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

Course Name: Policy Development in Information Assurance (IAP301)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 07/10/2023

PART A Elements of a Security Awareness & Training Policy

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	AUP
User or employee apathy towards information systems security policy	SAP
Accessing the Internet is like opening "Pandora's box" given the threat from attackers	AUP
Surfing the web can be a dangerous trek in unknown territory	AUP
Opening e-mails and unknown e-mail attachments can unleash malicious software and codes	AUP

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

PART B Elements of a Security Awareness & Training Policy

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

Create a Security Awareness & Training Policy for ABC Credit union/bank capturing the elements of the policy as defined. Use the following policy template for the creation of your Security Awareness & Training Policy definition

ABC Credit Union
Security Awareness & Training Policy

Policy Statement

ABC Credit Union is committed to protecting its confidential information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Security awareness and training are essential components of this commitment.

Purpose/Objectives

- Enhance the security culture and awareness of ABC Credit Union's workforce by providing them with the necessary knowledge and skills to protect information assets and systems.
- Reduce the risk of human error, negligence, or malicious actions that may compromise the security of information assets and systems.
- Ensure compliance with legal, regulatory, and contractual obligations related to information security.
- Support the implementation and enforcement of other information security policies and standards.

Scope

- All employees, contractors, and third parties who access or handle ABC Credit Union's information assets and systems, regardless of their location, role, or function.

- All information assets and systems owned, operated, or controlled by ABC Credit Union, including but not limited to computers, mobile devices, networks, servers, databases, applications, cloud services, email, websites, social media, etc.
- All seven domains of a typical IT infrastructure: user domain, workstation domain, LAN domain, LAN-to-WAN domain, WAN domain, remote access domain, and system/application domain.

Standards

- ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements
- NIST SP 800-50 Building an Information Technology Security Awareness and Training Program
- PCI DSS Requirement 12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures
- Workstation Domain standards as defined by ABC Credit Union's IT department

Procedures

- Designate a Security Awareness & Training Coordinator who will be responsible for developing, delivering, monitoring, and evaluating the security awareness and training program.
- Conduct a security awareness and training needs assessment to identify the target audience, learning objectives, topics, methods, frequency, and metrics for the program.
- Develop and maintain a security awareness and training curriculum that covers the following topics:
    - ABC Credit Union's information security policies and standards
    - Information security roles and responsibilities
    - Information classification and handling
    - Password management and authentication
    - Phishing and social engineering
    - Malware prevention and detection
    - Data backup and recovery
    - Encryption and decryption
    - Mobile device security
    - Remote access security
    - Incident reporting and response
    - Privacy and data protection laws and regulations
- Deliver the security awareness and training program using a combination of methods such as online courses, webinars, videos, newsletters, posters, quizzes, games, etc.
- Require all employees to complete a mandatory security awareness training course upon joining ABC Credit Union and annually thereafter.
- Require all contractors and third parties to complete a mandatory security awareness training course before accessing or handling ABC Credit Union's information assets and systems.
- Provide additional or specialized security training to employees who have specific roles or functions that involve higher levels of risk or responsibility for information security (e.g., IT staff, managers).
- Monitor the completion and effectiveness of the security awareness and training program using metrics such as participation rates, test scores, feedback surveys, etc.
- Evaluate the security awareness and training program periodically to identify gaps, challenges, and opportunities for improvement.

Guidelines

- Obtain senior management endorsement and sponsorship for the security awareness and training program.

- Allocate sufficient resources (e.g., time, money, staff) for the development, delivery, and evaluation of the security awareness and training program.
- Communicate the benefits, expectations, and requirements of the security awareness and training program to the workforce using various channels (e.g., email, intranet, meetings).
- Engage the workforce in the security awareness and training program by making it relevant, interactive, and fun.
- Use multiple and flexible methods to deliver the security awareness and training program to suit the different needs, preferences, and learning styles of the workforce.
- Ensure alignment and integration of the security awareness and training program with other information security policies and standards.
- Monitor and review the security awareness and training program regularly to keep it current, accurate, and effective.

PART C

Lab Assessment Questions & Answers

1. How does a security awareness & training policy impact an organization's ability to mitigate risks, threats, and vulnerabilities?
Answer: A security awareness and training policy can have a significant impact on an organization's ability to mitigate risks, threats, and vulnerabilities. By educating employees about security best practices, organizations can reduce the likelihood of human error being a factor in a security incident.

