Student Lab Manual

Security Policies and Implementation Issues

IS4550

Current Version Date: 11/23/2011

Table of Contents

Laboratory #1

Lab #1: Craft an Organization-Wide Security Management Policy for Acceptable Use

Learning Objectives and Outcomes

Upon completing this lab, students will be able to complete the following tasks:

- Define the scope of an acceptable use policy as it relates to the User Domain
- Identify the key elements of acceptable use within an organization as part of an overall security management framework
- Align an acceptable use policy with the organization's goals for compliance
- Mitigate the common risks and threats caused by users within the User Domain with the implementation of an acceptable use policy (AUP)
- Draft an acceptable use policy (AUP) in accordance with the policy framework definition incorporating a policy statement, standards, procedures, and guidelines

Required Setup and Tools

This is a paper-based lab. Internet access and the student's Microsoft Office applications are needed to perform this lab.

The following summarizes the setup, configuration, and equipment needed to perform Lab #1:

1. Standard onsite student workstation must have loaded the following software applications and access to the Internet to complete this lab:
    a. Microsoft Office 2007 or higher
    b. Adobe PDF reader
    c. Internet access

Recommended Procedures

Lab #1 – Student Steps

The following student steps are required to perform Lab #1: Create an Organization-Wide Security Management Policy for Acceptable Use:

1. Logon to your classroom workstation
2. Discuss the risks and threats within the User Domain
3. Discuss what organizations can do to mitigate the risks and threats identified within the User Domain. Explore issues related to the following circumstances:

- User apathy towards policies
- User inserts a CD or USB hard drive into the organization's workstation
- User downloads music, video, or other hidden malicious software or code
- User loses productivity by surfing the web
- User destruction or deletion of sensitive files and data
- Disgruntled employee
- Office romance "gone bad"
- Employee blackmail or extortion

4. Open your Internet Explorer web browser, and go to the following web sites:
   - Healthcare: http://it.jhu.edu/policies/itpolicies.html
   - Higher-Education: http://policies.georgetown.edu/31641.html
   - Banking: https://www.casecu.org/webfederal.asp?Cabinet=Home&Drawer=Main&Folder=MORTGAGE&SubFolder=Acceptable+Use+Policy&page_name=acceptable_use_policy
   - U.S. Federal Government: https://www.jointservicessupport.org/AUP.aspx
5. Review the key elements and scope of these sample acceptable use policies
6. Discuss how a risk can be mitigated within the User Domain with an acceptable use policy (AUP)
7. Review the Lab #1 scenario for the creation of an organization-wide security management policy for acceptable use
8. Conduct Lab #1: Craft an Organization-Wide Security Management Policy for Acceptable Use and Lab #1 – Assessment Questions & Answers

Deliverables

Upon completion of Lab #1: Create an Organization-Wide Security Management Policy for Acceptable Use, the students are required to provide the following deliverables:

1. Lab #1 – Craft an Organization-Wide Acceptable Use Policy (AUP)
2. Lab #1 – Assessment Questions & Answers

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #1 that the students must perform:

1. Was the student able to define the scope of an acceptable use policy as it relates to the User Domain? – [**20%**]

2. Was the student able to identify key elements of acceptable use within an organization as part of an overall security management framework? – [**20%**]
3. Was the student able to align an acceptable use policy with the organization's goals for compliance? – [**20%**]
4. Was the student able to mitigate common risks and threats caused by users within the User Domain with the implementation of an acceptable use policy (AUP)? – [**20%**]
5. Was the student able to create an acceptable use policy in accordance with the policy framework definition that incorporates a policy statement, standards, procedures, and guidelines? – [**20%**]

Lab #1 – Organization-Wide Security Management AUP Worksheet

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

In this lab, you are to create an organization-wide acceptable use policy (AUP) that follows a recent compliance law for a mock organization. Here is your scenario:

- Regional ABC Credit union/bank with multiple branches and locations throughout the region
- Online banking and use of the Internet is a strength of your bank given limited human resources
- The customer service department is the most critical business function/operation for the organization
- The organization wants to be in compliance with GLBA and IT security best practices regarding its employees
- The organization wants to monitor and control use of the Internet by implementing content filtering
- The organization wants to eliminate personal use of organization owned IT assets and systems
- The organization wants to monitor and control use of the e-mail system by implementing e-mail security controls
- The organization wants to implement this policy for all the IT assets it owns and to incorporate this policy review into an annual security awareness training

Instructions

Using Microsoft Word, create an Acceptable Use Policy for ABC Credit union/bank according to the following policy template:

ABC Credit Union

Policy Name

Policy Statement

{Insert policy verbiage here}

Purpose/Objectives

{Insert purpose of the policy as well as the objectives – bulleted list of the policy definition}

Scope

{Define this policy's scope and whom it covers.

Which of the seven domains of a typical IT infrastructure are impacted?

What elements or IT assets or organization-owned assets are within the scope of this policy?}

Standards

{Does this policy point to any hardware, software, or configuration standards? If so, list them here and explain the relationship of this policy to these standards.}

Procedures

[In this section, explain how you intend to implement this policy throughout this organization.}

Guidelines

[In this section, explain any road blocks or implementation issues that you must overcome and how you will overcome them per the defined policy guidelines.}

Note: Your policy document should be no more than 3 pages long.

Lab #1 – Assessment Worksheet

Craft an Organization-Wide Security Management Policy for Acceptable Use

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

In this lab, Create an Organization-Wide Security Management Acceptable Use Policy (AUP), the students participated in a classroom discussion about what is considered to be “acceptable use.” The weakest link in the seven domains of a typical IT infrastructure was identified as the User Domain. When given a scenario, the students created an organization-wide acceptable use policy for ABC Credit Union/Bank.

Lab Assessment Questions & Answers

1. What are the top risks and threats from the User Domain?

2. Why do organizations have acceptable use policies (AUPs)?

3. Can internet use and e-mail use policies be covered in an Acceptable Use Policy?

4. Do compliance laws such as HIPPA or GLBA play a role in AUP definition?

5. Why is an acceptable use policy not a failsafe means of mitigating risks and threats within the User Domain?

6. Will the AUP apply to all levels of the organization, why or why not?

7. When should this policy be implemented and how?

8. Why does an organization want to align its policies with the existing compliance requirements?

9. Why is it important to flag any existing standards (hardware, software, configuration, etc.) from an AUP?

10. Where in the policy definition do you define how to implement this policy within your organization?

11. Why must an organization have an Acceptable Use Policy (AUP) even for non-employees such as contractors, consultants, and other 3rd parties?

12. What security controls can be deployed to monitor and mitigate users from accessing external websites that are potentially in violation of an AUP?

13. What security controls can be deployed to monitor and mitigate users from accessing external webmail systems and services (i.e., Hotmail, Gmail, Yahoo, etc.)?

14. What security controls can be deployed to monitor and mitigate users from imbedding privacy data in e-mail messages and/or attaching documents that may contain privacy data?

15. Should an organization terminate the employment of an employee if he/she violates an AUP?

Laboratory #2

Lab #2: Develop an Organization-Wide Policy Framework Implementation Plan

Learning Objectives and Outcomes

Upon completing this lab, students will be able to complete the following tasks:

- Identify human nature and behavior patterns of employee types in both hierarchical and flat organizational structures
- Overcome user apathy with security awareness techniques in both hierarchical and flat organizational structures
- Identify how security policies can help shape organizational behavior and culture in both hierarchical and flat organizational structures
- Compare a hierarchical and flat organizational structure to equivalent IT security policy framework structures
- Create an organizational policy implementation plan for the combined organization

Required Setup and Tools

This is a paper-based lab. Internet access and the student's Microsoft Office applications are needed to conduct this lab.

The following summarizes the setup, configuration, and equipment needed to perform Lab #2:

1. Standard onsite student workstation must have the following software applications loaded and Internet access to conduct this lab:
    a. Microsoft Office 2007 or higher
    b. Adobe PDF reader
    c. Internet access

Recommended Procedures

Lab #2 – Student Steps

The student steps needed to conduct Lab #2: Develop an Organization-Wide Policy Framework Implementation Plan:

1. Discuss why the implementation of information systems security policies is difficult within organizations.

2. Discuss what organizations can do to help implement information systems security policies throughout the seven domains of a typical IT infrastructure

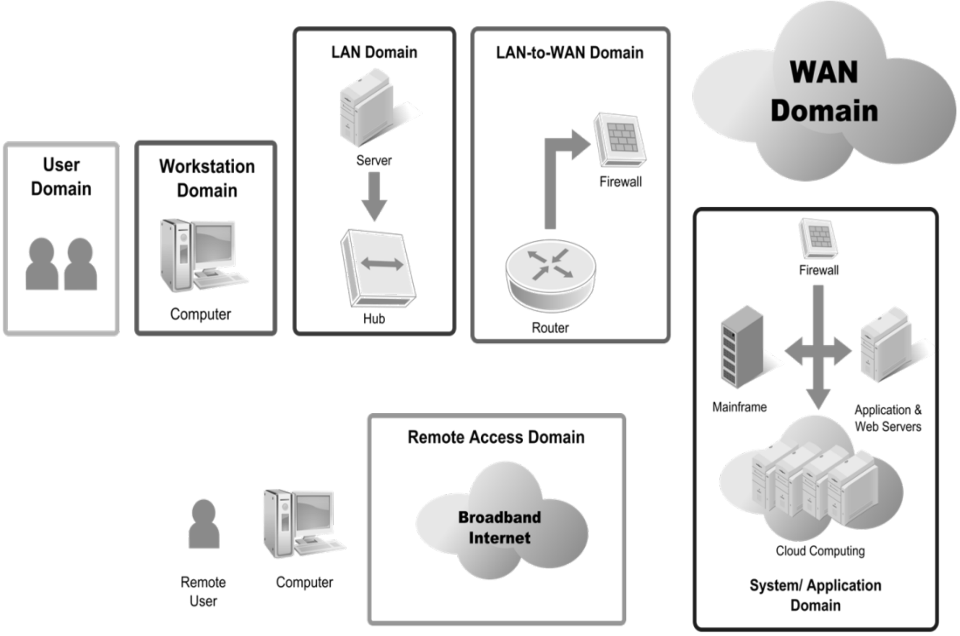


Figure 1 – Seven Domains of a Typical IT Infrastructure

3. Discuss why executive management, IT security policy enforcement monitoring, and human resources must have a unified front regarding disciplinary treatment of policy violations
   - ***Executive Management:*** Policy commitment and implementation must come from the CEO and the president's executive order for the entire organization with policy monitoring and disciplinary action taken for policy violations
   - ***IT Security Policy Enforcement Monitoring:*** Policy monitoring can be conducted via system logging, content filtering logging, and e-mail filtering logging with automated reporting to IT security personnel for monthly or quarterly policy compliance reviews
   - ***Human Resources:*** Employees or contractors/consultants must conform to all organization-wide policies. Violations of policies are considered to be an employer – employee issue upon which proper disciplinary actions must be taken. Repeat or continued violations of organization-wide policies may be grounds for termination of employment depending upon the severity of the violation. Non-employees should be provided with limited access and connectivity as per policy definition

