings available upon request
Course Web Page:	Available on Canvas LMS (http://onlinelearning.rutgers.edu/canvas/)

Course Overview:

Information Security is a topic that impacts every one of us in our everyday lives. This course will cover discuss the evolving world of Cyber Risk and establish the fundamentals of Information Security and Risk Management. Our objective will be to shift the lens of Information Security as a "technology issue" to understand cyber risk as business risk.

In this course, you will learn common frameworks and best practices for information security, and how they apply the development of an effective risk management strategy. Students will consider information security in the context of emerging risks with a focus on maintaining the confidentiality, integrity, and availability of information.

Couse Objectives:

- Understand the importance of cybersecurity in the context of business and the geopolitical landscape
- Understand best practices, frameworks, and methodologies for evaluating cyber risk
- Identify strategies to monitor, measure and report the effectiveness of cybersecurity programs to executive leaders
- Understand the importance of data and the importance of data protection

Required Course Materials:

Effective Cybersecurity: A Guide to Using Best Practices and Standards, Publisher - Pearson (2019)

Cybersecurity: The Insights You Need from Harvard Business Review

Selected Articles (see course schedule)

Course Requirements:

Students will be assigned a final grade based on the weighted scored computed using the components indicated below. The final grade will be based very approximately on a normal distribution.

Class Participation / Discussion Board	15%
Homework Assignments	20%
Case Studies	15%
Exam 1	25%
Exam 2	25%

Class Participation (15%): The course will be delivered using a combination of recorded lectures, case studies, videos, and discussion boards. Students are expected to prepare for class discussions as indicated in the course schedule, complete the required readings, review all lectures, and contribute meaningfully to class discussion boards. Consistent with other courses at the university, this course will assess contributions to the class discussion boards and consider the following:

- do your comments provide new insights?
- do the comments add to our understanding of the issues
- are the comments timely and linked to the comments of others?
- do the comments move the discussion along by giving a new perspective?
- are the comments clear and concise?
- do the comments reflect a concern for maintaining a constructive and comfortable classroom atmosphere?

Students are required to start their own thread responding to the discussion question by each Friday at 11:59 PM. Students must post a reply to another discussion by 11:59PM on the subsequent Monday.

Cyber security incidents occur in the news multiple times per day. Students are encouraged to monitor news outlets, tech blogs, and websites and start new threads on the discussion boards about emerging cyber incidents.

Homework Assignments (20%):
Review Questions (10%) – Many of the course modules will have accompanying review questions as outlined in the course schedule. Students are expected to complete the review questions individually and submit responses in Canvas.

Papers (10%) – In addition to review questions, there will be written papers required of students as outlined in the course schedule. The paper(s) must follow the guidelines as outlined in the assignment

instructions in the Canvas course module. Generally, papers should be approximately 3-5 pages in length. While this is not an English class or business communications class, it is expected that students present their ideas in a clear, concise, and grammatically correct fashion. The papers in this course are designed to provide students with an opportunity to combine objective knowledge of contemporary topics with their opinions and perspectives – the more personal the submissions the better.

Case Studies (15%): There will be 2 case studies assigned during the course. Case studies may be assigned to groups of 3 – 5 students or may be assigned to individuals. For group assignments, each group is required to complete the case as outlined in the case instructions posted and discussed during the lesson related to the case study topic. Case studies will have a written component and may also contain a presentation component. Case studies must be submitted electronically through Canvas. For group assignments, one member from each team may submit the case. All team members must be listed in the document. ***No late submissions will be accepted.***

Exams (50%): Two exams are planned for this course. All students will take the interim and final exam during the designated time. Make-up exams are not offered. Please take this exam schedule into consideration when you make your travel arrangements. All exams will be given in the regular classroom unless otherwise posted. If an exam is missed due to a qualified emergency / university approved reason, contact me to determine alternative arrangements.

