Syllabus

Course Overview

This course presents you with an opportunity to explore data communications, networking, cloud computing, and information security.

Networking technologies are at the heart of modern communications, and network infrastructures enable and support many—if not most—mission-critical business processes for organizations. The global economy exists, in large part, due to our ability to design, construct, and operate networks that scale to international size and scope. You will explore some of the core concepts related to enterprise network design, core network infrastructure hardware, configuration, and the architecture of contemporary computing networks and cloud platforms.

Cloud computing is a significant trend in the networking industry and represents both the commodification of many network-related services and a return to highly centralized computing functions similar to the mainframe computing days of the past. You explore information technologies that have enabled the development of cloud computing, the nature of cloud services, and the features of fundamental cloud architectures.

Information security involves efforts to protect the confidentiality, integrity, and availability of data. Given the realities of the world today, effective information security is vital to protecting critical infrastructures such as the power grid, banking, transportation systems, military capabilities, and a myriad of other systems that are crucial to maintaining a safe and civil society. You explore important aspects of enterprise network and cloud security, including risk assessment, vulnerability analysis, and the design and deployment of effective security controls.

This course requires you to read and think about networking, cloud, and security technologies each week so that you may begin to synthesize ideas about how these three vital areas of information technology are related to each other. It also challenges you to explore and expand your knowledge and skills. Your hard work and dedication combined with the support of your classmates and instructor will enable your success.

Technology Resources

This Capella course offers labs through Jones and Bartlett Learning. These labs offer guided practice in performing tasks related to achieving course competencies and completing assessments. If you require the use of assistive technology or alternative communication methods to participate in these activities, please contact DisabilityServices@Capella.edu to request accommodations.

Augmented Reality (AR) Experiences

Throughout this course, AR experiences will be made available as a supplement to the content. These experiences are provided to facilitate an understanding of potentially complex topics, they are not a required. Experiences can be accessed through a target or code and launched through a mobile device.

Course Competencies

(Read Only)

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

1. Apply core concepts, technologies, components, and issues related to communications and data networks.
2. Analyze common enterprise security threats and associated risk factors.
3. Evaluate core network infrastructure components and cloud-based solutions.

4 Describe security controls that mitigate common threats to enterprise network infrastructure.

5 Explain how enterprise network security controls serve to meet specific organizational or regulatory requirements.

6 Communicate effectively and professionally.

Course Prerequisites

Prerequisite(s): Completion of or concurrent registration in ITEC5002.

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

Capella University (Ed.). (2019). *ITEC5010: Security and enterprise networks* [Custom online lab bundle]. Burlington, MA: Jones & Bartlett. ISBN: 9781284375091.

Erl, T., Puttini, R., Mahmood, Z. (2013). *Cloud computing: Concepts, technology & architecture.* Upper Saddle River, NJ: Prentice Hall. ISBN: 9780133387520.

White, C. (2016). *Data communications and computer networks: A business user's approach* (8th ed.). Boston, MA: Cengage. ISBN: 9781305116634.

Library

The following required readings are provided in the Capella University Library or linked directly in this course. To find specific readings by journal or book title, use Journal and Book Locator. Refer to the Journal and Book Locator library guide to learn how to use this tool.

- Abubakar, G. B., Murray, D., & Armarego, J. (2017). A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. *Information and Computer Security, 25*(4), 475–492
- Agrafiotis, I. (2015). Identifying attack patterns for insider threat detection. *Computer Fraud & Security, 2015*(7), 9–17.
- Alotaibi, A. M., Alrashidi, B. F., Naz, S., & Parveen, Z. (2017). Security issues in protocols of TCP/IP model at layers level. *International Journal of Computer Networks and Communications Security, 5*(5), 96–104.

- Clapper, D., & Richmond, W. (2016). Small business compliance with PCI DSS. *Journal of Management Information and Decision Sciences, 19*(1), 54–67.
- Krombholz, K. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications,* 113–122.
- Palumbo, T. (2015). Patch management: The importance of implementing central patch management and our experiences doing so. *SIGUCCS '15 Proceedings of the 2015 ACM Annual Conference on SIGUCCS*, 105–108. doi:10.1145/2815546.2815561
- Paul, P. K., Kumar, K., & Senthamarai, R. (2015). Cloud based storage systems: An automated virtualization systems for intelligent world- A short communication. *Journal on Advances in Computing and Management, 6*(2), 7–11.
- Rechtman, Y., & Rashbaum, K. (2015). HIPAA security rule - demystified. *The CPA Journal, 85*(4), 68–70.
- Shaikh, S. A., & Kalutarage, H. K. (2016). Effective network security monitoring: From attribution to target-centric monitoring. *Telecommunication Systems, 62*(1), 167–178. doi:10.1007/s11235-015-0071-0
- Singh, G., Goyal, S., & Agarwal, R. (2015). Intrusion detection using network monitoring tools. *IUP Journal of Computer Sciences, 9*(4), 46–58.
- Thornycroft, P. (2016, March 21). Wi-Fi access for the internet of things can be complicated. *Network World (Online)*.
- Underwood, J. (2017). You say 'records,' and I say 'data': FERPA, the most widely used federal education law, has not kept pace with changing times. *Phi Delta Kappan, 98*(8), 74–75.
- Wall, J. D., Lowry, P. B., & Barlow, J. B. (2016). Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems, 17*(1), 39–76.
- Yimam, D. (2016). A survey of compliance issues in cloud computing. *Journal of Internet Services and Applications*, *7*(5), 1–12.
- Yu, J. T. (2016). Supporting hands-on networking lab exercise for on-line students. *Proceedings of the International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE)*, 48–53.

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.

- Capella University. (n.d.). AR & how to ... [Video]. Retrieved from https://cdnapisec.kaltura.com/index.php/extwidget/preview/partner_id/956951/uiconf_id/43830551/entry_id/1_x3frw2u8/embed/dynamic
- Microsoft. (n.d.). Create a network diagram. Retrieved from https://support.office.com/en-us/article/video-create-a-network-diagram-a2360cd9-5c9d-4839-b4f6-17b485e02262
- Smartsheet. (n.d.). What you need to succeed in the RFQ process. Retrieved from https://www.smartsheet.com/rfq-process
- Zappar. (n.d.). Retrieved from https://itunes.apple.com/gb/app/zappar/id429885268
- Zappar. (n.d.). Retrieved from https://play.google.com/store/apps/details?id=com.zappar.Zappar

Suggested

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.

Library

The following optional readings may be available in the Capella University Library. To find specific readings by journal or book title, use Journal and Book Locator. Refer to the Journal and Book Locator library guide to learn how to use this tool. If the full text is not available, you may be able to request a copy through the Interlibrary Loan service.

- Welton, T. (2016). Getting started with Visio 2016 [Video]. Skillsoft.

