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: IAP301

Student Name: Nguyễn Quốc Vượng

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	Acceptable Use Policy
User destroys data in application and deletes all files	Asset Protection Policy
Hacker penetrates your IT infrastructure and gains access to your internal network	Vulnerability Assessment & Management Policy
Intra-office employee romance gone bad	Asset Protection Policy
Fire destroys primary data center	Threat Assessment & Management Policy
Communication circuit outages	Asset Protection Policy
Workstation OS has a known software vulnerability	Asset Protection Policy
Unauthorized access to organization owned workstations	Security Awareness Training Policy
Loss of production data	Asset Protection Policy
Denial of service attack on organization e-mail server	Threat Assessment & Management Policy

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

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
   This policy defines the process for granting and revoking access to IT systems, applications, and data, based on job roles, responsibilities, and the principle of least privilege, to prevent unauthorized access

2. Business Continuity – Business Impact Analysis (BIA) Policy Definition
   This policy defines the process for identifying, prioritizing, and documenting critical business operations and functions, as well as the IT systems, applications, and data that support them, to enable effective business continuity planning

3. Business Continuity & Disaster Recovery Policy Definition
   This policy defines the process for developing and maintaining a comprehensive business continuity and disaster recovery plan, to ensure continuity of critical business operations and minimize the impact of disasters on IT systems and data

4. Data Classification Standard & Encryption Policy Definition
   This policy defines the standards and procedures for classifying data according to its sensitivity level, and the encryption methods required to protect it, to ensure the confidentiality, integrity, and availability of sensitive data

5. Internet Ingress/Egress Traffic & Web Content Filter Policy Definition
   This policy defines the standards and procedures for filtering Internet traffic, blocking access to known malicious websites, and controlling access to web content, to prevent unauthorized access, malware infections, and data breaches

6. Production Data Back-up Policy Definition
   This policy defines the standards and procedures for backing up critical production data, storing backup data offsite, and testing the recovery process, to ensure timely and reliable data recovery in case of data loss or corruption

7. Remote Access VPN Policy Definition
   This policy defines the standards and procedures for granting and securing remote access to IT systems, applications, and data, using VPN technology, to enable remote work while maintaining security and confidentiality

8. WAN Service Availability Policy Definition

   This policy defines the standards and procedures for ensuring the availability and reliability of WAN services, through redundancy, failover, and monitoring, to minimize downtime and disruption of critical business operations

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

   This policy defines the standards and procedures for protecting IT systems and networks from denial-of-service and distributed denial-of-service attacks, through the use of anti-DDoS technologies, network segmentation, and incident response planning, to ensure uninterrupted availability of critical IT services

10. Wireless LAN Access Control & Authentication Policy Definition

    This policy defines the standards and procedures for controlling and authenticating access to wireless LANs, through strong passwords, encryption, and access controls, to prevent unauthorized access and data breaches

11. Internet & E-Mail Acceptable Use Policy Definition

    This policy defines the standards and procedures for acceptable use of the Internet and e-mail systems, to prevent misuse, abuse, and security breaches, and to promote productivity and ethical behavior

12. Asset Protection Policy Definition

    This policy defines the standards and procedures for protecting physical and digital assets, such as hardware, software, data, and intellectual property, through physical security measures, access controls, and encryption, to prevent theft, loss, or damage

13. Audit & Monitoring Policy Definition

This policy defines the standards and procedures for monitoring and auditing IT systems, applications, and data, to detect security incidents, policy violations, and performance issues, and to ensure compliance with regulatory and industry standards

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

This policy defines the standards and procedures for responding to computer security incidents, such as malware infections, data breaches, and denial-of-service attacks, through a coordinated and documented incident response plan, to minimize the impact and scope of the incident

15. Security Awareness Training Policy Definition

This policy defines the standards and procedures for providing security awareness training to all employees, contractors, and third-party vendors, to promote a culture of security, awareness of threats and vulnerabilities, and adherence to security policies and procedures

Lab #10 – Assessment Worksheet

Part B – Craft an IT Security Policy Definition

Course Name: IAP301

Student Name: Nguyễn Quốc Vượng

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 ABC Credit Union recognizes the importance of protecting its sensitive data from unauthorized access or disclosure via email. This policy establishes standards for the proper use of email, email security controls, and the responsibilities of employees and third-party contractors

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

Purpose/Objectives This policy establishes an email security program to address risks identified in the gap analysis. It aims to protect sensitive data, ensure GLBA compliance, define security controls, outline responsibilities for employees and contractors, and promote responsible email use

{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 This policy applies to all ABC Credit Union employees and third-party contractors using organization-owned IT assets, systems, or email services. It affects the User, Workstation, and LAN Domains, covering all assets involved in email communications

{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 This policy mandates compliance with all relevant email security standards and regulations, including GLBA, HIPAA, PCI DSS, and ISO 27001/2

{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 ABC Credit Union will ensure compliance with this policy by regularly monitoring email activity, using spam filters and virus scanners, encrypting sensitive email information, setting guidelines for proper email use, and training employees and contractors on email security best practices

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

Guidelines ABC Credit Union recognizes potential challenges in implementing this policy, such as employee resistance and technical issues. To address these, it will set clear email use guidelines, provide comprehensive training, and allocate resources and support for successful implementation

{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.