Spring 2021

INA 4381 Cyber Policy

Instructor:
Patrick McCall
pmccall1@angelo.edu
717-856-7487

I am available between 12 PM and 7 PM M-F if you need to speak to me in person. I prefer corresponding via e-mail or text as this provides a tangible record of our interactions. This is a policy course and the first rule of policy is documentation.

This course familiarizes students with skills and best practices for developing and implementing effective cybersecurity policies within an organization-wide cybersecurity framework.

COURSE OVERVIEW

This course explores the various aspects of developing enforceable cyber security policies for users and organizations. Cybersecurity policies codify a uniform set of standards for behavior for activities such as the encryption of email attachments, privacy, and restrictions on the use of social media. Cybersecurity policies are important because cyberattacks and data breaches are potentially costly.
Cyber security policy provides working and enforceable guidelines for how your online systems and software are used to minimize risk. It helps everyone in businesses and organizations understand the processes in place to protect your company, data, and assets.

A sound Cyber security policy covers:

- The measures you've put in place to minimize threats
- The process for backing up and managing data will be backed up
- Best practice processes, this covers everything from setting passwords to the use of information technology
- The different responsibilities each employee bears regarding the protection of data and information technology assets
- Expectations for using social media at work, rules for using emails, and/or guidance for safeguarding data.

A well thought out cyber policies regulate all aspects of digital data exchange, including the Internet, data privacy and network usage – as well as cyber defense. ... As with all policy, cyber policy must strike a balance between necessary regulation and social freedom. As demonstrated on numerous occasions, data is now a commodity, and those with nefarious intentions, both inside and outside the organization, look for opportunities to exploit vulnerabilities.

A security policy describes information security objectives and strategies of an organization. The basic purpose of a security policy is to protect people and information, set the rules for expected behaviors by users, define, and authorize the consequences of violation The purpose of a cybersecurity policy is to set procedures and standards to safeguard user data against malware. Thus, it is important as it prevents cyberattacks and information breaches.

The bottom line for Cyber Security Policy is the bottom line. Cyber breaches are costly in terms of money and reputation for those organizations victimized by insiders and outside threats.

COURSE OBJECTIVES/LEARNING OUTCOMES

Upon successful completion of this course, students should demonstrate knowledge and proficiency in the following areas:

- Cybersecurity policy and governance
- Policy organization, format, and style
- Cybersecurity frameworks
- Governance and risk management
- Asset management and data loss prevention
- Human resources security
- Physical and environmental security
- Communications and operations security
- Access control management
- Information systems acquisition, development, and maintenance
- Cybersecurity incident response
- Business continuity management

REQUIRED TEXTS AND MATERIALS

Developing Cybersecurity Programs and Policies, Omar Santos, Pearson Education, 2019.
ISBN 13: 978-0-7897-5940-5

RECOMMENDED TEXTS

Cyber Security Policy Guidebook
Jennifer L. Bayuk, Jason Healey, Paul Rohmeyer, Marcus H. Sachs, Jeffrey Schmidt, Joseph Weiss
ISBN: 978-1-118-02780-6 April 2012 or https://www.programmer-books.com/wp-content/uploads/2018/07/Cyber-Security-Policy-Guidebook-1st-Edition-2012.pdf

To keep informed about current Internet developments, read a national or international publication such as The Financial Times, The Wall Street Journal, New York Times, or Foreign policy, Wired, The Washington Post, Journal of Cyber Security, and The Economist. These sources devote a fair amount of coverage to cyber and cyber security issues
EVALUATION AND GRADES

Graded assignments, activities, and percent of the overall course grade:

The grading system is as follows:

Graded Element	**Maximum Points**
Case Studies (8 @ 10 points each)	80
Weekly Discussions (8 x 15 points per week)	120
Total	**200**

Weekly Discussions start at 1201 AM on Monday and ends at end at 1159 PM on Sunday. Provide one well thought out posting (2-3 paragraphs) w/references. Respond to at least three student's posts with 2-3 well thought out paragraphs. Spelling and grammar count.

GRADING SYSTEM

Grades reflect the student's ability to organize the material, integrate relevant concepts and theories, and present them in appropriate forms. This course, by design, is a group discussion and requires active participation in the discussion forums. Course grades will be dependent upon completing course requirements and meeting the student learning outcomes.