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?
Answer: A security awareness and training policy is important for all employees, including new hires. While new hire orientation is a good opportunity to introduce employees to the organization's security policies and procedures, it is not enough to ensure that employees have the ongoing knowledge and skills they need to stay safe online.

3. What is the relationship between an Acceptable Use Policy (AUP) and a Security Awareness & Training Policy?
Answer:
- An AUP is a subset of a Security Awareness & Training Policy, as it specifies the dos and don'ts of using the organization's network, devices, applications, and data. A Security Awareness & Training Policy covers a broader range of topics, such as the objectives, scope, roles, responsibilities, and methods of delivering security education to the employees.
- An AUP supports and complements a Security Awareness & Training Policy, as it helps to communicate and enforce the security policies, standards, procedures, and best practices of the organization. A Security Awareness & Training Policy helps to educate and empower the employees to follow the AUP and protect the organization's information assets and data.

- An AUP requires and depends on a Security Awareness & Training Policy, as it needs to be regularly updated and reviewed to reflect the changing security threats and requirements. A Security Awareness & Training Policy needs to ensure that the employees are aware of and understand the current AUP and its implications.

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

Answer:

- Security risks. Malicious software, such as viruses, Trojan horses, and ransomware, can be disguised as legitimate applications and software. By downloading and installing software from unknown sources, users are putting themselves and their devices at risk of infection.
- Privacy risks. Some applications and software may collect personal information about users without their knowledge or consent. This information can then be used for malicious purposes, such as identity theft or targeted advertising.
- Compatibility issues. Software that is downloaded from the Internet may not be compatible with the user's device or operating system. This can lead to a variety of problems, including system crashes, data loss, and performance issues.
- Compliance risks. Organizations that are subject to industry regulations or standards may be required to prevent users from downloading or installing unauthorized software. Failure to comply with these requirements can result in fines, penalties, and other legal consequences.

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?

Answer:

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

A vulnerability management program is a systematic approach to identifying, assessing, and remediating vulnerabilities in software applications and systems. It helps organizations to prioritize their vulnerability remediation efforts and to identify and implement the most effective controls to mitigate the risk posed by vulnerabilities.

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

Answer:

- The Internet is a complex and dynamic environment. New threats and vulnerabilities are emerging all the time. It is important for users to be aware of these threats and vulnerabilities so that they can take steps to protect themselves.
- Users are often the weakest link in the security chain. Many cyberattacks succeed because users are tricked into revealing sensitive information or performing actions that compromise security. By educating users about security best practices, organizations can reduce the likelihood of users falling victim to these attacks.
- Security awareness training can help to create a more security-conscious culture within the organization. When employees understand the importance of security and their role in

protecting the organization, they are more likely to be vigilant and report suspicious activity.

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

Answer:

- Educate users about the risks of downloading and installing unauthorized software. Users should be aware of the potential consequences of downloading unauthorized software, such as malware infection, data loss, and compliance violations.
- Implement a software whitelist that restricts users to only installing software from approved sources. This can help to ensure that users only install software that has been vetted for security risks.
- Use a security solution that includes malware detection and prevention capabilities. This can help to protect devices from malware infections, even if users do accidentally download malicious software.
- Disable the ability to install software from unknown sources on devices. This can be done on most devices, including computers, smartphones, and tablets.
- Monitor network traffic for suspicious activity. This can help to identify and block attempts to download unauthorized software.
- Use a web filtering solution to block access to known malicious websites. This can help to prevent users from accidentally downloading malware from the Internet.

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

Answer: One strategy for preventing users from clicking on unknown email attachments and files is to educate them about the risks of doing so. Users should be aware that email attachments can contain malware, which can damage or disable their computers and systems, or steal their data. They should also be aware that phishing emails can be used to trick them into clicking on malicious links or opening malicious attachments.

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

Answer:

- Recognize the signs and methods of social engineering attacks, such as phishing, vishing, baiting, quid pro quo, pretexting, etc.
- Understand the motivations and goals of social engineers, such as stealing credentials, data, money, or access to systems or networks.
- Protect themselves and their organization from social engineering attacks, such as verifying the identity and legitimacy of the sender or caller, avoiding clicking on suspicious links or attachments, reporting any suspicious or unusual requests or activities, etc.