4. Review the organizational structure inherent in flat and hierarchical organizations and how people behave in such structures
   - ***Flat organizational structures are characterized by the following characteristics:***
     Management structure that is cross-functional and more open to employee input
     Dialogue and communications between employees may occur across organizational functions
     Employees tend to be more open and communicative
     Employees tend to be more creative and involved in business decisions
     Employees are not as constrained within their role or function and can see and interact across the organization more freely
   - ***Hierarchical organizational structures are characterized by the following:***
     Departments are separated by function, creating multiple functional silos.
     Business decision making performed at the executive management level.
     Dialogue and communications is more "top-down."
     Employees tend to be less communicative and more isolated within their business functions.
     Employees find it difficult to offer additional creativity or input to business decisions
     Employees are constrained within their roles and cannot interact outside of their business functions without going through a chain of command
5. Review the organizational structure inherent within hierarchical and flat organizations and how people behave in such a structure
   - Isolated communication vs. open and free communication
   - Silos vs. flat dialogue and communications
   - Executive managers make business decisions vs. employees provide input into business decisions.
   - Management to employee dialogue and communications vs. employee to employee dialogue and communications.
6. Review why conducting annual audits and security assessments for policy compliance is a critical security operations and management function to help mitigate risks and threats.
   - People constantly change.
   - People gravitate toward repetition and repetitive inputs.
   - Periodic security awareness training coupled with policy compliance monitoring can help mitigate the risks and threats caused by employees within the User Domain.

7. Review the scope of a Policy Implementation Plan and what elements are required for the plan as part of this lab's deliverables.
   - Publish Your Policies
   - Communicate Your Policies
   - Involve Human Resources & Executive Management
   - Incorporate Security Awareness and Training
   - Release a Monthly Organization-Wide Newsletter
   - Implement Security Reminders on System Login Screens
   - Incorporate On-Going Security Policy Maintenance
   - Obtain Employee Questions or Feedback

Deliverables

Upon completion of the Lab #2: Develop an Organization-Wide Policy Framework Implementation Plan, the students are required to provide the following deliverables as part of this lab:

1. Lab #2 – Develop an Organization-Wide Policy Framework Implementation Plan
2. Lab #2 – Assessment Questions & Answers

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #2 that the students must perform:

1. Was the student able to identify human nature and behavior patterns of employee types in both hierarchical and flat organizational structures? – [**20%**]
2. Was the student able to overcome user apathy with security awareness techniques in both hierarchical and flat organizational structures? – [**20%**]
3. Was the student able to identify how security policies can help shape organizational behavior and culture in both hierarchical and flat organizational structures? – [**20%**]
4. Was the student able to compare a hierarchical and flat organizational structure to equivalent IT security policy framework structures? – [**20%**]
5. Was the student able to create an organizational policy implementation plan for the combined organization? – [**20%**]

Lab #2 – Organization-Wide Policy Framework Implementation Plan Worksheet

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

In this lab, you are to create an organization-wide policy framework implementation plan for two organizations that are merging. The parent organization is a medical clinic under HIPAA compliance law. They recently acquired a remote medical clinic that provides a specialty service. This clinic is organized in a flat structure, but the parent organization is organized in a hierarchical structure with many departments and medical clinics.

Instructions

Using Microsoft Word, create a Policy Framework Implementation Plan according to the following policy implementation plan outline:

- Publish Your Policies for the Acquired Clinic – {Explain your strategy}
- Communicate Your Policies to the Acquired Clinic Employees – {How are you going to do this?}
- Involve Human Resources & Executive Management - {How do you do this smoothly?}
- Incorporate Security Awareness and Training for the New Clinic – {How can you make this fun and engaging?}
- Release a Monthly Organization-Wide Newsletter for All – {How can you make this short and to the point?}
- Implement Security Reminders on System Login Screens for All – {For access to sensitive systems only}
- Incorporate On-Going Security Policy Maintenance for All – {Review and obtain feedback from employees and policy compliance monitoring}
- Obtain Employee Questions or Feedback for Policy Board – {Review and incorporate into policy edits and changes as needed}

Parent Medical Clinic

Acquires Specialty Medical Clinic

Publish Your Policies for the New Clinic

{Explain your strategy}

Communicate Your Policies to the New Clinic Employees

{How are you going to do this?}

Involve Human Resources & Executive Management

{How do you do this smoothly?}

Incorporate Security Awareness and Training for the New Clinic

{How can you make this fun and engaging?}

Release a Monthly Organization Wide Newsletter for All

{How can you make this newsletter succinct?}

Implement Security Reminders on System Login Screens for All

{For access to sensitive systems only}

Incorporate On-Going Security Policy Maintenance for All

{Review and obtain feedback from employees and policy compliance monitoring}

Obtain Employee Questions or Feedback for Policy Board

{Review and incorporate into policy edits and changes as needed}

Note: Your policy framework implementation plan should be no more than three pages long.

Lab #2 – Assessment Worksheet

Develop an Organization-Wide Policy Framework Implementation Plan

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

In this lab, you participated in classroom discussions on information systems security policy implementation issues. These issues and questions included the following topics:

- How to deal with people and human nature
- What motivates people
- Understanding different personality types of employees
- Identifying the characteristics of a flat organizational structure
- Identifying the characteristics of a hierarchical organizational structure
- What makes an IT security policy “stick”?
- How do you monitor organizational compliance?
- What is the ongoing role of executive management?
- What is the ongoing role of human resources?
- Why is conducting an annual audit and security assessment for policy compliance important?

Lab Assessment Questions & Answers

1. What are the differences between a Flat and Hierarchical organizations?

2. Do employees behave differently in a flat versus hierarchical organizational structure?

3. Do employee personality types differ between these organizations?

4. What makes it difficult for implementation in flat organizations?

5. What makes it difficult for implementation in hierarchical organizations?

6. How do you overcome employee apathy towards policy compliance?

7. What solution makes sense for the merging of policy frameworks from both a flat and hierarchical organizational structure?

8. What type of disciplinary action should organizations take for information systems security violations?

9. What is the most important element to have in policy implementation?

10. What is the most important element to have in policy enforcement?

11. Which domain of the 7-Domains of a Typical IT Infrastructure would an Acceptable Use Policy (AUP) reside? How does an AUP help mitigate the risks commonly found with employees and authorized users of an organization's IT infrastructure?

12. In addition to the AUP to define what is acceptable use, what can an organization implement within the LAN-to-WAN Domain to help monitor and prevent employees and authorized users in complying with acceptable use of the organization's Internet link?

13. What can you do in the Workstation Domain to help mitigate the risks, threats, and vulnerabilities commonly found in this domain? Remember the Workstation Domain is the point of entry for users into the organization's IT infrastructure.

14. What can you do in the LAN Domain to help mitigate the risks, threats, and vulnerabilities commonly found in this domain? Remember the LAN Domain is the point of entry into the organization’s servers, applications, folders, and data.

15. What do you recommend for properly communicating the recommendations you made in Question #13 and Question #14 above for both a flat organization and a hierarchical organization?

Laboratory #3

Lab #3: Define an Information Systems Security Policy Framework for an IT Infrastructure

Learning Objectives and Outcomes

Upon completing this lab, students will be able to complete the following tasks:

- Identify risks and threats commonly found within the seven domains of a typical IT infrastructure
- Define security policies to address each identified risk and threat as they are organized within the seven domains of a typical IT infrastructure
- Align security policies to mitigate risks from threats and vulnerabilities found within the seven domains of a typical IT infrastructure
- Organize the security policies within an overall framework as part of an overall layered security strategy for the seven domains of a typical IT infrastructure
- Select the appropriate policy definitions needed throughout the seven domains of a typical IT infrastructure to mitigate the identified risks, threats, and vulnerabilities

Required Setup and Tools

This is a paper-based lab. Internet access and the student's Microsoft Office applications are needed to perform this lab.

The following summarizes the setup, configuration, and equipment needed to perform Lab #3:

1. Standard onsite student workstation must have the following software applications loaded and Internet access to perform this lab:
   a. Microsoft Office 2007 or higher
   b. Adobe PDF reader
   c. Internet access

Recommended Procedures

Lab #3 – Student Steps

The student steps that are needed to perform Lab #3: Define the Scope & Structure for an IT Risk Management Plan are listed here:

1. Review the seven domains of a typical IT infrastructure and identify common risks, threats, and vulnerabilities

2. Complete the Lab #3 – Assessment Worksheet, Part A on common risks, threats, and vulnerabilities found
3. Review how can these risks, threats, and vulnerabilities may be mitigated through policy definition within the seven domains of a typical IT infrastructure
4. Complete the Lab #3 – Assessment Worksheet, Part B on selecting policy definitions that may help mitigate the risks, threats, and vulnerabilities identified throughout the seven domains of a typical IT infrastructure
5. Answer Lab #3 – Assessment Questions & Answers and submit as part of your Lab #3 deliverables

Deliverables

Upon completion of Lab 3: Define an Information Systems Security Policy Framework for an IT Infrastructure, the students are required to provide the following deliverables as part of this lab:

1. Lab #3 – Assessment Worksheet, Part A
2. Lab #3 – Assessment Worksheet, Part B
3. Lab #3 – Assessment Questions & Answers

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #3 that the students must perform:

1. Was the student able to identify risks and threats commonly found within the seven domains of a typical IT infrastructure? – [**20%**]
2. Was the student able to define security policies to address each identified risk and threat within the seven domains of a typical IT infrastructure? – [**20%**]
3. Was the student able to align security policies to mitigate risks from threats and vulnerabilities found within the seven domains of a typical IT infrastructure? – [**20%**]
4. Was the student able to organize security policies within an overall framework as part of an overall layered security strategy for the seven domains of a typical IT infrastructure? – [**20%]**
5. Was the student able to select appropriate policy definitions needed throughout the seven domains of a typical IT infrastructure to mitigate the identified risks, threats, and vulnerabilities? – [**20%**]

Lab #3 – Assessment Worksheet

Part A – List of Risks, Threats, and Vulnerabilities Commonly Found in an IT Infrastructure

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

The following risks, threats, and vulnerabilities were found in a healthcare IT infrastructure serving patients with life-threatening situations. Given the following list, select where the risk, threat, or vulnerability resides in the seven domains of a typical IT infrastructure.