Administrative Comments:

Academic Integrity:

For the policy on Academic Integrity please see: http://academicintegrity.rutgers.edu/academic-integrity-at-rutgers

Academic Integrity means that you must:

- properly acknowledge and cite all use of the ideas, results, or words of others,
- properly acknowledge all contributors to a given piece of work,
- make sure that all work submitted as your own in a course activity is your own and not from someone else
- obtain all data or results by ethical means and report them accurately
- treat all other students fairly with no encouragement of academic dishonesty

Adherence to these principles is necessary in order to ensure that:

- everyone is given proper credit for his or her ideas, words, results, and other scholarly accomplishments
- all student work is fairly evaluated, and no student has an inappropriate advantage over others
- the academic and ethical development of all students is fostered
- the reputation of the University for integrity is maintained and enhanced.

For instance, you are responsible for preparing and entering your own work and properly referencing the work of others. Cheating, plagiarism, and other types of misconduct are not acceptable.

Penalties can include expulsion from the University. You are free to discuss any part of the course materials with your classmates.

However, you are not allowed to discuss (i.e., receive nor give any assistance on) any part of the exams with anyone. You may not refer to sources not permitted nor receive help from outside agencies. If any cheating is found, the most severe sanctions available will be

sought.

Students are responsible for understanding the principles of academic integrity and abiding by them in all aspects of their work at the University. Students are also encouraged to help educate fellow students about academic integrity and to bring all alleged violations of academic integrity they encounter to the attention of the appropriate authorities. Violations are taken seriously and will be handled according to University policy.

Student Code of Conduct

The University's Student Code of Conduct can be found at http://studentconduct.rutgers.edu/university-code-of-student-conduct

Violations of the Student Code of Conduct are considered serious infractions of student behavior and students who violate the code are subject to penalties relative to the level of the matter. In general,

students may not disturb normal classroom procedures by distracting or disruptive behavior. Violations of the Student Code of Conduct should be reported to the Dean of Students office deanofstudents@camden.rutgers.eduu or 856-225-6050.

Disability Services / Support Services:

Rutgers University welcomes students with disabilities into all of the University's educational programs. In order to receive consideration for reasonable accommodations, a student with a disability must contact the appropriate disability services office at the campus where you are officially enrolled, participate in an intake interview, and provide documentation: Details are available at Office of Disability Services web site at https://learn.camden.rutgers.edu/disability-services.

Course Schedule:

Week/Topic	Lesson Overview	Assigned Reading	Homework Assignment
Week 1: 1/17/2023 - Cyber Risk is Business Risk	- Course Expectations and Syllabus Review - Class Introductions - Overview of Cybersecurity - Recent events and the importance of Cybersecurity	Course Syllabus Week 1 - Cybersecurity Is Not (Just) a Tech Problem Week 1 - The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict	None
Week 2: 1/24/2023 - Documentary: The Perfect Weapon	- Each student will be required to view either "The Perfect Weapon" or "Zero Days" and prepare a 3-page response paper (instructions provided on Canvas) - Class discussion the following week will be on the importance of Cyber Security in business and geopolitical relations	"We're All in this Now" HBR prologue (page xi)	**Response Paper (assignment instructions available on Canvas) due Monday 1/30/2023 11:59 PM**
Week 3: 1/31/2023 - Understanding and Differentiating Security Frameworks	- Discuss the need for standards and best practices in Information Security - Discuss the role of the NIST CSF and differences from other frameworks - Discuss the CIS Critical Security controls and practical applications - Explain the concept of Security governance and provide an Overview of governance components - Discuss key topics that should be covered in a strategic Security plan	"Effective Cybersecurity" - Chapters 1 & 2	Chapter 1: Review question 2 Chapter 2: Review question 4
Week 4: 2/7/2023 - Managing Information Security and Human Risk	- Discuss the behavioral components of information security - Describe the need for a culture of information security	"Effective Cybersecurity" - Chapter 5 "The Best Cybersecurity Investment You Can Make Is Better Training" HBR article 6 (page 67) "The Key to Better Cybersecurity: Keep Employee Rules Simple" HBR article 8 (page 85)	Chapter 5: Review questions 10 and 11 Group selections due Monday 2/13/2023 11:59PM

