Cosumnes River College
CISS 350
Disaster Recovery
A Hybrid-Online Course
Fall 2017
(1st 8 weeks)

Instructor: Buddy Spisak **Office Hours**: Mon. 6:00-7:00 p.m. (Aug. 21 to Dec. 11)

Office: BSS-143
Voice Mail: (916) 286-3691 ext. 14162
Email: spisakj@crc.losrios.edu The turnaround time for responding to most emails is about one to two days. Be sure to include your name and the course number in each email so I can identify who you are and what the email is about.
Course Web page: https://canvas.losrios.edu/
Instructor Web page: http://crc.losrios.edu/spisakj/

Prerequisites: CISS 310
Advisory: None
Lecture: Online
Laboratory: Th 6:00 to 8:05pm in BS-153
Accepted for Credit: CSU
Class Credits: 3 units

Required Textbook:

Title:	*Principles of Incident Response and Disaster Recovery*, 2nd ed.
Authors:	Michael E. Whitman, Herbert J. Mattord, and Andrew Green
Publishing Info:	Course Technology, 2014
Textbook ISBN13:	978-1-111-13805-9
E-Book ISBN13:	978-1-285-71262-8

Optional Materials: A flash drive to store your work for the class

Course Description:

This course teaches students how to identify network vulnerabilities and how to take the appropriate countermeasures to prevent and mitigate failure risks for an organization. Students will gain an understanding of the steps needed for good disaster recovery, including how to prepare a disaster recovery plan, the various risks associated with an enterprise network, the diverse job functions of employees in a disaster recovery plan, and the methods needed to implement a plan once it is complete. In addition, each student will develop a disaster recovery plan with a group for a real or fictitious organization.

Student Learning Outcomes and Course Objectives:

- DEFINE AND EXPLAIN INFORMATION SECURITY (SLO #01).
  - Define and explain the basic concepts of risk management.
  - Identify and define the components of contingency planning.
  - Know and understand the role of information security policy in the development of contingency plans.

- MANAGE INCIDENT RESPONSE AND DISASTER RECOVERY PROCEDURES (SLO #02).
  - Identify an individual or group to create a contingency policy and plan.
  - Understand the elements needed to begin the contingency planning process.
  - Create an effective contingency planning policy.
  - Comprehend the steps needed for a business impact analysis report.
  - Summarize the steps needed to create and maintain a budget for enabling the contingency planning process.
- ANALYZE THE PROCESS OF INCIDENT RESPONSE PREPARATION (SLO #03).
  - Describe the process used to organize the incident response process.
  - Understand how policy affects the incident response planning process and how policy can be implemented to support incident response practices.
  - Describe the techniques that can be employed when forming a security incident response team (SIRT).
  - Learn the skills and components required to devise an incident response plan.
  - Know some of the concerns and trade-offs to be managed when assembling the final IR plan.
- IDENTIFY TRUE INCIDENTS FROM INCIDENT CANDIDATES AND FALSE POSITIVES (SLO #04).
  - Identify the elements necessary to detect incidents that pose risk to the organization.
  - Summarize the components of an intrusion detection system.
  - Explain the processes used in making decisions surrounding incident detection and escalation.
- UNDERSTAND THE ELEMENTS OF AN INCIDENT RECOVERY RESPONSE (SLO #05).
  - Build the elements of an incident recovery response, and be aware of the impact of selecting a reaction strategy, developing a notification mechanism, and the creation of escalation guidelines.
  - Explain how an organization plans for and executes the recovery process when an incident occurs.
  - Summarize the need for and the steps involved in the ongoing maintenance of the incident response plan.
  - Summarize what forensic analysis entails, and gain an improved understanding in the processes used to collect and manage data in an electronic environment.
- PLAN FOR BUSINESS RESUMPTION FOLLOWING AN INCIDENT (SLO #06).
  - Outline the relationships between the overall use of contingency planning and the subordinate elements of incident response, business resumption, disaster recovery, and business continuity planning.
  - Become familiar with the techniques used for data and application backup and recovery.
  - Outline the strategies employed for resumption of critical business processes at alternate and recovered sites.
- PLAN FOR A DISASTER RECOVERY (SLO #07).
  - Summarize the ways to classify disasters, both by speed of onset and source.
  - Explain who should form the membership of the disaster recovery team.
  - Summarize the key functions of the disaster plan. Explain the key concepts included in the NIST approach to technical contingency planning.
  - Describe the elements of a sample disaster recovery plan.
  - Identify the need for simultaneous wide access to the planning documents as well as the need for securing the sensitive content of the DR plans.
- SUMMARIZE THE KEY CHALLENGES AN ORGANIZATION FACES WHEN ENGAGED IN DISASTER RECOVERY OPERATION (SLO #08).
  - Recognize what actions organizations take to prepare for the activation of the DR plan.
  - Recognize what critical elements compose the response phase of the DR plan.
  - Comprehend what occurs in the recovery phase of the DR plan.
  - Identify how an organization uses the resumption phase of the DR plan.
  - Identify how an organization resumes normal operations using the restoration phase of the DR plan.
- OUTLINE THE ELEMENTS OF BUSINESS CONTINUITY (SLO #09).
  - Recognize who should be included in the business continuity team.
  - Recognize and be able to reference two sample business continuity plans.
  - Describe the steps taken to maintain the BC plan.