Unit 1 >> Introduction to Enterprise Networking and Cloud Computing

Introduction

In this unit, you will:

- Discuss network diagramming.
- Create a diagram mapping theTCP/IP to the OSI Reference Model.

Many primary functions of enterprise networking are driven by relatively mature technology, but more recent innovations have enabled the emergence of cloud computing. This week you explore the nature of cloud computing and the benefits and challenges associated with the trend of moving computing functions off premises and into the cloud. You will consider many of the foundational concepts, technologies (particularly the OSI Reference Model), and issues related to communications and data networks.

The OSI Reference Model was invented to move the computer networking industry away from proprietary systems towards open systems that supported vendor interoperability. The OSI Reference Model is only a conceptual framework that explains how data can be delivered from computer to computer across a network by traversing seven layers of functionality; the OSI Reference Model is not an actual working protocol stack.

TCP/IP is an actual working protocol stack; in fact it is a suite of protocols that are the de facto standard for almost all data communications today. The TCP/IP protocols define how data actually traverses almost all data communication networks, including the Internet.

Learning Activities

u01s1 - Studies

Readings

Read the following in your *Cloud Computing: Concepts, Technology & Architecture** text:

- Chapter 3, "Understanding Cloud Computing," pages 25–50.

Read the following in your *Data Communications and Computer Networks: A Business User's Approach* text:

- Chapter 1, "Introduction to Computer Networks and Data Communications," pages 1–26.
- Chapter 2, "Fundamentals of Data and Signals," pages 27–59.

Read the following in the Capella Library:

- Alotaibi, A. M., Alrashidi, B. F., Naz, S., & Parveen, Z. (2017). Security issues in protocols of TCP/IP model at layers level. *International Journal of Computer Networks and Communications Security, 5*(5), 96–104.
  - This paper gives an overview of the security issues in the Transmission Control Protocol (TCP)/Internet Protocol (IP) model, specifically the protocol of each layer.

Optional – Microsoft Tutorials

This course give you the option to complete assignments using MS Visio. Capella University supplies optional tutorials for these software products. Go to the Microsoft Office Software page to access these resources.

*** The *Cloud Computing: Concepts, Technology & Architecture* text was written in 2013, but is a seminal work that is relevant, current, and represents a top resource for cloud computing fundamentals.

u01s2 - Augmented Reality (AR) Experiences

Throughout this course, optional AR experiences will be made available as a supplement to the content. These experiences are provided to facilitate an understanding of potentially complex topics, they are not a required. Experiences can be accessed through a target or code and launched through a mobile device.

Click AR & How To... [Video] for an explanation of what Augmented Reality (AR) is and how to launch the experiences throughout the course.

To experience the AR activities in this course, download the Zappar app for iTunes or the Zappar app for Android.

u01s3 - Software Preparation and Technology Access

In this course, you will be using software and technology that is needed to complete designated activities and assignments. There is no additional cost for this software and technology. Some software packages will be made available to you at no additional cost through Capella's subscription with Microsoft, while other software packages are available for free download through open-source licensing.

Capella University requires learners to meet certain minimum computer requirements. Please note that some software required for a course may exceed these minimum requirements. Check the requirements for the software you may need to download and install to make sure it will work on your device. Most software will require a Windows PC. If you use a Mac, refer to Installing a Virtual Windows Environment.

The software and technologies below are strongly recommended to support you in completing the course objectives. If you have access to other tools that you believe may still meet course requirements or if you have any difficulties accessing this resource or completing the related assignments, please contact your course faculty member to discuss potential alternatives.

If you use assistive technology or any alternative communication methods to access course content, please contact DisabilityServices@Capella.edu with any access-related questions or to request accommodations.

For this course, follow the instructions provided through the links below to download and install software or register for an account, as required.

Microsoft Software

1. Log into Capella's Microsoft Office Software page for instructions on obtaining free Microsoft software.
2. Identify the version of MS Visio that is compatible with your operating system.
3. Download and install.

If you encounter any difficulties in the download and installation process, post a detailed question in the Ask Your Instructor section of the course. Your instructor should be able to help you or point you in the right direction for the answers you need.

Additional Online Resources

As a Capella learner, you have access to IT online resources through Capella's Skillsoft subscription, where you can find helpful materials.

u01d1 - Network Diagramming

This week, we exercise our diagramming skills. Discuss your diagramming experience and share any network diagrams that you may have created either on the job or for another course.

- Discuss its nomenclature or use of icons or other symbolism to represent various network hardware devices (for example, switches, routers, and firewalls).
- Discuss any tools, tips and tricks, or other relevant insights that may be helpful to learners less experienced in this skill.

If you do not have any experience drawing network diagrams, then please post a few examples that you find online. Be sure to properly cite the sources and explain in some depth how these may help to inform you as you work to create diagrams for this week’s assignment. You may also find Microsoft's "Create a Network Diagram" resource helpful.

Response Guidelines

Post detailed comments or questions to at least two other learners and discuss the lessons that you learned from studying their diagrams. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

The expectation within the course discussions is to respond to at least two posts by each Sunday evening. Responding over multiple days will help in stimulating a lively discussion. Start by submitting your initial post on (or before) Wednesday. If you provide responses to your peers on Thursday, Saturday, and Sunday, and your peers reciprocate with their responses, you will have more opportunity for in-depth interaction with your classmates and the instructor.

Course Resources
Graduate Discussion Participation Scoring Guide
Create a Network Diagram

u01a1 - Diagram TCP/IP to OSI Layers

Overview

In this assignment, you map the layers of the TCP/IP protocol architecture to the layers OSI Reference Model.

Preparation

Identify an appropriate graphics or diagramming tool (such as Visio) to complete the assignment diagram.

Directions

- Create a diagram that accurately maps the layers of the TCP/IP protocol architecture to the layers OSI Reference Model. Make sure to make the diagram clear and use common conventions for symbols and design. Copy and paste the diagram into a Word document.
- Describe the encapsulation process starting from the application layer down to the physical layer of the OSI Reference Model.

Submission Requirements

- Submit a single Word document.

- Font: Times New Roman, 12 point.
- Format: Double spaced lines. Use current APA style and format.

Course Resources

APA Style and Format

Unit 2 >> Fundamental Concepts and Protocols

Introduction

In this unit, you will:

- Discuss the TCP/IP suite.
- Draw a diagram of a typical data transmission path between an e-mail client and a cloud-based e-mail server.
- Explain the OSI functions and associated security issues.

This week, we turn our attention to the Internet, particularly the major networking protocols of the TCP/IP Protocol Suite that enable the transfer of digital data between networks. You will have the opportunity to read and review the Internet Engineering Task Force (IETF) Request for Comments (RFC). Additionally, you will explore some of the basic models of cloud computing including software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

Learning Activities

u02s1 - Studies

Readings

Read the following in your *Cloud Computing: Concepts, Technology & Architecture* text:

- Chapter 4, "Fundamental Concepts and Models," pages 51–78.