Risk – Threat – Vulnerability	**Primary Domain Impacted**
Unauthorized access from public Internet	
User destroys data in application and deletes all files	
Hacker penetrates your IT infrastructure and gains access to your internal network	
Intra-office employee romance “gone bad”	
Fire destroys the primary data center	
Communication circuit outages	
Workstation OS has a known software vulnerability	
Unauthorized access to organization owned Workstations	
Loss of production data	
Denial of service attack on organization e-mail server	

Risk – Threat – Vulnerability	**Primary Domain Impacted**
Remote communications from home office	
LAN server OS has a known software vulnerability	
User downloads an unknown e –mail attachment	
Workstation browser has software vulnerability	
Service provider has a major network outage	
Weak ingress/egress traffic filtering degrades Performance	
User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers	
VPN tunneling between remote computer and ingress/egress router	
WLAN access points are needed for LAN connectivity within a warehouse	
Need to prevent rogue users from unauthorized WLAN access	

Lab #3 – Assessment Worksheet

Part B – List of Risks, Threats, and Vulnerabilities Commonly Found in an IT Infrastructure

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

<u>Overview</u>

For each of the identified risks, threats, and vulnerabilities; select the most appropriate policy definition that may help mitigate the identified risk, threat, or vulnerability within that domain from the following list:

Policy Definition List

Acceptable Use Policy

Access Control Policy Definition

Business Continuity – Business Impact Analysis (BIA) Policy Definition

Business Continuity & Disaster Recovery Policy Definition

Data Classification Standard & Encryption Policy Definition

Internet Ingress/Egress Traffic Policy Definition

Mandated Security Awareness Training Policy Definition

Production Data Back-up Policy Definition

Remote Access Policy Definition

Vulnerability Management & Vulnerability Window Policy Definition

WAN Service Availability Policy Definition

Risk – Threat – Vulnerability	**Policy Definition Required**
Unauthorized access from public Internet	
User destroys data in application and deletes all files	
Hacker penetrates your IT infrastructure and gains access to your internal network	
Intra-office employee romance gone bad	
Fire destroys primary data center	
Communication circuit outages	
Workstation OS has a known software vulnerability	
Unauthorized access to organization-owned Workstations	
Loss of production data	
Denial of service attack on organization e-mail Server	
Remote communications from home office	
LAN server OS has a known software vulnerability	
User downloads an unknown e –mail attachment	
Workstation browser has software vulnerability	
Service provider has a major network outage	
Weak ingress/egress traffic filtering degrades Performance	

Risk – Threat – Vulnerability	**Policy Definition Required**
User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers	
VPN tunneling between remote computer and ingress/egress router	
WLAN access points are needed for LAN connectivity within a warehouse	
Need to prevent rogue users from unauthorized WLAN access	

Lab #3 – Assessment Worksheet

Define an Information Systems Security Policy Framework for an IT Infrastructure

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

In this lab, students identified risks, threats, and vulnerabilities throughout the seven domains of a typical IT infrastructure. By organizing these risks, threats, and vulnerabilities within each of the seven domains of a typical IT infrastructure information system security policies can be defined to help mitigate this risk. Using policy definition and policy implementation, organizations can "tighten" security throughout the seven domains of a typical IT infrastructure.

Lab Assessment Questions & Answers

1. A policy definition usually contains what four major parts or elements?

2. In order to effectively implement a policy framework, what three organizational elements are absolutely needed to ensure successful implementation?

3. Which policy is the most important one to implement to separate employer from employee? Which is the most challenging to implement successfully?

4. Which domain requires stringent access controls and encryption for connectivity to the corporate resources from home? What policy definition is needed for this domain?

5. Which domains need software vulnerability management & vulnerability window policy definitions to mitigate risk from software vulnerabilities?

6. Which domain requires AUPs to minimize unnecessary User-initiated Internet traffic and awareness of the proper use of organization-owned IT assets?

7. What policy definition can help remind employees within the User Domain about on-going acceptable use and unacceptable use?

8. What policy definition is required to restrict and prevent unauthorized access to organization owned IT systems and applications?

9. What is the relationship between an Encryption Policy Definition and a Data Classification Standard?

10. What policy definition is needed to minimize data loss?

11. Explain the relationship between the policy-standard-procedure-guideline structure and how this should be postured to the employees and authorized users.

12. Why should an organization have a remote access policy even if they already have an Acceptable Use Policy (AUP) for employees?

13. What security controls can be implemented on your e-mail system to help prevent rogue or malicious software disguised as URL links or e-mail attachments from attacking the Workstation Domain? What kind of policy definition should this be included in? Justify your answer.

14. Why should an organization have annual security awareness training that includes an overview of the organization's policies?

15. What is the purpose of defining of a framework for IT security policies?

Laboratory #4

Lab 4: Craft a Layered Security Management Policy – Separation of Duties

Learning Objectives and Outcomes

Upon completing this lab, students will be able to complete the following tasks:

- Identify roles and responsibilities for policy implementation throughout the seven domains of a typical IT infrastructure
- Identify physical separation of duties regarding responsibility for information systems security policy implementation
- Align responsibilities for policy implementation throughout the seven domains of a typical IT infrastructure
- Apply separation of duties to a layered security management policy throughout the seven domains of a typical IT infrastructure
- Create a layered security management policy defining separation of duties

Required Setup and Tools

This is a paper-based lab. Internet access and the student's Microsoft Office applications are needed to perform this lab.

The following summarizes the setup, configuration, and equipment needed to perform Lab #4:

1. Standard onsite student workstation must have the following software applications loaded and Internet access to perform this lab:
   a. Microsoft Office 2007 or higher
   b. Adobe PDF reader
   c. Internet access

Recommended Procedures

Lab #4 – Student Steps

The following steps are required to conduct this lab:

1. Review the seven domains of a typical IT infrastructure diagram, as shown in Figure 1
2. Discuss what the roles, responsibilities, and accountabilities are throughout the seven domains of a typical IT infrastructure regarding information systems security

3. Discuss how these roles, responsibilities, and accountabilities are crucial to define who is responsible for what throughout the IT infrastructure
4. Discuss the importance of separation of duties and how involving key personnel for a security incident response team is important
    - Separation of duties
    - No one individual should have too much authority or power to perform a function within a business or organization
    - Understanding one's domain of responsibilities and where that responsibility stops is critical to understand separation of duties
5. Review the deliverables needed for Lab 4: Create a Layered Security Management Policy - Separation of Duties
6. Review the Policy Definition Template they are to use for the creation of the Separation of Duties Policy Definition for a layered security management plan for an IT Infrastructure

Deliverables

Upon completion of Lab #4 – Craft a Layered Security Management Policy - Separation of Duties, the students are required to provide the following deliverables as part of this lab:

1. Lab #4 – Policy Definition for a Layered Security Management Plan – Separation of Duties
2. Lab #4 – Assessment Questions & Answers

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #4 that the student must perform:

1. Was the student able to identify the roles and responsibilities for policy implementation throughout the seven domains of a typical IT infrastructure? – [**20%**]
2. Was the student able to identify the physical separation of duties regarding responsibility for information systems security policy implementation? – [**20%**]
3. Was the student able to align responsibilities for policy implementation throughout the seven domains of a typical IT infrastructure? – [**20%**]
4. Was the student able to apply separation of duties to a layered security management policy throughout the seven domains of a typical IT infrastructure? – [**20%**]
5. Was the student able to create a layered security management policy defining separation of duties? – [**20%**]

Lab #4 – Assessment Worksheet

Craft a Layered Security Management Policy – Separation of Duties

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

In this lab, you are to create a security management policy that addresses the management and the separation of duties throughout the seven domains of a typical IT infrastructure. You are to define what the information systems security responsibility is for each of the seven domains of a typical IT infrastructure. From this definition, you must incorporate your definition for the separation of duties within the procedures section of your policy definition template. Your scenario is the same as in Lab #1 – ABC Credit Union/Bank.

- Regional ABC Credit union/bank with multiple branches and locations throughout the region
- Online banking and the use of the Internet is a strength of your bank given limited human resources
- The customer service department is the most critical business function/operation of the organization.
- The organization wants to be in compliance with GLBA and IT security best practices regarding employees.
- The organization wants to monitor and control use of the Internet by implementing content filtering.
- The organization wants to eliminate personal use of organization owned IT assets and systems.
- The organization wants to monitor and control the use of the e-mail system by implementing e-mail security controls.
- The organization wants to implement this policy for all IT assets owned by the organization and to incorporate this policy review into the annual security awareness training.
- The organization wants to define a policy framework including a Security Management Policy defining the separation of duties for information systems security.

Instructions

Using Microsoft Word, craft a Security Management Policy with Defined Separation of Duties using the following policy template:

ABC Credit Union

Policy Name

Policy Statement

{Insert policy verbiage here}

Purpose/Objectives

{Insert purpose of the policy as well as the objectives – bulleted list of the policy definition}

Scope

{Define whom this policy covers and its scope.

Which of the seven domains of a typical IT infrastructure are impacted? – All 7 Must Be Included in the Scope.

What elements or IT assets or organization-owned assets are within the scope of this policy? – In this case you are concerned about what IT assets and elements are within each of the domains that require information systems security management?}

Standards

{Does this policy point to any hardware, software, or configuration standards? If so, list them here and explain the relationship of this policy to these standards – Yes, you need to reference technical hardware, software, and configuration standards for IT assets throughout the seven domains of a typical IT infrastructure. For this lab, you can merely point them to “Workstation Configuration Standards”, etc.}

Procedures

{Explain how you intend to implement this policy for the entire organization. This is the most important part of the policy definition because you must explain and define your separation of duties throughout the seven domains of a typical IT infrastructure. All seven domains must be listed in this section as well as who is responsible for ensuring C-I-A and security policy implementation within that domain.}

Guidelines

{Explain any road blocks or implementation issues that you must overcome in this section and how you will surmount them per defined policy guidelines. Any disputes or gaps in the definition and separation of duties responsibility may need to be addressed in this section.}

Note: Your policy document must be no more than 3 pages.