The following grading scale is in use for this course:
A = 180-200 points
B = 160-179 points
C = 140-159 points
D = 120-139 points
F = 0-119 points

RUBRICS FOR ASSIGNMENTS

Quality Criteria	No/Limited Proficiency	Some Proficiency	Proficiency	High Proficiency	(Rating)
1. Thesis/Focus: (a) Originality	Thesis is missing	Thesis may be obvious or unimaginative	Thesis is somewhat original	Develops fresh insight that challenges the reader's thinking;	
2. Thesis/Focus: (b) Clarity	Reader cannot determine thesis & purpose OR thesis has no relation to the writing task	Thesis and purpose are somewhat vague OR only loosely related to the writing task	Thesis and purpose are fairly clear and match the writing task	Thesis and purpose are clear to the reader; closely match the writing task	
3. Organization	Unclear organization OR organizational plan is inappropriate to thesis. No transitions	Some signs of logical organization. May have abrupt or illogical shifts & ineffective flow of ideas	Organization supports thesis and purpose. Transitions are mostly appropriate. Sequence of ideas could be improved	Fully & imaginatively supports thesis & purpose. Sequence of ideas is effective. Transitions are effective	
4. Support/ Reasoning (a) Ideas (b) Details |	Offers simplistic, undeveloped, or cryptic support for the ideas. Inappropriate or off-topic generalizations, faulty assumptions, errors of fact	Offers somewhat obvious support that may be too broad. Details are too general, not interpreted, irrelevant to thesis, or inappropriately repetitive	Offers solid but less original reasoning. Assumptions are not always recognized or made explicit. Contains some appropriate details or examples	Substantial, logical, & concrete development of ideas. Assumptions are made explicit. Details are germane, original, and convincingly interpreted	
5. Use of sources/ Documentation	Neglects important sources. Overuse of quotations or paraphrase to substitute writer's own ideas. (Possibly uses source material without acknowledgement.)	Uses relevant sources but lacks in variety of sources and/or the skillful combination of sources. Quotations & paraphrases may be too long and/or inconsistently referenced	Uses sources to support, extend, and inform, but not substitute writer's own development of idea. Doesn't overuse quotes, but may not always conform to required style manual	Uses sources to support, extend, and inform, but not substitute writer's own development of idea. Combines material from a variety of sources, incl. pers. observation, scientific data, authoritative testimony. Doesn't overuse quotes.	

LATE WORK OR MISSED ASSIGNMENTS POLICY

The course is set up as weekly modules. The week begins on 12:01 AM Monday and ends on 11:59PM Sunday. Assignment due dates are shown on the calendar/schedule or posted within Blackboard. Late assignments ***are not accepted*** without prior approval of faculty. Faculty reserve the right to deduct points for late assignments that are accepted past the original due date.

ACADEMIC HONESTY

Academic honesty is expected on all work. Students are expected to maintain complete honesty and integrity in their online experiences. Any student found guilty of any form of dishonesty in academic work is subject of disciplinary action and possible expulsion from ASU.

PLAGIARISM

Plagiarism at ASU is a serious topic. The Angelo State University's Honor Code gives specific details on plagiarism and what it encompasses. Plagiarism is the action or practice of taking someone else's work, idea, etc., and passing it off as one's own. Plagiarism is literary theft.

In your discussions and/or your papers, it is unacceptable to copy word for word without quotation marks and the source of the quotation. We use the *APA Style Manual of the American Psychological Association* as a guide for all writing assignments. Quotes should be used sparingly. It is expected that you will summarize or paraphrase ideas giving appropriate credit to the source both in the body of your paper and the reference list. Papers are subject to be evaluated for originality via Bb Safe Assignment or Turnitin. Resources to help you understand this policy better are available at the ASU Writing Center http://www.angelo.edu/dept/writing_center/.

SYLLABUS CHANGES

The faculty member reserves the option to make changes as necessary to this syllabus and the course content. If changes become necessary during this course, the faculty will notify students of such changes by email, course announcements and/or via a discussion board announcement. It is the student's responsibility to look for such communications about the course on a daily basis.

