Lab #1:

Craft an Organization-Wide Security Management Policy for Acceptable Use

PART A: Organization-Wide Security Management AUP Worksheet

Course Name: Policy Development in Information Assurance (IAP301)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 09/09/2023

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 Acceptable Use Policy

Policy Statement
This policy defines the acceptable use of information technology (IT) resources at ABC Credit Union. It applies to all employees, contractors, and other third-party users who access or use IT resources owned or operated by ABC Credit Union.

Purpose/Objectives

- Protect the confidentiality, integrity, and availability of ABC Credit Union's IT resources.
- Comply with applicable laws and regulations.

- Promote the efficient and effective use of IT resources.
- Protect the privacy of customer data.

Scope

- Computers
- Laptops
- Mobile devices
- Network infrastructure
- Software
- Data

Standards

- The National Institute of Standards and Technology (NIST) Cybersecurity Framework
- The Payment Card Industry Data Security Standard (PCI DSS)
- The Gramm-Leach-Bliley Act (GLBA)

Procedures

- Train all employees, contractors, and other third-party users on the policy.
- Monitor IT usage for compliance with the policy.
- Investigate and take appropriate action for violations of the policy.

Guidelines

- Employees should only use IT resources for business purposes.
- Employees should not install unauthorized software on their computers.
- Employees should not share their passwords with others.
- Employees should report any security breaches or incidents immediately.
- Violations of this policy may result in disciplinary action, up to and including termination of employment.

This policy is subject to change at any time.

Effective Date: September 9th, 2023

Approvals

Approved by: CEO, ABC Credit Union
Date: September 9th, 2023

PART B: Craft an Organization-Wide Security Management Policy for Acceptable Use

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?

Answer:

In the case of ABC Credit Union/Bank, the following additional risks and threats from the User Domain should be considered:

- Financial fraud: This is the intentional deception or misrepresentation that is used to gain an unfair or unlawful advantage. Financial fraud can be committed by employees, customers, or third-party vendors.
- Data privacy violations: This is the unauthorized access, collection, use, or disclosure of personal information. Data privacy violations can have a significant impact on customers, such as financial losses, identity theft, and reputational damage.
- Regulatory compliance: ABC Credit Union/Bank is subject to a number of regulations, such as the Gramm-Leach-Bliley Act (GLBA) and the Payment Card Industry Data Security Standard (PCI DSS). These regulations require ABC Credit Union/Bank to take steps to protect the confidentiality, integrity, and availability of customer data.

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

Answer:

Organizations have acceptable use policies (AUPs) for a number of reasons, including:

- To protect their IT infrastructure and data: AUPs can help to prevent unauthorized access to IT systems and data, as well as the spread of malware and other malicious content.
- To comply with regulations: Many organizations are subject to regulations that require them to have an AUP in place. For example, financial institutions are required to have an AUP in place to comply with the Gramm-Leach-Bliley Act (GLBA).
- To protect their reputation: AUPs can help to protect an organization's reputation by deterring employees from engaging in inappropriate or illegal activities using the organization's IT resources.
- To provide guidance to employees: AUPs can provide employees with clear guidance on what is and is not acceptable use of the organization's IT resources. This can help to prevent accidental or unintentional misuse of these resources.
- To establish a framework for disciplinary action: AUPs can help to establish a framework for disciplinary action in the event of a violation. This can help to ensure that employees are held accountable for their actions.
- An AUP is an important part of an organization's overall information security program. By having a clear and concise AUP in place, organizations can help to protect their IT infrastructure, data, and reputation.

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

Answer:

Yes, internet use and e-mail use policies can be covered in an Acceptable Use Policy (AUP). In fact, these are two of the most important topics that should be addressed in an AUP.

The internet use policy should address the following topics:

- What websites are allowed and prohibited.
- What types of activities are allowed and prohibited, such as downloading files, streaming videos, and using social media.
- How employees should protect their privacy when using the internet.
- How to deal with spam and phishing emails.

The e-mail use policy should address the following topics:

- What types of emails are allowed and prohibited, such as personal emails and attachments.
- How employees should use e-mail for business purposes.
- How to deal with spam and phishing emails.
- How to protect sensitive information in e-mails.

4. Do compliance laws such as HIPPA or GLBA play a role in AUP definition?
Answer:
Yes, compliance laws such as HIPAA or GLBA play a role in the definition of an Acceptable Use Policy (AUP). These laws impose specific requirements on how organizations must protect certain types of information, such as personal health information (PHI) or financial information. As a result, organizations that are subject to these laws must ensure that their AUPs are compliant with the relevant requirements. The Gramm-Leach-Bliley Act (GLBA) is a similar law that applies to financial institutions. The GLBA requires financial institutions to protect the privacy of customer information, including financial account information. As part of their compliance efforts, financial institutions must also have an AUP in place that addresses the use of customer information on their IT systems.

