Preview: IAS5020 : Information Security Regulatory and Legal Environment

Syllabus

Course Overview

In this course, you will apply cyberdefense and information assurance within the context of the rules and guidelines that control them, and demonstrate an understanding of the security standards, responsibilities, rules, regulations, and issues that affect different types of organizations. You will also identify laws and policies related to cyberdefense, and show how these laws and policies relate to the storage and transmission of data. Finally, you will gain a greater understanding of the basic concepts of audit, evidence collection, and chain of custody rules.

Course Competencies

(Read Only)

To successfully complete this course, you will be expected to:

1. Analyze the applicable laws and policies related to cyberdefense.
2. Analyze how the type of legal dispute (for example, civil, criminal, or private) affects the evidence used to resolve it.
3. Conduct audits to determine compliance with laws.
4. Analyze the impact of legal or regulatory standards on a given system.
5. Communicate in a manner that is scholarly, professional, respectful, and consistent with expectations for professional practice.

Course Prerequisites

Prerequisite(s): Completion of or concurrent registration in IAS5015.

Syllabus >> Course Materials

Required

The materials listed below are required to complete the learning activities in this course.

Integrated Materials

Many of your required books are available via the VitalSource Bookshelf link in the courseroom, located in your Course Tools. Registered learners in a Resource Kit program can access these materials using the courseroom link on the Friday before the course start date. Some materials are available only in hard-copy format or by using an access code. For these materials, you will receive an email with further instructions for access. Visit the Course Materials page on Campus for more information.

Book

Grama, J. L. (2015). *Laboratory manual to accompany Legal Issues in Information Security, Version 2.0* (2nd ed.). Burlington, MA: Jones & Bartlett. ISBN: 9781284135442.

Grama, J. L. (2015). *Legal issues in information security* (2nd ed.). Burlington, MA: Jones & Bartlett. ISBN: 9781284054743.

External Resource

Please note that URLs change frequently. While the URLs were current when this course was designed, some may no longer be valid. If you cannot access a specific link, contact your instructor for an alternative URL. Permissions for the following links have been either granted or deemed appropriate for educational use at the time of course publication.

- U.S. Securities and Exchange Commission. (n.d.). EDGAR company filings. Retrieved from https://www.sec.gov/edgar/searchedgar/companysearch.html
- U.S. Securities and Exchange Commission. (n.d.). Latest filings received and processed at the SEC. Retreived from https://www.sec.gov/cgi-bin/browse-edgar?action=getcurrent

Suggested

The following materials are recommended to provide you with a better understanding of the topics in this course. These materials are not required to complete the course, but they are aligned to course activities and assessments and are highly recommended for your use.

External Resource

Please note that URLs change frequently. While the URLs were current when this course was designed, some may no longer be valid. If you cannot access a specific link, contact your instructor for an alternative URL. Permissions for the following links have been either granted or deemed appropriate for educational use at the time of course publication.

- Alcon, J. (2017, June 13). 5 credible cybersecurity threats to the financial services sector [Blog]. Retrieved from https://www.bitsighttech.com/blog/cybersecurity-threats-to-financial-sector
- Cameron, L. M. (2018, March 1). Future of digital forensics faces six security challenges in fighting borderless cybercrime and dark web tools. Retrieved from https://publications.computer.org/security-and-privacy/2018/03/01/digital-forensics-security-challenges-cybercrime
- Christidis, A. (2018, January 2). How to mitigate the risks of cyber security through contingency planning. Retrieved from http://metin-mitchell.com/how-to-mitigate-the-risks-of-cyber-security-through-contingency-planning
- Clearwater Compliance. (2013, January 17). *How the HITECH Act raised the ante for HIPAA compliance* [Video]. Retrieved from https://www.youtube.com/watch?v=cJrmqsppklg
- Diligent Corporation. (2016). Five best practices for information security governance [PDF]. Available from http://diligent.com

- FBI. (n.d.). Cyber crime. Retrieved from https://www.fbi.gov/investigate/cyber
- Federal Trade Commission. (n.d.). Data security. Retrieved from https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security
- Federal Trade Commission. (n.d.). Gramm-Leach-Bliley Act. Retrieved from https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act
- Fischer, E. A. (2014, December 12). *Federal laws relating to cybersecurity: Overview of major issues, current laws, and proposed legislation* (CRS Report No. R42114) [PDF]. Available from https://fas.org
- Gupta, P. (2017, June 7). Cyber security: A concern in education. Retrieved from http://edtechreview.in/dictionary/2814-cyber-security-in-education
- Hayes, W. (2016, October 20). Four ways to balance employee privacy and corporate security. Retrieved from https://www.forbes.com/sites/willhayes/2016/10/20/four-ways-to-balance-employee-privacy-and-corporate-security/#302e3f5523a9
- Lang, M. (2017, October 18). Electronic tracking spurs workplace privacy debate. Retrieved from http://www.govtech.com/policy/Electronic-Tracking-Spurs-Workplace-Privacy-Debate.html
- Lord, N. (2018, September 19). What is GLBA compliance? Understanding the data protection requirements of the Gramm-Leach-Bliley Act. Retrieved from https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act
- National Conference of State Legislatures. (2018, November 6). Cybersecurity legislation 2018. Retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx
- Reed, R. (2018, March 2). Workplace monitoring gets personal, and employees fear it's too close for comfort. They're right. *Chicago Tribune*. Retrieved from http://www.chicagotribune.com/business/columnists/reed/ct-biz-amazon-workplace-privacy-dilemma-robert-reed-0304-story.html
- Schwartz, M. A., & Omer, C. (n.d.). The constitutionality of state cybersecurity regulations. Retrieved from https://www.theclearinghouse.org/banking-perspectives/2017/2017-q2-banking-perspectives/articles/constitutionality-cybersecurity-regulations
- SecurityTubeCons. (2012, November 19). *Before, during, and after* [Video] | Transcript Retrieved from https://www.youtube.com/watch?v=vKCqUcj8f2s
- Shiang, L. (2018, May 3). Advice for new CISOs: How to get a head start on information security governance. Retrieved from https://deltarisk.com/blog/advice-for-new-cisos-how-to-get-a-head-start-on-information-security-governance
- Stevens, M. (2016, March 15). Cybersecurity vs. information security: Is there a difference? [Blog]. Retrieved from https://www.bitsighttech.com/blog/cybersecurity-vs-information-security
- Tsan, L. (2018, January 30). 4 steps to enhance financial data security in your organization [Blog]. Retrieved from https://blogs.oracle.com/infrastructure/4-steps-to-enhance-financial-data-security-in-your-organization
- Tuttle, H. (2018, February 1). 2018 cyberrisk landscape. Retrieved from http://www.rmmagazine.com/2018/02/01/2018-cyberrisk-landscape
- U.S. Department of Education, Protecting Student Privacy. (n.d.). Data security: K-12 and higher education. Retrieved from https://studentprivacy.ed.gov/Security
- U.S. Department of Health & Human Services. (n.d.). HITECH Act enforcement interim final rule. Retrieved from https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html

- University of York. (2018, October 2). Can we trust digital forensic evidence? *ScienceDaily*. Retrieved from https://www.sciencedaily.com/releases/2018/10/181002113953.htm
- Voigt, L. (2018, July 13). 5 best practices for your incident response plan [Blog]. Retrieved from https://www.exabeam.com/incident-response/improve-your-2018-incident-response-plan-with-the-latest-best-practices
- Wan, T. (2017, September 25). How to protect education data when no systems are secure. Retrieved from https://www.edsurge.com/news/2017-09-25-how-to-protect-education-data-when-no-systems-are-secure

Optional

The following optional materials are offered to provide you with a better understanding of the topics in this course. These materials are not required to complete the course.