COURSE EVALUATION

Students are provided the opportunity and are strongly encouraged to participate in a course evaluation at the end of the semester. Areas on the IDEA evaluation include:

1. Gaining factual knowledge (terminology, classifications, methods, trends)
2. Learning to apply course material (to improve thinking, problem solving, and decisions)
3. Developing specific skills, competencies, and points of view needed by professionals in the field most closely related to this course
4. Developing skill in expressing oneself orally or in writing
5. Learning how to find and use resources for answering questions or solving problems
6. Learning to analyze and critically evaluate ideas, arguments, and points of view
7. Acquiring an interest in learning more by asking questions and seeking answers

Course Organization

Week 1: Understanding Cybersecurity Policy and Governance
Cybersecurity Policy Organization, Format, and Styles

Learning Outcomes:

- Describe the significance of cybersecurity policies
- Evaluate the role policy plays in corporate culture and civil society
- Articulate the objective of cybersecurity-related policies
- Identity the different characteristics of successful cybersecurity policies
- Define the life cycle of a cybersecurity policy
- Explain the differences between a policy, a standard, a procedure, a guideline, and a plan
- Know how to use "plain language when creating and updating your cybersecurity policy"
- Identify the different policy elements
- Include the proper information in each element of a policy

Required Readings, Viewing, and Review:

Developing Cybersecurity Programs and Policies, Omar Santos, Pearson Education, 2019

Class Materials: Review both sets of slides for Week 1

Class Assignments:

Chapter 1: **Understanding Cybersecurity Policy and Governance**

Read pp. 2-27
Review questions 1-25, pp. 28-32
Projects 1.1 – 1.3, p. 34

Chapter 2: **Cybersecurity Policy Organization, Format, and Styles**

Read pp. 38-62
Review questions 1-30, pp. 63-68
Projects 2.1 – 2.3, p. 70

Answer the questions for the Clean Up the Library Lobby Case Study p. 70-71 (Submit in the Assignments folder in Blackboard)

Weekly Discussion:

Read about information security threats at http://searchsecurity.techtarget.com/topics/0,295493,sid14_tax299811,00.html.

Which threats are the most critical? Which threats present the hardest challenges to protection? Explain your reasoning for considering a threat more critical or harder to protect.

Web Resources

http://www.247.prenhall.com/ Pearson product support
http://searchsecurity.techtarget.com/bestWebLinks/0,289521,sid14_tax281891,00.html Security basics: Valuable resource links for those just entering the world of security
http://www.cert.org/ The CERT Coordination Center (CERT-CC)
http://www.us-cert.gov/ The United States Computer Emergency Readiness Team (US-CERT)
http://www.sans.org/resources/policies/ The SANS Institute provides sample policies and templates in many areas of information security along with other relevant information
https://www.infosecurity-magazine.com Information Security magazine is the enterprise security and risk managers' leading source of critical, objective information on strategic and practical security issues
https://www.dhs.gov/publication/dhs-cybersecurity-strategy Homeland Security Cybersecurity Strategy Fact Sheet and cybersecurity strategy

Week 2: Cybersecurity Framework
Governance and Risk Management

Learning Outcomes:

- Understand confidentiality, integrity, and availability (the CIA security model)
- Describe the security objectives of confidentiality, integrity, and availability
- Discuss why organizations choose to adopt a security framework
- Understand the intent of the National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Understand the intent of the ISO/IEC 27000-series of information security standards
- Outline the domains of an information security program
- Define governance.
- Explain cybersecurity governance and NIST's Cybersecurity Framework.
- Explain the importance of strategic alignment
- Know how to manage cybersecurity policies
- Describe cybersecurity-related roles and responsibilities
- Identify the components of risk management
- Create polices related to cybersecurity, governance, and risk management

Required Readings, Viewing, and Review:

Developing Cybersecurity Programs and Policies, Omar Santos, Pearson Education, 2019

Class Materials: Review both sets of slides for Week 2

Class Assignments:

Chapter 3: **Cybersecurity Framework**

Read pp. 72-93
Review questions 1-31, pp. 93-99
Projects 3.1 – 3.4, pp. 100-101

Chapter 4: **Governance and Risk Management**

Read pp. 104-133
Review questions 1-30, pp. 133-138
Projects 4.1 – 4.3, pp. 140-141

Answer the questions for the Determining the Likelihood and Impact of Occurrence Case Study, p. 141 (Submit in the Assignments folder in Blackboard)

Weekly Discussion:

Describe what is necessary to develop and implement an effective policy.

