BOR3309
Information Security Protection

Course Description

From the Course Catalog:

"BOR 3309 Information Security and Protection (3-0). This course prepares students to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation and maintenance of security devices, systems, and procedures. Reviews of past hacking, criminal, and terrorist (state and non-state) attacks on information networks are a component of this course."

Course Textbook:

Jason Andress (2011), The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice 1st Edition, Elsevier Inc ISBN 978-1-59749-653-7

Prerequisites

As with all online courses, students must be able to operate a computer and have the necessary technical skills to navigate around a web page. Additional technical skills are not a prerequisite for this course, nor are any academic skills except the ability to communicate fluently in the English language.

The last day to drop this course is March 25, 2013.

The last day to add this course is March 22, 2013.

Course Objectives/Learning Outcomes

Upon successful completion of this course, the student will demonstrate knowledge and ability to apply the following learning topics:

1. Define, discuss, and recognize important terminology, facts, concepts, principles, and theories taught in BOR3309 Information Security and Protection course.
2. Demonstrate an understanding of how to approach and apply reasonable Information Security and Protection solutions to Information Security and Protection problems.
3. Discuss the relevance and application of InfoSec to contemporary threats and events.
4. Improve student critical thinking and critical writing skills.

Students can expect to spend about 6 hours each week doing outside readings and working exercises. The lessons themselves take as long as the student will require to read the materials and watch or listen to media presentations.

Grading Policies

While I do not enforce a strict policy on grammar, I do reserve the right to stop reading your paper if spelling errors, sentence construction, or grammar is below the minimum expected for an undergraduate course. If I stop reading a particular paper or discussion thread you have written, for reasons listed above, the paper or discussion thread will receive a failing grade.

The University policy on grades of "Incomplete" is that the deficiency in performance must be addressed satisfactorily by the end of the next long (16 week) semester or the grade automatically becomes an "F". Grades of "I" will only be awarded to students who have demonstrated sufficient progress to earn the opportunity to complete the course outside of the normal course duration. The award of an "Incomplete" will only be made in rare circumstances, with the concurrence of the student and the professor on what specific tasks remain and when they are due for the grade to be changed to a higher grade. The determination of the need to award an "Incomplete" is entirely up to the professor's personal judgment.

By virtue of being online, this course emphasizes reading and writing. Because there is no lecture, all of the information you receive will come from your careful reading of the textbook, course overviews, and any assigned supplementary readings. You can ask questions of the instructor through Course E-Mail or of other students through the *Student Discussion* area in the "Discussions" section. There will be two (2) **types** of written assignments in this course, which are described below.

This course utilizes seven (7) discussion threads, two (2) self-assessment exercises, and a security assessment project to measure the student's comprehension of the presented materials. There is an extensive amount of reading assigned that will drive student responses to discussion questions and writing assignments and the student should be prepared to spend upwards of six (6) hours each week on this course:

Weekly Discussion Thread	50%
Self-Assessment Exercises	10%
Security Assessment Project	40%
Total	100%

Angelo State University employs a letter grade system. Grades in this course are determined on a percentage scale:

Percentage of Total Points	**Grade**
90%-100%	A
80%-89%	B
70%-79%	C
60%-69%	D
59% and Below	F

Discussion Threads

Each discussion thread is graded on a 100 point scale using a Discussion Rubric. A "Robust" initial posting is expected to be at least 250 words in length and include appropriate citations and references. Combined, the discussion threads will count for 45% of your course grade.

In general, good tests of the quality of your analyses are to ask yourself "Does this answer show that I read and understood the material in the text?" or "Could I have written this answer without reading the book?" While not always true, generally speaking, if a student could write the answer without the benefit of the course, then the answer doesn't adequately reflect the information taught in the course. Common sense and your prior experiences will seldom suffice when answering discussion topic assignments. Good answers will clearly demonstrate your comprehension of the concepts and terms introduced in the course.

Grades will reflect the instructor's judgment about the "quality" of the analysis, the application of theory to facts, and the "quality" of the writing. Because of the importance of writing in an online course, and the fact that you have a sufficient amount of time to draft and edit your responses, students are expected to write well-reasoned, concise, and clear answers. Answers must not be too terse or too detailed. As noted above, the equivalent of half a page should not be exceeded in presenting your assessment or observation to other student discussion postings. Replies to other student postings with too many words are usually a sign of poor editing; however, too few words can be a sign of poor analysis or the failure to apply relevant theories and concepts to the case's facts. The point is for you to write what you mean and mean what you write.

Writing Assignments

All writing assignments are expected to conform to a standard format and writing style. Text should be Times New Roman, 12 point font, with one-inch margins all around. Submitted papers will be double-spaced, have appropriate citations and a reference list where appropriate. Include a properly formatted reference list and cover page with every assignment. Written work will be graded by use of a Writing Rubric.