Unit 1 >> The U.S. Legal System and Criminal Law Issues

Introduction

Cybersecurity has generated the interest and attention of lawmakers and law enforcement at all levels, resulting in a matrix of cyber-related laws, regulations, and statutes. Unit 1 will begin with an introduction to this legislation and how it affects the field of information security. This unit will also take a closer look at the legal system and some criminal law issues. With this understanding, you can then proceed to examine more specialized legal issues in information security.

Learning Activities

u01s1 - Studies

Required Readings

The following readings cover information pertaining to federal security and privacy laws and will be useful in completing the discussion in this unit.

- Grama, J. L. (2015). *Legal issues in information security* (2nd ed.). Burlington, MA: Jones & Bartlett.
  - Chapter 3, “The American Legal System,” pages 68–91.
  - Chapter 12, “Criminal Law and Tort Law Issues in Cyberspace,” pages 350–390.

Suggested Resources

The following resources are not required, but may provide additional information that may be useful in the unit discussion and the course assignments.

- FBI. (n.d.). Cyber crime. Retrieved from https://www.fbi.gov/investigate/cyber
- Fischer, E. A. (2014, December 12). *Federal laws relating to cybersecurity: Overview of major issues, current laws, and proposed legislation* (CRS Report No. R42114) [PDF]. Available from https://fas.org
- National Conference of State Legislatures. (2018, November 6). Cybersecurity legislation 2018. Retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx
- SecurityTubeCons. (2012, November 19). *Before, during, and after* [Video] | Transcript. Retrieved from https://www.youtube.com/watch?v=vKCqUcj8f2s

u01s1 - Learning Components

- Explain criminal law concepts.
- Explain aspects of the U.S. legal system.
- Identify common criminal laws used in regard to cybercrimes.
- Apply criminal law concepts.

u01a1 - Cyberstalking or Cyberbullying and Laws to Protect Individuals

Preparation

This assignment requires you to complete Lab 8 in your *Laboratory Manual to Accompany Legal Issues in Information Security* lab manual. In a face-to-face courseroom, you might write your assignment in a paper-based copy of this lab manual and tear it out to give to your instructor. However, in this online course, you will only use the lab as a starting point. Do not create the files as indicated in the lab. Instead, read the lab information or case study, then complete the assignment as outlined below, using a Word document for your assignment submission.

Instructions

In your lab manual, complete the following:

- Grama, J. L. (2015). *Laboratory manual to accompany Legal Issues in Information Security, Version 2.0* (2nd ed.). Burlington, MA: Jones & Bartlett.
    - Lab 8, "Cyberstalking or Cyberbullying and Laws to Protect Individuals," page 57.

Complete the following sections of the lab:

- Introduction.
- Hands-On Steps.

    - *Note:* the Hands-On Steps provide a starting point for your research, but the requirements of this assignment are defined below.

Next, complete the following research:

- Conduct your own independent research on cyberstalking and cyberbullying, including its legal implications.
- Locate and research a specific case of cyberstalking or cyberbullying.
- Always record the citations for your resources, including the URLs for online materials. You will provide them in reference lists for your assignments.

Requirements

For this assignment, address the following:

- In your own words, define cyberstalking.
- In your own words, define cyberbullying.
- Explain the legal implications of cyberstalking and cyberbullying.
- Summarize the cyberstalking or cyberbullying case you located through your research. Be sure to include the citation for the case, including the URL.
    - Who was the victim?
    - How was the person victimized?
    - What was the outcome of the case?
- Outline a law you would create to protect the victim in the case you chose.
    - What elements would you include in the law?
    - How would your law protect the victim?
    - How would you enforce the law?

Use a minimum of three professional resources to support your statements in this assignment. Be sure to cite your sources correctly, following APA guidelines.

Additional Requirements

- **Formatting guidelines:** Include a title page and references page.
- **Length:** 2–4 pages, not including the title page and references page.
- **Number of resources:** Use at least 3 scholarly and/or professional sources.
- **Reference format:** Use APA style and format for citations and references.
- **Font:** Times New Roman, 12-point font, double-spaced.

Refer to the assignment scoring guide to ensure you have addressed all of the evaluation criteria for this assignment.

Submit your assignment as a Word document in the assignment area.

u01d1 - Cyberdefense Laws

Read the Discussion Participation Scoring Guide to learn how the instructor will evaluate your discussion participation throughout this course.

The resources provided in this unit explore the legal system and criminal law in the United States. Use these resources as well as your own research to discuss the following:

- Explain how regulatory agencies affect cyberdefense.
- Describe strategies for enforcing cyberdefense laws.

Response Guidelines

After posting your discussion, respond to the initial posts of at least two of your peers. Expand on the concepts covered in their posts.

Course Resources
Graduate Discussion Participation Scoring Guide

u01d1 - Learning Components

- Explain criminal law concepts.
- Explain aspects of the U.S. legal system.
- Apply graduate-level skill in research, critical thinking, and writing.
- Identify common criminal laws used in regard to cybercrimes.

Unit 2 >> Information Security Overview

Introduction

Cybersecurity has become the domain of local law enforcement, state politicians, the U.S. President, state and federal agencies, and congresses at the local, state, and federal levels. This maze of legal and regulatory activity has created the need for the security professional to understand the context, and to remain compliant with the entire range of laws and statutes when engaged in his or her work. Unit 2 will continue the exploration of existing laws and statutes, and how they affect the work of information security.

Learning Activities

u02s1 - Studies

Required Reading

The following reading covers information pertaining to information security and will be useful in completing the discussion in this unit.

- Grama, J. L. (2015). *Legal issues in information security* (2nd ed.). Burlington, MA: Jones & Bartlett.
    - Chapter 1, “Information Security Overview,” pages 2–32.

Suggested Resource

The following resource is not required, but may provide additional information that may be useful in the unit discussion and the course assignments.

- Stevens, M. (2016, March 15). Cybersecurity vs. information security: Is there a difference? [Blog]. Retrieved from https://www.bitsighttech.com/blog/cybersecurity-vs-information-security

u02s1 - Learning Components

- Analyze principles of privacy protection.
- Describe common threats to privacy.
- Identify privacy principles.

u02a1 - Creating an IT Infrastructure Asset List

Preparation

This assignment requires you to complete Lab 1 in your *Laboratory Manual to Accompany Legal Issues in Information Security* lab manual. In a face-to-face courseroom, you might write your assignment in a paper-based copy of this lab manual and tear it out to give to your instructor. However, in this online course, you will only use the lab as a starting point. Do not create the files as indicated in the lab. Instead, read the lab information or case study, then complete the assignment as outlined below, using a Word document for your assignment submission.

Instructions

In your lab manual, complete the following:

- Grama, J. L. (2015). *Laboratory manual to accompany Legal Issues in Information Security, Version 2.0* (2nd ed.). Burlington, MA: Jones & Bartlett.
    - Lab 1, "Creating an IT Infrastructure Asset List and Identifying Where Privacy Data Resides," page 1.

Complete the following sections of the lab:

- Introduction.
- Hands-On Steps.
    - *Note:* the Hands-On Steps provide a starting point for your research, but the requirements of this assignment are defined below.

Next, complete the following research:

- Conduct your own independent research on IT asset inventories, data classification, and data privacy.
- Always record the citations for your resources, including the URLs for online materials. You will provide them in reference lists for your assignments.

