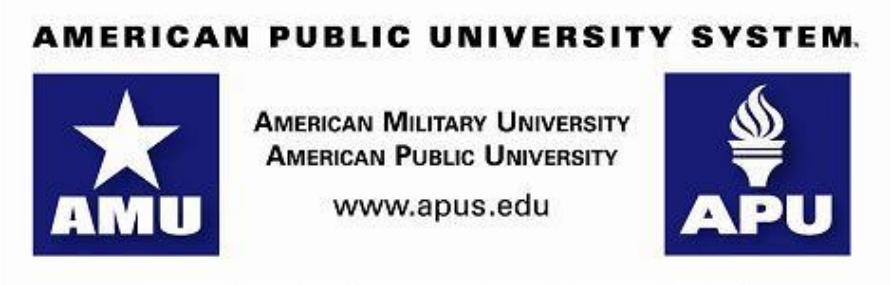
STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.



Department of Information Technology
ISSC422 Information Security (3 hours)
3 Credit Hours: 8-Weeks
Prerequisite(s): None

TABLE OF CONTENTS – TOC

INSTRUCTOR INFORMATION TOC

Instructor:
Email:
Phone:
Office hours:

NOTE: IT IS IMPORTANT THAT THE STUDENT READ THE ENTIRE STUDENT SYLLABUS THOROUGHLY. THIS DOCUMENT DETAILS MY GOALS AND EXPECTATIONS FOR THIS COURSE AND PROVIDES ALL OF THE NECESSARY INFORMATION CONCERNING ASSIGNMENTS, GRADING AND ADDITIONAL COURSE REQUIREMENTS.

COURSE DESCRIPTION (CATALOG) TOC

ISSC422 – Information Security
This course allows students to examine a broad range of computer security issues and provides the student with technical knowledge not normally addressed in traditional training. It explores the protection of proprietary information and security planning with an emphasis on networked computer vulnerabilities. It also focuses on detection (e.g. viruses, hackers, types of computer crime, computer forensic

examination, etc.), as well as disaster recovery and technology law. A primary focus is put on security of systems and computer crime prevention. Also addressed is the maturing criminal population with increased computer literacy, whose tendency is to move from violent actions to more profitable computer crime. Finally, issues of privacy and freedom of information are examined. This course meets the topical requirements of the 8570.1M Technical II and Management I categories.

COURSE SCOPE TOC

At the end of this course, you will have a firm foundation of the field of information security. Both the technical aspects of information security, as well as security management issues will be an integral part of this course as it applies to criminal justice, political science, information systems and accounting/business systems. Ongoing changes to the field of information security will be introduced and reviewed during this semester within Discussion Board Posting and writing assignments.

COURSE OBJECTIVES TOC

After you have completed this course, you should be able to:

1. Identify and prioritize information assets.
2. Identify and prioritize threats to information assets.
3. Define an information security strategy and architecture.
4. Plan for and respond to intruders in an information system
5. Describe legal and public relations implications of security and privacy issues.
6. Present a disaster recovery plan for recovery of information assets after an incident.

COURSE MATERIALS TOC

Required Text

Kim, David, Solomon, Michael. (2012). Fundamentals of Information System Security. Information Systems & Security Series. Sudbury, MA. Jones & Bartlett Learning.

Required Software

1. Microsoft Office Word
2. Adobe Acrobat Reader (Click here for free download)

COURSE DELIVERY METHOD TOC

This course delivered via distance learning will enable students to complete academic work in a flexible manner, completely online. Course materials and access to an online learning management system will be made available to each student. **Online assignments are due by the Friday or Sunday of each week** and include Discussion Forum questions (accomplished through a threaded discussion forum), examinations and quizzes (graded electronically), and individual assignments (submitted for review by the Faculty Member). Assigned faculty will support the students throughout this eight-week course.

EVALUATION PROCEDURES TOC

For the purposes of this course, a "**week**" is defined as the time period between Monday–Sunday, for all weeks 1 to 8. The **first week** begins on the first day of the semester and ends on midnight the following Sunday.

PHONE CALLS: Contact between students and faculty can occur in a number of ways: phone, fax, and electronic communications (Internet) are three examples. Students are expected to maintain routine contact with faculty throughout the course. And while the number of these may vary according to the specific course and individual student need, the University requires at least four contacts during the semester. Depending on the course, the professor may require these contacts to occur by phone. While these contacts will not be graded (unless indicated below) students should be aware that they count

toward the total of required course exercises. EMAIL/class message CONTACT IS ALWAYS ACCEPTABLE IN THIS CLASS!

EMAILS: When you contact me via email, please ensure you put the title of the course (ISSC422) and the current session you are in in the subject line. Per school policy, all matters concerning the class should be with the "messages: function within the class. This will help me align your email within the right course so I can quickly address any questions you may have, or resolve any problems that may come up.

