2023 Annual Conference & Exposition
Baltimore Convention Center, MD | June 25 - 28, 2023
The Harbor of Engineering Education for 130 Years
ASEE
Paper ID #39689

The Development, Assessment, and Advancement of a Student-Centered Cyber Risk Management Course

Dr. Joseph Benin, United States Coast Guard Academy

CAPT Benin is a graduate of the Coast Guard Academy (BSEE), having served as the Regimental Honor Officer and Chairman of the Cadet Standards of Conduct Board. He then served as the Electrical and Electronics Officer aboard the USCGC Healy (WAGB-20) completing his Engineer-Officer-In-Training (EOIT) qualifications. In 2005, he was selected as a member of the Permanent Commissioned Teaching Staff (PCTS) at the U.S. Coast Guard Academy. CAPT Benin focuses on the areas of computer networks, programming, and security. Dr. Benin has previously served as the Director of Academic Advising and presently is the chair of the USCGA Cyber Council and Cyber Systems Program Coordinator.

Mr. William Randall

William Randall spent over 30 years in Coast Guard C4IT/C5I including serving as the senior civilian for the engineering, development, and protection of the Coast Guard's IT infrastructure at the Coast Guard's Telecommunication and Information Systems Com

Angela G Jackson-Summers

The Development, Assessment, and Advancement of a Student-Centered Cyber Risk Management Course

Abstract

Managing risk is a key component to achieving a strong cyber security posture. Practitioners must consider a combination of human, technology, and policy-based factors when establishing their postures. To help students understand these interdependencies, we designed and developed a course to apply, analyze, synthesize, and evaluate these in a real-world environment. Students have gained an appreciation for various technical and managerial concepts related to cyber security and demonstrated the knowledge gained by developing submissions to the annual Maritime Cyber Risk Symposium student poster contest. This paper describes the multi-year developmental journey in standing up a Cyber Risk Management course linked to National Security Agency/Department of Homeland Security National Center of Academic Excellence in Cyber Education knowledge units, ABET outcomes for cybersecurity computing programs, and the National Institute of Standards and Technology framework and guidance. It includes student-centered individual classroom learning, project-based team learning, and team development of scholarly work for submission and external evaluation. The efficacy of this approach after two offerings is based upon student feedback, ABET and NCAE assessment, and external results. The paper concludes with how we see the course evolving as the cyber systems major evolves. Teaching cyber-focused concepts in an interdisciplinary manner is critical and, in that spirit, the teaching of this course is moving from the School of Engineering and Cyber Systems to the School of Leadership and Management.

Background

In May of 2022 the United States Coast Guard Academy (USCGA) graduated its first class of Cyber Systems majors. This major was introduced at the Coast Guard Academy (CGA) in order to provide a larger number of technically-competent leaders of character to accomplish the needs of the Service in the midst of growing demands in the cyber domain. The Cyber Systems major comprises a strong academic foundation in secure technical computing balanced with a managerial cyber emphasis. Program stakeholders repeatedly shared the importance of understanding risk within the cyber context. As a result, it was determined by the faculty that the Cyber Systems Major at CGA needed to address cyber risk management as part of its curriculum.

In developing this course, the authors hoped to do it in a way that students could relate to the material and that the content of the course would be applicable to their future in the Coast Guard and as cyber security professionals. While a Cyber Risk Management course had been offered as a Directed Studies previously, it had not been offered at CGA for a few years as the professor that specialized in this area was assigned to the standup of the Cybersecurity and Infrastructure Security Agency (CISA). The existing course material and the DHS/NSA CAE CDE (Department of Homeland Security and National Security Agency sponsored National Centers of Academic Excellence in Cyber Defense Education) Knowledge Units (KUs) were used as the basis for the course curriculum. The course was divided into three parts: (1) Introduction to

Cyber Risk Management and the Maritime Transportation System, (2) Building a Cyber Security Plan, and (3) a final team-based project to apply what has been learned to the annual Student Poster Competition of the Maritime Risk Symposium [1] (see the syllabi provided in Appendix I and II for additional information on the course schedule).

Course Content and Development

The Cyber Risk Management course at the United States Coast Guard Academy has two prerequisites: Fundamentals of Information Security (7218) and Systems Analysis and Design (8453). These course descriptions are provided in Appendix III. These courses provide students with the necessary cybersecurity knowledge to understand and analyze cyber security vulnerabilities and threats to assess the likelihood of an attack as well as begin to understand the impact of such an attack.

