Course Syllabus and Policy Requirement Statement

In order to access your course materials, you must agree to the following, by clicking the "Mark Reviewed" button below.

By checking the "Mark Reviewed" link below, you are indicating the following:

- You have read, understood, and will comply with the policies and procedures listed in the class syllabus, and that you have acquired the required textbook(s).
- You have read, understood, and will comply with class policies and procedures as specified in the online Student Handbook.
- You have read, understood, and will comply with computer and software requirements as specified in the Student Orientation Course.

ISSA 6312: Cyber Arms Race and the Intelligence-Policy Nexus

Course Description/Overview

Click this link for a printable version of the syllabus.

This course provides the foundation for understanding the key issues associated with protecting information assets, determining the levels of protection and response to security incidents, discussing the role of the U.S. military in defending the United States from cyber threats, and designing a consistent, reasonable information security system, with appropriate intrusion detection and reporting features. The purpose of the course is to provide the student with an overview of the field of information security and assurance. Students will be exposed to the spectrum of security activities, methods, methodologies, and procedures. Coverage will include inspection and protection of information assets, detection of and reaction to threats to information assets, and examination of pre- and post-incident procedures, technical and managerial responses, and an overview of the information security planning and staffing functions related to security policy.

Course Bibliography and Required Readings:

Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners 2nd Edition

Author: Jason Andress and Steve Winterfeld

Date: 2014

ISBN (paperback): 978-0-12-416672-1

Fundamentals of Information Systems Security 2nd Ed.

Author: Kim, D. and Michael Solomon

Date: 2014

ISBN (paperback): 978-1-284-03162-1

Course Objectives/Learning Outcomes. The student will demonstrate knowledge and ability to apply the following learning topics:

- Introduction to Information Security
- The Need for Security
- Legal, Ethical, and Professional Issues in Information Security
- Risk Management
- Planning for Security
- Security Technology: Firewalls, VPNs, and Wireless
- Security Technology: Intrusion Detection and Prevention Systems and Other Security Tools
- Cryptography
- Physical Security
- Implementing Information Security
- Security and Personnel
- Information Security Maintenance and eDiscovery

Grading Policies

This course utilizes three major writing assignments, several short writing assignments, and weekly discussions 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.

Assignment	Percent of Grade	Due
Writing Assignment 1	25%	Sunday, 11:59 pm Central Time, 3rd week of class.
Writing Assignment 2	30%	Sunday, 11:59 pm Central Time, 6th week of class
Final Project	20%	Wednesday, 11:59 pm, the 8th week of class
Participation in the Discussion Board	25%	Weekly (1st, 2nd, 4th, 5th)

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

A = 90 – 100 %
B = 80 – 89 %
C = 70 – 79 %
D = 60 – 69 %
F = 59 % and below.

Writing Guidelines

Each writing assignment deals with the topic under discussion. These writing assignments cumulatively account for 55% of the student's grade. All writing assignments are expected to be double spaced and 7-8 pages in length, with the exception of the final essay, which will be 8-10 pages.

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/.

The CHICAGO style will be acceptable. The Chicago Style guide can be found at http://www.chicagomanualofstyle.org. Papers should have 1-inch margins all around. You are expected to use a standardized font - preferably Times New Roman, 12 point. Also, the footnote format must be used instead of the parenthetical author-date format. Cite your references in EVERY instance and include a properly formatted reference list and cover page with every assignment.

Every writing assignment should be submitted as a WORD, RTF, 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 cannot be read and will not be accepted.

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

Exam

There is no final exam in this class. You will have a final research paper due in Week 8. This is your final project and will count as 20% of your course grade. It will close on Wednesday of Week 8 of the course.

Course Organization:

Lesson 1: Introduction to Information Security; IT Security Policy Framework
This first lesson establishes the foundation for understanding the broader field of information security. This is accomplished by defining key terms, explaining essential concepts, and reviewing the origins of the field and its impact on the understanding of information security.

