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

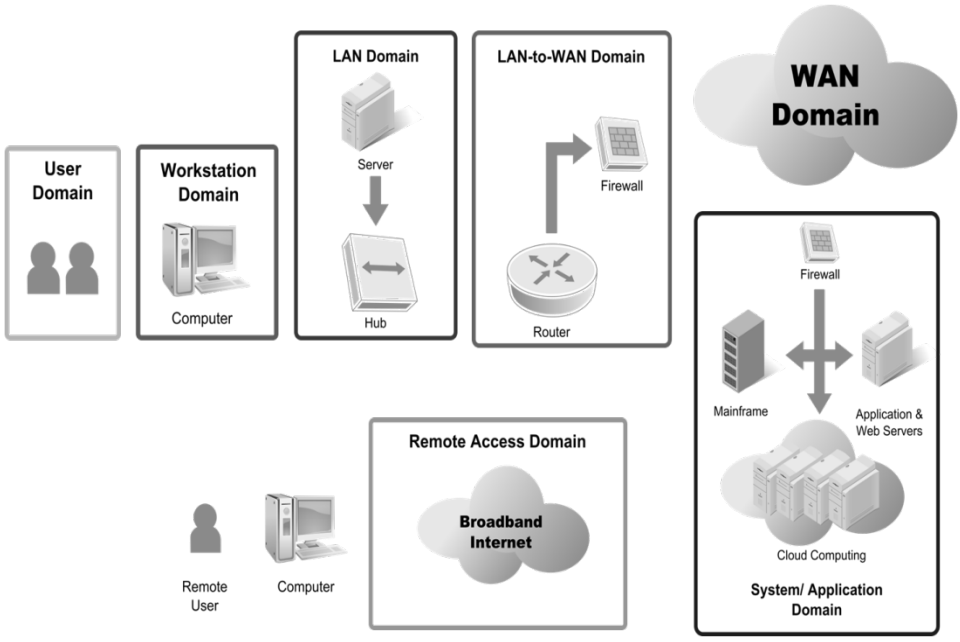

Figure 1 – Seven Domains of a Typical IT Infrastructure

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?