The first section of the course was designed to provide a general understanding of cyber risk management. In this course this starts with the DODI 8500.01 ("Cybersecurity") definition:

> "Cybersecurity Risk Management. Managing cybersecurity risks is a complex, multifaceted undertaking that requires the involvement of the entire organization, from senior leaders planning and managing DoD operations, to individuals developing, implementing, and operating the IT supporting those operations. Cybersecurity risk management is a subset of the overall risk management process for all DoD acquisitions as defined in Reference (av), which includes cost, performance, and schedule risk associated with the execution of all programs of record, and all other acquisitions of DoD. The risk assessment process extends to the logistics support of fielded equipment and the need to maintain the integrity of supply sources." [2]

The goal for the course is to help students to understand how computers and cyber dependent technologies in large-scale systems throughout the Coast Guard and on commercial vessels and in ports enable the MTS to operate leveraging the experience of many of the students who have served on cutters or at sectors. Then this course builds upon this by exploring how exploitation, misuse, or failure could disrupt the national defense, homeland security, and our economic well-being. The full list of learning outcomes are listed in the syllabus (please see Appendix I).

In order to achieve this, the course starts with broad coverage of systems engineering as it is applied to understanding the Maritime Transportation System, the Coast Guards' C5I (Command, Control, Communications, Computers, Cyber, and Intelligence) infrastructure, and some of the risks present in each. The following few weeks are dedicated to investigating the roles and responsibilities of various individuals with a stake in cybersecurity, common bodies of knowledge (with an emphasis on the Cybersecurity Body of Knowledge or CyBOK [3]), risk mitigation/transference/acceptance, and various risk management methodologies.

The next six weeks of the course are focused on the students, in small groups, developing a risk management assessment. For this assignment, we heavily rely upon the NIST Framework for Improving Critical Infrastructure Cybersecurity [4] and NIST Special Publication 800-30 Rev 1 Guide for Conducting Risk Assessments [5]. In order to scope this effort to the academic calendar, the assessment was scaled to primarily address:

- A^3, A^I, IdAM/ICAAM - Access, Authentication, Authorization, and Identification
- Configuration Management/System Identification
- Physical Security
- Patch and Change Control/Management
- Incident Response

By only selecting certain portions of a risk assessment, this portion of the course can remain dynamic from semester to semester. In the first offering of the course this was done by providing the students with a fictional network for the risk management assessment effort. In the second and following iteration of the course the student groups selected a major US port for developing their risk assessment.

The following table summarizes the flow of developing the risk management plan:

Table 1 Risk Management Plan Development Flow

Week	Tuesday	Thursday
1	Introduction	IdAM Session #1
2	IdAM #2	IdAM Class Presentations IdAM Section due Configuration Management #1
3	Configuration Management #2	CM Class Presentations CM section due Physical Security #1 *IdAM Section rewrite due*
4	Physical Security #2	Physical Security Presentations Physical Security Section due Patch/change management #1 *Configuration Management Section rewrite due*
5	Patch/change Management #2	Patch/Change Presentations Incident Response #1 *Physical Security Section rewrite due*
6	Incident Response #2	Incident Response Presentations Incident Response Section due *Patch/Change Section rewrite due*
7		*Incident Response Section rewrite due*

The students used the National Institute of Standards and Technology (NIST) SP 800-30 Rev. 1 as their guide for developing the Risk Assessment assignments.

The final third of the class was dedicated to developing a poster for the Maritime Risk Symposium [1]. The goals of this section of the course were:

1. Become familiar with current research in the field of cyber risk management
2. Think critically about the challenges facing the maritime industry with regard to technology and the benefits and risks associated
3. Practice research and citation skills

4. Effective communication in a short form poster
5. Effective verbal presentation skills

The students work as a group to create a poster that aligns with the requirements of the Maritime Risk Symposium Student Poster Competition [6]. The audience for the posters is a broad maritime audience and not necessarily cyber professionals.