Grades in this course are based on the following:

1) **Lab assignments:** You will have four lab assignments throughout the session, worth a combined total of 20% toward your final grade (5% each).

2) **Discussion Forum Postings**: I will be posting Discussion Forum topics related to Information Security throughout the class session. These postings will be directly tied to our assignments section for grading. These postings are worth a total of 52% for weeks 1-8. Discussion items will be posted within the Discussion Board area of the classroom. Your responses will clearly show whether you are up to date on your readings, so be sure to keep up with course work and respond based upon same. Opinions are always welcome…however, postings providing only opinions will be graded accordingly. Your grades for Discussion Forum postings are available throughout the semester as they are graded throughout the week. Please ensure you understand the Rubric grading matrix in the next page to guide your response and posting. I will be using this matrix to assign grades for your discussion forum postings.

Rubric for Learner Post (Assign point value in Grade Builder)

Topic coverage	Reflection	Correct APA citations	Writing standards	Timeliness
The response refers to course materials and shows a clear understanding of main ideas and concepts. There are no irrelevant comments and the information is on point. Ideas are clearly and properly organized.	The response provides personal examples that tie in with the course material being discussed. Reflection is evident and clearly ties in with the material presented. Insight was provided to some concept.	The response made proper reference to the course text or to other materials that were referenced or referred to in the discussion. Opinions were also included and were valid.	The writing is grammatically correct, clear and concise. The response is well formulated and easy to read and understand. Correct terminology was used when needed.	The posting was "not" submitted on time.
60%	20%	10%	10%	10% (deduction)

Rubric for Response to another Learner

Topic coverage	Writing standards	Timeliness
The other learner's ideas, questions, concerns were addressed. The response referenced reading or lecture materials when needed. The response addressed the learner's feelings if needed. There were no irrelevant or off-point comments. The posting reflects a clear understanding of the other learner's ideas.	The writing is grammatically correct, clear and concise. The response is well formulated and easy to read and understand. Correct terminology was used when needed.	The posting was "not" submitted on time.
80%	20%	10% (deduction)

3) **Concept Paper:** Worth 8% of your final grade. The content for the project paper is listed under the Week 4 of your syllabus

4) **Project/Research Paper:** There will be one individual project paper throughout the session, worth 20%. The content for the project paper is listed under the Week 7 of your syllabus.

GRADED EVENTS		% OF FINAL GRADE
Discussion Board Postings	Weeks 1-8	52 %
	Week 2 Lab	5 %
	Week 4 Lab	5 %
	Week 6 Lab	5 %
	Week 8 Lab	5 %
Papers	Concept Paper	8 %
	Individual Project Paper	20 %
Total		**100 %**

You must complete each and every one of the assignments, regardless of how well you do on the other assignments. This includes all requirements for quizzes, book reports, theme papers, term papers, and any other type of evaluation the professor has assigned. Failure to complete all assignments may result in an "F".

Evaluation Technique

The grading scale used in this course is the standard grading scale used by AMU. Grades are based on a 4.0 scale as follows:

Grading Scale

Please see the student handbook to reference the University's grading scale.

COURSE OUTLINE TOC

WEEK	DATES	LESSON SUBJECT	ASSIGNMENT – (*Graded)
1	Monday to Sunday of Week 1	Information Systems Security	Required Contact Info to Professor Chapter 1 *Disc: Intro. & DoD Dir 8570.1
2	Monday to Sunday of Week 2	Changing How People and Businesses Communicate Malicious Attacks, Threats, and Vulnerabilities	Chapters 2 & 3 *Week 2 Lab due *Disc: Social engineering *Malicious attacks & vulnerabilities
3	Monday to Sunday of Week 3	The Drivers of the Information Security Business Access Controls	Chapters 4 & 5 *Disc: Access Control
4	Monday to Sunday of Week 4	Security Operations & Administration Auditing, Testing, & Monitoring	Chapter 6 & 7 *Week 4 lab due *Concept Paper Due *Disc: Sec. Tech. Firewalls & VPNs
5	Monday to Sunday of Week 5	Risk, response, & Recovery Cryptography	Chapters 8 & 9 *Disc: Plan for Cont. - Cryptography
6	Monday to Sunday of Week 6	Networks & Telecommunications Malicious Code & Activity	Chapters 10 & 11 *Week 6 Lab due *Disc: Physical Security
7	Monday to Sunday of Week 7	Information Security Standards Information Security Education & Training	Chapters 12 & 13 *Individual Project Paper Due *Disc: Security Professionals

8	**Monday to Sunday of Week 8**	**Information Security Professional Certifications U.S. Compliance Laws**	**Chapters 14 & 15 Reading Week *Week 8 Lab due**

Course Outline – Overview

Course Deadlines/Milestones

- **Participation in discussions is required for Week 1 through Week 8**
- **End of Second Week: Chapters 1-3 completed and Week 2 lab due to Professor**
- **End of Fourth Week: Chapter 4-7 completed and Week 4 lab due to Professor**
- **End of Sixth Week: Chapters 8-11 completed and Week 6 lab due to professor**
- **End of Seventh Week: Chapters 12-13 completed and Project Paper due to Professor**
- **Eight Week: Chapters 14 & 15 completed and Week 8 lab due to Professor**

POLICIES

TOC

Please see the student handbook to reference all University policies. Quick links to frequently question asked about policies are listed below.