Web Resources

http://www.247.prenhall.com/ Pearson product support
http://www.iso.org/ More information about the ISO
http://www.nist.gov/ More about NIST
https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator A Common Vulnerability Scoring system (CVSS) Calculator
https://www.first.org/cvss/v2/guide A complete guide to the CVSS scoring system

Week 3: Asset Management and Loss Prevention
Human Resources Security

Learning outcomes:

- Assign information ownership responsibilities
- Develop and use information classification guidelines
- Understand information handling and labeling procedures
- Identify and inventory information systems
- Create and implement asset classification policies
- Understand data loss prevention technologies
- Define the relationship between cybersecurity and personnel practices
- Recognize the stages of the employee life cycle
- Describe the purpose of confidentiality and acceptable use agreements
- Understand appropriate security education, training, and awareness programs
- Create personnel-related security policies and procedures

Required Readings, Viewing, and Review:

Developing Cybersecurity Programs and Policies, Omar Santos, Pearson Education, 2019

Class Materials: Review both sets of slides for Chapters 5 and 6

Class Assignments:

Chapter 5: **Asset Management and Loss Prevention**

Read pp. 144-168
Review questions 1-30, pp. 168-173
Projects 5.1 – 5.3, pp. 175-176

Chapter 6: **Human Resources Security**

Read pp. 178-196
Review questions 1-30, pp. 197-202
Projects 6.1 – 6.3, pp. 204-205

Answer the questions for The NICE Challenge Project and CyberSeek Case Study, pp. 205-206
(Submit in the Assignments folder in Blackboard)

Weekly Discussion:

Why does the U.S. government require both a level of security clearance (at least equal to the classification of the information) and an appropriate "need to know" before information is released to an individual? Is this an adequate policy?

Web Resources

http://www.247.prenhall.com/ Pearson product support
http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci995767,00.html Security tips on standardizing information classification
http://www.molemag.net/index.htm ISO 27001 and 27002 newsletters provide guidance on various practical issues, plus commentary on recent information security incidents.
https://en.wikipedia.org/wiki/Bell%E2%80%93LaPadula_model Wikipedia page for the Bell LaPadula classification model
https://en.wikipedia.org/wiki/Biba_Model Wikipedia page for the Bibi classification model
https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html U.S. Social Security Administration: *The Story of the Social Security Number*
https://www.cisco.com/c/en/us/products/security/email-security-appliance/data-loss prevention-dlp.html
Cisco: What is Data Loss Prevention (DLP)?
http://www.sans.org/reading-room/whitepapers/auditing/information-classification-who-846
SANS Institute whitepaper on information classification

Week 4: Physical and Environmental Security
Communications and Operations Security

Learning outcomes:

- Define the concept of physical security and how it relates to information security
- Evaluate the security requirements of facilities, offices, and equipment
- Understand the environmental risks posed to physical structures, areas within those structures, and equipment
- Enumerate the vulnerabilities related to reusing and disposing of equipment
- Recognize the risks posed by the loss or theft of mobile devices and media
- Develop policies designed to ensure the physical and environmental security of information, information systems, and information-processing and storage facilities
- Create useful and appropriate standard operating procedures
- Implement change control processes
- Understand the importance of patch management
- Protect information systems against malware
- Consider data backup and replication strategies
- Recognize the security requirements of email and email systems
- Appreciate the value of log data and analysis
- Evaluate service provider relationships
- Understand the importance of threat intelligence and information sharing
- Write policies and procedures to support operational and communications security

Required Readings, Viewing, and Review:

Developing Cybersecurity Programs and Policies, Omar Santos, Pearson Education, 2019

Class Materials: Review both sets of slides for Chapters 7 and 8

Class Assignments:

Chapter 7: **Physical and Environmental Security**

Read pp. 208-226
Review questions 1-20, pp. 227-230
Projects 7.1 – 7.3, pp. 231-233

Answer the questions for The Physical Access Social Engineering Case Study, pp. 233-234 (Submit in the Assignments folder in Blackboard)

Chapter 8: **Communications and Operations Security**

Read pp. 236-283
Review questions 1-30, pp. 283-288
Projects 8.1 – 8.3, pp. 290-291

Weekly Discussion:

Why would a business want critical information processing facilities to be inconspicuous? Third-party data centers are not inconspicuous, so how do businesses protect critical assets located in these places?

