| User Domain Risks & Threats | Risk Mitigation Tactic/Solution |
|---|---|
| Dealing with humans and human nature | Conduct regular security awareness training programs to educate users about security best practices, social engineering tactics, and the importance of following security policies |
| User or employee apathy towards information systems security policy | Education and Awareness Programs<br>• Conduct regular training sessions to educate employees about the importance of information security.<br>• Clearly communicate the potential risks and consequences of not adhering to security policies.<br>• Provide real-world examples and case studies to make the information more relatable.<br>• Foster a culture of security awareness, making it a shared responsibility among all employees. |
| Accessing the Internet is like opening "Pandora's box" given the threat from attackers | Network Segmentation and Web Filtering<br>• Implement network segmentation to isolate critical systems from general internet access.<br>• Use web filtering tools to restrict access to potentially harmful websites based on content and reputation.<br>• Employ a proxy server to monitor and control web traffic, preventing users from accessing malicious sites. |
| Surfing the web can be a dangerous trek in unknown territory | Updated and Patched Systems, and Endpoint Protection<br>• Ensure all systems, including browsers, are regularly updated with the latest security patches.<br>• Implement endpoint protection solutions to detect and block |

| | |
|---|---|
| | malicious activities on individual devices.<br>• Use secure browsing practices, such as HTTPS, and consider deploying browser security extensions. |
| Opening e-mails and unknown e-mail attachments can unleash malicious software and codes | Email Security Measures and User Training<br><br>• Implement email filtering systems to identify and block suspicious emails.<br>• Use email authentication methods like DMARC, DKIM, and SPF to prevent email spoofing.<br>• Conduct phishing awareness training for employees to recognize and report suspicious emails.<br>• Encourage the use of email encryption for sensitive information. |

| **Workstation Domain Risks & Threats** | **Risk Mitigation Tactic/Solution** |
|---|---|
| Installing unauthorized applications, files, or data on organization-owned IT assets can be dangerous | Endpoint Protection and User Training<br><br>• **Tactic:** Implement endpoint protection solutions to block unauthorized installations.<br>• **Explanation:** Use endpoint protection tools that can prevent the installation of unauthorized software. Additionally, conduct user training to educate employees about the risks associated with installing unauthorized applications and emphasize the importance of adhering to IT policies. |
| Downloading applications or software with hidden malicious software or codes | Network Filtering and Regular Software Audits<br><br>• **Tactic:** Use network filtering tools to block access to malicious websites.<br>• **Explanation:** Regularly audit software and applications to ensure they are obtained from legitimate sources. Enforce policies that restrict |

| | |
|---|---|
| | the download and installation of software from unapproved sources. |
| Clicking on an unknown URL link with hidden scripts | Web Filtering and User Education<br><br>• **Tactic:** Implement web filtering to block access to malicious websites.<br>• **Explanation:** Conduct regular training to educate users about the dangers of clicking on unknown or suspicious links. Encourage the use of URL scanning tools to check the reputation of websites before accessing them. |
| Unauthorized access to workstation | Access Controls and User Authentication<br><br>• **Tactic:** Implement strong access controls and enforce user authentication.<br>• **Explanation:** Use role-based access controls to ensure users only have access to the resources necessary for their roles. Enforce strong authentication methods, such as multi-factor authentication, to prevent unauthorized access. |
| Operating system software vulnerabilities | Patch Management and Regular Updates<br><br>• **Tactic:** Implement a robust patch management system for operating systems and applications.<br>• **Explanation:** Regularly update and patch all software to address known vulnerabilities. Automate the patching process to ensure timely updates, reducing the window of exposure to potential exploits. |
| Application software vulnerabilities | Regular Software Updates and Patch Management:<br><br>• **Tactic:** Implement Patch Management Procedures |

| | |
|---|---|
| | • **Explanation:** Regularly update and patch all application software to address known vulnerabilities. Establish a structured process for testing and deploying patches promptly. Automated patch management tools can streamline this process. |
| Viruses, Trojans, worms, spyware, malicious software/code, etc. | Antivirus and Anti-malware Solutions<br>• **Tactic:** Install and regularly update antivirus and anti-malware software.<br>• **Explanation:** Use reputable security software to scan and detect malicious code. Keep antivirus definitions up-to-date to defend against the latest threats. |
| User inserts CDs, DVDs, USB thumb drives with personal files onto organization-owned IT assets | Endpoint Security with Device Control:<br>• **Tactic:** Implement Endpoint Security with Device Control<br>• **Explanation:** Utilize endpoint security solutions with robust device control features to manage and control the use of external storage devices. |
| User downloads unauthorized applications and software onto organization-owned IT assets | Endpoint Protection with Application Control:<br>• **Tactic:** Deploy Endpoint Protection Solutions<br>• **Explanation:** Install endpoint protection software that includes features like application control. These solutions can help monitor and control the types of applications users can download and install on their devices. |
| User installs unauthorized applications and software onto organization-owned IT assets | Application Whitelisting and User Education<br>• **Tactic:** Utilize application whitelisting to control software installations. |