Drop/Withdrawal Policy
Plagiarism Policy
Extension Process and Policy

WRITING EXPECTATIONS

All written submissions should be submitted in a font and page set-up that is readable and neat. It is recommended that students try to adhere to a consistent format, which is described below.

- Typewritten in double-spaced format with a readable style and font and submitted inside the electronic classroom (unless classroom access is not possible and other arrangements have been approved by the professor).
- Arial 11 or 12-point font or Times New Roman styles.
- Page margins Top, Bottom, Left Side and Right Side = 1 inch, with reasonable accommodation being made for special situations and online submission variances.

CITATION AND REFERENCE STYLE

Assignments completed in a narrative essay or composition format must follow the APA Citation Style guidelines. Students will use the citation and reference style using the APA style. Please refer to the student handbook for more details: *The Publication Manual of the American Psychological Association: Sixth Edition &* http://www.apus.edu/student-handbook/writing-standards/index.htm.

LATE ASSIGNMENTS

For each week that an assignment is late, two points may be deducted from your grade for the assignment unless the student contacts the instructor ahead of time about an extenuating situation.

DISCLAIMER STATEMENT

Course content may vary from the outline to meet the needs of this particular group.

ACADEMIC SERVICES

TOC

ONLINE LIBRARY RESEARCH CENTER & LEARNING RESOURCES

The Online Library Resource Center is available to enrolled students and faculty from inside the electronic campus. This is your starting point for access to online books, subscription periodicals, and Web resources that are designed to support your classes and generally not available through search engines on the open Web. In addition, the Center provides access to special learning resources, which the University has contracted to assist with your studies. Questions can be directed to orc@apus.edu.

- ***Charles Town Library and Inter Library Loan:*** The University maintains a special library with a limited number of supporting volumes, collection of our professors' publication, and services to search and borrow research books and articles from other libraries.
- ***Electronic Books:*** You can use the online library to uncover and download over 50,000 titles, which have been scanned and made available in electronic format.
- ***Electronic Journals:*** The University provides access to over 12,000 journals, which are available in electronic form and only through limited subscription services.
- ***Turnitin*** is a tool to improve student research skills that also detect plagiarism. Turnitin provides resources on developing topics and assignments that encourage and guide students in producing papers that are intellectually honest, original in thought, and clear in expression. This tool helps ensure adherence to the University's standards for intellectual honesty. Turnitin reviews students' papers for matches with Internet materials and with student papers in its database, and returns an Originality Report to instructors and/or students. Through the APUS Online Library all students can signup for an APUS student profile and can submit class assignments (see the Turnitin student instruction file) and can submit class assignments.
- ***Smarthinking:*** Students have access to 10 free hours of tutoring service per year through Smarthinking. Tutoring is available in the following subjects: math (basic math through advanced calculus), science (biology, chemistry, and physics), accounting, statistics, economics, Spanish**,** writing, grammar, and more. Additional information is located in the Online Research Center. From the ORC home page, click on either the "Writing Center" or "Tutoring Center" and then click "Smarthinking." All login information is available.
- ***Peer-reviewed Sources:*** Students are expected to become familiar with the use of peer-review articles/journals. Peer review (also known as refereeing) is the process of subjecting an author's work, research, or ideas to the scrutiny of others who are experts in the same field. Pragmatically, peer review refers to the work done during the screening of submitted manuscripts and funding applications. This process encourages authors to meet the accepted standards of their discipline and prevents the dissemination of irrelevant findings, unwarranted claims, unacceptable interpretations, and personal views. Publications that have not undergone peer review are likely to be regarded with suspicion by scholars and professionals. Some sources of peer reviewed articles are:
    1. ACM digital library: http://portal.acm.org/dl.cfm (requires membership - a resume enhancer)
    2. Google Scholar : http://scholar.google.com/ (free)
    3. IEEE digital library: http://www.computer.org/portal/web/csdl/home (requires membership - a resume enhancer)

Assignment Formatting and Dos and Don'ts:

All assignments in this course are given to you prior to the due date. The "due date" for all assignments is the week in which the assignment is due.