In 2021 the topics for the student research competition were:

- Decarbonization and Transition to Green Technologies
- Autonomous Vessels and Systems
- Maritime Cybersecurity
- Security and Resilience of the Maritime Supply Chain
- Arctic Maritime
- The Human Element

In 2022 the topics were:

- Assessing Risks to MTS Infrastructure from Climate Change and Planning for Long Term Resilience and Adaptation
- Training the Next Generation of Maritime Cyber Warriors
- Keeping the Inland Waterways Open: Balancing Maintenance and Operational Requirements Against Increasing Threats
- Engineering Resilience into the Inland MTS Under Environmental Threat
- Supply Chain Challenges to the MTS
- COVID Pandemic Impacts on MTS Human Elements

Each group is assigned a topic from one of the categories and provided with an initial reference. They then design a poster discussing their research into the assigned topic. While MRS provides a PowerPoint Poster template, there is no specific format for the poster and students are encouraged to present their material that best fits their research. Students are also encouraged to remember that posters are a visual experience so font size, organization, and graphics are all important at conveying your point and that language needs to be concise. The poster must include the following sections as a minimum:

- *Background*: Give an overview of the relevant history or technical details that inform the problem you are interested in.
- *Thesis/Problem Statement*: What specific aspect of the topic is your group focusing on? Make an assertion based on your research, what question would you like to answer, are there any areas that need additional research and you think deserves more attention?
- *Current State of the Research*: Provide the evidence for your assertions. Analyze your references for the important points.
- *Conclusions*: Connect your evidence to your thesis/problem statement.

- *References*: IEEE citation of the sources provided by the assignment and 3-4 additional references.

Course Assessment

At the end of each semester courses are assessed through an End of Course Review process. Twenty students took the course in fall 2021, 19 in spring 2022, and 19 are enrolled in spring 2023 (the course is now only offered in the spring). The course is used to assess three ABET performance indicators (of two student outcomes) [7] and eleven National Security Agency (NSA)/Department of Homeland Security (DHS) National Center of Academic Excellence (NCAE) in Cyber Defense Education (CDE) Knowledge Units [8] (these were not assess in fall 2021). These assessments are conducted utilizing the "EAMU" vectors following the practices outlined by Estell, et al. [9] and using instructor-developed rubrics.

The assessment information for the ABET outcomes is provided below:

ABET 3-2: Demonstrate effective writing for a nontechnical audience.

Fall 2021 Source: Source: Final Poster; Given topics from the 2021 Maritime Risk Symposium, research and create a poster on a cyber issue relevant to the maritime industry. EAMU Vector (12,8,0,0)

Spring 2022 Source: For homework assignment 1-3, the students were tasked with writing a 400-600 word journal entry on the "national security and homeland security impacts from disruptions to the Maritime Transportation System". EAMU Vector (10,6,1,2)

ABET 3-4: Demonstration effective presentation ability for a nontechnical audience.

Fall 2021 Source: Final Poster Presentation; Given topics from the 2021 Maritime Risk Symposium, research and present on a cyber issue relevant to the maritime industry. EAMU Vector (8,12,0,0)

Spring 2022 Source: Final Poster Presentation; Given topics from the 2022 Maritime Risk Symposium, research and present on a cyber issue relevant to the maritime industry. EAMU Vector (12,6,1,0)

ABET 6-1: Apply security principles and practices to maintain operations in presence of risks.

Fall 2021 Source: Cyber Risk Management Plan; Develop a Cyber Risk Management Plan for a small green power system. Includes an analysis of ICAM, configuration management, incident response and risk assessment. EAMU Vector (18,2,0,0)

Spring 2022 Source: Cyber Risk Management Port Security Plan; Develop a Cyber Risk Management Plan for a U.S. port. Includes an analysis of ICAM, configuration management, incident response and risk assessment. EAMU Vector (12,7,0,0)

Overall, the students did very well in achieving these ABET outcomes in this course.

The assessment information for the NSA/DHS NCAE CDE outcomes for the spring 2022 semester is provided below:

Non-Technical Core - Cybersecurity Planning and Management (CPM)

CPM-1: Examine the placement of security functions in a system and describe the strengths and weaknesses

Source: Final Project Individual Reflection Question 2 which provided a network diagram and asked students to identify strengths and weaknesses. EAMU Vector (19,0,0,0)

CPM-2: Develop contingency plans for various size organizations to include: business continuity, disaster recovery and incident response.