Lab #4 – Assessment Worksheet

Craft a Layered Security Management Policy – Separation of Duties

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

In this lab, you examined the seven domains of a typical IT infrastructure from an information systems security responsibility perspective. What are the roles and responsibilities performed by the IT professional, and what are the roles and responsibilities of the information systems security practitioner? This lab presented an overview of exactly what those roles and responsibilities are and, more importantly, how to define a security management policy that aligns and defines who is responsible for what. This is critical during a security incident that requires immediate attention by the security incident response team.

Lab Assessment Questions & Answers

1. For each of the seven domains of a typical IT infrastructure, summarize what the information systems security responsibilities are within that domain:

2. Which of the seven domains of a typical IT infrastructure requires personnel and executive management support outside of the IT or information systems security organizations?

3. What does separation of duties mean?

4. How does separation of duties throughout an IT infrastructure mitigate risk for an organization?

5. How would you position a layered security approach with a layered security management approach for an IT infrastructure?

6. If a system administrator had both the ID and password to a system, would that be a problem?

7. When using a layered security approaches to system administration, who would have the highest access privileges?

8. Who would review the organizations layered approach to security?

9. Why do you only want to refer to technical standards in a policy definition document?

10. Why is it important to define guidelines in this layered security management policy?

11. Why is it important to define access control policies that limit or prevent exposing customer privacy data to employees?

12. Explain why the seven domains of a typical IT infrastructure helps organizations align to separation of duties.

13. Why is it important for an organization to have a policy definition for Business Continuity and Disaster Recovery?

14. Why is it important to prevent users from downloading and installing applications on organization owned laptops and desktop computers?

15. Separation of duties is best defined by policy definition. What is needed to ensure its success?

Laboratory #5

Lab #5: Craft an Organization-Wide Security Awareness Policy

Learning Objectives and Outcomes

Upon completing this lab, students will be able to complete the following tasks:

- Relate how risks, threats, and software vulnerabilities impact the seven domains of a typical IT infrastructure
- Identify the risks and threats commonly found within the User Domain and Workstation Domain
- Mitigate the risks and threats identified in the User Domain and Workstation Domain by incorporating these topics in the organization's security awareness training program
- Identify the key elements of a security awareness training policy as part of an overall layered security strategy
- Create an organization-wide security awareness training policy mandating annual or periodic security awareness training for new and existing employees

Required Setup and Tools

This is a paper-based lab. Internet access and the student's Microsoft Office applications are needed to perform this lab.

The following summarizes the setup, configuration, and equipment needed to perform Lab #5:

1. Standard onsite student workstation must have the following software applications loaded and Internet access to perform this lab:
    a. Microsoft Office 2007 or higher
    b. Adobe PDF reader
    c. Internet access

Recommended Procedures

Lab #5 – Student Steps:

The following are the steps that the student must follow as part of Lab #5 – Create an Organization-Wide Security Awareness Policy:

1. Review with the class examples of security awareness & training policies found on the Internet:
   Healthcare: State of North Carolina Department of Health & Human Services
   http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/06security_training_and_awareness.pdf

Higher-Education: University of Massachusetts

http://www.massachusetts.edu/policyfaq/faq.cfm

U.S. Federal Government: Department of Defense Information Assurance Awareness

http://iase.disa.mil/eta/iaav9/iaa_v9/index.htm

Healthcare: Community Health Care of Washington

http://chpw.org/assets/file/Security-Awareness-and-Training-Policy.pdf

2. Discuss what the risks and threats are within the User Domain per the bulleted list provided:
    - Dealing with humans and human nature
    - User or employee apathy towards information systems security policy
    - Accessing the Internet is like opening “Pandora’s box.”
    - Surfing the web can be a dangerous trek in unknown territory
    - Opening e-mails and unknown e-mail attachments can lead to malicious software and codes
    - Installing unauthorized applications, files, or data onto organization owned IT assets
    - Downloading applications or software with hidden malicious software or codes
    - Clicking on an unknown URL links with hidden scripts
3. Discuss what organizations can do to mitigate the risks and threats identified within the User Domain
4. Discuss what the risks and threats are within the Workstation Domain per the bulleted list provided:
    - Unauthorized access to workstation
    - Operating system software vulnerabilities
    - Application software vulnerabilities
    - Viruses, Trojans, worms, spyware, malicious software/code, etc.
    - User inserts CDs, DVDs, USB thumb drives with personal data and files onto organization-owned IT assets
    - User downloads unauthorized applications and software onto organization-owned IT assets
    - User installs unauthorized applications and software onto organization-owned IT assets
5. Discuss what organizations can do to mitigate the risks and threats identified within the Workstation Domain
6. Create the deliverables for Lab #5 – Assessment Worksheet

7. Answer the Lab #5 – Assessment Questions & Answers that must be submitted with this lab exercise

Deliverables

Upon completion of Lab #5: Create an Organization-Wide Security Awareness Policy, the students must provide the following deliverables as part of this lab:

1. Lab #5 – Security Awareness Training Policy Elements Assessment Worksheet
2. Lab #5 – Create a Security Awareness Training Policy Definition
3. Lab #5 – Assessment Questions & Answers

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #5 that the student must conduct:

1. Was the student able to relate how risks, threats, and software vulnerabilities impact the seven domains of a typical IT infrastructure? – [**20%**]
2. Was the student able to identify risks and threats commonly found within the User Domain and Workstation Domain? – [**20%**]
3. Was the student able to mitigate the risks and threats identified in the User Domain and Workstation Domain by incorporating these topics in the organization's security awareness training program? – [**20%**]
4. Was the student able to identify the key elements of a security awareness training policy as part of an overall layered security strategy? – [**20%**]
5. Was the student able to create an organization-wide security awareness training policy mandating annual or periodic security awareness training for new and existing employees? – [**20%**]

Lab #5 – Assessment Worksheet

Elements of a Security Awareness & Training Policy

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

For each of the identified risks and threats within the User Domain and Workstation Domain, identify a security control or security countermeasure that can help mitigate the risk or threat.

User Domain Risks & Threats	Risk Mitigation Tactic/Solution
Dealing with humans and human nature	
User or employee apathy towards information systems security policy	
Accessing the Internet is like opening “Pandora’s box” given the threat from attackers	
Surfing the web can be a dangerous trek in unknown territory	
Opening e-mails and unknown e-mail attachments can unleash malicious software and codes	

Workstation Domain Risks & Threats	**Risk Mitigation Tactic/Solution**
Installing unauthorized applications, files, or data on organization owned IT assets can be dangerous	
Downloading applications or software with hidden malicious software or codes	
Clicking on an unknown URL link with hidden scripts	
Unauthorized access to workstation	
Operating system software vulnerabilities	
Application software vulnerabilities	
Viruses, Trojans, worms, spyware, malicious software/code, etc.	
User inserts CDs, DVDs, USB thumb drives with personal files onto organization-owned IT assets	
User downloads unauthorized applications and software onto organization-owned IT assets	
User installs unauthorized applications and software onto organization-owned IT assets	

Lab #5 – Assessment Worksheet

Craft an Organization-Wide Security Awareness & Training Policy

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

In this lab, you are to create an organization-wide security awareness & training policy for a mock organization to reflect the demands of a recent compliance law. Here is your scenario:

- Regional ABC Credit union/bank with multiple branches and locations throughout the region
- Online banking and use of the Internet is a strength of your bank given limited human resources
- The customer service department is the most critical business function/operation for the organization
- The organization wants to be in compliance with GLBA and IT security best practices regarding employees in the User Domain and Workstation Domain
- The organization wants to monitor and control use of the Internet by implementing content filtering
- The organization wants to eliminate personal use of organization owned IT assets and systems
- The organization wants to monitor and control use of the e-mail system by implementing e-mail security controls
- Organization wants to implement the security awareness & training policy mandated for all new hires and existing employees. Policy definition to include GLBA and customer privacy data requirements and mandate annual security awareness training for all employees

Instructions

Using Microsoft Word, create a Security Awareness & Training Policy for ABC Credit union/bank capturing the elements of the policy as defined in the Lab #5 – Assessment Worksheet. Use the following policy template for the creation of your Security Awareness & Training Policy definition.

ABC Credit Union

Security Awareness & Training Policy

Policy Statement

{Insert policy verbiage here}

Purpose/Objectives

{Insert purpose of the policy as well as the objectives – bulleted list of the policy definition}

Scope

{Define whom this policy covers and its scope.

Which of the seven domains of a typical IT infrastructure are impacted?

What elements or IT assets or organization-owned assets are within the scope of this policy?}

Standards

{Does this policy point to any hardware, software, or configuration standards? If so, list them here and explain the relationship of this policy to these standards. In this case, Workstation Domain standards should be referenced – make any necessary assumptions.}

Procedures

{Explain how you intend to implement this policy across the organization and how you intend to deliver annual or on-going security awareness training for employees.}

Guidelines

{Explain any road blocks or implementation issues that you must address in this section and how you will overcome them per defined policy guidelines.}

Note: Your policy document must be no more than 3 pages long.

Lab #5 – Assessment Worksheet

Craft an Organization-Wide Security Awareness & Training Policy

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

In this lab, the students reviewed and identified common risks and threats within the User Domain and Workstation Domain. From this, the elements of a security awareness training policy definition were aligned to policy definition goals and objectives. The students then created a Security Awareness & Training Policy definition focusing on the requirements as defined in the given scenario. This policy, coupled with actual security awareness training content customized to ABC Credit union/bank, can help mitigate the risks and threats within the User Domain and Workstation Domain and will contribute to the organization's overall layered security strategy.

Lab Assessment Questions & Answers

1. How does a security awareness & training policy impact an organization's ability to mitigate risks, threats, and vulnerabilities?

2. Why do you need a security awareness & training policy if you have new hires attend or participate in the organization’s security awareness training program during new hire orientation?

3. What is the relationship between an Acceptable Use Policy (AUP) and a Security Awareness & Training Policy?

4. Why is it important to prevent users from engaging in downloading or installing applications and software found on the Internet?

5. When trying to combat software vulnerabilities in the Workstation Domain, what is needed most to deal with operating system, application, and other software installations?

6. Why is it important to educate users about the risks, threats, and vulnerabilities found on the Internet and world wide web?

7. What are some strategies for preventing users or employees from downloading ad installing rogue applications and software found on the Internet?

8. What is one strategy for preventing users from clicking on unknown e-mail attachments and files?

9. Why should social engineering be included in security awareness training?

10. Which 2 domains of a typical IT infrastructure are the focus of a Security Awareness & Training Policy?

11. Why should you include organization-wide policies in employee security awareness training?

12. Which domain typically acts as the point-of-entry into the IT infrastructure? Which domain typically acts as the point-of-entry into the IT infrastructure's systems, applications, databases?