Read the following in your *Data Communications and Computer Networks: A Business User's Approach* text:

- Chapter 10, "The Internet," pages 269–304.

Read the following in the Capella Library:

- Thornycroft, P. (2016, March 21). Wi-Fi access for the internet of things can be complicated. *Network World (Online)*.
    - This article explores five ways to prepare WLANs for Internet of Things (IoT) security threats.

Multimedia

- View the IP Addressing animation on public versus private IP addressing.

Optional Video

- Welton, T. (2016). Getting started with Visio 2016 [Video]. Skillsoft.
- Microsoft. (n.d.). Create a network diagram. Retrieved from https://support.office.com/en-us/article/video-create-a-network-diagram-a2360cd9-5c9d-4839-b4f6-17b485e02262

Optional AR

This AR experience will allow you to build out a typical email data transmission path. Launch the experience with the shown target. From the menu, choose the required components for the transmission path. Once the correct components have been selected, drag to arrange the components to complete the path.

Course Resources

Unit 2 Zappar image

u02d1 - TCP/IP Protocol Suite

The job of the Internet Engineering Task Force (IETF) is to make the Internet work, and the IETF achieves that primarily by writing technical standards for network protocols. The TCP/IP Protocol Suite is a collection of protocols that ultimately enable us to share data across the Internet and other networks.

Search the Internet for information on one of the following IETF Request for Comments (try to pick one that has yet to be discussed on the message boards):

- IETF RFC 791 Internet Protocol.
- IETF RFC 792 Internet Control Message Protocol.
- IETF RFC 793 Transmission Control Protocol.
- IETF RFC 959 File Transfer Protocol.
- IETF RFC 854 Telnet.
- IETF RFC 1058 Routing Information Protocol.
- IETF RFC 1059 Network Time Protocol.
- IETF RFC 1350 Trivial File Transfer Protocol.
- IETF RFC 1939 Post Office Protocol.
- IETF RFC 2409 Internet Key Exchange.
- IETF RFC 2570 Simple Network Management Protocol.
- IETF RFC 3261 Session Initiation Protocol.
- IETF RFC 4251 Secure Shell.
- IETF RFC 4880 Pretty Good Privacy.
- IETF RFC 4291 IPv6 Addressing.

Discuss the primary function that makes the protocol unique from others. Describe the salient characteristics of the protocol including its relationship to the OSI Reference Model and discuss any security mechanisms that the protocol may have built into it. Write your own review of the prominent features of the protocol; do not include material directly copied from the associated IETF Request for Comments.

Response Guidelines

Post detailed comments or questions to at least two other learners and explain how their insights helped to inform your understanding of the specific protocol that they analyzed.

Course Resources

Graduate Discussion Participation Scoring Guide

u02a1 - TCP/IP and OSI Reference Model

Overview

While the OSI Reference Model provides us with a conceptual framework for talking about how networks function, it is the TCP/IP protocols that are essential for actually enabling modern networking and data communications.

Imagine that you are relaxing at your favorite local coffee shop enjoying a delicious beverage. You turn on your laptop or smartphone, connect to the shop's wireless local area network (WLAN), and use the Internet to access your cloud-based e-mail (for example Gmail). What protocols make it all work?

In this assignment, you explain and illustrate concepts and functioning of some TCP/IP protocol functions and interactions related to the use of cloud-based e-mail from a client connected to a WLAN.

Directions

Part 1 – E-mail client and Cloud-based E-mail Path Diagram

Draw a diagram of a typical data transmission path between an e-mail client and a cloud-based e-mail server depicting the following components involved in the data transmission.

- Physical media.
- Wireless access point.
- Local and remote switches and routers.
- Firewalls.
- ISPs and the Internet Cloud service provider.

Make sure to do the following:

- Create a network diagram that accurately depicts cloud-based e-mail server to remote client transmission.

Part 2 – The OSI Layer and Security

Write a detailed narrative explanation of the primary function of each OSI layer and describe its part in facilitating a typical data transmission from a cloud-based e-mail server to a remote client computer. After that, describe three or four security issues inherent to the TCP/IP protocol suite.

Make sure to do the following:

- Explain the primary function of each layer of the OSI model and its related TCP/IP protocols.
- Describe the OSI layers' part in facilitating a typical data transmission from a cloud-based e-mail server to a remote client computer.
- Describe security problems inherent to the TCP/IP protocol suite.
- Frame your explanations using vocabulary and frameworks that are appropriate for technical stakeholders.

Submission Requirements

- Submit a single Word document with both parts of this assignment.
- Font: Times New Roman, 12 point.
- Format: Double spaced lines. Use current APA style and format.

Unit 3 >> Local Area Networks and Cloud-Enabling Technologies

Introduction

In this unit, you will:

- Discuss virtualization technology.
- Explain how cloud-enabling technologies interact.

This week, we continue our study of core network technologies by exploring local area networks (LANs) which provide network connectivity to end-users. Meanwhile, our cloud studies will take us through the major cloud-enabling technologies such as the broadband networks and the Internet, the World Wide Web, data centers, virtualization, and multitenancy, which are prerequisites for creating cloud computing solutions.

Learning Activities

u03s1 - Studies

Readings

Read the following in your *Cloud Computing: Concepts, Technology & Architecture* text:

- Chapter 5, "Cloud-Enabling Technology," pages 79–116.
- Appendix B, "Industry Standards Organizations," pages 427–432.

Read the following in your *Data Communications and Computer Networks: A Business User's Approach* text:

- Chapter 7, "Local Area Networks Part I," pages 175–206.

Read the following in the Capella Library:

- Paul, P. K., Kumar, K., & Senthamarai, R. (2015). Cloud based storage systems: An automated virtualization systems for intelligent world- A short communication. *Journal on Advances in Computing and Management, 6*(2), 7–11.
  - This article explains the role of cloud computing in providing central remote servers to maintain application data storage.

u03d1 - Virtualization Technology

Virtualization technology is fundamental in enabling the development and operation of cloud computing services. Virtualization technology has evolved quickly; these days, we are not only virtualizing desktops and servers but also networks and even entire data centers.

Discuss the relative advantages and disadvantages of virtualization, particularly as it relates to enterprise networking and cloud computing. Ideally, you will speak from your own professional experience. If you do not have any professional experience related to virtualization technology, then please base your discussion on your own research and be sure to include citations.

Response Guidelines

Post detailed comments or questions to at least two other learners and explain how their insights helped to inform your understanding of the benefits and risks of virtualization.

Course Resources

Graduate Discussion Participation Scoring Guide

u03a1 - Cloud-Enabling Technologies

Overview

It is often necessary for information technologists to evaluate new and emerging technologies and to assess the potential impacts on an enterprise's current information technology (IT) operations and future IT project planning.