All assignments must be:

- spell-checked
- typewritten
- double-spaced
- in either Arial 11 or 12-point font OR Times New Roman style
- have 1 inch margins - top, bottom, and sides
- have special attention paid to the usage of:
    - its/it's
    - there/their – they're
    - your/you're
    - two/too/to
    - flaw/flow
    - centered around/centered on ("centered around" is **not** correct usage)
    - then/than
    - contractions (do **not** use contractions in your papers)

All assignments should be uploaded into the student folder, located in the electronic classroom, with an email to me that your assignment is ready for grading.

ASSIGNMENT COMPLETION:

As stated previously, you must complete each and every one of the assignments, regardless of how well you do on the other assignments. This includes all requirements quizzes, reports, papers, and any other type of evaluation the professor has assigned. Failure to complete all assignments may result in an "F". The testing requirements for quizzes are explained elsewhere in this Student Course Guide (either in the Weekly Study Section or in Appendix A). You will need to follow these instructions to gain the maximum grade points for the quiz. Please coordinate with the professor for any special test arrangements.

Please remember that no extensions to the course will be given unless the student has been in communication with the professor, as required, during the semester, and unless the student has completed at least two of the four assignments, with a grade of C or higher. If a student should have a significant medical or work related reason why an extension should be given, the student must communicate that to the professor prior to the due date of each assignment. Assignments will not be accepted if an extension for that assignment has not be requested prior to the due date of the assignment, or if the assignment is handed in more than 14 days late. Assignments handed in after the due date, without prior permission from the instructor, will be docked points for each day late after the due date.

Please make sure that in any emails you send, you put the course name, number, and semester, and assignment number, if relevant, in the subject line, so I can readily tell what school/class you are in.

Examination/Grading Policies and Procedures

Your quizzes will be given as a timed multiple choice/true-false and matching questions.

Course Outline – Week by Week

Week 1 – Introduction	**TOC**

Topic: Week 1 introduces the class, the class students and addresses the impact of DoD Dir. 9570.1 on the CIS/IT career field.

Learning Objectives: By the end of this week, you should be able to:
Understand the concept of Information System security.
List the seven domains of a typical IT infrastructure.
Explain IT security policy framework
Comprehend the requirements of DoD Dir. 8570.1.
Understand the challenges surrounding employment IAW DoD Dir 8570.1 compliance.

Assignments:

- **Readings:** Chapter 1; answer the chapter assessment beginning on pp. 45 (do not turn these in).
- DoD Dir 8570.1
  DoD CIO. (2010). *DoD 8570.01-M, Information Assurance Workforce Improvement Program*. Retrieved August 2, 2011 from http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf.
- **Send your contact info via email to professor by Saturday** (Name, email, phone numbers, best time to call, city and state/area currently residing, time zone).
- **Become familiar with AMU's Learning Management System (LMS)/on line classroom.**
- **Discussion Forum:**
  1. Introduce yourself in the Discussion Forum posting (NLT 250 words).
     - 1st paragraph: Your bio, including your past, current and future career, education, and certification plans. You can include classes, year in school, major, your location and time zone, government/military status, your personal interests, and any other information you may want to share with the rest of the class.
     - 2nd paragraph: How will (or will not) DOD directive 8570.1 (http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf) affect your career/education/certification plans?
     - 3rd paragraph: Please post at least three facts; two (2) TRUE and one (1) NOT TRUE, then try to guess your classmates "not true" statement. ;)
     - Submit by Friday of Week 1, 11:59 PM EST in order to receive timely peer input.
  2. Reply to at least two or more class members. Please make sure you keep your postings and responses in the thread of the original response, and do not exit to provide a separate response. Due by Sunday of Week 1 11:59 PM EST.

Week 2 – Chapters 2 & 3	**TOC**

Topic: Chapter 2 examines the concepts of Changing How People and Businesses Communicate. Chapter 3 examines the concepts of Malicious Attacks, Threats, and Vulnerabilities.

Learning Objectives: By the end of this week, you should be able to:
Describe how people and businesses communicate.

- Identify telephone security best practices.
- Differentiate VOIP, SIP risks, threats and vulnerabilities.

Explain the concepts of malicious attacks, threats, and vulnerabilities.

- Identify and describe malicious activity.
- Differentiate attack tools.