5. Why is an acceptable use policy not a failsafe means of mitigating risks and threats within the User Domain?
Answer:
An Acceptable Use Policy (AUP) is a document that outlines the rules and regulations for using an organization's IT resources. It is an important tool for mitigating risks and threats within the User Domain, but it is not a failsafe.

Here are some of the reasons why an AUP is not a failsafe:

- People make mistakes. Even the most well-written AUP cannot prevent people from making mistakes, such as clicking on a malicious link in an email or forgetting to change their password.
- People can be malicious. Some people may intentionally violate the AUP, even if they know the consequences. This could be due to a number of factors, such as financial gain, revenge, or ideology.
- Technology is constantly evolving. AUPs can quickly become outdated as new technologies emerge. This can create gaps in security that can be exploited by attackers.
- AUPs are not always enforced. Even if an AUP is well-written and enforced, there is no guarantee that it will be effective. This is because people may not be aware of the AUP, or they may not believe that they will be caught if they violate it.

- Despite these limitations, AUPs are still an important tool for mitigating risks and threats within the User Domain. By understanding the limitations of AUPs, organizations can take steps to improve their effectiveness.

6. Will the AUP apply to all levels of the organization, why or why not?
Answer:
Yes, an Acceptable Use Policy (AUP) should apply to all levels of an organization. This is because all users of an organization's IT resources should be expected to use them responsibly, irrespective of their role, title, and position.

The AUP should cover all aspects of the use of IT resources, including:

- Personal use of IT resources: Employees should not use IT resources for personal purposes, such as checking social media or shopping online.
- Prohibited activities: Employees should not engage in prohibited activities, such as downloading illegal content or sending spam emails.
- Security measures: Employees should take appropriate security measures to protect IT resources, such as using strong passwords and keeping their software up to date.
- Reporting of security incidents: Employees should report any security incidents they become aware of to the appropriate authorities.

7. When should this policy be implemented and how?
Answer:
An Acceptable Use Policy (AUP) should be implemented as soon as possible after it is created. This will help to ensure that all users of the organization's IT resources are aware of the rules and regulations for using these resources.

Here are some of the steps that can be taken to implement an AUP:

- Get buy-in from senior management. The AUP should be supported by senior management in order to be effective.
- Educate employees about the AUP. Employees should be given training on the AUP so that they understand the rules and regulations for using IT resources.
- Monitor employee activity. The organization's IT staff should monitor employee activity to ensure that the AUP is being followed.
- Enforce the AUP consistently. Employees who violate the AUP should be disciplined consistently, regardless of their role or position in the organization.
- By following these steps, organizations can ensure that their AUPs are implemented effectively and that all users of IT resources are aware of the rules and regulations for using these resources.

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

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

An organization wants to align its policies with the existing compliance requirements because it helps them:

- Comply with regulations: Many organizations are subject to regulations that require them to have certain policies and procedures in place. For example, financial institutions are required to comply with the Gramm-Leach-Bliley Act (GLBA), which requires them to have a privacy policy in place. By aligning their policies with the existing compliance requirements, organizations can help to ensure that they are in compliance with the law.
- Protect their reputation: A good reputation is essential for any organization. By aligning their policies with the existing compliance requirements, organizations can help to protect their reputation by demonstrating that they are taking steps to protect their customers' data and privacy.
- Reduce risk: By aligning their policies with the existing compliance requirements, organizations can help to reduce their risk of being fined or penalized by regulators.
- Improve efficiency: By aligning their policies with the existing compliance requirements, organizations can help to improve their efficiency by reducing the need to create and maintain multiple sets of policies and procedures.
- Increase employee awareness: By aligning their policies with the existing compliance requirements, organizations can help to increase employee awareness of the importance of compliance and the consequences of non-compliance.

10. Where in the policy definition do you define how to implement this policy within your organization?
Answer:
The specific location of the implementation details in a policy definition will vary depending on the policy itself and the organization's specific requirements. However, some common places to include implementation details include:

- The policy statement itself: The policy statement should provide a high-level overview of the policy and its requirements. It may also include some specific implementation details, such as who is responsible for enforcing the policy.
- The policy procedures section: The policy procedures section should provide more detailed instructions on how to implement the policy. This section may include step-by-step instructions, checklists, or templates.
- The policy appendices or attachments: The policy appendices or attachments may include additional information that is not essential to the policy itself, but that may be helpful for implementation purposes. This information may include sample forms, templates, or checklists.

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

- To protect the organization's IT infrastructure and data: Even though non-employees are not directly employed by the organization, they may still have access to the organization's IT resources. By having an AUP in place, organizations can help to protect their IT infrastructure and data from unauthorized access, use, or disclosure.