Source: Final Project Individual Reflection Question 3 which provided three scenarios and had students answer how to achieve various goals. EAMU Vector (18,1,0,0)

CPM-3: Develop system specific plans for (a) The protection of intellectual property, (b) The implementation of access controls, and (c) Patch and change management

Source: Final Project Individual Reflection Question 4 which asked students to develop plans to accomplish these goals. EAMU Vector (15,2,1,1)

CPM-4: Outline and explain the roles of personnel in planning and managing security:

Source: Port Security Plan Individual Assignment Question 2 which listed these roles and asked students to outline and explain them. EAMU Vector (19,0,0,0)

Non-Technical Core - Security Program Management (SPM)

SPM-1: Apply their knowledge to develop a security program, identifying goals, objectives and metrics.

Source: Port Security Plan Assignment 1 that required students to outline the goals, objectives, and metrics of a security plan. EAMU Vector: (7,12,0,0)

SPM-2: Apply their knowledge to effectively manage a security program.

Source: Port Security Plan Assignment 1 that required students to layout how they would manage a security program. EAMU Vector: (7,12,0,0)

SPM-3: Assess the effectiveness of a security program.

Source: Port Security Plan Individual Assignment Question 3 which had students assess the security plan they developed for an actual U.S. port. EAMU Vector (12,7,0,0)

Non-Technical Core - Security Risk Analysis (SRA)

SRA-1: Describe how risk relates to a system security policy.

Source: Port Security Plan Individual Assignment Question 1 which had students describe and explain this relationship. EAMU Vector (19,0,0,0)

SRA-2: Describe various risk analysis methodologies.

Source: Homework 4 which had students present their research on a risk analysis methodology and compare and contrast it to other methodologies presented by the other students in the class. EAMU Vector: (8,8,3,0)

SRA-3: Evaluate and categorize risk a) with respect to technology; b) with respect to individuals, and c) in the enterprise, and recommend appropriate responses.

Source: Final Project Individual Reflection Question 1 which had students evaluate and categorize the risk present in three scenarios. EAMU Vector: (13,5,0,1)

SRA-4: Select the optimal methodology based on needs, advantages and disadvantages.

Source: Port Security Plan Individual Assignment Question 4 which had students select the optimal methodology for their port and identify its advantages and disadvantages. EAMU Vector (12,7,0,0)

Overall, the students again achieved these outcomes. Of note is SRA-2 where three students only achieved this outcome at a marginal level. To improve this outcome, during the Spring 2023 school term, this course was offered in two sections. In each section, the class was divided into four (4) groups to support specific in-class activities. An initial group activity focused on researching and delivering group presentations on the top five (5) information (cyber) security risk management frameworks. Instructor feedback planned to support the initial introduction of information security risk management frameworks and their related differences. For student learning reinforcement, the prior Homework 4 assignment was revised to recognize applicable risk management frameworks and when such risk management frameworks may be appropriate for use depending upon the organizational nature and business need.

Another method of assessment is student feedback. The following table provides themes and comments provided for the fall 2021 and spring 2022 courses.

Fall 2021	• I think that there should be less self-learning and more learning done in class • While one student stated that "We did not use the text at all, but the references were great most of the time" another student strongly agreed that the textbook helped with understanding course content • I think that often the grading was too harsh for the assignments at hand and was focused on areas where there should have been less concern • These topics were very tangible, realistic, and relevant • Every respondent agreed or strongly agreed that the final project was well organized and contributed to learning CRM • Students spent 2-4 hours per week on this course outside of lecture
Spring 2022	• Meeting with each group was very helpful between assignments • Students do not like open-ended problems and having to think deeply about them to identify a problem and explore solutions • Students prefer to pick their own teammates • When teams get too large (4), not all members contribute equally • Giving class time to work on team assignments was really appreciated

	• Student appreciated having the final project broken into steps to guide the process; a few expressed a desire to start the project sooner and have more time to work on it

The instructors appreciated the students' seeing the relevancy of the topics in the course and the value of the final project.

With the moving of the course to the spring semester, the students in the spring 2022 course had the option (but not requirement) of submitting their posters to the 2022 MRS Student Poster competition. Two groups opted to participate and one group won 2nd place! The instructors were proud of all the students and particularly appreciated this external validation of the great work they completed as part of this course.