In this assignment, you write about the interaction of cloud-enabling technologies.

Directions

Pick two of the following cloud-enabling technologies that directly interact with one another:

- Broadband network technology.
- Data center technology.
- Internet technology.
- Virtualization technology.
- World Wide Web (WWW) technology.
- Multitenant technology.
- Service technology.

Write 3–4 pages explaining how your chosen cloud-enabling technologies function. Explain how they interact with one another to create a cloud consumer network, a cloud provider network, an enterprise internet connection, or another cloud component.

Make sure to do the following:

- Describe the primary functions of cloud-enabling technologies.
- Explain how cloud-enabling technologies interact to create a cloud component.

Submission Requirements

- Submit a single 3–4 page Word document with both parts of this assignment.
- Font: Times New Roman, 12 point.
- Format: Double spaced lines. Use current APA style and format.

Course Resources

APA Style and Format

Unit 4 >> Local Area Networks and Cloud Infrastructure Mechanisms

Introduction

In this unit, you will:

- Discuss network diagramming.

- Create diagrams that depict various parts of a coffee retailer's cloud-managed network.

This week, we will begin to shift the focus of our studies to some core network infrastructure components and cloud infrastructure mechanisms such as virtual servers, cloud storage devices, and cloud usage monitors. Also, we will wrap-up our work on local area networks (LANs) that we began last week. You will have the opportunity to apply the concepts that you are learning as you work to create a series of network diagrams that demonstrate the relationship between network and cloud infrastructure components.

Learning Activities

u04s1 - Studies

Reading

Read the following in your *Cloud Computing: Concepts, Technology & Architecture* text:

- Chapter 7, "Cloud Infrastructure Mechanism," pages 139–168.

Read the following in your *Data Communications and Computer Networks: A Business User's Approach* text:

- Chapter 8, "Local Area Networks Part II," pages 207–240.
- Chapter 9, "Introduction to MANs and WANs," pages 241–268.

Read the following in the Capella Library:

- Yu, J. T. (2016). Supporting hands-on networking lab exercise for on-line students. *Proceedings of the International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE)*, 48–53.
    - This paper provides a pedagogical overview of the importance of hands-on lab exercises in information technology education, and explicitly explains the distinction between a physical network diagram and a logical network diagram.

Optional AR

This AR experience is designed to practice your ability to produce network diagrams with professional quality production values. Use the AR to identify then build the correct components and sequence of a network diagram. Launch the experience with the shown target. From the menu, choose the required components for a network diagram. Once the correct components have been selected, drag to arrange the components to complete the diagram.

Course Resources

Unit 4 Zappar image

u04d1 - Network Diagramming

One of our learning challenges this week is to grow in our ability to produce network diagrams with professional quality production values. Please carefully review the Network Diagram Examples [PDF] document that contains six examples of flawed network diagrams which represent a range of aesthetic and technical approaches to creating network diagrams.

Discuss your ideas about at least three of the example diagrams, and explain your rationale for features that you do and do not like.

Finally, include a reflection on your own diagramming skills or experience, and express your intentions for how you will seek to improve your skills during your Unit 4 learning experience.

Response Guidelines

Read the posts of your peers and respond to two (minimum) and expand on the concepts covered in their initial post. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources
Graduate Discussion Participation Scoring Guide
Network Diagram Examples [PDF]

u04a1 - WAN and LAN Diagrams

Overview

Information technologists, particularly network administrations, routinely document networks by creating diagrams. A good network diagram may represent the primary features and design of a particular network's logical and physical configuration.

In this assignment, you create three diagrams that depict various parts of a coffee retailer's cloud-managed network. Your diagrams should depict how the coffee shop retailer might effectively configure its LANs, WLAN, and WAN.

Preparation

- Read the Coffee Retailer Description document located in the resources.

Directions

Complete the following two parts of the assignment:

Part 1 – Network Diagrams

Draw diagrams that reasonably depict a network infrastructure that will enable Coffee Retailer to achieve the company's strategic goal of offering customers public wireless Internet access. Make sure to list any assumptions regarding the company or your design that you need to make in order to design and draw a realistic diagram.

Make sure to do the following:

1. Create a logical wide area network (WAN) diagram showing major enterprise locations including the corporate headquarters, one typical retail location, and a cloud service provider.
2. Create a physical WAN diagram that places core and distribution-layer routers and switches in locations that optimize network performance. Justify your choices.
3. Create a physical local area network (LAN) and wireless LAN (WLAN) diagram for a typical retail location.
4. Evaluate how well **one** of your diagram depicts a working cloud-based solution for Coffee Retailer. What are the most important criteria?

Submission Requirements

- Submit a single Word document with both parts of this assignment.
- Font: Times New Roman, 12 point.
- Format: Double spaced lines. Use current APA style and format.

Course Resources

Coffee Retailer Description [DOCX]

APA Style and Format

Unit 5 >> Wide Area Networks and Service Quality Metrics

Introduction

In this unit, you will:

- Discuss cloud computing services.
- Write a cloud services Request for Quotation (RFQ).

This week, we continue to explore core network infrastructure components and begin to think about service quality metrics including availability, capacity, and scalability. Given that most organizations will purchase rather than host cloud computing services, this week’s assignment is very practical; you will be writing a request for quotation for a cloud-based data storage service. We will also be discussing opportunities to deploy cloud computing services such as software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), or anything as a service (XaaS) within the context of a particular organization.

Learning Activities

u05s1 - Studies

Readings

Read the following in your *Cloud Computing: Concepts, Technology & Architecture* text:

- Chapter 16, "Service Quality Metrics and SLAs," pages 403–420.
- Appendix F, "Cloud Provisioning Contracts," pages 449–460.

Read the following RFQ resource on the Internet:

- Smartsheet. (n.d.). What you need to succeed in the RFQ process. Retrieved from https://www.smartsheet.com/rfq-process
    - This article provides information about how to create an effective request for quotation (RFQ).

u05d1 - Cloud Computing Services

Cloud computing is fundamentally about the delivery of computing services, platforms, and infrastructures using the Internet rather than designing, building, and operating and maintaining enterprise information systems on premises.

Discuss how an employer could use cloud computing services. Frame your discussion in terms of software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), or anything as a service (XaaS). Be sure to explicitly discuss which of an organization’s business processes are supported by a cloud deployment, such as how the cloud deployment serves the organization’s strategic business goals.

Finally, please explore the availability, reliability, and performance metrics that you think need to be measured to ensure that an organization is properly managing its cloud deployment.

Response Guidelines

Post detailed comments or questions to at least two other learners and explain how their insights helped to inform your understanding of the potential for the strategic deployment of cloud computing services for an organization.