Assignments:

- **Readings:** Chapter 2 & 3; answer the chapter assessments beginning on pp. 79 & 115 (do not turn these in).
- **Week 2 lab (Due by Sunday of Week 2 11:59 PM EST)**
- **Discussion Forum Part 1– Social Engineering:**
    1. Please look at the file "Killing With Keyboards" (keyboards.ppt) from the class Course Materials then answer the following questions: What is at risk here? Identify 5 possible threats, and 5 vulnerabilities in this scenario. Discuss measures that could be taken to reduce the risks. Submit by Friday of Week 1, 11:59 PM EST in order to receive timely peer input.
        Grading rubric for the Killing with Keyboard assignment
        a. Risks
        b. Threats
        c. Vulnerabilities
        d. Measures
        e. Writing standards (approx. 130 words)

    2. After responding, reply to at least one or more class members. Please make sure you keep your postings and responses in the thread of the original response, and do not exit to provide a separate response. Due by Sunday of Week 2 11:59 PM EST.
    1. **Discussion Forum Part 2 – Authentication systems:**
    2. **Describe** malicious attacks, threats and vulnerabilities. Submit by Friday of Week 2, 11:59 PM EST in order to receive timely peer input.
        Rubric for this discussion assignment
        a. Topic coverage (approx. 130 words).
        b. Reflection/application from personal experience
        c. Correct APA Citations including citing the textbook
        d. Writing Standards
    3. After responding, reply to at least two or more class members. Please make sure you keep your postings and responses in the thread of the original response, and do not exit to provide a separate response. Due by Sunday of Week 2 11:59 PM EST.

Week 3 – Chapter 4 & 5	**TOC**

Topic: Chapter 4 examines the drivers of the Information Security business. Chapter 5 examines Access controls.

Learning Objectives: By the end of this week, you should be able to:
Define risk management.
Describe implanting a BIA, a BCP, and a DRP.
Describe the four parts of access control.
Describe authentication process and requirements.

- Authentication types
- Single Sign-On (SSO).

Assignments:

- **Readings:** Chapters 4 & 5; answer assessments beginning pp. 139 and pp. 180. (do not turn these in).
- **Discussion Forum– Role-based Security:**
  3. What is Access Control? What is SSO and what are some of parts and types of Access Control? Submit by Friday of Week 3, 11:59 PM EST in order to receive timely peer input.
     Rubric for this discussion assignment
     a. Topic coverage (approx. 260 words).
     b. Reflection/application from personal experience
     c. Correct APA Citations including citing the textbook
     d. Writing Standards
  4. After responding, reply to at least one or more class members. Please make sure you keep your postings and responses in the thread of the original response, and do not exit to provide a separate response. Due by Sunday of Week 3 11:59 PM EST.

Week 4 - Mid Term exam / Chapters 6 & 7 TOC

Topic: Chapter 6 examines the concepts of security operations and administration. Chapter 7 examines auditing, testing and monitoring.

Learning Objectives: You should be able to complete the Midterm Examination by the end of this week. Also:
Explain security administration.
Demonstrate how to review security logs.
Describe the infrastructure for an IT security policy.
Explain the System Life Cycle (SLC) and the System Development Life Cycle (SDLC).
Explain Security auditing and analysis.
Describe audit data collection methods.
List post-audit activities.
Explain how to verify security controls.
Describe monitoring and testing security systems.

Assignments:

- **Readings:** Chapters 6 & 7; answer assessment questions beginning pp. 212 & 247 (do not turn these in).
- **Week 4 lab. Due by Sunday of Week 4 11:59 PM EST.**
- **Discussion Forum – Security Administration:**
  1. Describe how security administration works to plan, design, implement, and monitor man organization's security plan. Submit by Friday of Week 4, 11:59 PM EST in order to receive timely peer input.
     Rubric for this discussion assignment
     a. Topic coverage (approx. 260 words).
     b. Reflection/application from personal experience
     c. Correct APA Citations including citing the textbook
     d. Writing Standards

  2. After responding, reply to at least two or more class members. Please make sure you keep your postings and responses in the thread of the original response, and do not exit to provide a separate response. Due by Sunday of Week 4 11:59 PM EST.

Concept Paper: (Due by Sunday of Week 4, 11:59 PM EST)

1. Submit a concept (also know as an idea paper) paper IAW APA format on an approved topic (see pre-approved topics below). This paper sets the stage for your research paper. Paper organization will include (use as headings).
   - Introduction.
   - Problem Statement.
   - Relevance and Significance.
   - References (at least five).

2. Pre-approved topics:
   - Authentication/Digital signatures
   - Data collections tools (hardware & software)
   - E-business/e-commerce security
   - End user security issues.
   - Government vs. commercial organization security issues.
   - Identity Theft
   - Incident handling
   - ID&IH Management and Legal Issues

- Instant Messaging security
- Intrusion detection
- Sarbannes Oxley or HIPAA
- Security Threats & Vulnerabilities
- Wireless technology security

You may use resources from the APUS Online Library, any library, government library, or any peer-reviewed reference (Wikipedia and any other publicly-reviewed source is not accepted). The paper must by at least 3 pages double-spaced, 1" margin all around, black12 point fonts (Times New Roman, Arial, or Courier) with correct citations of all utilized references/sources, not counting any pictures, graphics, etc. A minimum of 5 references are needed. The paper may be submitted to Turnitin to check for proper citation attribution.

Week 5 – Chapters 8 & 9 TOC

Topic: Chapter 8 examines risk, response and recovery. Chapter 9 examines cryptography.