13. Why does an organization need a policy on conducting security awareness training annually and periodically?

14. What other strategies can organizations implement to keep security awareness top of mind with all employees and authorized users?

15. Why should an organization provide updated security awareness training when a new policy is implemented throughout the User Domain or Workstation Domain?

Laboratory #6

Lab #6: Define a Remote Access Policy to Support Remote Healthcare Clinics

Learning Objectives and Outcomes

Upon completing this lab, students will be able to complete the following tasks:

- Define the scope of an remote access policy as it relates to the Remote Access Domain
- Identify the key elements of a remote access policy within an organization as part of an overall security management framework
- Align the remote access policy with the organization's goals for compliance
- Mitigate common risks and threats found within the Remote Access Domain with proper security controls and countermeasures as defined in the remote access policy definition
- Create a remote access policy definition incorporating a policy statement, standards, procedures, and guidelines

Required Setup and Tools

This is a paper-based lab. Internet access and the student's Microsoft Office applications are needed to perform this lab.

The following summarizes the setup, configuration, and equipment needed to perform Lab #6:

1. Standard onsite student workstation must have the following software applications loaded and Internet access to perform this lab:
   a. Microsoft Office 2007 or higher
   b. Adobe PDF reader
   c. Internet access

Recommended Procedures

Lab #6 – Student Steps

1. Review with the instructor sample Remote Access Policy documents found on the Internet:
   SANS Institute: Remote Access Policy Template
   http://www.sans.org/security-resources/policies/Remote_Access_Policy.pdf

   Higher-Education: Clark University
   http://www.clarku.edu/offices/its/policies/remoteaccess.cfm

Higher-Education: Purdue University

http://www.purdue.edu/policies/pages/information_technology/v_1_6.shtml

Healthcare: UNC School of Medicine & Healthcare Clinic

http://www.med.unc.edu/security/hipaa/documents/SOM%20Remote%20Access%20Policy%202009%20Final.pdf

2. Discuss what the risks and threats are within the Remote Access Domain per the bulleted list provided:
   - Brute force user ID and password attacks
   - Users or employees unaware of the risks, threats, and dangers of the Internet and shared Wi-Fi or broadband Internet access
   - Multiple access attempts and login retries
   - Unauthorized access to IT systems, applications, and data
   - Privacy data or confidential data is compromised remotely
   - Data leakage occurs in violation of Data Classification Standard
   - Remote worker's laptop is stolen
   - Remote worker's token device is stolen
   - Remote worker requires access to patient medical records system through public Internet
3. Discuss what organizations can do to mitigate the risks and threats identified within the Remote Access Domain
4. Complete the Lab #6 – Assessment Worksheet deliverables: Identify Elements of a Remote Access Policy Definition, Create a Remote Access Policy Definition for Multiple Healthcare Clinics
5. Complete the Lab #6 – Assessment Questions & Answers and submit with this lab.

Deliverables

Upon completion of the Lab #6: Define a Remote Access Policy to Support Remote Healthcare Clinics, the students are required to provide the following deliverables:

1. Lab #6 – Assessment Worksheet: Identify Elements of a Remote Access Policy Definition
2. Lab #6 – Assessment Worksheet: Create a Remote Access Policy Definition for Multiple Remote Healthcare Clinics
3. Lab #6 – Assessment Questions & Answers

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #6 that the students must demonstrate:

1. Was the student able to define the scope of a remote access policy as it relates to the Remote Access Domain? – [**20%**]
2. Was the student able to identify the key elements of remote access policy within an organization as part of an overall security management framework? – [**20%**]
3. Was the student able to align the remote access policy with the organization's goals for compliance? – [**20%**]
4. Was the student able to mitigate common risks and threats found within the Remote Access Domain with proper security controls and countermeasures as defined in the remote access policy definition? - [**20%**]
5. Was the student able to create a remote access policy definition incorporating a policy statement, standards, procedures, and guidelines? – [**20%**]

Lab #6 – Assessment Worksheet

Elements of a Remote Access Domain Policy

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

For each of the identified risks and threats within the Remote Access Domain, identify a security control or security countermeasure that can help mitigate the risk or threat. These security controls or security countermeasures will become the basis of the scope of the Remote Access Domain Policy definition to help mitigate the risks and threats commonly found within the Remote Access Domain.

Remote Access Domain Risks & Threats	**Risk Mitigation Tactic/Solution**
Brute force user ID and password attacks	
Multiple login retries and access control attacks	
Unauthorized remote access to IT systems, applications, and data	
Privacy data or confidential data is compromised remotely	
Data leakage in violation of existing Data Classification Standards	

Remote Access Domain Risks & Threats	**Risk Mitigation Tactic/Solution**
Mobile worker laptop is stolen	
Mobile worker token or other lost or stolen authentication device	
Remote worker requires remote access to medical patient online system through the public Internet	
Users and employees are unaware of the risks and threats caused by the public Internet	

Lab #6 – Assessment Worksheet

Define a Remote Access Policy to Support Remote Healthcare Clinics

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

In this lab, you are to create an organization-wide Remote Access Policy for a mock organization under a recent compliance law. Here is your scenario:

- Regional ABC Healthcare Provider with multiple remote, healthcare branches and locations throughout the region
- Online access to patients' medical records through the public Internet is required for remote nurses and hospices providing in-home medical services
- Online access to patients' medical records from remote clinics is done through SSL VPN secure web application front-end through the public Internet
- The organization wants to be in compliance with HIPAA and IT security best practices regarding remote access through the public Internet in the Remote Access Domain
- The organization wants to monitor and control the use of remote access by implementing system logging and VPN connections
- The organization wants to implement a security awareness & training policy mandating that all new hires and existing employees obtain remote access security training. Policy definition to include HIPAA and ePHI (electronic personal healthcare information) security requirements and a mandate for annual security awareness training for all remote or mobile employees

Instructions

Using Microsoft Word, create a Remote Access Policy Definition capturing the elements of the policy as defined in the Lab #6 – Assessment Worksheet. Use the following policy template for the creation of your Remote Access Policy definition for a regional healthcare provider with remote medical clinics.

ABC Healthcare Provider

Remote Access Policy for Remote Workers & Medical Clinics

Policy Statement

{Insert policy verbiage here}

Purpose/Objectives

{Insert purpose of the policy as well as the objectives – bulleted list of the policy definition}

Scope

{Define this policy's scope and whom it covers.

Which of the seven domains of a typical IT infrastructure are impacted?

What elements or IT assets or organization-owned assets are within the scope of this policy?}

Standards

{Does this policy point to any hardware, software, or configuration standards? If so, list them here, and explain the relationship of this policy to these standards. In this case, Remote Access Domain standards should be referenced such as encryption standards, SSL VPN standards, – make any necessary assumptions.}

Procedures

{Explain how you intend to implement this policy organization-wide and how you intend to deliver the annual or on-going security awareness training for remote workers and mobile employees.}

Guidelines

{Explain any road blocks or implementation issues that you must address in this section and how you will overcome them per defined policy guidelines.}

Note: Your policy document must be no more than 3 pages long.

Lab #6 – Assessment Worksheet

Define a Remote Access Policy to Support Remote Healthcare Clinics

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

This lab presents the risks and threats commonly found in the Remote Access Domain and how the use of the public Internet introduces new challenges regarding security and compliance for organizations. The students created a Remote Access Policy definition specific to a healthcare organization requiring remote access to patients' medical records systems from remote clinics and patient homes from mobile nurses and healthcare providers in the field.

Lab Assessment Questions & Answers

1. What are the biggest risks when using the public Internet as a WAN or transport for remote access to your organization's IT infrastructure?

2. Why does this mock healthcare organization need to define a Remote Access Policy to properly implement remote access through the public Internet?

3. What is the relationship between an Acceptable Use Policy (AUP) and a Security Awareness & Training Policy?

4. One of the major prerequisites for this scenario was the requirement to support nurses and healthcare professionals that are mobile and who visit patients in their homes. Another requirement was for remote clinics to access a shared patient medical records system via a web browser. Which type of secure remote VPN solution is recommended for these two types of remote access?

5. When trying to combat unauthorized access and login attempts to IT systems and applications, what is needed within the LAN-to-WAN Domain to monitor and alarm on unauthorized login attempts to the organization's IT infrastructure?

6. Why is it important to mobile workers and users about the risks, threats, and vulnerabilities when conducting remote access through the public Internet?

7. Why should social engineering be included in security awareness training?

8. Which domain (not the Remote Access Domain) throughout the seven domains of a typical IT infrastructure supports remote access connectivity for users and mobile workers needing to connect to the organization's IT infrastructure?

9. Where are the implementation instructions defined in a Remote Access Policy definition? Does this section describe how to support the two different remote access users and requirements as described in this scenario?

10. A remote clinic has a requirement to upload ePHI data from the clinic to the organization's IT infrastructure on a daily basis in a batch-processing format. How should this remote access requirement be handled within or outside of this Remote Access Policy definition?

11. Why is a remote access policy definition a best practice for handling remote employees and authorized users that require remote access from home or on business trips?

12. Why is it a best practice of a remote access policy definition to require employees and users to fill in a separate VPN remote access authorization form?

13. Why is it important to align standards, procedures, and guidelines for a remote access policy definition?

14. What security controls, monitoring, and logging should be enabled for remote VPN access and users?

15. Should an organization mention that they will be monitoring and logging remote access use in their Remote Access Policy Definition?

Laboratory #7

Lab #7: Identify Necessary Policies for Business Continuity – BIA & Recovery Time Objectives

Learning Objectives and Outcomes

Upon completing this lab, students will be able to complete the following tasks:

- Identify the major elements of a Business Continuity Plan (BCP)
- Align the major elements of a Business Continuity Plan with required policy definitions
- Review the results of a qualitative Business Impact Analysis (BIA) for a mock organization
- Review the results of defined Recovery Time Objectives (RTOs) for mission-critical business functions and applications
- Create a BCP policy defining an organization's prioritized business functions from the BIA with assigned RTOs

Required Setup and Tools

This is a paper-based lab. Internet access and the student's Microsoft Office applications are needed to perform this lab.