- Summarize the methods used to continuously improve the BC process.

- CREATE AND DEVELOP A CRISIS MANAGEMENT PLAN (SLO #10).
  - Recognize the role of crisis management in the typical organization.
  - Conduct the creation of a plan preparing for crisis management.
  - Value and deal with post-crisis trauma and work toward getting people back to work after a crisis.
  - Identify the impact of the decisions regarding law enforcement involvement.
  - Manage a crisis communications process.
  - Prepare for the ultimate crisis in an organization through succession planning.

Methods of Measuring Student Learning Outcomes:

- You will demonstrate knowledge of network and internet security applications and standards through class discussions and achievement on quizzes and final examination.
- You will demonstrate competence in the coursework by completing projects and participating in discussions during the semester.

Student Obligations:

- **Attendance**: Since this course is online, only attendance at the On-Campus Orientation on August 24 and the Final on October 5 is necessary. There will be weekly lab time on campus, and it is up to you to complete the lab assignments during the lab time or at home.
- **Discussions**: I want everyone to take a pro-active approach to learning this material. This includes using the Discussions link to ask questions and also answer other students' questions. I will also post questions each week that you can answer to further your understanding of the material. I expect two postings each week unless otherwise noted.
- **Projects**: There will be six hands-on projects and six case projects credited for homework for the class. The projects will help reinforce what you are learning in each lesson. The due dates are located in the **SCHEDULE** portion of this handout. You will submit your results into the Canvas discussions area in order to receive points for that assignment. On all projects you are expected to do your own work.
- **Quizzes**: After each lesson you will be required to take a short quiz, which will test you on the material covered. It is open-book and open-notes. You can take the quiz multiple times to improve your score, but be aware that the questions will change each time and that your most recent score will be the one counted as the grade.
- **Final Exam**: The final exam will consist of two parts. One part of the exam will be a hands-on practical demonstration of assigned tasks, and the other part will be an exam taken in Canvas.
- **Late Work**: Unless noted, all assignments are due on Sunday by midnight each week. Late work will be accepted ONLY if you have contacted me prior to the due date either by email or voice mail. In general, late work is due the next week, and no late assignments may be turned in after one week from the original due date, regardless of the reason. For every day an assignment is late, you will lose 10% of its grade.
- **Due Dates**: Unless noted, all assignments will be submitted in Canvas. If, for any reason, you cannot access Canvas or are unable to submit the assignment on time, please email it to me instead so that you are not penalized for being late. Quizzes cannot be taken, nor can discussion items be completed after their due dates. If you miss a quiz and you want to make up points, you can take advantage of the extra credit assignments posted in Canvas. Everyone is welcome to work on the extra credit assignments. Typically, they are five to ten points each, depending on the difficulty of the assignment.
- **Plagiarism Policy**: It is inappropriate, and a violation of academic policy, to copy information from any source (including, but not limited to, textbooks, magazine articles, newspaper articles and internet articles) without giving proper credit to the author by using standard quotation procedures such as in-line quotes, footnotes, endnotes, etc. Quotes may not exceed 25% of the

assignment's total length. You will receive no credit (0 points) for any assignment that copies any material from any other source without giving proper credit to the author(s). Repeat offenders of this policy are subject to academic discipline as outlined in the policies published by the college.