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

Answer: The two domains that are the focus of a Security Awareness & Training Policy are the user and the system/application domains. These are the domains where the human factor plays a significant role in ensuring the security of the IT infrastructure. Users need to be aware of the

security policies and procedures that apply to their roles and responsibilities, as well as the potential threats and risks they face when using IT resources. System/application administrators need to be trained on how to securely configure, maintain, and monitor the systems and applications they manage, as well as how to respond to security incidents and breaches. A Security Awareness & Training Policy should provide guidance on how to design, develop, implement, and evaluate an effective security education and training program for these two domains.

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

- To educate employees about the organization's security requirements. Employees need to be aware of the organization's security policies and procedures in order to comply with them. Security awareness training can help to ensure that employees understand the organization's security requirements and why they are important.
- To reduce the risk of data breaches and other security incidents. Human error is a major factor in many security incidents. By educating employees about the organization's security policies and procedures, security awareness training can help to reduce the risk of human error and make the organization more secure.
- To create a more security-conscious culture within the organization. When employees understand the importance of security and their role in protecting the organization, they are more likely to be vigilant and report suspicious activity. Security awareness training can help to create a more security-conscious culture within the organization, which can make the organization more secure overall.

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?
Answer:

- The domain that typically acts as the point-of-entry into the IT infrastructure is the remote access domain. This is the domain where a mobile user, such as a contractor, vendor or employee, works remotely (instead of within the office) and accesses the corporate local area network remotely with the help of a VPN. The remote access domain can pose a significant security risk as it exposes the IT infrastructure to external threats from untrusted networks and devices.
- The domain that typically acts as the point-of-entry into the IT infrastructure's systems, applications, databases is the system/application domain. This is the domain where all the software components of an IT infrastructure are located, such as web servers, operating systems, content management systems, enterprise resource planning, productivity applications and more. The system/application domain is where users interact with the IT services and solutions that are delivered by the IT infrastructure. It is also where system/application administrators configure, maintain, and monitor the systems and applications they manage. The system/application domain can be vulnerable to security breaches if the software components are not properly secured, updated, and patched.

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

- To ensure that employees are aware of the latest security threats and best practices. The security landscape is constantly evolving, with new threats and vulnerabilities emerging all the time. By providing employees with regular security awareness training, organizations can help to ensure that employees are aware of the latest threats and best practices, and know how to protect themselves and the organization.
- To reduce the risk of human error. Human error is a major factor in many security incidents. By providing employees with regular security awareness training, organizations can help to reduce the risk of human error and make the organization more secure.
- To create a more security-conscious culture within the organization. When employees understand the importance of security and their role in protecting the organization, they are more likely to be vigilant and report suspicious activity. By providing employees with regular security awareness training, organizations can help to create a more security-conscious culture within the organization.

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

- Regularly communicate security messages and updates. Organizations can use a variety of channels to communicate security messages and updates to employees, such as email, newsletters, intranet postings, and social media. Security messages should be clear, concise, and relevant to the audience.
- Provide employees with resources to learn more about security. Organizations can provide employees with access to a variety of resources to learn more about security, such as online training modules, articles, and videos. These resources can help employees to stay informed about the latest security threats and best practices.
- Hold security awareness events and contests. Organizations can hold security awareness events and contests to engage employees and raise awareness of security issues. For example, organizations could hold a phishing awareness contest to see how many employees can identify phishing emails.
- Gamify security awareness. Organizations can use gamification to make security awareness more engaging and fun for employees. For example, organizations could develop a security awareness game where employees can earn points and badges for completing security tasks.
- Recognize and reward employees for good security behavior. Organizations can recognize and reward employees for good security behavior, such as reporting suspicious activity or completing security training modules. This can help to motivate employees to be more security-conscious.

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

- New policies may introduce new security risks. New policies may introduce new security risks, such as new requirements for employees to use new software or to change their passwords. Employees need to be aware of these new risks and know how to mitigate them.

- New policies may require employees to change their behavior. New policies may require employees to change their behavior in order to comply. For example, a new policy on password security may require employees to create stronger passwords or to change their passwords more frequently. Employees need to be aware of these new requirements and be motivated to comply with them.
- New policies may create confusion. New policies can be confusing, especially if they are implemented quickly. Employees need to have the opportunity to learn about new policies and to ask questions.