The following summarizes the setup, configuration, and equipment needed to perform Lab #7:

1. Standard onsite student workstation must have the following software applications loaded and Internet access to perform this lab:
    a. Microsoft Office 2007 or higher
    b. Adobe PDF reader
    c. Internet access

Recommended Procedures

Lab #7 – Student Steps

The following represents the steps that students need to follow for this lab:

1. Review the sample BCP outline provided with this lab
2. Participate in class discussions on the sample BCP outline. Note the difference between Part 1 and Part 2 and where BCP policy definitions are required within Part 1

3. Participate in class discussions on the sample BIA report. Take notice of the prioritization of the mission-critical business functions from the Lab #7 – Assessment Worksheet – BIA
4. Identify which IT systems and applications are impacted by the prioritization of mission critical business functions in the BIA
5. Review these BIA/BCP metrics and incorporate into the BCP Policy Definition:

   Recovery Time Objective (RTO) - defines how quickly IT systems, servers, applications, and access to data services and processes must be operational following some kind of incident, including recovery of applications and data and end-user access to those applications.

   Recovery Point Objective (RPO) - defines the point in time that marks the end of the period during which data can still be recovered using backups, journals or transaction logs.

   The following defines the RTO and RPO metrics for Lab #7 - Identify Necessary Policies for Business Continuity - BIA & Recovery Time Objectives:

Critical:	**RTO: 8 Hours**	**RPO: 0 Hours**
Major:	**RTO: 24 Hours**	**RPO: 8 Hours**
Minor:	**RTO: 1 Week**	**RPO: 3 Days**
None:	**RTO: 1 Month**	**RPO: 7 Days**

6. Review the BCP/BIA Policy Definition template and ask questions if you need clarification.
7. Create a Business Continuity Plan Policy Definition – Business Impact Analysis and reference the RTO and RPO standards in the Standards Section of the policy definition.
8. Answer the Lab #7 – Assessment Questions & Answers

Deliverables

Upon completion of the Lab #7 – Identify Necessary Policies for Business Continuity – BIA & Recovery Time Objectives, students are required to provide the following deliverables as part of this lab:

1. Lab #7 – Assessment Worksheet, Part B – BCP Policy Definition – BIA
2. Lab #7 - Assessment Questions & Answers

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #7 that the student must meet:

1. Was the student able to identify the major elements of a Business Continuity Plan (BCP)? – [**20%**]

2. Was the student able to align the major elements of a Business Continuity Plan to the required policy definitions? – [**20%**]
3. Was the student able to review the results of a qualitative Business Impact Analysis (BIA) for a mock organization? – [**20%**]
4. Was the student able to review the results of defined Recovery Time Objectives (RTOs) for mission-critical business functions and applications? – [**20%**]
5. Was the student able to create a BCP policy defining an organization's prioritized business functions from the BIA with assigned RTOs? – [**20%**]

Lab #7 – Assessment Worksheet

Part A – Sample Business Impact Analysis for an IT Infrastructure

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

When conducting a BIA, you are trying to assess and align the affected IT systems, applications, and resources to their required recovery time objectives (RTOs). The prioritization of the identified mission-critical business functions will define what IT systems, applications, and resources are impacted. The RTO will drive what type of business continuity and recovery steps are needed to maintain IT operations within the specified time frames.

1. Sample BIA with prioritization in (parentheses):

Business Function Or Process	Business Impact Factor	RTO/RPO	IT Systems/Apps Infrastructure Impacts
Internal and external voice communications with customers in real-time			
Internal and external e-mail communications with customers via store and forward messaging			
DNS – for internal and external IP communications			
Internet connectivity for e-mail and store and forward customer service			
Self-service website for customer access to information and personal account information			

e-Commerce site for online customer purchases or scheduling 24x7x365			
Payroll and human resources for employees			
Real-time customer service via website, e-mail, or telephone requires CRM			
Network management and technical support			
Marketing and events			
Sales orders or customer/ student registration			
Remote branch office sales order entry to headquarters			
Voice and e-mail communications to remote branches			
Accounting and finance support: Accts payable, Accts receivable, etc.			

Lab #7 – Assessment Worksheet

Part B – Craft a Business Continuity Plan Policy – Business Impact Analysis

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

When conducting a BIA, you are trying to assess and align the affected IT systems, applications, and resources to their required recovery time objectives (RTOs). The prioritization of the identified mission-critical business functions will define what IT systems, applications, and resources are impacted. The RTO will drive what type of business continuity and recovery steps are needed to maintain IT operations within the specified time frames. In this lab, you are to create a Business Continuity Plan Policy Definition – Business Impact Analysis that points to the RTOs and RPOs for the identified mission-critical business functions of the organization.

Instructions

Using Microsoft Word, create a Business Continuity Plan Policy Definition using the following policy template:

ABC Credit Union

Policy Name

Policy Statement

{Insert policy verbiage here}

Purpose/Objectives

{Insert purpose of the policy as well as the objectives – bulleted list of the policy definition. This should mirror the purpose/objectives of a Business Impact Analysis (BIA).}

Scope

{Define this policy's scope and whom it covers.

Within a BCP outline, what are this policy's scope and boundaries?

What elements or criteria are within the scope of this policy?}

Standards

{Does this policy point to any hardware, software, or configuration standards? In this case, we need to reference the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPO) as standards and metrics within the policy definition itself. List them here and explain the relationship of this policy to these standards.}

Procedures

{Explain how you intend to implement this policy across the entire organization.}

Guidelines

{Explain any road blocks or implementation issues that you must address in this section and how you will overcome them per defined policy guidelines.}

Note: Your policy document may be no more than 3 pages long.

Lab #7 – Assessment Worksheet

Perform a Business Impact Analysis for an IT Infrastructure

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

After completing your Business Continuity Plan Policy Definition, answer the following Lab #7 – Assessment Worksheet questions. These questions are specific to the sample BIA report provided with this lab.

Lab Assessment Questions & Answers

1. Why must an organization define policies for an organization's Business Continuity and Disaster Recovery Plans?

2. When should you define a policy definition and when should you not define one?

3. What is the purpose of having a Business Continuity Plan policy definition that defines the organization's Business Impact Analysis?

4. Why is it critical to align the RTO and RPO standards within the policy definition itself?

5. What is the purpose of a Business Impact Analysis (BIA)?

6. Why is a business impact analysis (BIA) an important first step in defining a business continuity plan (BCP)?

7. How does risk management and risk assessment relate to a business impact analysis for an IT infrastructure?

8. True or False – If the Recovery Point Objective (RPO) metric does not equal the Recovery Time Objective (RTO), you may potentially lose data or not have data backed-up to recover. This represents a gap in potential lost or unrecoverable data.

9. What question should an organization answer annually to update its BCP, BIA, and RTOs and RPOs?

10. Why is it a good idea to have critical documentation recordkeeping defined in a policy definition?

11. From Part A - Sample BIA for an IT Infrastructure Worksheet, which systems, applications, and functions were mission critical to this organization?

12. From Part B – Define a Policy Definition for a BCP/DRP, how did you answer the procedures for how to implement this policy throughout your business?

13. True or False. It is a best practice to define policy definitions for an organization-wide BCP and DRP.

14. True or False. An organization must have a Business Impact Analysis and list of prioritized business functions and operations defined first prior to building a BCP and DRP.

15. Explain how having proper security controls and documented BIA, BCP, and DRP can help organizations reduce their business liability insurance premiums and errors and omissions insurance premiums.

Laboratory #8

Lab #8: Craft a Security or Computer Incident Response Policy – CIRT Response Team

Learning Objectives and Outcomes

Upon completing this lab, students will be able to complete the following tasks:

- Define the purpose of a security or computer incident response team
- Identify the major elements of a security or computer incident response methodology
- Align the roles and responsibilities to elements of a CIRT response team
- Identify critical management, HR, Legal, IT, and information systems security personnel required for the CIRT response team
- Create a CIRT Response Policy Definition that defines the purpose and goal of the CIRT Response Team and the Authority Granted During an Incident

Required Setup and Tools

This is a paper-based lab. Internet access and the student's Microsoft Office applications are needed to perform this lab.

The following summarizes the setup, configuration, and equipment needed to perform Lab #8:

1. Standard onsite student workstation must have the following software applications loaded and Internet access to perform this lab:
   a. Microsoft Office 2007 or higher
   b. Adobe PDF reader
   c. Internet access

Recommended Procedures

Lab #8 – Student Steps

The following presents the steps needed to perform Lab #8 – Create a Security or Computer Incident Response Policy – CIRT Response Team:

1. Review the sample Incident Response Plan outline and discuss the overall purpose and scope of the plan
2. Discuss the goal and purpose of a Security or Computer Incident Response Plan

3. Review the policy definitions that are required with a Security or Computer Incident Response Plan using the sample outline
4. Discuss what organizations can do to mitigate the risks and threats by having a Security or Incident Response Plan and Team
5. Review the 6-step methodology for performing incident response
6. Review the Chain of Custody and integrity of physical evidence in a court of law

   Chain of Custody: The movement and location of physical evidence from the time it is obtained until the time it is presented in court.

7. Discuss the need for a Security or Computer Incident Response Team Policy Definition that addresses the delegation of authority to the CIRT response team members during an incident response emergency
8. Review how to perform Lab #8 – Create a Security or Computer Incident Response Policy – CIRT Response Team
9. Answer the Lab #8 – Assessment Questions & Answers

Deliverables

Upon completion of the Lab #8: Create a Security or Computer Incident Response Policy – CIRT Response Team, the students are required to provide the following deliverables as part of this lab:

1. Lab #8 – Assessment Worksheet – Create an Incident Response Team Policy Definition
2. Lab #8 – Assessment Questions & Answers

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #8 that the students must perform:

1. Was the student able to define the purpose of a security or computer incident response team? – [**20%**]
2. Was the student able to identify the major elements of a security or computer incident response methodology? – [**20%**]
3. Was the student able to align the roles and responsibilities to elements of a CIRT response team? – [**20%**]

4. Was the student able to identify critical management, HR, Legal, IT, and information systems security personnel required for the CIRT response team? – [**20%**]
5. Was the student able to create a CIRT Response Policy Definition that defines the purpose and goal of the CIRT Response Team and the Authority Granted During an Incident? – [**20%**]

Lab #8 – Assessment Worksheet

Craft a Security or Computer Incident Response Policy – CIRT Response Team

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

In this lab, you are to create an organization-wide policy defining and authorizing a Security or Computer Incident Response Team to have full access and authority to all IT systems, applications, data and physical IT assets when a security or other incident occurs. Here is your scenario:

- Regional ABC Credit union/bank with multiple branches and locations throughout the region
- Online banking and use of the Internet is a strength of your bank given limited human resources
- The customer service department is the most critical business function/operation for the organization
- The organization wants to be in compliance with GLBA and IT security best practices regarding employees
- The organization wants to monitor and control the use of the Internet by implementing content filtering
- The organization wants to eliminate personal use of organization owned IT assets and systems
- The organization wants to monitor and control the use of the e-mail system by implementing e-mail security controls
- The organization wants to create a Security or Computer Incident Response Team to deal with security breaches and other incidents if attacked providing full authority for the team to perform whatever activities are needed to maintain Chain of Custody in performing forensics and evidence collection
- The organization wants to implement this policy throughout the organization to provide full authority to the CIRT team members during crisis to all physical facilities, IT assets, IT systems, applications, and data owned by the organization

Instructions

Using Microsoft Word, create a Security or Computer Incident Response Policy granting team members full access and authority to perform forensics and to maintain Chain of Custody for physical evidence containment. Use the following policy template:

ABC Credit Union

Computer Incident Response Team – Access & Authorization Policy

Policy Statement

{Insert policy verbiage here}

Purpose/Objectives

{Insert purpose of the policy as well as the objectives – bulleted list of the policy definition
Define the Security Incident Response Team Members and the Authorization and Authority granted to them during a crisis or securing incident situation.}

Scope

{Define this policy's scope and whom it covers.