Learning Objectives: By the end of this week, you should be able to:

- Describe risk management and information security.
- Explain the process of risk management.
- List approaches for risk management.
- Describe the primary steps to disaster recovery.
- Describe business and security requirements for cryptography.
- List cryptographic applications and their uses in information system security.
- Explain cryptographic principles, concepts, and terminology.
- Discuss principles of certificates and key management.

Assignments:

- **Readings:** Chapters 8 & 9; answer assessment questions beginning pp. 279 & pp. 315 (do not turn these in).
- **Discussion Forum – Public Key Infrastructure:**
  1. Which one of the following statements is most correct about data encryption as a method of protecting data?
     A. It should sometimes be used for password files
     B. It is usually easily administered
     C. It makes few demands on system resources
     D. It requires careful key Management

     Answer:
  2. Explanation (one paragraph with citations). Submit by Friday of Week 5, 11:59 PM EST in order to receive timely peer input.

     Rubric for this discussion assignment
     e. Topic coverage (approx. 260 words).
     f. Reflection/application from personal experience
     g. Correct APA Citations including citing the textbook
     h. Writing Standards

  3. After responding, reply to at least two or more class members. Please make sure you keep your postings and responses in the thread of the original response, and do not exit to provide a separate response. Due by Sunday of Week 5 11:59 PM EST.

Week 6 – Chapters 10 & 11 TOC

Topic: Chapter 10 examines networks and telecommunications. Chapter 11 examines malicious code and activity.
*
Learning Objectives: By the end of this week, you should be able to:

- Explain the OSI reference model.
- Identify types of networks.
- Describe TCP/IP and how it works.
- Explain basic security defense tools.
- Describe the main types of malware
- Explain the anatomy of an attack.
- List attack prevention tools and techniques.

Assignments:

- **Readings:** Chapters 10 and 11; answer assessment questions beginning pp. 338 and pp. 379 (do not turn these in).
- **Week 6 lab. Due by Sunday of Week 6 12:00 PM EST.**
- **Discussion Board – IP Addressing:**
  1. Describe the IP address classes and ranges. Provide examples of internal vs. external address ranges. What configuration changes would you make in a network wireless router to enable a base level of security? Submit by Friday of Week 6, 11:59 PM EST in order to receive timely peer input.
     Rubric for this discussion assignment
     a. Topic coverage (approx. 260 words).
     b. Reflection/application from personal experience
     c. Correct APA Citations including citing the textbook
     d. Writing Standards
  2. After responding, reply to at least two or more class members. Please make sure you keep your postings and responses in the thread of the original response, and do not exit to provide a separate response. Due by Sunday of Week 6 11:59 PM EST.

Week 7 – Chapters 12 & 13 TOC

Topic: Chapter 12 examines information security standards. Chapter 13 examines information security education and training.

Learning Objectives: By the end of this week, you should be able to:

- List the various standards organizations.
- Explain the different security standards.
- Describe the different avenues of information security educations and traning.
- Differentiate between training, education and experience.

Assignments:

- **Readings:** Chapters 12 and 13; answer assessment questions beginning pp. 398 and pp. 417 (do not turn these in)
- **Individual Project Paper (see below for details). Due by Sunday of Week 7 11:59 PM EST (15% of grade).**
- **Discussion Forum – Security Education & Training:**

1. What avenues should an aspiring information security professional use in acquiring professional credentials? Submit by Friday of Week 7, 11:59 PM EST in order to receive timely peer input.
2. Rubric for this discussion assignment
    a. Topic coverage (approx. 260 words).
    b. Reflection/application from personal experience
    c. Correct APA Citations including citing the textbook
    d. Writing Standards
3. After responding, reply to at least two or more class members. Please make sure you keep your postings and responses in the thread of the original response, and do not exit to provide a separate response. Due by Sunday of Week 7 11:59 PM EST.

Project Paper: Due by Sunday of Week 7 11:59 PM EST.

2. Submit a 6-8 page research paper with APA standard annotations on an approved topic (see pre-approved topics below).
3. Pre-approved research topics
    - Authentication/Digital signatures
    - Data collections tools (hardware & software)
    - E-business/e-commerce security
    - End user security issues.
    - Government vs. commercial organization security issues.
    - Identity Theft
    - Incident handling
    - ID&IH Management and Legal Issues
    - Instant Messaging security
    - Intrusion detection
    - Sarbannes Oxley or HIPAA
    - Security Threats & Vulnerabilities
    - Wireless technology security

You may use resources from the APUS Online Library, any library, government library, or any peer-reviewed reference (Wikipedia and other non-peer-reviewed sources are not acceptable). The paper must by at least 6-8 pages double-spaced (plus title page and reference page), 1" margin all around, black12 point fonts (Times New Roman, Arial, or Courier) with correct APA format citations. Graphics are allowed but do not apply for the minimum page count. A minimum of 10 references are needed. The paper may be subjected to Turnitin against plagiarism. Turnitin

is accessed through the APUS Online Library, all students can signup for an APUS student profile (see the Turnitin student instruction file) and can submit class assignments.
Some sources of Peer reviewed articles are:

- ACM digital library: http://portal.acm.org/dl.cfm
- IEEE digital library: http://www.computer.org/portal/web/csdl/home
- Google Scholar : http://scholar.google.com

Week 8 – Chapters 14 & 15 TOC

Topic: Chapter 14 examines information security professional certifications. Chapter 15 examines U.S.A. compliance laws.
Conclusion of course. Complete Quiz 4.