Requirements

For this assignment, address the following:

- Create an IT asset inventory checklist organized within the seven domains of a typical IT infrastructure.
    - What risks, threats, and vulnerabilities are typically found within the seven domains of a typical IT infrastructure?
- Complete an asset identification and classification grid for a typical IT infrastructure.
    - Create a grid or table like the one found on page 5 of the lab manual.
- Explain how a data classification standard is linked to customer privacy data protection and proper security controls.
- Identify where privacy data can reside or travel throughout the seven domains of a typical IT infrastructure.
- Identify where privacy data protection and proper security controls are needed to help an organization maintain compliance.

Use a minimum of two professional resources to support your statements in this assignment. Be sure to cite your sources correctly, following APA guidelines.

Additional Requirements

- **Formatting guidelines:** Include a title page and references page.
- **Length:** 2–4 pages, not including the title page and references page.
- **Number of resources:** Use at least 2 scholarly and/or professional sources.
- **Reference format:** Use APA style and format for citations and references.
- **Font:** Times New Roman, 12-point font, double-spaced.

Refer to the assignment scoring guide to ensure you have addressed all of the evaluation criteria for this assignment.

Submit your assignment as a Word document in the assignment area.

u02d1 - Managing Critical Infrastructure

Veterans in the field of information security have long been concerned with potential areas of weakness in IT infrastructure. Use the resources provided in this unit as well as your own research to discuss the following:

- Describe basic information security concepts.
- Identify common information security concerns and explain the mechanisms to secure them.
- Explain different types of data and how they are secured.

Response Guidelines

After posting your discussion, respond to the initial posts of at least two of your peers. Have they identified concerns that are different from the ones you identified? Can you provide additional information that might be useful to them?

Course Resources
Graduate Discussion Participation Scoring Guide

u02d1 - Learning Components

- Analyze principles of privacy protection.
- Describe common threats to privacy.

Unit 3 >> Privacy Overview

Introduction

Units 1 and 2 focused on the United States legal system and information security. A number of common information security models and standards organizations are increasingly creating common practice guidelines

for information security professionals. In Unit 3, the focus will shift to privacy in the workplace and confidential information.

Learning Activities

u03s1 - Studies

Required Reading

The following reading covers information pertaining to privacy and will be useful in completing the discussion in this unit.

- Grama, J. L. (2015). *Legal issues in information security* (2nd ed.). Burlington, MA: Jones & Bartlett.
    - Chapter 2, "Privacy Overview," pages 33–67.

Suggested Resources

The following resources are provided to expand your knowledge and understanding of the unit topic, and may be useful in completing course assignments.

- Hayes, W. (2016, October 20). Four ways to balance employee privacy and corporate security. Retrieved from https://www.forbes.com/sites/willhayes/2016/10/20/four-ways-to-balance-employee-privacy-and-corporate-security/#302e3f5523a9
- Lang, M. (2017, October 18). Electronic tracking spurs workplace privacy debate. Retrieved from http://www.govtech.com/policy/Electronic-Tracking-Spurs-Workplace-Privacy-Debate.html
- Reed, R. (2018, March 2). Workplace monitoring gets personal, and employees fear it's too close for comfort. They're right. *Chicago Tribune.* Retrieved from http://www.chicagotribune.com/business/columnists/reed/ct-biz-amazon-workplace-privacy-dilemma-robert-reed-0304-story.html

u03s1 - Learning Components

- Analyze principles of privacy protection.
- Describe common threats to privacy.

u03a1 - Issues Related to Sharing Consumers' Confidential Information

Preparation

This assignment requires you to complete Lab 5 in your *Laboratory Manual to Accompany Legal Issues in Information Security* lab manual. In a face-to-face courseroom, you might write your assignment in a paper-

based copy of this lab manual and tear it out to give to your instructor. However, in this online course, you will only use the lab as a starting point. Do not create the files as indicated in the lab. Instead, read the lab information or case study, then complete the assignment as outlined below, using a Word document for your assignment submission.

Instructions

In your lab manual, complete the following:

- Grama, J. L. (2015). *Laboratory manual to accompany Legal Issues in Information Security, Version 2.0* (2nd ed.). Burlington, MA: Jones & Bartlett.
    - Lab 5, "Case Study on Issues Related to Sharing Consumers' Confidential Information," page 35.

Complete the following sections of the lab:

- Introduction.
- Hands-On Steps.
    - *Note:* the Hands-On Steps provide a starting point for your research, but the requirements of this assignment are defined below.

Next, complete the following research:

- Conduct your own independent research on the Electronic Frontier Foundation (EFF), privacy law, and confidential information.
- Always record the citations for your resources, including the URLs for online materials. You will provide them in reference lists for your assignments.

Requirements

For this assignment, address the following:

- Explain the purpose of the Electronic Frontier Foundation (EFF).
- Analyze the privacy issues in the case study.
    - Identify the issues.
    - Explain the importance of the issues and this case.
- Analyze the implications of the privacy law violations in the case study on privacy and confidential information.
    - Consider the legal, ethical, and information systems security perspectives.

Use a minimum of three professional resources to support your statements in this assignment. Be sure to cite your sources correctly, following APA guidelines.

Additional Requirements

- **Formatting guidelines:** Include a title page and references page.
- **Length:** 2–4 pages, not including the title page and references page.

- **Number of resources:** Use at least 3 scholarly and/or professional sources.
- **Reference format:** Use APA style and format for citations and references.
- **Font:** Times New Roman, 12-point font, double-spaced.

Refer to the assignment scoring guide to ensure you have addressed all of the evaluation criteria for this assignment.

Submit your assignment as a Word document in the assignment area.

u03d1 - Privacy Threats

The goal of information security is to protect data. Over the last several years, privacy and protecting personal data have become major concerns for everyone. Identity theft and breaches of personal information have become the most important privacy concerns.

Use the unit resources and your own research to discuss the following:

- Explain the difference between information security and privacy.
- Evaluate different threats to data privacy.
- Describe best practices for privacy protection.

Response Guidelines

After posting your discussion, respond to the initial posts of at least two of your peers. Did you evaluate threats differently from your peers? Have they listed best practices you did not?

Course Resources
Graduate Discussion Participation Scoring Guide

u03d1 - Learning Components

- Analyze principles of privacy protection.
- Describe common threats to privacy.

Unit 4 >> Security and Privacy of Consumer Financial Information and Educational Records

Introduction

Information security professionals become involved in legal issues that involve security and privacy laws. Units 1, 2, and 3 provided background on the legal system and overviews of information security and privacy. Unit 4 will begin the exploration of specific concerns in information security and privacy. It will also examine sharing confidential consumer information and educational records privacy.

Learning Activities

u04s1 - Studies

Required Readings

The following readings cover topics pertaining to financial information and educational records and will be useful in completing the discussion in this unit.

- Grama, J. L. (2015). *Legal issues in information security* (2nd ed.). Burlington, MA: Jones & Bartlett.
  - Chapter 4, "Security and Privacy of Consumer Financial Information," pages 92–102.
  - Chapter 5, "Security and Privacy of Information Belonging to Children and in Educational Records," pages 121–147.

Suggested Resources

The following resources are provided to expand your knowledge and understanding of the unit topic, and may be useful in completing course assignments.