| | |
|---|---|
| | • **Explanation:** Allow only approved applications to run on organizational devices. Educate users about the importance of obtaining IT approval before downloading or installing any software on their workstations. |

Part 2

# ABC Credit Union

## Security Awareness & Training Policy

**Policy Statement:**

ABC Credit Union is committed to maintaining the highest standards of security and privacy for our customers and their data. In alignment with the Gramm-Leach-Bliley Act (GLBA) and IT security best practices, this Security Awareness & Training Policy outlines the guidelines and expectations for all employees in the User and Workstation Domains to ensure the protection of sensitive customer information and the secure use of organization-owned assets.

**Purpose/Objectives:**

The purpose of this policy is to establish a comprehensive framework for security awareness and training to mitigate the risks associated with the User and Workstation Domains. The key objectives include:

- Ensuring compliance with GLBA and safeguarding customer privacy data.
- Implementing annual security awareness training for all employees.
- Controlling and monitoring internet usage through content filtering.
- Eliminating personal use of organization-owned IT assets and systems.
- Implementing email security controls to enhance data protection.

**Scope:**

This policy applies to all employees of ABC Credit Union, including new hires and existing staff. The policy covers the User and Workstation Domains within the IT infrastructure. Elements within the scope include organization-owned assets such as computers, laptops, mobile devices, and any other hardware or software used by employees in the course of their duties.

**Standards:**

This policy references the Workstation Domain standards outlined in the organization's IT Security Standards document. These standards detail the configuration and usage guidelines for workstations, ensuring that they align with security best practices and GLBA requirements.

**Procedures:**

1. **Security Awareness Training:**
    - All new hires must complete a comprehensive security awareness training program during their onboarding process.
    - Existing employees are required to undergo annual security awareness training to stay informed about evolving threats and best practices.
2. **Internet Usage:**
    - Content filtering will be implemented to monitor and control internet usage, ensuring compliance with GLBA and preventing access to potentially harmful content.
3. **Personal Use of IT Assets:**
    - Personal use of organization-owned IT assets and systems is strictly prohibited. Employees are expected to use these resources exclusively for work-related activities.
4. **Email Security Controls:**
    - Email security controls will be implemented to prevent phishing attacks, unauthorized access, and the transmission of sensitive information via email.

**Guidelines:**

- Addressing Resistance: Acknowledge potential resistance to policy implementation and establish communication channels to address concerns, providing clarity on the importance of security measures.
- Periodic Audits: Conduct periodic audits to ensure compliance with the policy and promptly address any deviations through corrective action and additional training if necessary.
- Feedback Mechanism: Establish a feedback mechanism for employees to report security concerns or suggest improvements to the security awareness and training program.
- Continuous Improvement: Regularly review and update the policy, considering emerging threats and changes in technology, to ensure its effectiveness in safeguarding customer data and meeting compliance requirements.

Part 3

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

A security awareness and training policy significantly impacts an organization's ability to mitigate risks, threats, and vulnerabilities in several key ways:

1. **Human Firewall:** Employees are often the first line of defense against cyber threats. A well-implemented security awareness program empowers employees to recognize and respond to potential risks. By cultivating a security-conscious culture, employees become a human firewall, reducing the likelihood of falling victim to social engineering attacks such as phishing or pretexting.
2. **Data Protection and Privacy:** Training employees on the importance of protecting sensitive data and customer privacy helps prevent data breaches. Understanding the value of information and the potential consequences of mishandling it encourages employees to adhere to security protocols, reducing the risk of data leaks or unauthorized access.
3. **Compliance Adherence:** Security awareness training ensures that employees understand and comply with relevant regulations and industry standards. For example, in the scenario provided, adherence to GLBA regulations is crucial. A well-informed workforce is better equipped to handle customer data responsibly, reducing the organization's exposure to legal and regulatory risks.
4. **Reduced Insider Threats:** Employees who are aware of security policies and the potential consequences of their actions are less likely to engage in malicious activities. By promoting a sense of responsibility and accountability, organizations can mitigate the risk of insider threats, intentional or unintentional.
5. **Effective Use of Security Tools:** A trained workforce is more likely to understand and effectively use security tools and technologies. This includes implementing and following procedures related to content filtering, email security controls, and other protective measures. Proper utilization of security tools enhances the organization's overall cybersecurity posture.
6. **Timely Incident Response:** Security awareness training prepares employees to recognize signs of a security incident and report them promptly. This facilitates quicker incident response, enabling the organization to contain and mitigate the impact of security breaches before they escalate.
7. **Consistent Security Practices:** Standardized security training ensures that all employees have a consistent understanding of security protocols and best practices. This consistency is crucial for maintaining a cohesive security posture across the organization, minimizing gaps in protection that could be exploited by attackers.
8. **Crisis Preparedness:** Training programs often include exercises and simulations that prepare employees for real-world cybersecurity incidents. This helps the organization respond more effectively during a crisis, reducing downtime and potential financial losses.

## 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?

Ongoing Education: New hire orientation provides an introduction to security practices, but cybersecurity is a dynamic field with evolving threats. A comprehensive policy ensures that employees receive ongoing education and updates on the latest security threats and best practices.

Annual or periodic training, as mandated by the policy, helps reinforce and expand employees' understanding of security measures over time.

Compliance Requirements: Many industries, including finance (as in the scenario provided with GLBA), healthcare, and others, have specific compliance requirements. A policy outlines the organization's commitment to meeting these regulatory standards and ensures that employees are aware of their responsibilities in maintaining compliance.

Policy Awareness: A policy serves as a central document that outlines the organization's expectations regarding security. It helps in clearly communicating the importance of security to all employees, emphasizing that adherence to security practices is an ongoing commitment, not just a one-time event during orientation.

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

An Acceptable Use Policy (AUP) and a Security Awareness & Training Policy are related but serve distinct purposes.

- **Acceptable Use Policy (AUP):** Defines acceptable behavior regarding the use of organizational IT assets and resources.
- **Security Awareness & Training Policy:** Focuses on educating employees about security practices, threats, and the organization's specific security requirements.

While an AUP sets guidelines for proper use of IT resources, the Security Awareness & Training Policy aims to enhance understanding and awareness of security measures. The AUP is more about behavioral expectations, while the Security Awareness & Training Policy is about educating employees on the broader aspects of cybersecurity. They often complement each other to create a comprehensive approach to security within an organization.

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

Preventing users from downloading or installing applications and software found on the Internet is important to:

**1. Security:** Mitigate the risk of downloading malicious software, reducing the likelihood of malware infections, data breaches, and other cybersecurity threats.

**2. Compliance:** Adhere to organizational policies and industry regulations, ensuring that only authorized and vetted software is used to maintain data integrity and privacy.

**3. System Stability:** Prevent potential conflicts, system instability, and performance issues that can arise from unauthorized or incompatible software installations.

**4. Standardization:** Maintain a standardized and secure computing environment, facilitating easier management, troubleshooting, and support for IT administrators.

**5. Resource Optimization:** Preserve network bandwidth and system resources by controlling the installation of unnecessary or unauthorized applications, contributing to overall system efficiency.

## 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?

**Regular Patching and Updates** are needed most for operating systems, applications, and other software installations. Regular updates help to address security vulnerabilities, enhance system stability, and protect against emerging threats.

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

It is important to educate users about the risks, threats, and vulnerabilities found on the Internet and worldwide web to:

Empower Awareness: Enable users to recognize and avoid potential cyber threats, reducing the likelihood of falling victim to scams, phishing attacks, malware, and other online risks.

Promote Responsible Behavior: Foster a culture of responsible online behavior, encouraging users to make informed decisions, protect sensitive information, and contribute to overall cybersecurity.

Mitigate Security Incidents: Educated users are better equipped to identify and report security incidents promptly, allowing for quicker response and mitigation of potential damages.

Protect Personal and Organizational Assets: Enhance the security of both personal and organizational assets by equipping users with the knowledge to navigate the online landscape safely and securely.