Proposed Changes/Advancement

As the course has evolved, the second portion of the course has gone from a fictional green power generation plant to actual US ports, and now to inclusion of real-world application exercises involving both actual US ports and corporate business/IT processes. The application exercises involving corporate business/IT processes will involve students to examine process flows, identify controls and weaknesses, and document findings and recommendations.

While the initial iteration of the course was held in the fall semester, the fact that this did not line up with the MRS schedule prevented the students from actually submitting and presenting their work. By offering this class in the spring of each year, the work the students do can now allow them to participate in the annual symposium.

Finding a book that captures the essence of Cyber Risk Management for an undergraduate students that builds upon the curriculum of an institution is no easy feat. This course has combined using a textbook for the first third with using NIST guidance for the latter two thirds. This semester a new textbook, *Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework* by Cynthia Brumfield with Brian Haugli (2022) [10], was chosen and made a required course reading. This textbook consists of six (6) chapters serving as the foundational reference in support of learning outcomes and supporting reference for in-class activities and take-home assignments. Also, this textbook was adopted because of its reading structure supporting a simplistic approach to the introduction of cybersecurity risk management, including its focus on the NIST framework. We recognize that the NIST framework primarily supports USCG risk management processes, related activities and procedures, and any governing policies or regulatory compliance practices.

Selecting a group size for group work is a perennial challenge for educators. In the past groups have ranged from three to five. How one scopes the project is the number one factor in determining the optimal group size. Based upon our experience, groups of three is the ideal size for the Student Competition of the MRS and most groups will be three going forward.

Starting in the spring of 2023, the Cyber Risk Management course is now being taught by a former risk management professional. This professor intends to share real-world examples of how risk management is driven from a department level to an organizational level within varying industries. Using the flipped classroom method, in-class, activity-based exercises will be given to students to allow them to demonstrate their achievements of prescribed learning objectives.

During the early weeks of course delivery, the professor will be establishing the introduction of risk management by building a foundational understanding of the following topics.

1. The Use and Importance of a Capability Maturity Model Involving Risk Management Towards Overall Maturity
2. Application of Knowledge Development Regarding Information Technology in Organizations
3. Organizational Focus of Business and IT Strategic Alignment Risk Management Needs
4. Risk Management as a Continuous Organizational Process

During weeks 1-8 of the 16-week course, the topics above are covered in-depth through the facilitated use of a new textbook. Subsequently through week 11, risk management exercises are administered to reinforce learning. Weeks 12-15 involve a comprehensive final project that renders student posters for the upcoming Maritime Risk Symposium event. Lastly, week 16 brings the Cyber Risk Management course delivery to an end via a comprehensive final exam. Please see Appendix II for the current course syllabus and schedule.

Conclusion

Managing risk is a key component to achieving a strong cyber security posture. Practitioners must consider a combination of human, technology, and policy-based factors when establishing their postures. To help students understand these interdependencies, we designed and developed a course to apply, analyze, synthesize, and evaluate these in a real-world environment. Students have gained an appreciation for various technical and managerial concepts related to cyber security and demonstrated the knowledge gained by developing submissions to the annual Maritime Cyber Risk Symposium student poster contest. The efficacy of our approach after two offerings is based upon student feedback, ABET and NCAE assessment, and external results. The paper concludes with how we see the course evolving as the cyber systems major evolves. Teaching cyber-focused concepts in an interdisciplinary manner is critical to the proper understanding of cyber in the 21st century. Developing cyber professionals must have a well-grounded technical understanding of the cyber and then utilize and extend this knowledge to broader, nonlinear, and risk-infused environments. We hope this paper helps the reader examine how to implement this in an academic environment in order to graduate the next generation of well-balanced cyber professionals.

Works Cited

[1] "Maritime Risk Symposium," [Online]. Available: https://www.maritimerisksymposium.org/. [Accessed 22 January 2023].

[2] Department of Defense, "Cybersecurity," 7 October 2019. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf. [Accessed 22 January 2023].

[3] University of Bristol, "Cyber Security Body Of Knowledge," [Online]. Available: https://www.cybok.org/. [Accessed 22 January 2023].

[4] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," 16 April 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. [Accessed 22 January 2023].

[5] National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," Computer Security Resource Center, September 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. [Accessed 22 January 2023].

[6] "Maritime Risk Symosium Student Competition," [Online]. Available: https://www.maritimerisksymposium.org/student-poster-competition. [Accessed 2 February 2023].