- Alcon, J. (2017, June 13). 5 credible cybersecurity threats to the financial services sector [Blog]. Retrieved from https://www.bitsighttech.com/blog/cybersecurity-threats-to-financial-sector
- Federal Trade Commission. (n.d.). Data security. Retrieved from https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security
- Gupta, P. (2017, June 7). Cyber security: A concern in education. Retrieved from http://edtechreview.in/dictionary/2814-cyber-security-in-education
- Tsan, L. (2018, January 30). 4 steps to enhance financial data security in your organization [Blog]. Retrieved from https://blogs.oracle.com/infrastructure/4-steps-to-enhance-financial-data-security-in-your-organization
- U.S. Department of Education, Protecting Student Privacy. (n.d.). Data security: K-12 and higher education. Retrieved from https://studentprivacy.ed.gov/Security
- Wan, T. (2017, September 25). How to protect education data when no systems are secure. Retrieved from https://www.edsurge.com/news/2017-09-25-how-to-protect-education-data-when-no-systems-are-secure

- Analyze business challenges facing financial institutions.
- Analyze Federal Trade Commission red flags and payment card industry standards.

u04a1 - Case Study on PCI DSS Noncompliance: CardSystems Solutions

Preparation

This assignment requires you to complete Lab 3 in your *Laboratory Manual to Accompany Legal Issues in Information Security* lab manual. In a face-to-face courseroom, you might write your assignment in a paper-based copy of this lab manual and tear it out to give to your instructor. However, in this online course, you will only use the lab as a starting point. Do not create the files as indicated in the lab. Instead, read the lab information or case study, then complete the assignment as outlined below, using a Word document for your assignment submission.

Instructions

In your lab manual, complete the following:

- Grama, J. L. (2015). *Laboratory manual to accompany Legal Issues in Information Security, Version 2.0* (2nd ed.). Burlington, MA: Jones & Bartlett.
    - Lab 3, "Case Study on PCI DSS Non-compliance: CardSystems Solutions," page 18.

Complete the following sections of the lab:

- Introduction.
- Hands-On Steps.
    - *Note:* the Hands-On Steps provide a starting point for your research, but the requirements of this assignment are defined below.

Next, complete the following research:

- Conduct your own independent research online to find a real-world case study on Payment Card Industry Data Security Standard (PCI DSS) noncompliance.
- Always record the citations for your resources, including the URLs for online materials. You will provide them in reference lists for your assignments.

Requirements

For this assignment, address the following:

- Explain the implications of the case study from the field of information security that you located online.
    - Remember to provide the URL for the case study.

- Analyze the case study in the lab manual.
    - Identify the privacy data breach that occurred.
    - Explain if CardSystems Solutions broke any laws.
    - Assess the auditor's findings.
    - Determine if CardSystems Solutions can or should sue the auditor.
    - Determine which party was negligent.
    - Evaluate the actions of the Federal Trade Commission.
        - Did the actions of CardSystems Solutions warrant an "unfair trade practice" designation?
- Recommend PCI DSS-compliant mitigation strategies to prevent the same thing from happening again.

Use a minimum of three professional resources to support your statements in this assignment. Be sure to cite your sources correctly, following APA guidelines.

Additional Requirements

- **Formatting guidelines:** Include a title page and references page.
- **Length:** 2–4 pages, not including the title page and references page.
- **Number of resources:** Use at least 3 scholarly and/or professional sources.
- **Reference format:** Use APA style and format for citations and references.
- **Font:** Times New Roman, 12-point font, double-spaced.

Refer to the assignment scoring guide to ensure you have addressed all of the evaluation criteria for this assignment.

Submit your assignment as a Word document in the assignment area.

u04d1 - Determining Jurisdiction

For this discussion, use the following scenario:

John Miller is the information security and privacy officer of a local bank. He is new to his position and began his work by evaluating the bank's existing security and privacy controls. He is also new to information security, having only recently graduated with a BS in information security, with professional experience as an active-directory administrator for two years. This work with active directory created his interest in pursuing a position in the field of security. He has the most experience in the areas of account management; user creation and management; and groups, roles, and group policy, so these are the areas in which he began his work.
John found literally hundreds of idle accounts, indicating that users are created but are not properly discontinued when employees move on and no longer need access to the data collected and stored by the bank. This discovery inspired him to begin digging into other aspects of the security controls, and he found evidence of

malware on the servers that house the credit card data collected and stored for use by the bank. His next discovery was the most alarming. The objective of the malware that had deeply infested the bank's systems was to package and transmit all available data to a remote host located in a foreign country. John is clearly in over his head at this point, and needs to act quickly to resolve the situation and stop the flow of financial information to an unauthorized third party.

Use the unit resources and your own research to discuss the following:

- What primary laws, regulations, or statutes have been violated by this lack of attention to controls, leading to this serious breach of security?
- What channels of communication should John enlist to assist him in resolving this matter, and in what order should those communication sources be contacted?
- What tools and other supporting resources are available to John to determine the breadth of the breach and the mitigations available to secure those assets?

Response Guidelines

After posting your discussion, respond to the initial posts of at least two of your peers. Do you and your peers agree on the channels of communication and the order in which they should be contacted?

Course Resources
Graduate Discussion Participation Scoring Guide

u04d1 - Learning Components

- Analyze business challenges facing financial institutions.
- Analyze Federal Trade Commission red flags and payment card industry standards.

Unit 5 >> Federal Cyberlaws and Regulations

Introduction

The federal government collects and stores a large amount of highly sensitive information that is often the target of attackers. These attackers range from single individuals with a personal or profit motive, to highly organized legions of state-sponsored hackers. The Stuxnet virus infection is an example of the progressive escalation of this kind of cyberwarfare, taking the need for skilled cybersecurity professionals to a new level. Cybersecurity has also generated the interest and attention of lawmakers and law enforcement at all levels, resulting in a matrix of cyber-related laws, regulations, and statutes. Unit 5 will examine this legislation and how it affects the field of information security and privacy.

Learning Activities

u05s1 - Studies

Required Reading

The following reading covers information pertaining to federal cyberlaws and regulations and will be useful in completing the discussion in this unit.

- Grama, J. L. (2015). *Legal issues in information security* (2nd ed.). Burlington, MA: Jones & Bartlett.
    - Chapter 8, “Federal Government Information Security and Privacy Regulations,” pages 218–247.

Suggested Resources

The following resources are not required, but may provide additional information that may be useful in the unit discussion and the course assignments.

- FBI. (n.d.). Cyber crime. Retrieved from https://www.fbi.gov/investigate/cyber
- Fischer, E. A. (2014, December 12). *Federal laws relating to cybersecurity: Overview of major issues, current laws, and proposed legislation* (CRS Report No. R42114) [PDF]. Available from https://fas.org
- National Conference of State Legislatures. (2018, November 6). Cybersecurity legislation 2018. Retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx
- SecurityTubeCons. (2012, November 19). *Before, during, and after* [Video] | Transcript. Retrieved from https://www.youtube.com/watch?v=vKCqUcj8f2s

u05s1 - Learning Components

- Define the scope of federal cyberdefense laws.
- Analyze the objectives and challenges of enforcing federal cyberdefense laws.
- Identify federal laws that relate to cyberdefense.
- Identify strategies for enforcing cyberdefense laws within a federal government agency.

u05a1 - Case Study on U.S. Veteran Affairs and Loss of Private Information

Preparation

This assignment requires you to complete Lab 2 in your *Laboratory Manual to Accompany Legal Issues in Information Security* lab manual. In a face-to-face courseroom, you might write your assignment in a paper-based copy of this lab manual and tear it out to give to your instructor. However, in this online course, you will only use the lab as a starting point. Do not create the files as indicated in the lab. Instead, read the lab information or

case study, then complete the assignment as outlined below, using a Word document for your assignment submission.