Course Resources

Graduate Discussion Participation Scoring Guide

u05a1 - Cloud Services: Request for Quotation (RFQ)

Overview

According to CIO magazine, "cloud services now account for a third of the IT outsourcing market" (Overby, 2016). As more and more organizations choose to buy cloud services such as SaaS, PaaS, and IaaS, many information technologists find themselves needing to prepare formal RFQs to begin the process of engaging a cloud provider.

In this assignment, you create a detailed RFQ for cloud-based data storage services for the Coffee Retailer enterprise.

Preparation

- Review the Coffee Retailer Description document located in the resources as needed.

Directions

Create a detailed RFQ for cloud-based data storage services to enable daily backups of Coffee Retailer's point of sale (POS) data to mitigate the risk of catastrophic data loss. The RFQ should provide enough information so that a cloud computing company can provide an accurate quotation for basic data storage services.

You will also want to identify reasonable performance and security metrics that a system like this might require. Please state any assumptions that you need to make to flesh out your choice.

Make sure to do the following:

- Create a professional RFQ that accurately represents the information required by a vendor for a proper response.
- Create a professionally formatted RFQ appropriate for distribution to stakeholders.
- Specify reasonable performance and security metrics for data uploads and downloads.

Submission Requirements

- Font: Times New Roman, 12 point.
- Format: Double spaced lines. Use current APA style and format.

Reference

Overby, S. (2016). Cloud services now account for a third of IT outsourcing market. Retrieved from http://www.cio.com/article/3099091/cloud-computing/cloud-services-now-account-for-a-third-of-it-outsourcing-market.html

Course Resources

Coffee Retailer Description [DOCX]

APA Style and Format

Unit 6 >> Network Security and Specialized Cloud Mechanisms

Introduction

In this unit, you will:

- Discuss security breaches in the news.
- Investigate and responding to security incidents in a virtual lab.
- Analyze the risk factors associated with an incident and recommend actions to avoid future incursions.

It may seem hard to believe, but we have worked through the first half of the course already. This week, we will turn our attention to learning about common enterprise security threats and associated risk factors related to data communications and networking. We will also explore specialized cloud mechanisms including automated scalers, load balancers, service level agreement (SLA) monitors, and failover systems. You will have an opportunity to apply your skills as you work to analyze an information security incident and write a report to key stakeholders.

Learning Activities

u06s1 - Studies

Readings

Read the following in your *Cloud Computing: Concepts, Technology & Architecture* text:

- Chapter 8, "Specialized Cloud Mechanisms," pages 169–212.

Read the following in your *Data Communications and Computer Networks: A Business User's Approach* text:

- Chapter 12, "Network Security," pages 339–372.

Read the following from the Capella Library:

- Krombholz, K. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications,* 113–122.
    - This paper provides a taxonomy of well-known social engineering attacks.
- Wall, J. D., Lowry, P. B., & Barlow, J. B. (2016). Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems, 17*(1), 39–76.

Optional AR

This AR experience is designed to practice your ability to produce network diagrams with professional quality production values. This time you are to include network security and cloud mechanisms. Launch the experience, and identify and incorporate the necessary levels of security within the built network.

Course Resources

Unit 6 Zappar image

u06d1 - Security Breaches in the News

A major data breach may be one of the most serious types of security incidents, which may result in legal and regulatory sanctions as well as serious reputational damage to an organization’s brand.

Provide a brief summary of an instance where a company fell victim to a major data breach. (Please be sure to first read all the posts in this discussion to date so that you are reviewing a company whose data breach incident has not already been covered by a classmate.)

Discuss the features that characterize the data breach. Describe the salient features of the attack, when and how the breach incident was discovered, the data that was illegally accessed, and the consequences of the breach to the organization and the actions taken in its wake.

Please choose one company who was victimized by a significant data breach from the following list, or you may choose to discuss a data breach incident with which you were professionally involved:

- Adobe.
- Adult Friend Finder.
- Anthem.
- Ashley Madison.
- Ebay.
- Equifax.
- Heartland Payment Systems.
- Home Depot.
- JP Morgan Chase.
- National Security Agency (NSA).
- RSA Security.
- Sony's PlayStation Network.
- TJX Companies, Inc.
- VeriSign.
- Yahoo.
- US Office of Personnel Management (OPM).

Response Guidelines

Post detailed comments or questions to at least two other learners and discuss how the incident they reviewed compares and contrasts with the incident that you studied.

Course Resources

Graduate Discussion Participation Scoring Guide

u06v1 - Lab: Investigating and Responding to Security Incidents

Overview

This week's hands-on lab provides you with an opportunity to use malware scanning tools in a Windows environment. You will learn how to identify, isolate, and eradicate malware on an infected workstation. You will write an appropriate security incident response report to document your work.

Directions

Read the requirements for all related course activities before completing this lab so you can take notes as needed to help you complete those activities. Select the linked title heading above to access a lab arranged through Jones & Bartlett Learning.

1. Follow the lab instructions carefully. **Note:** You are only responsible for completing Sections 1 and 2 of the lab.
2. Download the Assignment Template found in the resources and use it for **both your lab screenshots and your assignment responses**.
3. Take the following screenshots during the lab:
    - Section 1:
        - Part 2, Step 7.
        - Part 3, Steps 2, 10.
    - Section 2:
        - Part 2, Step 8.
        - Part 3, Steps 2 and 9.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing JBL virtual labs, contact Jones & Bartlett Learning Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

Course Resources

Assignment Template [DOCX]

u06a1 - Security Incident Report

By now you should have completed the unit lab and saved your screenshots to a Word document for submission with this assignment.

Overview

Imagine that you are employed as a cybersecurity team member at the coffee retailer that you have been working with in previous assignments**.** You have discovered that on September 2 and 8 of last year, two data center servers located at the corporate headquarters were infected with a Trojan horse, resulting in a potential security breach that exposed the credit card data and personal information of tens of thousands of individual customers.

A detailed log analysis suggests that a server administrator, who violated policy by surfing Web sites while signed in to an administrator account, may have fallen prey to a social engineering e-mail attack and inadvertently installed the malware Trojan horse program. The incident is in clear violation of established Payment Card Industry Data Security Standard (PCI DSS), and the company may face fines for each security breach.

In this assignment you analyze the risk factors associated with this incident and recommend actions to avoid future incursions.

Preparation

- Review the Coffee Retailer Description document located in the resources as needed.

Directions

Use the Assignment Template with your screenshots for the lab documentation and the assignment.

Lab Documentation

Briefly describe what you learned from or observed in the lab and include it in the section with your screenshots in the Assignment Template. Be specific.

Assignment

Do the following:

- Analyze the security threat and the associated risk factors presented in the Overview section.
- Recommend three specific network security controls that could prevent a similar incident in the future. Support your recommendation.
- Explain how each of your three recommended network security controls serves to meet specific organizational or regulatory requirements.