[7] ABET, "Criteria for Accrediting Computing Programs, 2023 – 2024," [Online]. Available: https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2023-2024/. [Accessed 2 February 2023].

[8] NSA, "National Centers of Academic Excellence in Cybersecurity," [Online]. Available: https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/. [Accessed 2 February 2023].

[9] J. Estell, J. Yoder and B. Morrison, "Improving upon best practices: FCAR 2.0," in *119th ASEE Annual Conference and Exposition*, 2012.

[10] C. Brumfield and B. Haugli, Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework, Wiley, 2021.

[11] United States Coast Guard Academy, "Catalog of Courses 2021-2022," 2022. [Online]. Available: https://cgaportal.uscga.edu/academics/registrar/Course%20Catalogs/COURSE%20CATALOG%202021-2022.pdf. [Accessed 22 January 2023].

Appendix I – Cyber Risk Management Course 7385 Spring 2022 Syllabus

U.S. Coast Guard Academy
Department of Engineering
Cyber Risk Management (7385)
Course Syllabus

Introduction

Course: 7385 Cyber Risk Management
Course Offering: Spring 2022
Prerequisite: 7218 (Fundamentals of Info Security) and 8453 (Systems Analysis and Design)
Credits: 3.0
Textbook: The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities, (Wiley Finance) 1st Edition by Domenic Antonucci (ISBN-13: 978-1119308805/ ISBN-10: 1119308801). Available for free through USCG access to Skillport.

Instructor

CDR Joseph Benin, PhD

Course Description

Cyber Risk Management is designed to introduce students to Systems Engineering concepts to assess risks of cyber related vulnerabilities in the Maritime Transportation System (MTS) and Coast Guard C5I systems. The course will help students to understand how computers and cyber dependent technologies in large-scale systems throughout the Coast Guard and on commercial vessel and in ports enable the MTS to operate, as well as, how exploitation, misuse, or failure could disrupt the national defense and homeland security. This course will cover the Security Risk Assessment, Security Program Management, and Cybersecurity Planning & Management knowledge units from the DHS/NSA CAE Cyber Defense designation. This course will culminate in an innovative project normally themed in concert with the annual Maritime Risk Symposium.

Course Background

DoDI 8500.01 notes, “Cybersecurity Risk Management. Managing cybersecurity risks is a complex, multifaceted undertaking that requires the involvement of the entire organization, from senior leaders planning and managing DoD operations, to individuals developing, implementing, and operating the IT supporting those operations. Cybersecurity risk management is a subset of the overall risk management process for all DoD acquisitions as defined in Reference (av), which includes cost, performance, and schedule risk associated with the execution of all programs of record, and all other
acquisitions of DoD. The risk assessment process extends to the logistics support of fielded equipment and the need to maintain the integrity of supply sources.”

Note: This course and syllabus, including course requirements and grading, are subject to change. Any change will be posted on D2L.

Course Learning Outcomes

1. Apply knowledge to develop a security program, identifying goals, objectives, and metrics.
2. Apply knowledge to effectively manage a security program.
3. Assess the effectiveness of a security program.
4. Describe how risk relates to a system security policy.
5. Describe various risk analysis methodologies.
6. Evaluate and categorize risk
7. Select the optimal methodology based on needs, advantages, and disadvantages.
8. Examine the placement of security functions in a system and describe the strengths and weaknesses
9. Develop contingency plans for various size organizations to include business continuity, disaster recovery, and
incident response.
10. Develop system specific plans for: The protection of intellectual property, the implementation of access controls, and patch and change management Policies

Class Attendance

Except if otherwise instructed, every student must attend every class. If you must miss a session, please e-mail your instructor. If you expect to miss class on a date that an assignment is due, you are responsible for ensuring that your work is submitted on time. Students are responsible for all content covered each class.

Collaboration Policy

The collaboration policy for each assignment will be expressly stated in each handout. Submitted work must be your own (i.e. you must have developed and have a reasonable understanding of what you submit) or that of a teammate for group assignments (you must also understand what they have prepared). You may not make arrangements with another (for fee or free) to complete work for yourself and submit it as your own. Students who are unable to explain work submitted can lose up to all points for that assignment. All resources used (excluding class text and notes), collaboration, and assistance received (except from faculty) must be cited on submitted work. Simply copying another's work (either past or present) is expressly prohibited. The use and studying of previous year's course material is explicitly allowed. You are ultimately responsible for knowing and following the appropriate collaboration policy of each assignment and must discuss any questions with your instructor.