Instructions

In your lab manual, complete the following:

- Grama, J. L. (2015). *Laboratory manual to accompany Legal Issues in Information Security, Version 2.0* (2nd ed.). Burlington, MA: Jones & Bartlett.
    - Lab 2, "Case Study on U.S. Veteran Affairs and Loss of Private Information," page 9.

Complete the following sections of the lab:

- Introduction.
- Hands-On Steps.
    - *Note:* the Hands-On Steps provide a starting point for your research, but the requirements of this assignment are defined below.

Next, complete the following research:

- Conduct your own independent research online to find a real-world case study on privacy law violation and the implications for the person affected as well as the organization in violation.
- Always record the citations for your resources, including the URLs for online materials. You will provide them in reference lists for your assignments.

Requirements

For this assignment, address the following:

- Explain the implications of your chosen case study for the individual involved, the organization in violation, and the field of information security and privacy.
    - Remember to provide the URL for the case study.
- Explain how privacy law differs from information systems security.
- Analyze the case study from Lab 2.
    - Explain whether you believe the employee was justified in taking home official data.
    - Describe the potential consequences of the data loss.
    - Explain whether the loss of privacy data was a Health Insurance Portability and Accountability Act (HIPAA) compliance violation.
    - Determine the actions the agency can take against the employee.
- Recommend mitigation strategies to prevent the same data loss from happening again.

Use a minimum of three professional resources to support your statements in this assignment. Be sure to cite your sources correctly, following APA guidelines.

Additional Requirements

- **Formatting guidelines:** Include a title page and references page.
- **Length:** 2–4 pages, not including the title page and references page.
- **Number of resources:** Use at least 3 scholarly and/or professional sources.
- **Reference format:** Use APA style and format for citations and references.
- **Font:** Times New Roman, 12-point font, double-spaced.

Refer to the assignment scoring guide to ensure you have addressed all of the evaluation criteria for this assignment.

Submit your assignment as a Word document in the assignment area.

u05d1 - Identification and Analysis of Federal Cyberlaws

Use the unit resources and your own research to discuss the following:

- Identify five major federal laws related to cyberdefense.
- Define the scope of each of the five federal laws you identified.
- Analyze the objectives and challenges of enforcing federal cyberdefense laws.

Response Guidelines

After posting your discussion, respond to the initial posts of at least two of your peers.

- Did you choose the same laws as your peers?
- Do you agree with their definitions of the scope of the laws?
- Are there other objectives and challenges that they have not analyzed?

Course Resources
Graduate Discussion Participation Scoring Guide

u05d1 - Learning Components

- Define the scope of federal cyberdefense laws.
- Analyze the objectives and challenges of enforcing federal cyberdefense laws.
- Apply graduate-level skill in research, critical thinking, and writing.
- Identify federal laws that relate to cyberdefense.
- Identify strategies for enforcing cyberdefense laws within a federal government agency.

Introduction

In addition to federal laws and statutes, cybersecurity has also become the domain of local law enforcement, state politicians, state and federal agencies, and local and state congresses. This maze of legal and regulatory activity has created the need for the security professional to understand the context and to remain compliant with the entire range of state and local laws and statutes when engaged in his or her work.

Learning Activities

u06s1 - Studies

Required Reading

The following reading covers information pertaining to state laws and will be useful in completing the discussion in this unit.

- Grama, J. L. (2015). *Legal issues in information security* (2nd ed.). Burlington, MA: Jones & Bartlett.
    - Chapter 9, “State Laws Protecting Citizens’ Information and Breach Notices,” pages 248–275.

Suggested Resources

The following resources are not required, but may provide additional information that may be useful in the unit discussion and the course assignments.

- National Conference of State Legislatures. (2018, November 6). Cybersecurity legislation 2018. Retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx
- Schwartz, M. A., & Omer, C. (n.d.). The constitutionality of state cybersecurity regulations. Retrieved from https://www.theclearinghouse.org/banking-perspectives/2017/2017-q2-banking-perspectives/articles/constitutionality-cybersecurity-regulations

u06s1 - Learning Components

- Describe applicable state and local laws, regulations, or statutes related to cybersecurity.
- Explain the practices of state and local law enforcement related to jurisdiction and division of labor.
- Analyze the objectives and challenges of enforcing local cybersecurity laws, regulations, or statutes.

u06a1 - Identifying the Scope of State Data and Security Breach Notification Law

Preparation

This assignment requires you to complete Lab 6 in your *Laboratory Manual to Accompany Legal Issues in Information Security* lab manual. In a face-to-face courseroom, you might write your assignment in a paper-based copy of this lab manual and tear it out to give to your instructor. However, in this online course, you will only use the lab as a starting point. Do not create the files as indicated in the lab. Instead, read the lab information or case study, then complete the assignment as outlined below, using a Word document for your assignment submission.

Instructions

In your lab manual, complete the following:

- Grama, J. L. (2015). *Laboratory manual to accompany Legal Issues in Information Security, Version 2.0* (2nd ed.). Burlington, MA: Jones & Bartlett.
    - Lab 6, "Identifying the Scope of Your State's Data and Security Breach Notification Law," page 42.

Complete the following sections of the lab:

- Introduction.
- Hands-On Steps.
    - *Note:* the Hands-On Steps provide a starting point for your research, but the requirements of this assignment are defined below.

Next, complete the following research:

- Conduct your own independent research to find your state's data and security breach notification law. Then, locate the law for another state of your choice.
- Always record the citations for your resources, including the URLs for online materials. You will provide them in reference lists for your assignments.

Requirements

For this assignment, address the following:

- Explain the relationship between state data security breach notification laws and individual privacy.
- Explain the rationale for state governments to have data security breach notification laws.
    - How do state laws differ from federal laws?
- Analyze the data security breach notification laws from two different states.
    - Provide the citation for each state's law.
    - How do they compare in terms of scope and depth of the privacy protection they offer citizens?
    - What are the challenges of enforcing the laws?
- Suggest ways the law in your state could be improved.

Use a minimum of two professional resources to support your statements in this assignment. Be sure to cite your sources correctly, following APA guidelines.

Additional Requirements

- **Formatting guidelines:** Include a title page and references page.
- **Length:** 2–4 pages, not including the title page and references page.
- **Number of resources:** Use at least 2 scholarly and/or professional sources.
- **Reference format:** Use APA style and format for citations and references.
- **Font:** Times New Roman, 12-point font, double-spaced.

Refer to the assignment scoring guide to ensure you have addressed all of the evaluation criteria for this assignment.

Submit your assignment as a Word document in the assignment area.

u06d1 - The Effect of State Privacy Laws on Information Security

Within the landmark California SB 1386 bill, one of the greatest concerns for information security and privacy professionals is language that includes liability related to the personally identifiable information of California residents, regardless of where that data is collected and stored.

For this discussion, use the following scenario:

Tasty Candy Store is a candy manufacturer in Las Vegas, Nevada. It has a special line of high-priced chocolate liqueur truffles that are a popular favorite of visitors to Las Vegas. Tasty Candy owners saw the potential for expanding their sales by creating a website, allowing customers to purchase their favorite sweet treats over the Internet. Their predictions were accurate, and soon the Tasty Candy website was busy processing orders from customers all over the world. Their customer base includes a large number of California residents. Two years after Tasty Candy set up their website, the site fell victim to hackers who gained access to all of the credit card and demographic data for all of Tasty Candy's 12,000 customers.