Formal academic writing uses standardized styles and citation formats. The preferred format is the APA style. To access the APA writing guidelines go to this link: http://owl.english.purdue.edu/owl/resource/560/01/.

Should you wish to use CHICAGO style that will be acceptable. The Chicago Style guide can be found at http://www.chicagomanualofstyle.org.

Every writing assignment should be submitted as a WORD or PDF document. If you do not have Microsoft Office or Adobe Acrobat, then copy the text you have written directly into the assignment section of Blackboard during the appropriate week. Do NOT submit writing assignments in Word Perfect, Microsoft Works, or some e-mail format. They will not be accepted.

For the purposes of this course, an abstract is not necessary on written assignments.

Self-Assessments

There are two (2) self-assessment exercises which will be graded using the Writing Rubric. Specific instructions on the content of the self-assessments will be addressed in Lesson 1 and Lesson 7.

A **self-assessment** helps you gain insight into yourself and your preferences. As such, there normally is no right or wrong answers to self-assessment exercises, but the accuracy of your personal analysis and insight will be graded. In relating to the required questions to be answered what you choose to reflect upon is up to you. Points will be deducted for incomplete or incorrectly self-assessment exercises, and if you do not discuss the accuracy of the questions are asked to evaluate.

Security Assessment Project

Scenario: You have been asked by your Supervisor to research a subject that you feel needs to be addressed relating to your organization's (your choice or type of company) Information Security and Protection Program and how it relates to your company so that it can be shared with the CEO and Executive Staff.

You must develop a Power-Point presentation not to exceed five (5) slides (including reference slide) covering your issue, how it effects your company, and suggested corrective action. This must be accompanied by a three (3) page executive summary covering the information in your Power-Point presentation (reference page needed). Must use and cite at least four (4) sources. This assignment must be sent to the instructor no later than Friday midnight (CST) of week eight (8) of class. Send Final Power-Point Presentation and Executive Summary to instructor as a PDF.

Rubrics

Discussion forums and writing assignments will be graded using a standardized rubric. It is recommended that you be familiar with these grading criteria and keep them in mind as you complete the writing assignments. There are two rubrics. Click the link to download the PDF document:

Discussion Rubric
Writing Assignment Rubric

Date and Time of Final Exam

This course uses a final InfoSec project in lieu of an exam to measure student comprehension and synthesis of the course materials. This final project is due on Friday of the last week of class.

Office Hours and/or hours of outside-of class contact

This is an online course. My office hours will be posted under Instructor Information in Blackboard. I will make every endeavor to reply to phone and e-mail messages within 24 hours. But like you, I have travel obligations that may preclude me from always being expeditious in my response.

Course Organization:

Lesson One:

In this lesson, we will cover some of the most basic concepts of information security. Information security is vital in the era in which data regarding countless individuals and organizations is stored in a variety of computer systems, often not under our direct control. We will talk about the diametrically opposing concepts of security and productivity, the models that are helpful in discussing security concepts, such as the confidentiality, integrity, and availability (CIA) triad and the Parkerian hexad, as

well as the basic concepts of risk and controls to mitigate it. Lastly, we will cover defense in depth and its place in the information security world.

- Self-Assessment Exercise (Week 1)

Lesson Two:

In this lesson, we will cover the security principles of identification and authentication. We will discuss identification as a process by which we assert the identity of a particular party, whether this is true or not. We will talk about the use of authentication as the means of validating whether the claim of identity is true. We will also cover multifactor authentication and the use of biometrics and hardware tokens to enhance surety in the authentication process.

Additional, we will discuss the use of authorization and access control. Authorization is the next step in the process that we will work through in order to allow entities access to resources. We will cover the various access control models that we will use when putting together such systems such as discretionary access control, mandatory access control, and role-based access control. We will also talk about multilevel access control models, including Bell LaPadula, Biba, Clark-Wilson, and Brewer and Nash. In addition to the commonly discussed concepts of logical access control, we will also go over some of the specialized applications that we might see when looking specifically at physical access control.

Lesson Three:

In this lesson we will discuss the use of auditing and accountability. We will talk about the need to hold others accountable when we provide access to the resources on which our businesses are based, or to personal information of a sensitive nature. We will also go over the processes that we carry out in order to ensure that our environment is compliant with the laws, regulations, and policies that bind it, referred to as auditing. In addition, we will address the tools that we use to support audit, accountability, and monitoring activities, such as logging and monitoring.