Which of the seven domains of a typical IT infrastructure are impacted?

What elements or IT assets or organization-owned assets are within the scope of this policy?

What access and authority are granted to the incident response team members that may be outside of standard protocol?}

Standards

{Does this policy point to any hardware, software, or configuration standards? If so, list them here and explain the relationship of this policy to these standards.}

Procedures

{Explain how you intend to implement this policy across the organization.

Also, define and incorporate the 6-step incident response approach here along with how the Chain of Custody must be maintained throughout any evidence collection process.}

Guidelines

{Explain any road blocks or implementation issues that you must address in this section and how you will overcome them per defined policy guidelines.}

Note: Your policy document must be no more than 3 pages long.

Lab #8 – Assessment Worksheet

Craft a Security or Computer Incident Response Policy – CIRT Response Team

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

In this lab, you are to create an organization-wide policy defining and authorizing a Security or Computer Incident Response Team to have full access and authority to all IT systems, applications, data and physical IT assets when a security or other incident occurs. A review of the 6-step incident response methodology and an outline of a Security or Computer Incident Response Plan was presented. The students also learned about the Chain of Custody and what forensic procedures and protocols must be followed to allow physical evidence to be admissible in a court of law.

Lab Assessment Questions & Answers

1. What are the 6-steps in the incident response methodology?

2. If an organization has no intention of prosecuting a perpetrator or attacker, does it still need an incident response team to handle forensics?

3. Why is it a good idea to include human resources on the Incident Response Management Team?

4. Why is it a good idea to include legal or general counsel in on the Incident Response Management Team?

5. How does an incident response plan and team help reduce risks to the organization?

6. If you are reacting to a malicious software attack such as a virus and its spreading, during which step in the incident response process are you attempting to minimize its spreading?

7. If you cannot cease the spreading, what should you do to protect your non-impacted mission-critical IT infrastructure assets?

8. When a security incident has been declared, does a PC technician have full access and authority to seize and confiscate a vice president's laptop computer? Why or why not?

9. Which step in the incident response methodology should you document the steps and procedures to replicate the solution?

10. Why is a port mortem review of an incident the most important step in the incident response methodology?

11. Why is a policy definition required for Computer Security Incident Response Team?

12. What is the purpose of having well documented policies as it relates to the CSIRT function and distinguishing events versus an incident?

13. Which 4 steps in the incident handling process requires the Daubert Standard for Chain-of-Custody evidence collection?

14. Why is syslog and audit trail event correlation a critical application and tool for CSIRT incident response handling?

15. Why is File Integrity Monitoring alerts/alarms a critical application and tool for the CSIRT incident response identification?

Laboratory #9

Lab #9: Assess and Audit an Existing IT Security Policy Framework Definition

Learning Objectives and Outcomes

Upon completing this lab, students will be able to complete the following tasks:

- Identify risks, threats, and vulnerabilities in the seven domains of a typical IT infrastructure
- Review existing IT security policies as part of a policy framework definition
- Align IT security policies throughout the seven domains of a typical IT infrastructure as part of a layered security strategy
- Identify gaps in the IT security policy framework definition
- Recommend other IT security policies that can help mitigate all known risks, threats, and vulnerabilities throughout the seven domains of a typical IT infrastructure

Required Setup and Tools

This is a paper-based lab. Internet access and the student's Microsoft Office applications are needed to perform this lab.

The following summarizes the setup, configuration, and equipment needed to perform Lab #9:

1. Standard onsite student workstation must have the following software applications loaded and Internet access to perform this lab:
    a. Microsoft Office 2007 or higher
    b. Adobe PDF reader
    c. Internet access

Recommended Procedures

Lab #9 – Student Steps:

The following represents the steps that must be followed for Lab #9 – Assess and Audit an Existing IT Security Policy Framework Definition:

1. Discuss the seven domains of a typical IT infrastructure
2. Discuss what risks, threats, and vulnerabilities are commonly found throughout the seven domains of a typical IT infrastructure
3. Review the Lab #9 – Assessment Worksheet, Part A – Risks, Threats, & Vulnerabilities Found in a Typical IT Infrastructure

4. Review the sample IT security policy framework provided in Lab #9 – Assessment Worksheet, Part B – Identify Gaps in a Given IT Security Policy Framework Definition
5. Review the list of IT security policy definitions that can help fill identified gaps in the IT security policy framework definition
6. Complete Lab #9 – Assessment Worksheet, Part B
7. Answer the Lab #9 – Assessment Questions & Answers

Deliverables

Upon completion of Lab #9: Assess and Audit an Existing IT Security Policy Framework Definition, students are required to provide the following deliverables as part of this lab:

1. Lab #9 – Assessment Worksheet, Part B – IT Security Policy Framework Gap Recommendations
2. Lab #9 – Assessment Worksheet questions and answers

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #9 – Assess and Audit an Existing IT Security Policy Framework Definition that the students must perform:

1. Was the student able to identify risks, threats, and vulnerabilities in the seven domains of a typical IT infrastructure? – [**20%**]
2. Was the student able to review existing IT security policies as part of a policy framework definition? – [**20%**]
3. Was the student able to align IT security policies throughout the seven domains of a typical IT infrastructure as part of a layered security strategy? – [**20%**]
4. Was the student able to identify gaps in the IT security policy framework definition? – [**20%**]
5. Was the student able to recommend other IT security policies that can help mitigate all known risks, threats, and vulnerabilities throughout the seven domains of a typical IT infrastructure? – [**20%**]

Lab #9 – Assessment Worksheet

Part A – Risks, Threats, & Vulnerabilities in the Seven Domains of a Typical IT Infrastructure

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

For each of the identified risks, threats, and vulnerabilities – review the following chart to determine which domain from the seven domains of a typical IT infrastructure is impacted.

Risk – Threat – Vulnerability	**Primary Domain Impacted**
Unauthorized access from public Internet	
User destroys data in application and deletes all files	
Hacker penetrates your IT infrastructure and gains access to your internal network	
Intra-office employee romance gone bad	
Fire destroys primary data center	
Communication circuit outages	
Workstation OS has a known software vulnerability	
Unauthorized access to organization owned Workstations	
Loss of production data	
Denial of service attack on organization e-mail Server	
Remote communications from home office	

Risk – Threat – Vulnerability	**Primary Domain Impacted**
LAN server OS has a known software vulnerability	
User downloads an unknown e –mail attachment	
Workstation browser has software vulnerability	
Service provider has a major network outage	
Weak ingress/egress traffic filtering degrades Performance	
User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers	
VPN tunneling between remote computer and ingress/egress router	
WLAN access points are needed for LAN connectivity within a warehouse	
Need to prevent rogue users from unauthorized WLAN access	

Lab #9 – Assessment Worksheet

Part B – Sample IT Security Policy Framework Definition

Course Name: ____

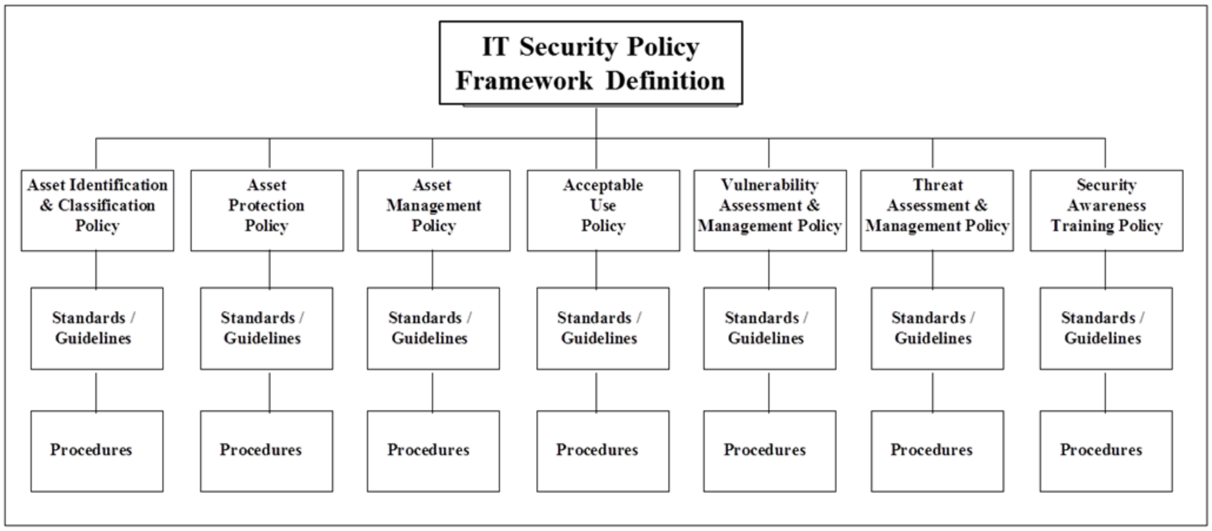
Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

Given the following IT security policy framework definition, specify which policy probably can cover the identified risk, threat, or vulnerability. If there is none, then identify that as a gap. Insert your recommendation for an IT security policy that can eliminate the gap.