Use the resources provided in this unit and your own research to discuss the following:

- What are the mitigating factors that would work to the benefit of Tasty Candy in meeting the requirements of SB 1386 that pertain to information breach reporting related to California residents?
- What are the responsibilities of Tasty Candy in terms of reporting this breach of data specific to California residents?
- Are there other state or federal regulations that would affect how and when Tasty Candy reported this data breach to the general public or to specific segments of their customer base?

Response Guidelines

After posting your discussion, respond to the initial posts of at least two of your peers. Comment on the similarities and differences in what you and your peers have stated are the responsibilities of Tasty Candy.

Course Resources

Graduate Discussion Participation Scoring Guide

u06d1 - Learning Components

- Describe applicable state and local laws, regulations, or statutes related to cybersecurity.
- Explain the practices of state and local law enforcement related to jurisdiction and division of labor.
- Apply graduate-level skill in research, critical thinking, and writing.
- Analyze the objectives and challenges of enforcing local cybersecurity laws, regulations, or statutes.

Unit 7 >> Corporate Information Security and Privacy

Introduction

Unit 7 will examine the issues specific to corporate information security and privacy. You will learn why financial reporting is important, and how securities law reform came about, by examining a case study on the Enron scandal. The reform following that scandal determined which types of companies need to follow new laws, and why. You will also explore corporations' privacy issues, and how they comply with federal and state laws. Corporate security and privacy concerns also involve considerations such as intellectual privacy laws and contracts.

Learning Activities

u07s1 - Studies

Required Readings

The following readings cover topics pertaining to corporate information security and privacy and will be useful in completing the discussion in this unit.

- Grama, J. L. (2015). *Legal issues in information security* (2nd ed.). Burlington, MA: Jones & Bartlett.
  - Chapter 7, “Corporate Information Security and Privacy Regulations,” pages 188–217.
  - Chapter 10, “Intellectual Privacy Law,” pages 276–313.
  - Chapter 11, “The Role of Contracts,” pages 314–349.

Required Research

The U.S. Securities and Exchange Commission's (SEC's) Electronic Data Gathering, Analysis, and Retrieval (EDGAR) database contains the documentation that all publicly traded companies are required to submit to the SEC. In preparation for the discussion in this unit, choose a publicly traded company. Research your chosen company and locate and examine its most recent Form 10-K report, using one of the following EDGAR websites:

- U.S. Securities and Exchange Commission. (n.d.). EDGAR company filings. Retrieved from https://www.sec.gov/edgar/searchedgar/companysearch.html
- U.S. Securities and Exchange Commission. (n.d.). Latest filings received and processed at the SEC. Retreived from https://www.sec.gov/cgi-bin/browse-edgar?action=getcurrent

u07s1 - Learning Components

- Explain intellectual property laws and the effect they have on a corporation.
- Explain the differences between public and private information security and privacy regulations.
- Analyze issues of corporate regulations and privacy laws.

u07a1 - Case Study on the Digital Millennium Copyright Act: Napster

Preparation

This assignment requires you to complete Lab 7 in your *Laboratory Manual to Accompany Legal Issues in Information Security* lab manual. In a face-to-face courseroom, you might write your assignment in a paper-based copy of this lab manual and tear it out to give to your instructor. However, in this online course, you will only use the lab as a starting point. Do not create the files as indicated in the lab. Instead, read the lab information or case study, then complete the assignment as outlined below, using a Word document for your assignment submission.

Instructions

In your lab manual, complete the following:

- Grama, J. L. (2015). *Laboratory manual to accompany Legal Issues in Information Security, Version 2.0* (2nd ed.). Burlington, MA: Jones & Bartlett.
    - Lab 7, "Case Study on Digital Millennium Copyright Act: Napster," page 54.

Complete the following sections of the lab:

- Introduction.
- Hands-On Steps.

- *Note:* the Hands-On Steps provide a starting point for your research, but the requirements of this assignment are defined below.

Next, complete the following research:

- Conduct your own independent research online and in the Capella library to find information on the Napster music piracy case.
- Always record the citations for your resources, including the URLs for online materials. You will provide them in reference lists for your assignments.

Requirements

For this assignment, address the following:

- Summarize the Digital Millennium Copyright Act and its provisions.
- Explain how the Digital Millennium Copyright Act relates to the Napster music piracy case.
- Explain why Napster was not able to use the defense of the Digital Millennium Copyright Act.
- Analyze the implications of violating copyright and the Digital Millennium Copyright Act from a legal, ethical, and information systems security perspective.

Use a minimum of two professional resources to support your statements in this assignment. Be sure to cite your sources correctly, following APA guidelines.

Additional Requirements

- **Formatting guidelines:** Include a title page and references page.
- **Length:** 2–4 pages, not including the title page and references page.
- **Number of resources:** Use at least 2 scholarly and/or professional sources.
- **Reference format:** Use APA style and format for citations and references.
- **Font:** Times New Roman, 12-point font, double-spaced.

Refer to the assignment scoring guide to ensure you have addressed all of the evaluation criteria for this assignment.

Submit your assignment as a Word document in the assignment area.

u07d1 - Sarbanes Oxley Section 404

If you have not already done so in preparation for this discussion, choose a publicly traded company. Using one of the links provided in the Resources, research your chosen company on the U.S. Securities and Exchange

Commission's EDGAR filings database. Locate and examine the company's most recent Form 10-K report.

Use your EDGAR research, the unit resources, and your own further research to discuss the following:

- Analyze the Sarbanes Oxley Act.
  - Why was it initiated?
  - What types of corporations does it apply to?
- Describe the Form 10-K report of the company you researched.
  - What does this report tell us?
- What have you learned about the company you selected?

Response Guidelines

After posting your discussion, respond to the initial posts of at least two of your peers. How does the information they provided differ from yours? Is the information similar? In what ways?

Course Resources
Graduate Discussion Participation Scoring Guide
EDGAR Company Filings
Latest Filings Received and Processed at the SEC

u07d1 - Learning Components

- Explain intellectual property laws and the effect they have on a corporation.
- Explain the differences between public and private information security and privacy regulations.
- Apply graduate-level skill in research, critical thinking, and writing.

Unit 8 >> Security and Privacy of Health Information

Introduction

The Health Information Technology for Economic and Clinical Health Act, or HITECH Act, is a component of the American Recovery and Reinvestment Act of 2009 (ARRA). Included in the HITECH Act is language that strengthens the security and privacy language first implemented with the original HIPAA regulations. Unit 8 will explore the details of the HITECH Act that are important for the information security professional to understand.

Learning Activities

u08s1 - Studies

Required Reading

The following reading covers topics pertaining to the security and privacy of health information and will be useful in completing the discussion in this unit:

- Grama, J. L. (2015). *Legal issues in information security* (2nd ed.). Burlington, MA: Jones & Bartlett.
  - Chapter 6, "Security and Privacy of Health Information," pages 148–187.