Course Topics and General Schedule

Week 1 – Introduction and the MTS Side
Topic:
Broad coverage of the systems engineering as it is applied to understanding the Maritime Transportation System and
the CG's C5I infrastructure

Week 2 – The CG Side
Topic:
Broad coverage of the systems engineering as it is applied to understanding the Maritime Transportation System and
the CG's C5I infrastructure

Week 3 – Roles and Responsibilities
Topics:
1. Define the roles and responsibilities within the security organization
2. Examine C-Level Functions which impact cybersecurity
3. Define the goals and objectives of a security program
4. Describe various risk analysis methodologies

Week 4 – Cyber Security BOK (Body of Knowledge) or CBK (Common Body of Knowledge)
Topics:
1. Broad coverage of the cybersecurity Common Body of Knowledge (CBK) and how it affects planning and
management
2. Differentiate and provided examples of Operational, Tactical, and Strategic Planning and Management
3. Making cybersecurity a strategic essential (part of core organizational strategy)

Week 5 – Risk Mitigation/Acceptance/Transference
Topics:
1. Risk Assessment/Analysis Methodologies
2. Risk Measurement and Evaluation Methodologies
3. Risk Management Models
4. Risk Mitigation Economics
5. Communication of Risk

Weeks 6-10 – Lets build a port security plan!
Topics:
1. Goals and objectives of a security program
2. Risk Assessment: Measuring the effectiveness of a security program (metrics)
3. Risk Management Processes
4. What are you protecting?
a. Protection of Intellectual Property
b. A^3, A^I, IdAM/ICAAM - Access, Authentication, Authorization, Identification (The world behind the CAC)
c. Configuration Management/System Identification
d. Physical Security
e. Patch and Change Control/Management
f. Incident Response

Weeks 11-15 – Final Project
Theme that is aligned with the Maritime Risk Symposium (MRS) student poster contest

Appendix II – Cyber Risk Management Syllabus Spring 2023

U.S. Coast Guard Academy
Department of Engineering
Cyber Risk Management (7385)
Course Syllabus

Introduction

Course: 7385 Cyber Risk Management
Course Offering: Spring 2023
Prerequisite: 7218 (Fundamentals of Info Security) and 8453 (Systems Analysis and Design)
Credits: 3.0
Textbook: Cybersecurity Risk Management: Mastering the Fundamentals using the NIST Cybersecurity Framework,
(Wiley) 1st Edition by Cynthia Brumfield with Brian Haugli (ISBN-Digital: 978-1-1198-1634-8; ISBN-Print: 978-1-1198-1628-7. E-book available for free via the Coast Guard Academy Library.

Instructor

Angela Jackson-Summers, PhD

Course Description

Cyber Risk Management is designed to introduce students to Systems Engineering concepts to assess risks of cyber related vulnerabilities in the Maritime Transportation System (MTS) and Coast Guard C5I systems. The course will help students to understand how computers and cyber dependent technologies in large-scale systems throughout the Coast Guard and on commercial vessel and in ports enable the MTS to operate, as well as, how exploitation, misuse, or failure could disrupt the national defense and homeland security. This course will cover the Security Risk Assessment, Security Program Management, and Cybersecurity Planning & Management knowledge units from the DHS/NSA CAE Cyber Defense designation. This course will culminate in an innovative project normally themed in concert with the annual Maritime Risk Symposium.

Course Background

DoDI 8500.01 notes, “Cybersecurity Risk Management. Managing cybersecurity risks is a complex, multifaceted undertaking that requires the involvement of the entire organization, from senior leaders planning and managing DoD operations, to individuals developing, implementing, and operating the IT supporting those operations. Cybersecurity risk management is a subset of the overall risk management process for all DoD acquisitions as defined in Reference (av), which includes cost, performance, and schedule risk associated with the execution of all programs of record, and all other acquisitions of DoD. The risk assessment process extends to the logistics support of fielded equipment and the need to maintain the integrity of supply sources.”