Web Resources

http://www.247.prenhall.com/ Pearson product support
http://it.emory.edu/security/standards/physical_environmental_security.html Comprehensive physical and environmental security guidelines for Emory University
https://csrc.nist.gov/publications/white-paper NIST Computer Security Resource Center's list of publications
https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf Amazon Web Services: Overview of Security Processes
https://www.microsoft.com/en-us/cybersecurity/default.aspx Home page for Microsoft's Cybersecurity policy
http://en.wikipedia.org/wiki/Malware#Academic_Research_on_Malware:_A_Brief_Overview Wikipedia's entry on malware
http://www.csoonline.com/ Online resource for security executives
http://www.scmagazine.com/us/ Website of *SC* media, a cybersecurity source
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-177.pdf NIST's whitepaper on Trustworthy Email

https://www.fedramp.gov Federal Risk and Authorization Management Program's (FedRAMP) information on a standardized approach to security assessment and monitoring for cloud services
https://www.nationalisacs.org/member-isacs National Council of ISACs

Week 5: Access Control Management
Information Systems Acquisition, Development, and Maintenance

Learning outcomes:

- Explain access control fundamentals
- Apply the concepts of default deny, need-to-know, and least privilege
- Understand secure authentication
- Protect systems from risks associated with internet connectivity, remote access, and telework environments
- Manage and monitor user and administrator access
- Develop policies to support access control management
- Understand the rationale for the systems development life cycle (SDLC)
- Recognize the stages of software releases
- Appreciate the importance of developing secure code
- Be aware of the most common application development security faults
- Explain cryptographic components
- Develop policies related to systems acquisition, development, and maintenance

Required Readings, Viewing, and Review:

Developing Cybersecurity Programs and Policies, Omar Santos, Pearson Education, 2019

Class Materials: Review both sets of slides for Chapters 9 and 10

Class Assignments:

Chapter 9: **Access Control Management**

Read pp. 294-329
Review questions 1-20, pp. 329-333
Projects 9.1 – 9.3, p. 335

Answer the questions for Assessing a Current Security Breach Case Study, p. 336 (Submit in the Assignments folder in Blackboard)

Chapter 10: **Information Systems Acquisition, Development, and Maintenance**

Read pp. 338-358
Review questions 1-10, pp. 358-364
Projects 10.1 – 10.3, p. 366

Weekly Discussion:

As the system administrator for a medium-sized company, how would you convince users that letting the computer operating system or browser application remember their passwords is against good security practices?

Web Resources

http://www.247.prenhall.com/ Pearson product support
https://csrc.nist.gov/publications/ NIST Computer Security Resource Center
https://csrc.nist.gov/News/2012/NIST-Interagency-Report-(IR)-7874 NIST Guidelines for Access Control System
https://www.securitysolutionsmedia.com/ Security Solutions Media home page
http://www.comptechdoc.org/independent/security/policies/remote-access-policy.html Sample remote access policy (other sample security policies including a mobile computer policy are available in the left navigation on the web page) from The Computer Technology Documentation Project, http://www.comptechdoc.org/.
http://www.nsa.gov/ia/ National Security Agency (NSA) division of Information Assurance
http://www.owasp.org/ The Open Web Application Security Project (OWASP), dedicated to finding and fighting the causes of insecure software
http://searchappsecurity.techtarget.com/ SearchAppSecurity.com is the online community for developers, architects, and executives interested in building secure enterprise applications
http://en.wikipedia.org/wiki/Cryptography Wikipedia article on cryptography
https://www.sans.org/critical-security-controls/http://www.sans.org/top20/ The SANS (SysAdmin, Audit, Network, Security) Institute: CIS Critical Security Controls
https://cwe.mitre.org/data/ Common Weakness Enumeration (CWE) home page; A community-driven list of common security weaknesses in software and hardware