Suggested Resources

The following resources address the unit topic and may be useful in your course assignments and discussions:

- Clearwater Compliance. (2013, January 17). *How the HITECH Act raised the ante for HIPAA compliance* [Video]. Retrieved from https://www.youtube.com/watch?v=cJrmqsppklg
  - *Note:* Closed captioning is provided at the link.
- Federal Trade Commission. (n.d.). Gramm-Leach-Bliley Act. Retrieved from https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act
- Lord, N. (2018, September 19). What is GLBA compliance? Understanding the data protection requirements of the Gramm-Leach-Bliley Act. Retrieved from https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act
- U.S. Department of Health & Human Services. (n.d.). HITECH Act enforcement interim final rule. Retrieved from https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html

u08s1 - Learning Components

- Explain business challenges facing the health care industry.
- Analyze the HIPAA and HITECH acts.
- Explain the role of state laws in protecting the confidentiality of medical records.
- Identify the benefits and challenges of implementing the information security aspects of HIPAA and HITECH within the health care sector.

u08a1 - Security and Privacy of Health Information

Preparation

This assignment requires you to complete Lab 4 in your *Laboratory Manual to Accompany Legal Issues in Information Security* lab manual. In a face-to-face courseroom, you might write your assignment in a paper-based copy of this lab manual and tear it out to give to your instructor. However, in this online course, you will only use the lab as a starting point. Do not create the files as indicated in the lab. Instead, read the lab information or case study, then complete the assignment as outlined below, using a Word document for your assignment submission.

Instructions

In your lab manual, complete the following:

- Grama, J. L. (2015). *Laboratory manual to accompany Legal Issues in Information Security, Version 2.0* (2nd ed.). Burlington, MA: Jones & Bartlett.
    - Lab 4, "Analyzing and Comparing GLBA and HIPAA," page 27.

Complete the following sections of the lab:

- Introduction.
- Hands-On Steps.
    - *Note:* the Hands-On Steps provide a starting point for your research, but the requirements of this assignment are defined below.

Next, complete the following research:

- Conduct your own independent research online and in the Capella library to find information on GLBA and HIPAA.
- Always record the citations for your resources, including the URLs for online materials. You will provide them in reference lists for your assignments.

Requirements

For this assignment, address the following:

- Analyze the differences and similarities between GLBA and HIPAA.
    - What agency is responsible for enforcing each act?
    - Who do they protect?
    - Who must comply?
    - What are the major components of each act?
- Explain how GLBA and HIPAA requirements align with information systems security.
- Explain the privacy data elements for both GLBA and HIPAA.
- Describe the specific security controls and security countermeasures that support GLBA and HIPAA compliance.

Use a minimum of three professional resources to support your statements in this assignment. Be sure to cite your sources correctly, following APA guidelines.

Additional Requirements

- **Formatting guidelines:** Include a title page and references page.
- **Length:** 2–4 pages, not including the title page and references page.
- **Number of resources:** Use at least 3 scholarly and/or professional sources.
- **Reference format:** Use APA style and format for citations and references.
- **Font:** Times New Roman, 12-point font, double-spaced.

Refer to the assignment scoring guide to ensure you have addressed all of the evaluation criteria for this assignment.

Submit your assignment as a Word document in the assignment area.

u08d1 - HITECH Act Technology and Controls

The HITECH Act requires providers applying for financial incentives for meaningful use to engage in a number of very specific data collection, storage, and exchange activities. A large percentage of health care providers that might qualify for these financial incentives are small practices—essentially, small businesses. These small businesses rarely have the resources available to purchase and maintain the technology necessary to qualify for these incentives. As a result, the providers have chosen a variety of solutions, including partnering with large health systems that might provide the services as part of the partnership, or choosing to outsource the work to a third party.

For this discussion, use the following scenario:

Dr. Taylor has been providing health care for his neighbors since the 1960s. Over the years, he has shared a clinic space with several other independent physicians, sharing expenses, support staff, and on-call responsibilities. Dr. Taylor and his partners have decided that they do not want to follow the path of many of their peers by joining forces with a large health insurance company. At a partners' meeting, Dr. Taylor was tasked with finding a cloud provider to help the partners implement an appropriate electronic health record (HER). The HER would need to meet all criteria, including security and privacy regulations, that would qualify these health providers for meaningful use financial incentives.

Use the unit resources and your own research to discuss the following:

- Explain the steps necessary to select an appropriate cloud provider that will provide access to an HER and host data storage for a small provider practice.
- Discuss the security and privacy controls that the selected cloud provider must be able to implement to comply with the HITECH Act criteria.

- Explain the roles and responsibilities of the cloud provider and the health care providers in ensuring that the HITECH Act security and privacy regulations are met.

Response Guidelines

After posting your discussion, respond to the initial posts of at least two of your peers. Have you and your peers included the same information, or is there information you provided that they missed?

Course Resources
Graduate Discussion Participation Scoring Guide

u08d1 - Learning Components

- Explain business challenges facing the health care industry.
- Explain the role of state laws in protecting the confidentiality of medical records.
- Identify the benefits and challenges of implementing the information security aspects of HIPAA and HITECH within the health care sector.

Unit 9 >> Information Security Governance Introduction

Introduction

Previous units have looked at the federal, state, and local regulations that affect information security. In this unit, the focus will shift to the private side of information security standards and policies. A number of common information security models and standards organizations are increasingly creating common practice guidelines for information security professionals.

Learning Activities

u09s1 - Studies

Required Readings

The following reading covers topics pertaining to information security and will be useful in completing the discussion in this unit.

- Grama, J. L. (2015). *Legal issues in information security* (2nd ed.). Burlington, MA: Jones & Bartlett.
  - Chapter 13, “Information Security Governance,” pages 390–425.
  - Chapter 14, “Risk Analysis, Incident Response, and Contingency Planning,” pages 426–460.

Suggested Resources

The following resources address the unit topic and may be useful in your course assignments and discussions.

- Christidis, A. (2018, January 2). How to mitigate the risks of cyber security through contingency planning. Retrieved from http://metin-mitchell.com/how-to-mitigate-the-risks-of-cyber-security-through-contingency-planning
- Diligent Corporation. (2016). Five best practices for information security governance [PDF]. Available from http://diligent.com
- Shiang, L. (2018, May 3). Advice for new CISOs: How to get a head start on information security governance. Retrieved from https://deltarisk.com/blog/advice-for-new-cisos-how-to-get-a-head-start-on-information-security-governance
- Tuttle, H. (2018, February 1). 2018 cyberrisk landscape. Retrieved from http://www.rmmagazine.com/2018/02/01/2018-cyberrisk-landscape
- Voigt, L. (2018, July 13). 5 best practices for your incident response plan [Blog]. Retrieved from https://www.exabeam.com/incident-response/improve-your-2018-incident-response-plan-with-the-latest-best-practices

u09s1 - Learning Components

- Identify cybersecurity standards and policies that are commonly enforced within private sector organizations.
- Explain the objectives and challenges of cybersecurity standards and policies that are commonly enforced within private sector organizations.
- Define the scope of cybersecurity standards and policies that are commonly enforced within private sector organizations.

u09a1 - IT Security Policies to Help Mitigate Risk

Preparation

This assignment requires you to complete Lab 9 in your *Laboratory Manual to Accompany Legal Issues in Information Security* lab manual. In a face-to-face courseroom, you might write your assignment in a paper-based copy of this lab manual and tear it out to give to your instructor. However, in this online course, you will only use the lab as a starting point. Do not create the files as indicated in the lab. Instead, read the lab information or case study, then complete the assignment as outlined below, using a Word document for your assignment submission.

Instructions

In your lab manual, complete the following:

- Grama, J. L. (2015). *Laboratory manual to accompany Legal Issues in Information Security, Version 2.0* (2nd ed.). Burlington, MA: Jones & Bartlett.
    - Lab 9, "Recommending IT Security Policies to Help Mitigate Risk," page 63.

Complete the following sections of the lab:

- Introduction.
- Hands-On Steps.
    - *Note:* the Hands-On Steps provide a starting point for your research, but the requirements of this assignment are defined below.