- To comply with regulations: Many organizations are subject to regulations that require them to have an AUP in place for all users of their IT resources, including non-employees. For example, financial institutions are required to have an AUP in place for all third-party vendors who have access to customer data.
- To protect the organization's reputation: By having an AUP in place, organizations can help to protect their reputation by deterring non-employees from engaging in inappropriate or illegal activities using the organization's IT resources.
- To establish a framework for disciplinary action: An AUP can help to establish a framework for disciplinary action in the event of a violation. This can help to ensure that non-employees are held accountable for their actions.

12. What security controls can be deployed to monitor and mitigate users from accessing external websites that are potentially in violation of an AUP?
Answer:
There are a number of security controls that can be deployed to monitor and mitigate users from accessing external websites that are potentially in violation of an AUP. Some of these controls include:

- Web filtering: Web filtering is a technique that allows organizations to block access to certain websites or categories of websites. This can be done by using a web filter appliance or software solution.
- Application whitelisting: Application whitelisting is a technique that allows organizations to allow only certain applications to run on their devices. This can be done by using an application whitelisting appliance or software solution.
- Data loss prevention (DLP): DLP is a set of technologies that can be used to prevent sensitive data from being leaked. DLP solutions can be used to monitor and block outbound traffic that contains sensitive data.
- User behavior analytics (UBA): UBA is a technique that can be used to analyze user behavior and identify potential threats. UBA solutions can be used to identify users who are accessing prohibited websites or who are engaging in other risky behavior.
- Intrusion detection systems (IDS): IDSs are systems that can be used to detect malicious activity on a network. IDSs can be used to detect users who are accessing prohibited websites or who are engaging in other risky behavior.
- Network segmentation: Network segmentation is a technique that divides a network into smaller, more secure segments. This can help to prevent the spread of malware or other malicious activity if a user does access a prohibited website.

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.)?
Answer:

There are a number of security controls that can be deployed to monitor and mitigate users from accessing external webmail systems and services. Some of these controls include:

- Web filtering: Web filtering is a technique that allows organizations to block access to certain websites or categories of websites. This can be done by using a web filter appliance or software solution.

- Application whitelisting: Application whitelisting is a technique that allows organizations to allow only certain applications to run on their devices. This can be done by using an application whitelisting appliance or software solution.
- Data loss prevention (DLP): DLP is a set of technologies that can be used to prevent sensitive data from being leaked. DLP solutions can be used to monitor and block outbound traffic that contains sensitive data.
- User behavior analytics (UBA): UBA is a technique that can be used to analyze user behavior and identify potential threats. UBA solutions can be used to identify users who are accessing prohibited websites or who are engaging in other risky behavior.
- Intrusion detection systems (IDS): IDSs are systems that can be used to detect malicious activity on a network. IDSs can be used to detect users who are accessing prohibited websites or who are engaging in other risky behavior.
- Network segmentation: Network segmentation is a technique that divides a network into smaller, more secure segments. This can help to prevent the spread of malware or other malicious activity if a user does access a prohibited website.

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?
Answer:
There are a number of security controls that can be deployed to monitor and mitigate users from embedding privacy data in e-mail messages and/or attaching documents that may contain privacy data. Some of these controls include:

- Data loss prevention (DLP): DLP is a set of technologies that can be used to prevent sensitive data from being leaked. DLP solutions can be used to monitor and block outbound traffic that contains sensitive data, such as privacy data.
- Content filtering: Content filtering is a technique that allows organizations to block certain types of content from being sent or received. This can be used to block emails that contain privacy data.
- User behavior analytics (UBA): UBA is a technique that can be used to analyze user behavior and identify potential threats. UBA solutions can be used to identify users who are sending or receiving emails that contain privacy data.
- Intrusion detection systems (IDS): IDSs are systems that can be used to detect malicious activity on a network. IDSs can be used to detect users who are sending or receiving emails that contain privacy data.
- Encryption: Encryption can be used to protect sensitive data, such as privacy data, from being intercepted. This can be done by encrypting emails before they are sent or by encrypting documents before they are attached to emails.

15. Should an organization terminate the employment of an employee if he/she violates an AUP?
Answer:
Whether or not an organization should terminate the employment of an employee who violates an AUP is a complex decision that depends on a number of factors, including the severity of the violation, the organization's policies and procedures, and the employee's history of compliance. In general, organizations should have a clear and concise AUP that outlines the consequences of violating the policy. The AUP should be communicated to all employees and should be reviewed on a regular basis.

If an employee violates the AUP, the organization should first investigate the matter to determine the severity of the violation. If the violation is minor, the organization may choose to issue a warning to the employee. However, if the violation is more serious, the organization may choose to suspend or terminate the employee's employment.

The organization should also consider the employee's history of compliance when making a decision about whether to terminate employment. If the employee has a history of violating the AUP, the organization may be more likely to terminate employment. However, if the employee has a good history of compliance, the organization may be more likely to give the employee a second chance.

Ultimately, the decision of whether or not to terminate an employee's employment for violating an AUP is a difficult one that should be made on a case-by-case basis.