Learning Objectives: By the end of this week, you should be able to:

- Describe vendor-neutral professional certifications.
- Describe vendor-specific professional certifications.
- Explain DoD Directive 8570.1
- Explain compliance and U.S. law.
- Describe the Federal Information Security Management Act.
- Explain the Health Insurance Portability and Accountability Act.

Assignments:

- **Readings:** Chapters 14 and 15; answer assessment questions beginning pp. 431 and pp. 462 (do not turn these in)
- **Discussion Forum – U.S. Compliance Laws**
  1. Describe DoD Dir 8570.1, the type of certifications involved and how it may/may not evolve in the future as a result of US compliance law. Submit by Friday of Week 8, 11:59 PM EST in order to receive timely peer input.
  2. Rubric for this discussion assignment
     a. Topic coverage (approx. 260 words).
     b. Reflection/application from personal experience
     c. Correct APA Citations including citing the textbook
     d. Writing Standards
  3. After responding, reply to at least two or more class members. Please make sure you keep your postings and responses in the thread of the original response, and do not exit to provide a separate response. Due by Sunday of Week 8 11:59 PM EST.

- **Week 8 lab. Due on Sunday of Week 8 11:59 PM EST – no exceptions.**

TOC

DAVID ANDERSSON

Your Instructor's Bio: Doctor Andersson has an Ed.D. (Technology Management), an Ed.S. (Computing Technology), an MS (Information Technology), and an MA (Public Administration). He has the MCT, MCSE, CCNA, CCWLANSS, Master CIW Administrator, CIW Security Analyst, CIW Security Professional, CompTIA as well as other technical certifications and currently serves as a consultant for e-commerce and business IT security for public and private organizations such as Worth Ltd. and as an Assistant Professor of CIS.

Doctor Andersson has worked as a training advisor for the New Military Technology System Special Projects Group for Raytheon, a Senior Systems Engineer for Allstate Insurance, and as a Lieutenant Colonel, Operations and Security, US Army - Kuwait, and the 2nd ACR Border Operations Officer on the East-West German border. In 1978-79 he represented the USA in the Canadian Army Trophy International Competition and in 1986 commanded the unit ranked 2nd in the USA for Operations Excellence. He is the current leader of the US-based Bronze Star Association.

His publications include:

Andersson, D. (2009) Chapter 7 OSPF, Cisco CCNA/CCENT Exam 640-802, 640-822, 640-816 Preparation Kit. Liu, D. Editor. Rockland, MA. Syngress Publishing.

Andersson, D. (2009). Information Technology Industry Certification's Impact on Undergraduate Student Perception of Instructor Effectiveness. UMI Dissertation Publishing Group, Volume 7005A. Publication No. 3358241.

Andersson, D. and Reimers, K. (2009). IT Certifications - Does It Matter If Your IT Professors Are Certified? Certification Magazine. Chicago, IL. MediaTec Publishing (pending).

Andersson, D. and Reimers, K. (2010). Academia and IT Certifications - Program Administration Trends and Implications. The Open Education Journal, Oak Park, IL, Benham Science Publishing (pending).

Andersson, D. and Reimers, K. (2010). CIS and IT Certifications - Education Program Trends and Implications. i-Manager's Journal of Educational Technology, Nagercoli, India, i-Manager Publishing.

Doctor Andersson teaching experience includes information technology topics, network security and digital forensics. His awards include the College Senate Committee for Distance Learning Program Development - 2003, Raytheon Performance Award, Allstate NBS Performance Award, Kuwait Liberation Medal, Southwest Asia Service Ribbon (3 Campaign Stars), Bronze Star, and Meritorious Service Medal. His hobbies include sailing, running, sailing, Clumber Spaniels, military history and he has a wife and two children. He is an active and continued member of IEEE and ACM and is the current national director of the US Bronze Star Medal association.

