HSEM 417: Cyber Security Resiliency (Fall 2016)
Credits: 3
Location: TBD based on classroom availability
Prerequisites: HSEM 301 or permission of instructor
Instructor: Tom Langdon
Adjunct Professor
School of Management, University of Alaska Fairbanks
Office: 230A Bunnell
Office Hours: TBD
Telephone: 907.474.1869
E-mail: tjlangdon@alaska.edu

Course Description:

This course focuses on the challenges faced by organizational leadership resisting, responding, and recovering from cyber-attacks impacting business critical data. This course will further the understanding of a new and demanding career field emerging within the emergency management and homeland security fields. Without the knowledge of how to build a cyber security resilient organization, the future emergency manager will be lacking critical skills.

Course Objectives:

Develop an understanding of:

- Relevancy of Cyber Security to organizations today
- Prevention and responses to cyber security incidents
- Assessment and management of ongoing cyber security risks
- Understanding of cyber security resiliency to protecting business continuity
- Understand industry best practices for resilient cyber architecture and infrastructure

Student Learning Objectives:

Student will be able to:

- Understand how to update systems to prevent cybercrime through resiliency.
- Explain the importance of cyber resiliency to today’s IT industry.
- Utilize cyber resilience designs to update their IT systems.
- Address the risks and opportunities that cyber systems are induced with.

Course Text Books:

1. Rance, Stuart, Mike St John-Green, and Moyn Uddin. *Cyber Resilience Best Practices*. Stationery Office, 2015. Print.
2. Vincent, Jerome. *Whaling for Beginners*. Vol. Book 1. Axelos, 2015. Print.

Additional Reading:

Additional reading assignments have been selected from articles and Web Sites. Where possible, the course author has obtained permission to include session handouts of the assigned reading.

Instructional Method:

The course format includes lecture, directed reading assignments, class discussion board topics and internet-based assignments via Blackboard. Case Study presentations will additionally be utilized as part of the instructional method with guest speakers facilitating discussions through lecture and questions developed as a class. Recommended preparation: 9 hours weekly beyond class instruction

Evaluations:

1. Weekly Assignments/Discussion Board Management 30%.
   - A. Total of 5 Quizzes are worth 20 points each.
   - B. Total of 10 Discussion Board Posts are worth 20 points each.
     - i. Discussion Board Posts are required to be approximately 250 words in length.
       - 1. The first post will be worth 10 points
     - ii. Students will also be required to comment, constructively, on at least 2 other student's posts each week. These comment should be no less than 150 words.
       - 1. Each of the 2 comments on another's posts will be worth 5 points for a total of 10 points.

2. Written Projects = 65%

   - A. Five (5) case study papers (100 points each): The papers are to be 3-4 pages in length and consistent with the APA format.
     - i. These case studies will require you to identify a cyber security incident, research, and evaluate the incident. In your paper you will build a brief of the incident and how it was managed by the affected organization.
     - ii. A grading rubric for the case studies is attached to the back of this syllabus.
   - B. Create a cyber disaster recovery and business continuity plan for a public or private organization (150 points)
     - i. This plan should be 5-7 pages in length and will be developed in consultation with the instructor.
     - ii. The grading rubric for the BCP is attached to the end of this syllabus.

   ***For additional information on APA formatting: https://owl.english.purdue.edu/owl/resource/560/01/

3. IS – 523 Certificate = 5%
   - A. Completion of IS 523 FEMA Certificate = 5% (FEMA will only award the certificate with a passing score of 70%)

Grading:

Quizzes (5) & Discussion Board Management (10) = 30% (300 points)
Case Study Briefs (5 papers) = 50% (500 points)
Cyber Disaster & Business Continuity Plan = 15% (150 points)

IS 523 Certificate = 5% (50 points)
Total = 1000 points

A= 90-100% B= 80-89% C= 70-79% D= 60-69% F= 59 % or less

Course Policies:

Students are expected to attend and participate in both the class and discussions generated. Students will be penalized for the late submission of class assignments by losing 10% of available points each day, up to 100%. Students will also be penalized for non—attendance (outside of emergency or mutually agreed upon circumstances). Plagiarism on assignments and cheating on exams will not be tolerated. Work is to be original efforts to address the specific assignment at hand (in other words, don't submit work from another course). Students caught plagiarizing or cheating will be disciplined according to the appropriate University of Alaska guidelines.
**Discussion Board etiquette: When both posting and responding to the discussion board requirements, remember that these are graded activities. Content is to address the requirement at hand and in terms of a response, be respectful and constructive in nature. Be sure to read the discussion board rubric found in the rubric folder for the course.