Course Learning Outcomes

1. Apply knowledge to develop a security program, identifying goals, objectives and metrics.
2. Apply knowledge to effectively manage a security program.
3. Assess the effectiveness of a security program.
4. Describe how risk relates to a system security policy.
5. Describe various risk analysis methodologies.
6. Evaluate and categorize risk
7. Select the optimal methodology based on needs, advantages, and disadvantages.
8. Examine the placement of security functions in a system and describe the strengths and weaknesses
9. Develop contingency plans for various size organizations to include business continuity, disaster recovery, and incident response.
10. Develop system specific plans for: The protection of intellectual property, the implementation of access controls, and patch and change management policies.

Collaboration Policy

All INDIVIDUAL assigned work for completion and submission for grading, including homework as take-home assignments, readings, and quizzes should be performed as an individual effort, which means NO collaboration with others should be engaged. If any individual assigned work is deemed to have not been performed as an individual effort (i.e., cheating, plagiarized), the specific assignment will be marked as a zero (0) grade.

Collaboration, including group discussions and review of weekly chapter readings from Brumfield and Haugli (2022) is highly encouraged. Students may study together and help each other to understand course concepts and meet stated learning objectives.

Submitted work must be your own (i.e. you must have developed and have a reasonable understanding of what you submit) or that of a teammate for group assignments (you must also understand what they have prepared). You may not make arrangements with another (for fee or free) to complete work for yourself and submit it as your own.

Students who are unable to explain work submitted can lose up to all points for that assignment.

All resources used (excluding class text and notes), collaboration, and assistance received (except from faculty) must be cited on submitted work. Simply copying another's work (either past or present) is expressly prohibited. The use and studying of previous year's course material is explicitly allowed. You are ultimately responsible for knowing and following the appropriate collaboration policy of each assignment and must discuss any questions with your instructor.

Class Attendance

If you are going to miss class, please inform the Instructor in advance of your designated class start time.

Planned Course Schedule

Weeks 1-5

- Welcome & Course Overview
- Introduce Information Systems/Cyber/IT Risk Management in Organizations
    - Risk Management Capability & Maturity Model Importance
    - Information (Cyber) Security Risk Management Frameworks
    - Organizational Risk Management Posture
- Introduce Cyber Risk Management and Scope of Importance to the USCG
    - Preface – Overview of the NIST Framework (Brumfield, 2022)
    - Ch. 1 – Cybersecurity Risk Planning and Management (Brumfield, 2022)

Weeks 6-8

- Understand the Cyber Risk Management Process, Internal/External Critical Activities, and Supporting Tools and Techniques
    - Ch. 2 – User and Network Infrastructure Planning and Management (Brumfield, 2022)
    - Ch.3 – Tools and Techniques for Detecting Cyber Incidents (Brumfield, 2022)
- Build a Port Security Plan

Weeks 10-12

- Understand the Cyber Risk Management Process, Internal/External Critical Activities, and Supporting Tools and Techniques cont'd
    - Ch. 4 – Developing a Continuity of Operations Plan (Brumfield, 2022)
    - Ch. 5 – Supply Chain Risk Management (Brumfield, 2022)
    - Ch. 6 – Manufacturing and Industrial Control Systems Security (Brumfield, 2022)
- Build a Port Security Plan cont'd

Weeks 12-16

Comprehensive Final Project

Theme aligned with the Maritime Risk Symposium (MRS) student poster contest

Appendix III – Cyber Risk Management Prerequisite Course Descriptions

7218 FUNDAMENTALS OF INFORMATION SECURITY

Fundamentals of Information Security is designed to provide an introduction to information security, information assurance, and cyber systems. The Course will help students to begin to develop a common lexicon and to start to delve into the threats to information systems, the risk those threats pose to systems, the vulnerabilities that may be exploited, and the mitigations to those vulnerabilities.

Credit Hours: 3.00
Format: Class
Prerequisites: None
Projected Offering: Fall

8453 SYSTEMS ANALYSIS AND DESIGN

Examination of the concepts, tools, and development methodologies used in information systems analysis and design. Feasibility study, requirements analysis, design, and development documentation are covered. The system development life cycle, prototyping, data modeling, and user involvement are also covered. Course prepares students to improve organizational functions through the System Development Life-Cycle in roles varying from System Analyst to System User. A real-world application is conducted through a term project.

Credit Hours: 3.00
Format: Class/Project/Cases
Prerequisites: 8331 or equivalent
Projected Offering: Fall

Source: USCGA Course Catalog [11]