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

Strategies for preventing users or employees from downloading and installing rogue applications and software:

1. **Implement Application Whitelisting:** Allow only approved applications to run on workstations, preventing the execution of unauthorized or unverified software.
2. **Use Endpoint Protection Solutions:** Employ endpoint security tools that include features like application control and behavior monitoring to detect and block malicious software.
3. **Educate Users:** Provide comprehensive security awareness training to educate users about the risks of downloading and installing unauthorized software, emphasizing the importance of adhering to organizational policies.
4. **Enforce Least Privilege Access:** Limit user permissions to install software, granting administrative privileges only to authorized personnel, reducing the likelihood of rogue installations.
5. **Regularly Update and Patch Software:** Keep operating systems and applications up to date with the latest security patches to address vulnerabilities and minimize the risk of exploitation.
6. **Deploy Content Filtering:** Use content filtering solutions to restrict access to websites known for hosting malicious software or unapproved applications.
7. **Monitor Network Traffic:** Implement network monitoring tools to detect and block suspicious download activities, providing an additional layer of defense against rogue installations.
8. **Establish a Clear Acceptable Use Policy (AUP):** Clearly communicate the organization's policies regarding software installations and use, reinforcing the consequences of violating these policies.
9. **Conduct Regular Audits:** Periodically audit systems to identify and remove unauthorized or unapproved applications, ensuring a clean and secure computing environment.
10. **Implement Security Controls in Email:** Use email filtering and security controls to prevent the distribution of malicious software through email attachments or links.

## 8. What is one strategy for preventing users from clicking on unknown email attachments and files?

One strategy for preventing users from clicking on unknown email attachments and files is to implement robust email filtering and scanning mechanisms. This includes using email security solutions that automatically identify and filter out potentially malicious attachments, reducing the likelihood of users interacting with harmful content.

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

Social engineering should be included in security awareness training because:

- Humans as Targets: Social engineering exploits human psychology to manipulate individuals into divulging sensitive information or taking unauthorized actions, making it crucial for individuals to recognize and resist such manipulative tactics.
- First Line of Defense: Employees are often the first line of defense against social engineering attacks. Training equips them with the knowledge to identify and respond appropriately to phishing, pretexting, and other social engineering attempts.
- Risk Mitigation: Awareness training helps reduce the risk of falling victim to social engineering, minimizing the potential impact of data breaches, unauthorized access, and other security incidents.
- Cultivate Vigilance: Educating employees about social engineering tactics cultivates a culture of vigilance and skepticism, encouraging them to approach unexpected or suspicious communications with caution.

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

The User Domain and the Workstation Domain are the primary focus of a Security Awareness & Training Policy.

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

- **Clarity and consistency:** Ensures everyone understands expected behavior, reducing ambiguity and promoting uniform adherence.
- **Compliance:** Helps meet regulatory requirements and industry best practices, potentially mitigating legal and financial risks.
- **Alignment with security goals:** Connects specific policies to broader security objectives, fostering employee buy-in and responsibility.
- **Accountability:** Makes consequences for policy violations clear, deterring misconduct and encouraging compliance.

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

**Most commonly:**

- **User Domain:** Manages user accounts, authenticates logins, and grants access permissions, serving as the first line of defense.

**Other possibilities:**

- **Workstation Domain:** Contains information about user workstation configurations and policies, influencing access control.
- **Network Domain:** Defines network configuration and access rules, potentially serving as an entry point depending on architecture.

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

**Importance:**

- **Threat landscape keeps evolving:** New threats and attack methods emerge, requiring frequent updates to employee knowledge.
- **New employees:** Onboarding requires security education, and existing staff may need reminders or training on changes.
- **Policy revisions:** Updates on internal policies necessitate informing employees about adjustments.
- **Reinforcement:** Regular training strengthens retention and encourages consistent application of security practices.

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

- **Regular phishing campaigns:** Simulated attacks test and improve employee vigilance against real-world phishing attempts.
- **Security newsletters and updates:** Share timely information about emerging threats, best practices, and policy changes.
- **Security posters and reminders:** Visual cues in workspaces can prompt ongoing awareness and vigilance.
- **Gamification and incentives:** Make learning engaging and encourage participation through contests, rewards, or recognition programs.
- **Open communication:** Foster a culture where employees feel comfortable asking questions and reporting security concerns.

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

- Ensure understanding: Clarify implications of the new policy and how it affects employees' daily activities.
- Address potential concerns: Provide explanations and answer questions to alleviate confusion or resistance.
- Promote compliance: Emphasize the importance of following the new policy and its role in enhancing security.