Submit your Word document in this assignment.

Course Resources

Coffee Retailer Description [DOCX]

Unit 7 >> Network Design and Mobile Security

Introduction

In this unit, you will:

- Discuss issues regarding "Bringing Your Own Device (BYOD).
- Analyze protocols with Wireshark and the risk factors associated with an incident and recommend actions to avoid future incursions.

This week, we will continue to explore security threats and some related risk factors that threaten the confidentiality, integrity, and availability of networked information resources. We focus specifically on threats to operating systems (OS) security and think about ways to harden OSs deployed in enterprise environments. Additionally, we will explore mobile computing and the emerging bring your own device trend, which presents a significant information security challenge for many organizations.

Learning Activities

u07s1 - Studies

Readings

Read the following in your *Cloud Computing: Concepts, Technology & Architecture* text:

- Appendix E, "Emerging Technologies," pages 443–448.

Read the following in your *Data Communications and Computer Networks: A Business User's Approach* text:

- Chapter 13, "Network Design and Management," pages 373–400.

Read the following from the Capella Library:

- Abubakar, G. B., Murray, D., & Armarego, J. (2017). A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. *Information and Computer Security, 25*(4), 475–492.

Optional AR

This AR experience can be used as a reference to get a visual understanding of a TCP/IP 3-way handshake. Launch the AR experience to interact through the process of a client and server exchanging synchronization and acknowledgment packets.

Course Resources

Unit 7 Zappar image

u07d1 - Bring Your Own Device (BYOD)

Bring your own device (BYOD) is a trend towards allowing employee-owned mobile computing devices, especially smartphones, to access enterprise networks, systems, and data.

For this discussion, explore the relative advantages and disadvantages of BYOD, particularly as it relates to mobile device management and securing the confidentiality and integrity of proprietary enterprise data. Ideally, you will speak from your own professional experience. If you do not have any professional experience related to BYOD policies or management, then please base your discussion on your own research and be sure to include citations.

Response Guidelines

Post detailed comments or questions to at least two other learners and explain how their insights helped to inform your understanding of the benefits and risks to organizations that allow BYOD.

Course Resources

Graduate Discussion Participation Scoring Guide

u07v1 - Lab: Analyzing Protocols with Wireshark

Overview

This week's hands-on lab provides you with an opportunity to deploy a packet capture and analysis tool. You will learn how to apply filters to focus in on the traffic that may be most interesting to you. You will also learn to how to appropriately place probes in the network to optimize traffic analysis capabilities. You will perform an analysis of IP packets to assess traffic from specific host machines.

Directions

Read the requirements for all related course activities before completing this lab so you can take notes as needed to help you complete those activities. Select the linked title heading above to access a lab arranged through Jones & Bartlett Learning.

1. Follow the lab instructions carefully. **Note:** You are only responsible for completing Sections 1 and 2 of the lab.
2. Download the Assignment Template found in the Resources and use it for **both your lab screenshots and your assignment responses**.
3. Take the following screenshots during the lab:
    - Section 1:
        - Part 1, Step 15.
        - Part 2, Steps 7, 19, 36.
    - Section 2:
        - Part 1, Steps 13 and 16.
        - Part 2, Steps 16, 21, 24, 27.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing JBL virtual labs, contact Jones & Bartlett Learning Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

Course Resources

Assignment Template [DOCX]

u07a1 - Securing an Operating System

By now you should have completed the unit lab and saved your screenshots to a Word document for submission with this assignment.

Overview

Microsoft Windows products have held the largest portion of the operating system market for decades. Mobility is often crucial to the productivity of an enterprise's workforce. The shift to mobile devices has introduced a variety of operating systems into the market, and the bring your own device (BYOD) trend is creating more complexity for organizations and for those charged with securing those operating systems.

In this assignment you analyze security threats associated with BYOD devices in the workplace.

Preparation

- Research security features of a mobile OS of your choice.

Directions

Use the Assignment Template with your screenshots for the lab documentation and the assignment.

Lab Documentation

Briefly describe what you learned from or observed in the lab and include it in the section with your screenshots in the Assignment With Lab Template. Be specific.

Assignment

Analyze network security threats, risks, and solutions presented by mobile devices in BYOD workplaces.

Do the following:

- Analyze three common security threats for enterprises employing a BYOD policy.
- Explain the risk factors associated with mobile device security threats.
- Analyze how two significant features of a specific mobile OS keep their devices secure.

Submit your Word document in this assignment.

Unit 8 >> Network Media and Cloud Management

Introduction

In this unit, you will:

- Discuss third party patching tools.
- Create a scheduled backup and replicating system in a virtual lab.
- Analyze the aspects of data backup and restore and patch management.

This week, we strive to better understand network media as well as security controls that mitigate common threats to an enterprise data network infrastructure. Our hands-on lab work focuses on system backup and restore functions. We will work to understand how these capabilities serve as effective security controls to mitigate threats to the integrity of mission-critical enterprise data. We will also evaluate the importance of effective patch management for on-premises and cloud-based systems and discuss the features of some third-party patch management tools.

Learning Activities

u08s1 - Studies

Readings

Read the following in your *Cloud Computing: Concepts, Technology & Architecture* text:

- Chapter 9, "Cloud Management Mechanisms," pages 213–228.

Read the following in your *Data Communications and Computer Networks: A Business User's Approach* text:

- Chapter 3, "Conducted and Wireless Media," pages 61–100.

Read the following from the Capella Library:

- Palumbo, T. (2015). Patch management: The importance of implementing central patch management and our experiences doing so. *SIGUCCS '15 Proceedings of the 2015 ACM Annual Conference on SIGUCCS*, 105–108.
    - This paper discusses why patch management is an increasingly necessary solution in all sectors.

u08d1 - Third-Party Tools

There are myriad tools available for managing the patching of information systems. While some network and server administrators choose to use tools from their network operating system (NOS) vendor, others take a best-of-breed approach by using third-party network management applications.

Please choose from the following list or you may choose another third-party patch management tool that you use professionally:

- ANSA by Autonomic Software.
- Auditor Enterprise by Ecora Software.
- Automox by Automox.
- ConnectWise Automate by ConnectWise.
- CorrelatedVM by NetSPI.
- GFI LanGuard by GFI Software.
- Kaseya VSA by Kaseya.
- Kenna by Kenna Security.
- Lumension Patch & Remediation by Lumension.
- Patch Manager by Cloud Management Suite.
- Patch Manager Plus by ManageEngine.
- Patch Manager by SolarWinds.
- Server Manager by Ivanti.
- Shavlik by Ivanti.
- SnaPatch by SmiKar Software.
- SysAid by SysAid Technologies.
- System Management by Cisco WebEx.

Discuss one of its distinguishing features and other characteristics of the tool, including its feature set, cost, and ease of use.