- **Cheating**: Students who cheat will receive a failing grade for the course. [See the Student Behavior and Academic Integrity page of the college website (https://www.crc.losrios.edu/catalog/geninfo/integrity).]
- **CRC Honor Code:** Academic integrity requires honesty, fairness, respect and responsibility. [See the Cosumnes River College Honor Code posted on the college website (https://www.crc.losrios.edu/facstaff/resourceguide/faculty/student-behavior-academic-integrity/honorcode - https://www.crc.losrios.edu/facstaff/resourceguide/faculty/student-behavior-academic-integrity/honorcode)].
- **Email**: Every student will be required to have an email account. If you do not have an email account, the college provides free email accounts for all current students. To activate your account, go to https://apps.losrios.edu/login.html and follow the directions provided.
- **Email etiquette**: I will not tolerate rude and demeaning comments or emails to anyone in this class. Please keep your comments and emails topic-related. If I determine that a comment or email to anyone else in the class is rude or demeaning, I will warn you once. If your behavior continues to be unacceptable, I will refer you to the administration of the college for disciplinary action.
- **Personal belongings**: No food or drinks are allowed in the classroom. All cell phones, beepers, pagers, etc. should be turned off or set to vibrate.
- **Disabilities:** If you have a documented disability and wish to discuss academic accommodations, please contact me or contact the Office of Disabled Student Programs and Services at 691-7275 as soon as possible.
- **Campus Police**: You can call 558-2221 to request a safety escort.
- **Canvas:** This class utilizes a product called "Canvas." It is highly recommended that you check the website frequently for scheduling updates and homework assignments. Most of the homework assignments and quizzes will be done on Canvas.
- **Course Responsibilities:** This course requires significant self-motivation. You must not get behind. Labs and weekly assignments can take up to eight hours to finish. Please don't try to finish them in one day. Not all activities are created equal. Some may take a bit longer than others. You would normally spend 3 hours per week in class for this course: total of 54 hours. Allow yourself at least 8 hours per week to complete the activities online, including the time spent writing for the postings to the discussions page. You should plan additional time to read the textbook and study for the quizzes. Some people believe this is a much easier way to study this subject than an on-campus framework because they love to read and avoid the parking problems. Others feel very intimidated at first. Be patient as you work your way through the activities.

Grading:

Course Topic		Points	Total	Approximate % the of Grade
Hands-on Projects (6)		50	300	30
Case Projects (6)		20	120	13
Orientation Quiz (1)		10	10	1
Quizzes (6)		30	180	19
Discussions (6)		20	120	13
Final Exam (1)		200	200	24

Point System: There are 930 total assigned points.

Grade Ranges: A= 837-930, B=744-836, C=651-743, D=558-650, F=0-557

Schedule: It is tentative and can change during the course for the term.

Week:	Day:	Date:	Proposed Schedule:	Assignment Due:	Due Date (By Midnight):
Week 1	Thurs.	8/24	Orientation and Introductions	Discussion #1	Sun., Sept. 3
			View the Online Orientation	Orientation Quiz	
			Read Ch 1: An Overview of Information Security and Risk Management Read Ch 2: Planning for Organizational Readiness		
			Do all Hands-on Projects and one Case Project from either Chapter 1 or 2	Quiz #1	
				Hands-on Project #1	
				Case Project #1	
Week 2	Thurs.	8/31	Read Ch 3: Contingency Strategies, IR/DR/BC Read Ch 4: Principles of Incident Response and Disaster Recovery	Discussion #2	Sun., Sept. 10
			Do all Hands-on Projects and one Case Project from Chapter 3 or 4	Quiz #2	
				Hands-on Project #2	
				Case Project #2	
Week 3	Thurs.	9/7	Read Ch 5: IR: Detection and Decision-Making Read Ch 6: IR: Organizing and Preparing the CSIRT	Discussion #3	Sun., Sept. 17
			Do all Hands-on Projects and one Case Project from Chapter 5 or 6	Quiz #3	
				Hands-on Project #3	
				Case Project #3	
Week 4	Thurs.	9/14	Read Ch 7: IR: Response Strategies Read Ch 8: IR: Recovery and Maintenance	Discussion #4	Sun., Sept. 24
			Do all Hands-on Projects and one Case Project from Chapter 7 or 8	Quiz #4	
				Hands-on Project #4	
				Case Project #4	
Week 5	Thurs.	9/21	Read Ch 9: DR: Preparation and Implementation Read Ch 10: DR: Operation and Maintenance	Discussion #5	Sun., Oct. 1
			Do all Hands-on Projects and one Case Project from Chapter 9 or 10	Quiz #5	
				Hands-on Project #5	
				Case Project #5	
Week 6	Thurs.	9/28	Read Ch 11: Business Continuity Planning Read Ch 12: Crisis Management and International Standards in IR/DR/BC	Discussion #6	Sun. Oct. 8
			Do all Hands-on Projects and one Case Project from Chapter 11 or 12	Quiz #6	
				Hands-on Project #6	
				Case Project #6	
Week 7	Thurs.	10/5	Final Exam		