We also examine the business drivers behind the security analysis design process, including current needs for security in organizations and technology. One principal concept is that information security is primarily an issue of management, as well as technology. Best practices apply technology only after considering the security basics.

Lesson 2: Legal Ethical, and Professional Issues in Information Security
As a fundamental part of the Information Security investigation process, a careful examination of current legislation, regulation, and common ethical expectations of both national and international entities provides key insights into the regulatory constraints that govern business. This lesson examines several key laws that shape the field of information security, and it presents a detailed examination of computer ethics necessary to better educate those implementing security. Although ignorance of the law is no excuse, it's considered better than negligence

(knowing and doing nothing). This lesson also presents several legal and ethical issues that are commonly found in today's organizations, as well as formal and professional organizations that promote ethics and legal responsibility.

Lesson 3: Risk Management; Planning for Security
This lesson examines the processes necessary to undertake formal risk management activities in the organization. Risk management is the process of identifying, assessing, and reducing risk to an acceptable level and implementing effective control measures to maintain that level of risk. This is done with a number of processes from risk analysis through various types of feasibility analyses, including quantitative and qualitative assessment measures and evaluation of security controls.

This lesson also presents a number of widely accepted security models and frameworks and examines the planning processes that support information security continuity, disaster recovery, and incident response. It examines best practices and standards of due care and due diligence, and it offers an overview of the development of security policy.

Critical Writing Assignment One Due Sunday, end of Week 3.

Lesson 4: Security Technology: Firewalls and VPNs; Security Technology
This lesson discusses various authentication and access control methods. The lesson also discusses the various approaches to firewall technologies and content filtering. The emphasis on the first part of this lesson is on technical controls for both network and system access control.

This lesson next discusses the use of intrusion detection and prevention systems as well as their deployment in networks. We also discuss tools used to fingerprint a network, and tools used to find weaknesses in the fingerprinted network.

Lesson 5: Cryptography
This lesson presents the underlying foundations of modern cryptosystems, as well as a discussion of the architectures and implementations of those cryptosystems. It also examines some of the mathematical techniques that comprise cryptosystems, including hash functions. The lesson then extends this discussion by comparing traditional and modern symmetric encryption systems. We will describe the role of asymmetric systems as the foundation of public-key encryption systems. Also covered in this lesson are the cryptography-based protocols used in secure communications; these include protocols such as SHTTP, SMIME, SET, SSH.

Lesson 6: Physical Security
As a vital part of any information security process, physical security is concerned with the management of the physical facilities, the implementation of physical access control, and the oversight of environmental controls. Lesson 6 examines special considerations for physical security threats, including the need for a secure data center, the relative value of guards and watchdogs, and the technical issues of fire suppression and power conditioning.

Critical Writing Assignment Two Due Sunday, end of Week 6.

Lesson 7: Implementing Information Security
This lesson examines the elements that are critical to implementing the design that was created in the previous stages. Key areas in this lesson include the bull's-eye model for implementing information security and a discussion of whether an organization should outsource each component of security. Change management, program improvement, and additional planning for the business continuity efforts are also discussed.

Final Project Due Wednesday of Week 8.

Lesson 8: Social Engineering and Psychological Weapons

This lesson examines how gaining access to the target's information can facilitate attacks. Psychological Operations are planned actions to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.

Final paper due Wednesday of Week 8.

Reading assignment: Chapter 8 in the Cyber Warfare book.

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
ASU is committed to the principle that no qualified individual with a disability shall, on the basis of disability, be excluded from participation in or be denied the benefits of the services, programs or activities of the university, or be subjected to discrimination by the university, as provided by the Americans with Disabilities Act of 1990 (ADA), the Americans with Disabilities Act Amendments of 2008 (ADAAA), and subsequent legislation.

Student Affairs 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 emailing studentservices@angelo.edu, or by contacting:

Office of Student Affairs
University Center, Suite 112
325-942-2047 Office
325-942-2211 FAX

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.