Next, complete the following research:

- Conduct your own independent research online and in the Capella library to find information on FERPA.
- Always record the citations for your resources, including the URLs for online materials. You will provide them in reference lists for your assignments.

Requirements

For this assignment, address the following:

- Based on the case study in the lab, create an IT asset list for the school.
    - Create a table like the one on pages 66–67 of the lab manual.
    - List at least 10 assets typically found in a school.
        - Rank the importance of each asset.
        - Identify which of the seven domains each asset resides in.
        - Prioritize each asset as critical, major, or minor.
    - Determine where student data resides and assess the security controls protecting that data.
- Describe the top five risk exposures found in your IT asset assessment.
- Recommend IT security policies that can help mitigate the risk exposures.

Use a minimum of three professional resources to support your statements in this assignment. Be sure to cite your sources correctly, following APA guidelines.

Additional Requirements

- **Formatting guidelines:** Include a title page and references page.
- **Length:** 2–4 pages, not including the title page and references page.
- **Number of resources:** Use at least 3 scholarly and/or professional sources.
- **Reference format:** Use APA style and format for citations and references.
- **Font:** Times New Roman, 12-point font, double-spaced.

Refer to the assignment scoring guide to ensure you have addressed all of the evaluation criteria for this assignment.

Submit your assignment as a Word document in the assignment area.

u09d1 - Infosec Policies and Standards in the Private Sector

Application of information security standards and policies can be better defined in industries and organizations that must comply with specific regulations. As more industries become regulated, and as the regulations themselves become more standardized into common practice, this puts pressure on nonregulated industries to conform their practices too. Legal theory in the United States is heavily tilted towards establishing what is “reasonable,” making the practice of all organizations best aligned in common practice where possible.

Use the unit resources and your own research to discuss the following:

- Describe the relationship between information security standards organizations and the creation of internal information security policy within private sector organizations.
- Explain how the adoption of standards and the creation of policies must be accepted within the context of the core business goals and objectives of an organization.
- Explain how information security professionals can ensure that there is adequate consideration and approval for diverging from common practice in situations where that is necessary.

Response Guidelines

After posting your discussion, respond to the initial posts of at least two of your peers. Ask questions and offer feedback on their coverage of the discussion topic.

Course Resources
Graduate Discussion Participation Scoring Guide

u09d1 - Learning Components

- Identify cybersecurity standards and policies that are commonly enforced within private sector organizations.
- Explain the objectives and challenges of cybersecurity standards and policies that are commonly enforced within private sector organizations.
- Define the scope of cybersecurity standards and policies that are commonly enforced within private sector organizations.

Introduction

Information security professionals may become involved in a variety of investigations that range from failure to comply with internal organizational policies to significant criminal activity. The effective approach to investigating criminal activities involves a thorough understanding of evidence handling and legal and regulatory frameworks. This unit will examine the interaction of information security professionals in criminal investigations, including an exploration of which legal and regulatory agency is most likely to be the primary agency handling a particular criminal investigation.

Learning Activities

u10s1 - Studies

Required Reading

The following reading covers information pertaining to computer forensics and investigations and will be useful in completing the discussion in this unit.

- Grama, J. L. (2015). *Legal issues in information security* (2nd ed.). Burlington, MA: Jones & Bartlett.
    - Chapter 15, “Computer Forensics and Investigations,” pages 461–490.

Suggested Resources

The following resources address the unit topic and may be useful in your course assignments and discussions.

- Cameron, L. M. (2018, March 1). Future of digital forensics faces six security challenges in fighting borderless cybercrime and dark web tools. Retrieved from https://publications.computer.org/security-and-privacy/2018/03/01/digital-forensics-security-challenges-cybercrime
- University of York. (2018, October 2). Can we trust digital forensic evidence? *ScienceDaily*. Retrieved from https://www.sciencedaily.com/releases/2018/10/181002113953.htm

u10s1 - Learning Components

- Explain the roles of federal, state, local, and private-sector organizations and agencies in computer forensics.
- Explain appropriate evidence handling for a cybersecurity-related investigation.
- Explain how the type of legal dispute affects the evidence used to resolve it.

u10a1 - Computer Forensics

Preparation

This assignment requires you to complete Lab 10 in your *Laboratory Manual to Accompany Legal Issues in Information Security* lab manual. In a face-to-face courseroom, you might write your assignment in a paper-based copy of this lab manual and tear it out to give to your instructor. However, in this online course, you will only use the lab as a starting point. Do not create the files as indicated in the lab. Instead, read the lab information or case study, then complete the assignment as outlined below, using a Word document for your assignment submission.

Instructions

In your lab manual, complete the following:

- Grama, J. L. (2015). *Laboratory manual to accompany Legal Issues in Information Security, Version 2.0* (2nd ed.). Burlington, MA: Jones & Bartlett.
    - Lab 10, "Case Study on Computer Forensics: Pharmaceutical Company," page 73.

Complete the following sections of the lab:

- Introduction.
- Hands-On Steps.
    - *Note:* the Hands-On Steps provide a starting point for your research, but the requirements of this assignment are defined below.

Next, complete the following research:

- Conduct your own independent research online and in the Capella library to find information on computer forensics.
- Always record the citations for your resources, including the URLs for online materials. You will provide them in reference lists for your assignments.

Requirements

For this assignment, address the following in **3–5** pages:

- Identify the steps for maintaining a chain of custody for digital evidence.
- Explain the importance of following the chain of custody when gathering evidence.
- Analyze the challenges of computer forensics investigations.
    - Identify the challenges. (Think about the complexity of where information is stored, formats, privacy issues, methods of hiding information, jurisdiction, and so on.)
    - Explain how the challenges affect computer forensics investigations.
- Explain the relationship between incident response and computer forensics in a corporate environment.
- Recommend strategies and tools to facilitate the gathering of digital evidence.

Use a minimum of three professional resources to support your statements in this assignment. Be sure to cite your sources correctly, following APA guidelines.

Additional Requirements

- **Formatting guidelines:** Include a title page and references page.
- **Length:** 3–5 pages, not including the title page and references page.
- **Number of resources:** Use at least 3 scholarly and/or professional sources.
- **Reference format:** Use APA style and format for citations and references.
- **Font:** Times New Roman, 12-point font, double-spaced.

Refer to the assignment scoring guide to ensure you have addressed all of the evaluation criteria for this assignment.

Submit your assignment as a Word document in the assignment area.

u10d1 - Applying Information Security

Throughout this course, you have researched information security from a variety of perspectives. For this discussion, apply what you learned to the organization you work for, or to an organization you have previously worked for.

Use the course resources and your own research to discuss the following:

- Explain the cybersecurity laws that apply to the organization, based on the business location(s).
- Explain the cybersecurity laws that apply to the organization, based on the type of organization (public, private, government, nonprofit, etcetera).
- Explain the cybersecurity laws that apply to the organization, based on industry standards.
- How can the organization ensure that it is in compliance with all relevant cybersecurity laws?

Response Guidelines

After posting your discussion, respond to the initial post of at least **one** of your peers. Try to choose someone who wrote about an organization in a different industry than the one you discussed.

- How are the relevant laws different or similar?
- How do your compliance strategies compare?

Course Resources

Graduate Discussion Participation Scoring Guide

u10d1 - Learning Components

- Explain the roles of federal, state, local, and private-sector organizations and agencies in computer forensics.
- Apply graduate-level skill in research, critical thinking, and writing.