Additionally, we will discuss the use of cryptography. We will go over the history of such tools, from very simple substitution ciphers to the fairly complex electromechanical machines that were used just before the invention of the first modern computing systems and how they form the basis for many of our modern algorithms. We will cover the three main categories of cryptographic algorithms: symmetric key cryptography, also known as private key cryptography, asymmetric key cryptography, and hash functions. We also talk about digital signatures that can be used to ensure that data has not been altered and certificates that allow us to link a public key to a particular identity. In addition, we will cover the mechanisms that we use to protect data at rest, in motion, and, to a certain extent, in use.

Lesson Four:

In this lesson we will cover operational security. We will talk about the history of operational security, which reaches at least as far back as the writings of Sun Tzu in the sixth century BC to the words of George Washington, writings from the business community, and formal methodologies from the U.S. government. We will talk about the five major steps of operations security: identifying critical information, analyzing threats, analyzing vulnerabilities, determining risks, and planning countermeasures. We will also go over the Laws of OPSEC, as penned by Kurt Haas. In addition to discussing the use of operations security in the worlds of business and government, we also address how it is used in our personal lives, although perhaps in a less formal manner.

Additionally, we will discuss physical security. We will address the main categories of physical security controls, to include deterrent, detective, and preventive measures, and discuss how they might be put in place to mitigate physical security issues. We will talk about the foremost concern in physical security: ensuring the safety of our people and talk about how data and equipment can generally be replaced, when proper precautions are taken, though people can be very difficult to replace. We will also cover the protection of data, secondary only to protecting our people, and how this is a highly critical activity in our world of technology-based business. Lastly, we will discuss protecting our equipment, both outside of and within our facilities.

Lesson Five:

In this lesson, we will examine how we might protect our networks from a variety of different angles. We go over secure network design and segmentation properly, ensuring that we have the proper choke points to enable control of traffic, and that we are redundant where such is needed. We will look into the implementation of security devices such as firewalls and intrusion detection systems, the protection of our network traffic with virtual private networks (VPNs) and security measures specific to wireless networks when we need to use them, and make use of secure protocols. We will also consider a variety of security tools, such as Kismet, Wireshark, nmap, honeypots, and other similar utilities.

Additionally, we will explore hardening as one of the primary tools for securing the operating system and the steps that we take to do so. We will also review the additional security-related software that we might use to secure our systems including anti-malware tools, software firewalls, and host-based intrusion detection systems in order to protect us from a variety of attacks. Lastly, we will touch on some of the security tools that we can use from an operating perspective, including port scanners such as nmap, vulnerability analysis tools such as Nessus, and exploit frameworks such as Metasploit.

Lesson Six:

In this lesson, we will consider the various ways in which we might secure our applications. We will go over the vulnerabilities common to the software development process, including buffer overflows, race conditions, input validation attacks, authentication attacks, authorization attacks, and cryptographic attacks, and how we might mitigate these by following secure coding guidelines. We will talk about Web security, the areas of concern on both the client-side issues and server side of the technology. We introduce database security and cover protocol issues, unauthenticated access, arbitrary code execution, and privilege escalation, and the measures that we might take to mitigate such issues. Lastly, we will examine security tools from an application perspective, including sniffers such as Wireshark, fuzzing tools including some developed by Microsoft, and Web application analysis tools such as Burp Suite in order to better secure our applications

Lesson Seven:

This week's lesson is a cumulative of all ten chapters in preparation of week eight final. The objective of this week's lesson is to evaluate what did you get from this class (?) as it relates to Information Security and Protection; what area do you find that you are strongest in (?), weakest in (?), which assignment was your favorite (?), and who's peer review article did you enjoy the most and why?

- Self-Assessment Exercise (Week 7)

Lesson Eight:

This week we conclude the course. Students demonstrate their comprehension of InfoSec and an ability to apply the materials from this course to a final project.

- Security Assessment Project Due (Week 8)

University Policies

Academic Integrity

Angelo State University expects its students to maintain complete honesty and integrity in their academic pursuits. Students are responsible for understanding and complying with the university Academic Honor Code and the ASU Student Handbook.

Accommodations for Disability

The Student Life Office is the designated campus department charged with the responsibility of reviewing and authorizing requests for reasonable accommodations based on a disability, and it is the student's responsibility to initiate such a request by contacting the Student Life Office at (325) 942-2191 or (325) 942-2126 (TDD/FAX) or by e-mail at Student.Life@angelo.edu to begin the process. The Student Life Office will establish the particular documentation requirements necessary for the various types of disabilities.

Student absence for religious holidays

A student who intends to observe a religious holy day should make that intention known in writing to the instructor prior to the absence. A student who is absent from classes for the observance of a religious holy day shall be allowed to take an examination or complete an assignment scheduled for that day within a reasonable time after the absence.