Week 5: 2/14/2023 - Risk Management: Methodologies, Assessments, and Risk Quantification	- Discuss risk management methodologies - Understand the difference between Inherent risk and Residual risk - Identify practical applications of risk management frameworks - Discuss risk quantification and the applicability to executives and business users	"Effective Cybersecurity" - Chapter 3 "Why the Entire C-Suite Needs to Use the Same Metrics for Cyber Risk" HBR article 5 (page 59)	Chapter 3: Review questions 3 and 4
Week 6: 2/21/2023 - Supply Chain Risk and Third-Party Risk Management	- Discuss supply chain risk and third-party risk management - Discuss the interconnectedness and dependencies organizations have on key suppliers - Learn repeatable and practical framework for evaluation of third parties/supply chain vendors	"Effective Cybersecurity" - Chapter 13	Chapter 13: Review questions 2, 6, and 7 Case study presentation submissions due Monday 2/27/2023 11:59PM
Week 7: 2/28/2023 - Case Study Presentations: Security Awareness	- Groups will present their security awareness campaign materials as required by the Case Study Assignment. - This will be a live presentation, conducted over zoom. - An agreeable time will be determined between the instructor and the class between 2/28/2023 and 3/6/2023	None	None
Week 8: 3/7/2023 - MIDTERM EXAM			
Week 9: 3/14/2023 - SPRING BREAK			
Week 10: 3/21/2023 - Business Continuity and Resilience	- Provide an Overview of business continuity and business impact analysis - Understand the key elements of business continuity programs - Discuss business continuity operations and responding to events	"Effective Cybersecurity" - Chapter 17	Chapter 17: Review questions 3 and 5.
Week 11: 3/28/2023 - Industrial Control Systems, Physical Security and Physical Asset Management	- Understand the risks and vulnerabilities related to physical assets - Understand the difference between Information Technology (IT) systems and Operational Technology (OT) / Industrial Controls Systems (ICS) - Discuss physical security and environmental protections for physical devices in the context of data protection	"Effective Cybersecurity" - Chapter 16 "Effective Cybersecurity" - Chapter 7 Cybersecurity and Physical Security Convergence_508_01.05.2021_0	Chapter 16: Review question 6 Chapter 7: Review question 8

Week 12: 4/4/2023 - Privacy and Implications, Information Management, and Data Protection	- Discuss data privacy and responsibilities of data collectors (response to documentary) - Discuss the data governance lifecycle - Understand data classification, labeling, and handling	"Effective Cybersecurity" - Chapter 6 "Cybersecurity is Putting Customer Trust at the Center of Competition" HBR article 11 (page 117) "Privacy and Cybersecurity are Converging" HBR article 12 (page 125)	Chapter 6: Review questions 2 and 9
Week 13: 4/11/2023 - Documentary: Terms and Conditions Apply	- Each student will be required to view either "The Great Hack" or "Terms and Conditions Apply" - Students will complete the privacy case study in advance of the next lesson.	Case Study: HBR Alexa	**Case Study response paper submissions due Monday 4/17/2023 at 11:59 PM**
Week 14: 4/18/2023 - Logging, Monitoring, and Behavioral Analysis	- Understand the importance of event logging and monitoring - Understand how logging and monitoring data can be mined to determine behavioral analyses, anomalies, and Identify insider threats - Understand the difference between a Security event and Security incident - Understand the nature and value of threat intelligence data	"Effective Cybersecurity" - Chapter 15	Chapter 15: Review questions 5 and 7
Week 15: 4/25/2023 - Monitoring, Measurement, KPIs, and Reporting	- Understand key risk indicators and key performance indicators that support effective Information Security programs - Discuss the perspective and responsibilities of the Board of Directors with regards to oversight of Information Security	"Effective Cybersecurity" - Chapter 18	None
Week 16: 5/2/2023 - FINAL EXAM			