Support Services:

Students are encouraged to schedule an initial appointment and utilize the UAF Writing Center in 801 Gruening, ph 474-5314, http://www.uaf.edu/english/writing-center/ for the first written case study review. Further assistance through the writing center is encouraged as needed to assist in the development and refinement of written products. Please contact me as required should you need to contact other subject matter support services relevant to the development of your leadership or classroom projects/topics.
Distance students have access to the tutoring as well.

Students with Disabilities:

Students with learning or other disabilities who may need classroom accommodations are encouraged to make an appointment with the Office of Disability Services (Phone # 474-5655). Please inform me of your needs and if I need to meet with the Office of Disability Services to provide the appropriate accommodations and support to assist you in meeting the goals of the course.

Course Schedule:

Week 1:
Introduction
Review Syllabus
Assign Cyber Continuity Plan

Week 2:
Reading:
-Chapter 1 in Whaling Text
-Chapter 1 in Axelos Text
Discussion Board #1: Introductions

Week 3:
Reading:
-Chapter 2-4 in Whaling Text
Discussion Board #2
Assign Case Study #1

Week 4:
Reading:
-Chapter 2 in Axelos Test
Discussion Board #3: Risk Approaches

Week 5:
Reading:
-Chapter 3 in Axelos Text
Quiz 1
Case Study #1 Due

Week 6:
Reading:
-Chapter 4 Axelos Text
Quiz 2

Week 7:
Reading:
-Chapter 4 in Axelos Text
Discussion Board #4
Assign Case Study #2

Week 8
FEMA IS 523
Quiz #3
Discussion Board # 5

Week 9
Reading:
-Chapter 5 Axelos Text
Case Study #2 Due
Discussion Board #6

Assign Case Study #3

Week 10
Reading
-Chapter 6 Axelos Text
Discussion Board #7

Week 11
Reading
-Chapter 7 Axelos Text
Quiz 4
Case Study #3 Due
Assign Case Study #4

Week 12
Reading
-Chapter 7 Axelos Text
Discussion Board #8

Week 13
Reading
-Chapter 8 Axelos Text
Discussion Board #9
Case Study #4 Due
Assign Case Study #5

Week 14
Reading
-Chapter 9 Axelos Text
Quiz 5

Week 15
Reading
-current event topic defined by instructor
Case Study #5 Due
Discussion Board #10

Week 16
Finals Week (no finals for this course)
Cyber Continuity Plan Due

417 Case Study Rubric

Written Paper

Students will be required to research and analyze a cyber security incident for the case studies. After analyzing the incident, students will provide an introduction with background information of the incident, as well as how the incident was resolved (whether it was successful or unsuccessful). Furthermore, students will provide at least 3 lessons learned from the events that can be used as examples of what was done right (or wrong) during the incident resolution.

Additionally, your paper needs to be double spaced, and include a cover page (this does not count as one of the 3-4 pages). It will be worth **100 points** and it will be evaluated using the grading criteria listed below. All papers must be written APA format and all sources need to be cited appropriately.

Organization	*/15*
Style	*/15*
Content	*/50*
Grammar/spelling	*/20*

Papers turned in after the due date will be penalized.

417: Final Paper
Cyber Disaster Recovery Plan and Business Continuity Plan

Paper Requirement

To complete this, individuals will develop a business continuity plan "portfolio" based upon the analysis of either a private or public sector organization. Developing a plan for the organization you work for is the ideal direction of the plan, but not necessarily the only option in completing the project. Students are required to work with the instructor during the development of this plan and a consultation will need to occur at least once. This paper should be around 5-7 pages in length (double spaced with a cover page) and should encompass all of the elements utilized in business continuity plans. Templates are available in Blackboard to assist students with the development of their plans. To supplement the BCP elements found in the text, a folder in the Course Materials area has been set up (entitled Business Continuity Planning Documents) to provide you with examples and templates. **This part of the project will be worth 150 points.**

The points allocated for the **first** portion of writing:

Organization	*/30*
Format	*/20*
Content	*/50*
Grammar/spelling	*/30*
Instructor input	*/20*

***Papers turned in after finals week (May 6th) will not be accepted.**