IT Security Policy Framework Definition
Asset Identification & Classification Policy
Asset Protection Policy
Asset Management Policy
Acceptable Use Policy
Vulnerability Assessment & Management Policy
Threat Assessment & Management Policy
Security Awareness Training Policy
Standards / Guidelines
Procedures

Risk – Threat – Vulnerability	**IT Security Policy Definition**
Unauthorized access from public Internet	
User destroys data in application and deletes all files	
Hacker penetrates your IT infrastructure and gains access to your internal network	
Intra-office employee romance gone bad	
Fire destroys primary data center	
Communication circuit outages	
Workstation OS has a known software vulnerability	
Unauthorized access to organization owned Workstations	
Loss of production data	
Denial of service attack on organization e-mail server	
Remote communications from home office	
LAN server OS has a known software vulnerability	
User downloads an unknown e –mail attachment	
Workstation browser has software vulnerability	
Service provider has a major network outage	
Weak ingress/egress traffic filtering degrades performance	
User inserts CDs and USB hard drives with personal photos, music, and videos	

Risk – Threat – Vulnerability	**IT Security Policy Definition**
VPN tunneling between remote computer and ingress/egress router	
WLAN access points are needed for LAN connectivity within a warehouse	
Need to prevent rogue users from unauthorized WLAN access	

For each identified gap, insert a recommendation for an IT security policy to help mitigate the risk, threat or vulnerability:

Lab #9 – Assessment Worksheet

Assess and Audit an Existing IT Security Policy Framework Definition

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

In this lab, you were presented with a list of common risks, threats, and vulnerabilities commonly found in the seven domains of a typical IT infrastructure. The students were presented with a sample IT security policy framework definition. Most of these policy definitions cover the identified risks, threats, and vulnerabilities. Some have gaps that must be mitigated with recommendations for other IT security policies. This lab demonstrated how to assess and audit an IT security policy framework definition by performing a gap analysis with remediation.

Lab Assessment Questions & Answers

1. What is the purpose of having a policy framework definition as opposed to individual policies?

2. When should you use a policy definition as a means of risk mitigation and element of a layered security strategy?

3. In your gap analysis of the IT security policy framework definition provided, which policy definition was missing for all access to various IT systems, applications, and data throughout the scenario?

4. Do you need policies for your telecommunication and Internet service providers?

5. Which policy definitions from the list provided in Lab #9 – Part B helps optimize performance of an organization’s Internet connection?

6. What is the purpose of a Vulnerability Assessment & Management Policy for an IT infrastructure?

7. Which policy definition helps achieve availability goals for data recovery when data is lost or corrupted?

8. Which policy definitions reference a Data Classification Standard and use of cryptography for confidentiality purposes?

9. Which policy definitions from the sample IT security policy framework definition mitigate risk in the User Domain?

10. Which policy definition from the sample IT security policy framework definition mitigates risk in the LAN-to-WAN Domain?

11. How does an IT security policy framework make it easier to monitor and enforce throughout an organization?

12. Which policy definition requires an organization to list its mission critical business operations and functions and the accompanying IT systems, applications, and databases that support it?

13. Why is it common to find a Business Continuity Plan (BCP) Policy Definition and a Computer Security Incident Response Team (CSIRT) Policy Definition?

14. True or False. A Data Classification Standard will define whether or not you need to encrypt the data while residing in a database.

15. True or False. Your upstream Internet Service Provider must be part of your Denial of Service / Distributed Denial of Service risk mitigation strategy at the LAN-to-WAN Domain's Internet ingress/egress. This is best defined in a policy definition for Internet ingress/egress availability.

Laboratory #10

Lab #10: Align an IT Security Policy Framework to the 7 Domains of a Typical IT Infrastructure

Learning Objectives and Outcomes

Upon completing this lab, students will be able to complete the following tasks:

- Define the policy statements for various IT security policy definitions
- Identify key elements of IT security policy definitions as part of a framework definition
- Reference key standards and requirements for IT security policy definitions needed for a framework definition
- Incorporate procedures and guidelines into an IT security policy definition example needed to fill a gap in a framework definition
- Create an IT security policy definition for a risk mitigation solution for an IT security policy framework definition

Required Setup and Tools

This is a paper-based lab. Internet access and the student's Microsoft Office applications are needed to perform this lab.

The following summarizes the setup, configuration, and equipment needed to perform Lab #10:

1. Standard onsite student workstation must have the following software applications loaded and Internet access to perform this lab:
    a. Microsoft Office 2007 or higher
    b. Adobe PDF reader
    c. Internet access

Recommended Procedures

Lab #10 – Student Steps

The following presents the steps needed to perform Lab #10 – Align an IT Security Policy Framework to the Seven Domains of a Typical IT Infrastructure:

1. Review your Lab #9, Part B deliverables and IT security policy framework definition

2. Review the gap analysis performed and which policy definitions you selected to fill those identified gaps in the overall IT security policy framework definition, Lab #9, Part B – Policy Framework Definition Gap Analysis
3. Review Lab #10, Part A – Align an IT Security Policy Framework to the Seven Domains of a Typical IT Infrastructure – Create Policy Statements
4. Define policy definition statements for the list of policy definitions in Lab #10, Part A – Align an IT Security Policy Framework to the Seven Domains of a Typical IT Infrastructure – Create Policy Statements
5. Review the key elements of the IT security policy template in Lab #10, Part B
6. Reference key standards and requirements for IT security policy definitions needed for a framework definition to cover all gaps
7. Incorporate procedures and guidelines into an IT security policy definition example needed to fill a gap in a framework definition
8. Create an IT security policy definition for one of the selected policy definitions to mitigate risk for an identified gap in the security policy framework definition
9. Answer the Lab #10 – Assessment Worksheets

Deliverables

1. Lab #10 – Assessment Worksheet, Part A – Policy Statements (This deliverable is required in lieu of submitting Lab Assessment Questions)
2. Lab #10 – Assessment Worksheet, Part B – Craft an IT Security Policy Definition

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #10: Align an IT Security Policy Framework to the Seven Domains of a Typical IT Infrastructure that the student must meet:

1. Was the student able to define the policy statements for various IT security policy definitions? – [**20%**]
2. Was the student able to identify key elements of IT security policy definitions as part of a framework definition? – [**20%**]
3. Was the student able to reference key standards and requirements for IT security policy definitions needed for a framework definition? – [**20%**]

4. Was the student able to incorporate procedures and guidelines into an IT security policy definition example needed to fill a gap in a framework definition? – [**20%**]
5. Was the student able to craft an IT security policy definition for a risk mitigation solution for an IT security policy framework definition? – [**20%**]

Lab #10 – Assessment Worksheet

Part A – Policy Statement Definitions

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

Create a policy statement that defines how these policies mitigate the risk, threat, or vulnerability as indicated in the gap analysis matrix below for each of the gaps identified and recommended policy definitions.

Risk – Threat – Vulnerability	**IT Security Policy Definition**
Unauthorized access from public Internet	
User destroys data in application and deletes all files	
Hacker penetrates your IT infrastructure and gains access to your internal network	
Intra-office employee romance gone bad	
Fire destroys primary data center	
Communication circuit outages	
Workstation OS has a known software vulnerability	
Unauthorized access to organization owned workstations	
Loss of production data	
Denial of service attack on organization e-mail server	

Risk – Threat – Vulnerability	**IT Security Policy Definition**
Remote communications from home office	
LAN server OS has a known software vulnerability	
User downloads an unknown e –mail attachment	
Workstation browser has software vulnerability	
Service provider has a major network outage	
Weak ingress/egress traffic filtering degrades performance	
User inserts CDs and USB hard drives with personal photos, music, and videos	
VPN tunneling between remote computer and ingress/egress router	
WLAN access points are needed for LAN connectivity within a warehouse	
Need to prevent rogue users from unauthorized WLAN access	

For each identified gap, insert a recommendation for an IT security policy to help mitigate the risk, threat or vulnerability:

Define a policy statement (2 or 3 sentences max) for each of the following policy definitions that are needed to remediate the identified gap analysis for the IT security policy framework:

1. Access Control Policy Definition

2. Business Continuity – Business Impact Analysis (BIA) Policy Definition

3. Business Continuity & Disaster Recovery Policy Definition

4. Data Classification Standard & Encryption Policy Definition

5. Internet Ingress/Egress Traffic & Web Content Filter Policy Definition

6. Production Data Back-up Policy Definition

7. Remote Access VPN Policy Definition

8. WAN Service Availability Policy Definition

9. Internet Ingress/Egress Availability (DoS/DDoS) Policy Definition

10. Wireless LAN Access Control & Authentication Policy Definition

11. Internet & E-Mail Acceptable Use Policy Definition

12. Asset Protection Policy Definition

13. Audit & Monitoring Policy Definition

14. Computer Security Incident Response Team (CSIRT) Policy Definition

15. Security Awareness Training Policy Definition

Lab #10 – Assessment Worksheet

Part B – Craft an IT Security Policy Definition

Course Name: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

In this lab, you are to create an organization-wide policy defining from the list provided in Lab #10 – Part A. Here is your scenario:

- Regional ABC Credit union/bank with multiple branches and locations throughout the region
- Online banking and use of the Internet is a strength of your bank given limited human resources
- The customer service department is the most critical business function/operation for the organization
- The organization wants to be in compliance with GLBA and IT security best practices regarding employees
- The organization wants to monitor and control use of the Internet by implementing content filtering
- The organization wants to eliminate personal use of organization owned IT assets and systems
- The organization wants to monitor and control use of the e-mail system by implementing e-mail security controls
- The organization wants to fill the gaps identified in the IT security policy framework definition
- Select one of the identified policy definitions from the gap analysis and define an entire IT security policy definition for this needed policy definition

Instructions

Using Microsoft Word, create an IT security policy definition of your choice to mitigate the risks, threats, and vulnerabilities identified in the gap analysis. Use the following policy template:

ABC Credit Union

{ Insert Policy Definition Name Here }

Policy Statement

{Insert policy verbiage here from Lab #10, Part A for your selected IT security policy definition}

Purpose/Objectives

{Insert purpose of the policy as well as the objectives – bulleted list of the policy definition.

Be sure to explain how this policy definition fills the identified gap in the overall IT security policy framework definition and how it mitigates the risks, threats, and vulnerabilities identified.}

Scope

{Define this policy and its scope and whom it covers.

Which of the Seven Domains of a typical IT infrastructure are impacted?

What elements or IT assets or organization-owned assets are within the scope of this policy?

Etc.?}

Standards

{Does this policy point to any hardware, software, or configuration standards? If so, list them here and explain the relationship of this policy to these standards.}

Procedures

{Explain in this section how you intend on implementing this policy organization-wide.}

Guidelines

{Explain in this section any roadblocks or implementation issues that you must address in this section and how you will overcome them as per defined policy guidelines.}

Note: Your policy document must be no more than 3 pages long.