Week 6: Cybersecurity Incident Response
Business Continuity Management

Learning outcomes:

- Prepare for a cybersecurity incident
- Identify a cybersecurity incident
- Understand the incident response plan
- Understand the incident response process
- Understand information sharing and coordination
- Identify incident response team structure
- Understand federal and state data breach notification requirements

- Consider an incident from the perspective of the victim
- Create policies related to security incident management
- Define a disaster
- Appreciate the importance of emergency preparedness
- Analyze threats, risks, and business impact assessments
- Explain the components of a business continuity plan and program
- Develop policies related to business continuity management

Required Readings, Viewing, and Review:

Developing Cybersecurity Programs and Policies, Omar Santos, Pearson Education, 2019

Class Materials: Review both sets of slides for Chapters 11 and 12

Class Assignments:

Chapter 11: **Cybersecurity Incident Response**

Read pp. 368-412
Review questions 1-23, pp. 412-416
Projects 11.1 – 11.3, pp. 418-419

Answer the questions for An Exercise in Cybercrime Incident Response Case Study, pp. 419-423 (Submit in the Assignments folder in Blackboard)

Chapter 12: **Business Continuity Management**

Read pp. 426-454
Review questions 1-17, pp. 454-457
Projects 12.1 – 12.3, pp. 459-460

Weekly Discussion:

Why should the IT department not be solely responsible for business continuity?

Web Resources

http://www.247.prenhall.com/ Pearson product support
http://www.forensicfocus.com/ Forensic Focus—computer forensics and data recovery news and discussion
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf NIST Computer Security Incident Handling Guide

http://www.sans.org/reading-room/whitepapers/incident/computer-incident-response-team-641 SANS Institute Computer Incidence Response Team guidelines
https://digital-forensics.sans.org/blog/2018/01/08/meltdown-and-spectre-enterprise-action-plan SANS Digital Forensics and Incident Response Blog
https://www.youtube.com/watch?v=du6g__lgS3Q A Cybersecurity Simulation video via The Economist.
https://support.pearson.com/getsupport/s/ Pearson product support
http://www.continuitycentral.com/ Continuity Central provides a constantly updated one-stop resource of business continuity news, jobs, and information
http://en.wikipedia.org/wiki/Business_Continuity_Planning The Wikipedia entry for Business Continuity Planning
https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final NIST site to download Contingency Planning Guide for Federal Information Systems

Week 7: Regulatory Compliance for Financial Institutions
Regulatory Compliance for the Health-Care Sector

Learning Outcomes:

- Understand different financial institution cybersecurity regulatory compliance requirements
- Understand the components of a GLBA-compliant information security program
- Examine other financial services regulations, such as the New York Department of Financial Services (DFS) Cybersecurity Regulation
- Prepare for a regulatory examination
- Understand data privacy and new trends in international regulatory compliance
- Explain health-care-related information cybersecurity regulatory compliance requirements
- Understand the components of a HIPAA/HITECH-compliant information security program
- Prepare for a regulatory audit
- Know how to respond to an ePHI security incident
- Write HIPAA-related policies and procedures
- Understand the HIPAA compliance enforcement process

Required Readings, Viewing, and Review:

Developing Cybersecurity Programs and Policies, Omar Santos, Pearson Education, 2019

Class Materials: Review both sets of slides for Chapters 13 and 14

Class Assignments:

Chapter 13: **Regulatory Compliance for Financial Institutions**

Read pp. 462-490
Review questions 1-30, pp. 490-497
Projects 13.1 – 13.3, pp. 498-499

Answer the questions for Indiana Medicaid and the HealthNow Networks Breaches Case Study, p. 499 (Submit in the Assignments folder in Blackboard)

Chapter 14: **Regulatory Compliance for the Health-Care Sector**

Read pp. 502-534
Review questions 1-30, pp. 534-540
Projects 14.1 – 14.3, pp. 542-543

Weekly Discussion:

Why are covered entities required to obtain satisfactory assurances that business associates are appropriately safeguarding ePHI?