Any insights that you can share based on your personal or professional experience using the tool in an enterprise environment are welcome. You must write your own review of the tools prominent features; please do not include material directly copied from the vendor's Web site or promotional materials.

Response Guidelines

Post detailed comments or questions to at least two other learners and discuss how the tool they reviewed compares and contrasts with the tool that you reviewed.

Course Resources

Graduate Discussion Participation Scoring Guide

u08v1 - Lab: Creating a Scheduled Backup and Replicating System Folders

Overview

This week's hands-on lab provides you with an opportunity to install Distributed File System (DFS) in a Microsoft Windows environment. You will learn to use DFS to replicate data from a Windows server. You will deploy a command line interface to install a data backup utility, schedule automatic backups, and verify successful replication.

Directions

Read the requirements for all related course activities before completing this lab so you can take notes as needed to help you complete those activities. Select the linked title heading above to access a lab arranged through Jones & Bartlett Learning.

1. Follow the lab instructions carefully. **Note:** You are only responsible for completing Sections 1 and 2 of the lab.
2. Download the Assignment Template found in the Resources and use it for **both your lab screenshots and your assignment responses**.
3. Take the following screenshots during the lab:
    - Section 1:
        - Part 2 Steps 8, 26, 30.
        - Part 3 Steps 18, 36.
    - Section 2:
        - Part 1 Step 9.
        - Part 3 Step 16.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing JBL virtual labs, contact Jones & Bartlett Learning Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

Course Resources
Assignment Template [DOCX]

u08a1 - System Management and Backup

By now you should have completed the unit lab and saved your screenshots to a Word document for submission with this assignment.

Overview

Information security has become a bit of a cat-and-mouse game between network and server administrators and security managers on one side, and those with an interest in exploiting and damaging the confidentiality, integrity, and availability of enterprise information assets on the other. Two of the activities that may serve as effective controls against threats to the integrity of mission-critical enterprise data include proactive patch management and automated backups stored both locally and remotely.

In this assignment you analyze aspects of patch management and data backup and restore.

Directions

Use the Assignment Template with your screenshots for the lab documentation and the assignment.

Lab Documentation

Briefly describe what you learned from or observed in the lab and include it in the section with your screenshots in the Assignment Template found in the resources. Be specific.

Assignment

Analyze aspects of data backup and restore and patch management. Do the following:

- Explain three best practices for data backup and restore to prevent data loss.
- Describe three tools that are available to network and server administrators to ensure that system patches and data backups are occurring effectively.
- Describe important things to consider when deploying system patches.

Course Resources

Assignment Template [DOCX]

Unit 9 >> Voice, Data, and Cloud Security

Introduction

In this unit, you will:

- Discuss insider security threats.
- Perform reconnaissance and probing using common tools in a virtual lab.
- Explain various monitoring tools and methods available to network administrators.

This week, we continue to explore security controls that mitigate common threats to enterprise network infrastructure by first turning our attention to how packet inspection of network traffic may serve as an effective security control to mitigate threats to the confidentiality, integrity, and availability of mission-critical enterprise data in on-premises and cloud-based enterprise network environments.

We also explore the nature of information security threats from trusted insiders, such as employees, cloud vendors, and information technology contractors, which can be particularly challenging because the attacker has legitimate credential on enterprise systems and networks.

Learning Activities

u09s1 - Studies

Readings

Read the following in your *Cloud Computing: Concepts, Technology & Architecture* text:

- Chapter 6, "Fundamental Cloud Security," pages 169–212.

Read the following in your *Data Communications and Computer Networks: A Business User's Approach* text:

- Chapter 11, "Voice and Data Delivery Networks," pages 307–338.

Read the following from the Capella Library:

- Agrafiotis, I. (2015). Identifying attack patterns for insider threat detection. *Computer Fraud & Security, 2015*(7), 9–17.
  - This paper discusses information security threats that insiders pose to businesses, institutions, and governmental organizations.

- Shaikh, S. A., & Kalutarage, H. K. (2016). Effective network security monitoring: From attribution to target-centric monitoring. *Telecommunication Systems, 62*(1), 167–178. doi:10.1007/s11235-015-0071-0
    - This paper reviews the structural, operational, and legal reasons underlying a shift away from attribution in favor of a target-centric monitoring approach.
- Singh, G., Goyal, S., & Agarwal, R. (2015). Intrusion detection using network monitoring tools. *IUP Journal of Computer Sciences, 9*(4), 46–58.
    - The paper focuses on how network monitoring tools can be helpful in the protection of communication networks and how different kinds of network attacks are performed.

u09d1 - Insider Security Threats

While threats to the confidentiality, integrity, and availability of data may originate from many types of attackers, the information security threats from trusted insiders—such as employees, vendors, and contractors—can be particularly insidious because the attackers have legitimate credentials on enterprise systems and networks. Insider threats may be difficult to detect because it can be challenging to differentiate between potentially harmful actions and an employee’s authorized work.

Share a relevant story—ideally based on your personal or professional experiences—about how a security incident originated with an attack vector that was opened, either maliciously or accidentally, by a trusted insider. Focus your discussion on the features that make this particular insider attack unique by describing the salient features of the attack, when and how the breach incident was discovered, the data that was illegally accessed, and the short- and long-term consequences of the attack to the organization.

Response Guidelines

Post detailed comments or questions to at least two other learners and discuss how the insider attack they reviewed compares and contrasts with the attack that you reviewed.

Course Resources
Graduate Discussion Participation Scoring Guide

u09v1 - Lab: Performing Reconnaissance and Probing using Common Tools

Overview

This week’s hands-on lab provides you with an opportunity to work with common network scanning tools to perform reconnaissance by probing a variety of computer systems in order to understand how attackers might use these tools to penetrate enterprise networks. You will create a chart to enable the visualization of relationships between networked devices.

Directions

Read the requirements for all related course activities before completing this lab so you can take notes as needed to help you complete those activities. Select the linked title heading above to access a lab arranged through Jones & Bartlett Learning.

1. Follow the lab instructions carefully. **Note:** You are only responsible for completing Sections 1 and 2 of the lab.

2. Download the Assignment Template found in the Resources and use it for **both your lab screenshots and your assignment responses**.
3. Take the following screenshots during the lab:
    - Section:
        - Part 1, Steps 18 and 25.
        - Part 3, Step 17.
    - Section 2
        - Part 1, Steps 8, 23, 40.
        - Part 2, Step 14.
        - Part 3, Steps 5and 7.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing JBL virtual labs, contact Jones & Bartlett Learning Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

Course Resources
Assignment Template [DOCX]

u09a1 - Network Monitoring and Security Control

By now you should have completed the unit lab and saved your screenshots to a Word document for submission with this assignment.