ISSC422 - Information Security Current Article References* TOC

Beegle, Lynn Erla (2007). Rootkits and Their Effects on Information Security. *Information Systems Security*, May2007, Vol. 16 Issue 3, p164-176, 13p; (*AN 25728920*) PDF Full Text (163K)

Curran, Kevin, & Canning, Paul (2007). Wireless Handheld Devices Become Trusted Network Devices. *Information Systems Security*, May2007, Vol. 16 Issue 3, p134-146, 13p, 2 charts, 2 diagrams, 4bw; (*AN 25728923*) PDF Full Text (688K)

Dunham, Ken (2007). OrderGun.A: A Sophisticated Rootkit. *Information Systems Security***,** Mar/Apr2007, Vol. 16 Issue 2, p123-126, 4p, 3 diagrams; (*AN 24726592*) PDF Full Text (609K)

Fleming, Sam (2007). Implicit Trust Can Lead to Data Loss. *Information Systems Security*, Mar/Apr2007, Vol. 16 Issue 2, p109-113, 5p; (*AN 24726584*) PDF Full Text(90K)

Freeman, Edward H. (2007). Vulnerability Disclosure: The Strange Case of Bret McDanel. *Information Systems Security*, Mar/Apr2007, Vol. 16 Issue 2, p127-131, 5p; (*AN 24726591*) PDF Full Text (106K)

Freeman, Edward H. (2007a). Email Privacy and the Wiretap Act: U.S. v. Councilman. *Information Systems Security*, May2007, Vol. 16 Issue 3, p182-185, 4p; (*AN 25728918*) PDF Full Text (97K)

Ginty, Ed (2007). Secure Data-Archiving: How to Protect and Store Your Data. *Information Systems Security*, Mar/Apr2007, Vol. 16 Issue 2, p90-92, 3p; (*AN 24726587*) PDF Full Text (77K)

Kim, D., and Solomon, M. (2012). Fundamentals of Information System Security. Information Systems & Security Series. Sudbury, MA. Jones & Bartlett Learning.

Klein, Andrea (2007). Building an Identity Management Infrastructure for Today...and Tomorrow. *Information Systems Security,* Mar/Apr2007, Vol. 16 Issue 2, p74-79, 6p, 2 diagrams; (*AN 24726589*) PDF Full Text (877K)

Namuduri, Kamesh (2007). From the Editor's Desk. *Information Systems Security*, Mar/Apr2007, Vol. 16 Issue 2, p73-73, 1p; (*AN 24726590*) PDF Full Text (124K)

Namuduri, Kamesh (2007a). From the Editor's Desk. *Information Systems Security*, May2007, Vol. 16 Issue 3, p133-133, 1p; (*AN 25728924*) PDF Full Text (46K)

Ortega, Ross (2007). Defending the Corporate Crown Jewels from the Dangers that Lurk Within - Effective Internal Network Security Focuses on Behavior. *Information Systems Security*, Jan2007, Vol. 16 Issue 1, p54-60, 7p; (*AN 24581865*) PDF Full Text (550K)

Rainer, R. Kelly, Marshall, Thomas E., Knapp, Kenneth J., Montgomery, & Gina H. (2007). Do Information Security Professionals and Business Managers View Information Security Issues Differently? *Information Systems Security*, Mar/Apr2007, Vol. 16 Issue 2, p100-108, 9p, 6 charts, 1 diagram; (*AN 24726585*) PDF Full Text (129K)

Rao, N. Vyaghreswara, & Pandit, S. N. Narahari (2007). Multimedia Digital Rights Protection Using Watermarking Techniques. *Information Systems Security,* Mar/Apr2007, Vol. 16 Issue 2, p93-99, 7p; (*AN 24726586*) PDF Full Text (117K)

Reed, Bill (2007). Implementing Information Lifecycle Security (ILS). *Information Systems Security*, May2007, Vol. 16 Issue 3, p177-181, 5p; (*AN 25728919*) PDF Full Text (87K)

Schlarman, Steven (2007). Selecting an IT Control Framework. *Information Systems Security*, May2007, Vol. 16 Issue 3, p147-151, 5p, 1 diagram; (*AN 25728922*) PDF Full Text (128K)

Tracy, Richard P. (2007). IT Security Management and Business Process Automation: Challenges, Approaches, and Rewards. *Information Systems Security*, Mar/Apr2007, Vol. 16 Issue 2, p114-122, 9p, 3 diagrams; (*AN 24726583*) PDF Full Text (1.5MB)

Wei She, & Thuraisingham, Bhavani (2007). Security for Enterprise Resource Planning Systems. *Information Systems Security*, May2007, Vol. 16 Issue 3, p152-163, 12p, 3 diagrams; (*AN 25728921*) PDF Full Text (334K)

Yarberry, William A. (2007). Effective Change Management: Ensuring Alignment of IT and Business Functions. *Information Systems Security*, Mar/Apr2007, Vol. 16 Issue 2, p80-89, 10p, 4 charts, 2 diagrams; (*AN 24726588*) PDF Full Text (231K)

***These PDF documents can be found under Course Materials > References**