Web Resources

https://support.pearson.com/getsupport/s/ Pearson product support.
http://www.ftc.gov/privacy/privacyinitiatives/glbact.html The FTC site for privacy initiatives covers the FTC's Safeguards Rule and the Financial Privacy Rule
http://en.wikipedia.org/wiki/Gramm-Leach-Bliley_Act The Wikipedia article on the Gramm-Leach-Bliley Act (GLBA)
http://www.consumer.gov/idtheft/ The FTC's identify theft website
https://support.pearson.com/getsupport/s/ Pearson product support
http://www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/ Description of the Omnibus Rule
http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act Wikipedia article on Health Insurance Portability and Accountability Act (HIPAA)
https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html Summary of the HIPAA Privacy Rule
http://www.hipaacomply.com/ The definitive source for up-to-date information regarding HIPAA security and privacy compliance
https://www.hhs.gov/hipaa/index.html Health Information Privacy site
https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-ocr-enforces-the-hipaa-privacy-and-security-rules/index.html HHS site: How OCR Enforces the HIPAA Privacy & Security Rules

Week 8: PCI Compliance for Merchants
NIST Cybersecurity Framework

Learning Outcomes:

- Understand the Payment Card Industry Data Security Standard (PCI DSS)
- Recognize merchant responsibilities
- Explain the 12 top-level requirements
- Understand the PCI DSS validation process
- Implement practices related to PCI compliance
- Understand the overall goal of the NIST Cybersecurity Framework
- Identify the Framework's Core, Profile, and Implementation Tiers
- Explain how the NIST Cybersecurity Framework can be used by any organization as a reference to develop a cybersecurity program

Required Readings, Viewing, and Review:

Developing Cybersecurity Programs and Policies, Omar Santos, Pearson Education, 2019

Class Materials: Review both sets of slides for Chapters 15 and 16

Class Assignments: PCI Compliance for Merchants

Chapter 15: **PCI Compliance for Merchants**

Read pp. 546-569
Review questions 1-30, pp. 569-575
Projects 15.1 –15.3, pp. 577-578

Chapter 16: **NIST Cybersecurity Framework**

Read pp. 582-601
Review questions 1-13, pp. 601-604
Project 16.1, p. 605

Answer the questions for Intel and McAfee Adoption of the NIST Cybersecurity Framework Case Study, p. 606 (Submit in the Assignments folder in Blackboard)

Weekly Discussion:

When a company is looking for potential vendors/suppliers for a project, what would be the impact if the company asked vendors submitting proposals to provide information about their cybersecurity framework profile? How would that affect the supplier-customer relationship?

Web Resources

https://support.pearson.com/getsupport/s/ Pearson product support.
https://www.pcisecuritystandards.org/ Description of the PCI Standard
https://www.pcisecuritystandards.org/merchants/ Information on how to ensure a business is PCI-compliant
https://www.pcicomplianceguide.org/ A guide on PCI compliance
https://en.wikipedia.org/wiki/Luhn_algorithm Wiki article on the Luhn algorithm
https://www.creditcards.com/credit-card-news/assets/Luhn.pdf A pdf to calculate the Luhn formula
https://support.pearson.com/getsupport/s/ Pearson product support
https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improvingcritical-infrastructure-cybersecurity Executive Order—"Improving Critical Infrastructure Cybersecurity"
https://www.congress.gov/bill/113th-congress/senate-bill/1353/text Cybersecurity Enhancement Act of 2014
https://www.nist.gov/cyberframework NIST Cybersecurity Framework
https://www.nist.gov/cyberframework/framework-resources-0 NIST Cybersecurity Framework Interactive Framework Resources
https://www.nist.gov/cyberframework/related-efforts-roadmap NIST Cybersecurity Framework Roadmap
https://securingtomorrow.mcafee.com/executive-perspectives/tried-nist-framework-works-2 "We Tried the NIST Framework and It Works," McAfee
https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurityframework_6thworkshop_intel_corp.pdf "Cybersecurity Framework: Intel's Implementation Tools and Approach"
https://www.eac.gov/file.aspx?&A=Us%2BFqgpgVZw6CIHjBnD2tHKX0PKbwfShtOKsIx2kbEE%3D Applying the NIST Cybersecurity Framework to Elections