Overview

There are several lines of defense available to network and security administrators, including intrusion prevention and detection technologies. The activities and tools that are available to monitor and test the security levels on a modern network are varied. They range from free open source to very expensive and sophisticated technologies. They come in single-use solutions and best-of-breed solutions, which are typically suites of network management applications that perform a variety of activities.

In this assignment you explain various monitoring tools and methods available to network administrators.

Directions

Use the Assignment Template with your screenshots for the lab documentation and the assignment.

Lab Documentation

Briefly describe what you learned from or observed in the lab and include it in the section with your screenshots in the Assignment Template found in the resources. Be specific.

Assignment

Write 3–4 pages in which you consider the following aspects of network monitoring.

- Choose a common packet inspection tool and explain how it works to mitigate threats.
- Describe three criteria that a network or security administrator might use when selecting a network monitoring tool.
- Describe a security policy that is designed to ensure that an organization’s information is not compromised by internal IT staff.

Submission Requirements

- Font: Times New Roman, 12 point.
- Format: Double spaced lines. Use current APA style and format.

Course Resources

APA Style and Format

Unit 10 >> Cloud Security Controls

Introduction

In this unit, you will:

- Discuss the impact of regulatory requirements on enterprise networks.
- Recognize risks and threats associated with emerging tech in a virtual lab.
- Address security issues related to information security-related regulatory compliance.

We have made it to the last week of the course and now turn our attention to studying how enterprise network security controls serve to meet specific organizational and regulatory requirements. We will consider the information security in the light of regulatory requirements including Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and others.

Learning Activities

u10s1 - Studies

Readings

Read the following in your *Cloud Computing: Concepts, Technology & Architecture* text:

- Chapter 10, "Cloud Security Mechanisms," pages 229–254.

Read the following from the Capella Library:

- Clapper, D., & Richmond, W. (2016). Small business compliance with PCI DSS. *Journal of Management Information and Decision Sciences, 19*(1), 54–67.
  - This study examines business compliance with PCI DSS.
- Rechtman, Y., & Rashbaum, K. (2015). HIPAA security rule - demystified. *The CPA Journal, 85*(4), 68–70.
  - This article dispels the myths surrounding HIPAA compliance preparation so that advisors can prepare businesses for a possible data breach in a fairly painless, pragmatic manner.
- Underwood, J. (2017). You say 'records,' and I say 'data': FERPA, the most widely used federal education law, has not kept pace with changing times. *Phi Delta Kappan, 98* (8), 74–75.
  - This paper addresses FERPA's goal, which is to prevent unauthorized disclosure of students' personally identifiable information.
- Yimam, D. (2016). A survey of compliance issues in cloud computing. *Journal of Internet Services and Applications*, *7*(5), 1–12.
  - This paper explores current trends in regulatory compliance approaches.

Multimedia

- View the VPN Animation multimedia piece.
  - In this animation, you will learn about the nomenclature and function of VPN networks.

u10d1 - Regulatory Requirements

Choose one of the following regulatory frameworks and discuss in detail its impacts on a particular enterprise or organization, ideally based on your own personal or professional experience.

Focus your discussion on how compliance with the regulation drove (or could drive) the design of network modification or the deployment of a security control. Alternately, you can discuss a case of regulatory noncompliance and its consequences. Consider the following:

- Family Educational Rights and Privacy Act (FERPA).
- Federal Information Security Management Act (FISMA)
- Gramm–Leach–Bliley Act (GLBA).
- Health Insurance Portability and Accountability Act (HIPAA).
- Payment Card Industry Data Security Standard (PCI DSS).
- Sarbanes–Oxley Act (SOX).
- Another of your choosing.

Response Guidelines

Post detailed comments or questions to at least two other learners and discuss how the organizational impact of the information security regulation they reviewed compares and contrasts with the impact of the information security regulation on the organization that you reviewed.

Course Resources

Graduate Discussion Participation Scoring Guide

u10v1 - Lab: Recognizing Risks and Threats Associated with Emerging Technologies

Overview

This week's hands-on lab provides you with an opportunity to learn about information security risks associated with social networking websites. You will analyze risks and vulnerabilities of mobile computing devices, and learn about how attackers may strike by ways of these attack vectors. You will explore the pros and cons of storing sensitive data using cloud computing service providers, and learn about best practices for securing cloud based resources.

Directions

Read the requirements for all related course activities before completing this lab so you can take notes as needed to help you complete those activities. Select the linked title heading above to access a lab arranged through Jones & Bartlett Learning.

1. Follow the lab instructions carefully. **Note:** You are only responsible for completing Sections 1 and 2 of the lab.

2. Download the Assignment Template found in the Resources and use it for **both your lab screenshots and your assignment responses**.
3. Take the following screenshots during the lab:
    - Section 2,:
        - Part 2, Steps 26 and 51.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing JBL virtual labs, contact Jones & Bartlett Learning Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

Course Resources

Assignment Template [DOCX]

u10a1 - Deploying a Cloud Security Control

By now you should have completed the unit lab and saved your screenshots to a Word document for submission with this assignment.

Overview

Information security, which involves assuring the confidentiality, integrity, and availability of mission-critical data, is typically a primary concern of regulators. Business executives are responsible for aligning corporate policies to the requirements of regulation and follow up to ensure that the policies and associated controls are being enforced.

Regulatory compliance requires that enterprise IT departments meet certain technical standards that conform to specific requirements that are defined by either an external authoritative governmental or industry organization or by internal enterprise policies. Both internal and external regulations may have significant impacts on enterprise IT operations. Complying with any regulatory rule often constrains IT managers by imposing network and system design features that may be quite costly. Likewise, the cost of not complying with regulations may lead to both civil and criminal penalties.

In this assignment, you address security issues related to information security-related regulatory compliance.

Preparation

Identify and research a specific information security-related regulatory requirement whose compliance is dictated by one of the following regulatory rules:

- Family Educational Rights and Privacy Act (FERPA).
- Gramm–Leach–Bliley Act (GLBA).
- Health Insurance Portability and Accountability Act (HIPAA).
- Payment Card Industry Data Security Standard (PCI DSS).
- Sarbanes–Oxley Act (SOX).

Directions

Use the Assignment Template with your screenshots for the lab documentation and the assignment.

Lab Documentation

Briefly describe what you learned from or observed in the lab and include it in the section with your screenshots in the Assignment Template found in the resources. Be specific.

Assignment

Assume an organization is planning to move a significant IT function, such as data storage or office productivity applications, to a public cloud computing service provider. Identify one of the regulatory rules above as one that would likely govern or be important to the organization and a security control that is appropriate for achieving compliance with it.

Make sure to do the following:

- Explain how your security control protects your cloud data.
- Create a logical network diagram that indicates the appropriate placement of your security control.
- Explain how your security control enables regulatory compliance.

Submit your Word document in this assignment.

Course Resources

Assignment Template [DOCX]