501CISO

501C CYBERSECURITY LEADERSHIP

Powered by ClearTone Consulting, LLC

SECURITY AWARENESS TRAINING PROGRAM

Prepared by

Brian Scott

SECURITY AWARENESS TRAINING PROGRAM OVERVIEW

In today's rapidly evolving cybersecurity risk landscape, cybersecurity risk is a shared responsibility that extends to every member of our organization. This comprehensive security awareness training program is designed to equip all employees, from new hires to board members, with the knowledge and skills necessary to safeguard our assets and data. Through a structured approach that includes onboarding training, quarterly or annual refreshers, monthly phishing tests, and targeted education for those needing additional support, the aim is to foster a proactive security culture. This program also includes specific training for our Board of Directors to ensure effective oversight of cybersecurity risk management.

Onboarding Training

Objective: Introduce new hires to the organization's security policies, best practices, and the importance of maintaining a secure work environment from the start.

Components:

- Security Orientation Session:
    - Overview of the company's security policies.
    - Introduction to data protection and privacy laws. (if applicable)
    - Basic cybersecurity concepts (e.g., phishing, malware, secure password practices).
- Initial Training Modules:
    - Secure use of company devices (e.g., laptops, mobile phones).
    - Email security and identifying phishing attempts.
    - Safe internet usage and recognizing unsafe websites.
    - Secure handling of sensitive information.
- Interactive Activities:
    - Phishing simulation exercises.

  - Quizzes to reinforce key security concepts.
- Sign-off on Acceptable Use Policy (AUP):
  - Present the AUP and require acknowledgment and signature.
  - AUP covers acceptable use of company systems, email, internet, and handling of data.

Quarterly or Annual Security Awareness Training

Objective: Provide ongoing, bite-sized security awareness training throughout the year to reinforce key concepts and address emerging threats.

Components broke into quarters:

Quarter 1: Foundational Security Practices

- Focus Areas:
  - Review of basic cybersecurity principles.
  - Secure password practices and the importance of multi-factor authentication (MFA).
  - Review of phishing and how to identify suspicious emails.
- Training Format:
  - Interactive e-learning module with videos and quizzes.
- Assessment:
  - Short quiz to reinforce learning outcomes.
- Acknowledgment:
  - Require employees to acknowledge completion of the module or track compliance via the learning platform

Quarter 2: Data Privacy and Protection

- Focus Areas:

  - Overview of data privacy laws and regulations (e.g., GDPR, CCPA).
  - Data classification and handling procedures (public, internal, confidential).
  - Best practices for protecting sensitive information (e.g., encryption, secure sharing).
- Training Format:
  - Webinar or e-learning module with scenario-based exercises.
- Assessment:
  - Quiz focused on data protection scenarios.
- Acknowledgment:
  - Require employees to acknowledge completion of the module or track compliance via the learning platform.

Quarter 3: Advanced Threats and Secure Remote Work

- Focus Areas:
  - Deep dive into advanced threats (e.g., ransomware, social engineering).
  - Secure remote work practices, including the use of VPNs and secure Wi-Fi.
  - Recognizing and reporting security incidents.
- Training Format:
  - Interactive training with real-world case studies and video content.
- Assessment:
  - Simulation exercises (e.g., identifying potential threats in an email).
- Acknowledgment:
  - Require employees to acknowledge completion of the module or track compliance via the learning system.

Quarter 4: Incident Response and Secure Use of Technology

- Focus Areas:
    - Overview of the company's incident response plan.
    - How to respond to and report security incidents.
    - Secure use of company devices and software, including mobile device management.
- Training Format:
    - E-learning module with a focus on incident response procedures.
- Assessment:
    - Final quiz covering key points from all four quarters.
- Acknowledgment:
    - Require employees to acknowledge completion of the module or track compliance via the learning platform.

Monthly Phishing Tests

Objective: Regularly test and reinforce employees' ability to identify phishing attempts, fostering a proactive security culture. Track scores, set organizational goals, and track improvement and progress towards the goals.

Components:

- Simulated Phishing Campaigns:
    - Conduct monthly phishing simulations using realistic scenarios.
    - Move consistently to more difficult email templates after achieving goals
    - Always utilize “Credential Theft” phishing options
- Immediate Feedback:
    - Instant feedback to employees who fail a simulation, explaining what they missed and how to identify phishing.
- Reporting Mechanism:

    - Encourage reporting of phishing attempts through a dedicated channel (e.g., "Report Phishing" button in email client).
- Metrics and Reporting:
    - Track and report overall success rates and areas for improvement.
    - Share anonymized results with staff to promote awareness.
    - Set organizational goal and leadership to encourage staff to hit the target

Tiered Failure Training Program

Objective: Address repeated failures in phishing tests with a structured remediation program tailored to the level of risk exhibited.

Components:

- Tier 1: First Failure
    - Notification and Education:
        - Notify the employee of the failure.
        - Provide a brief video refresher course on identifying phishing attempts.
    - Acknowledgment:
        - Require acknowledgment of understanding the refresher content.

- Tier 2: Second Failure
    - Interactive Training:
        - Enroll the employee in a more in-depth, interactive training module focusing on phishing.
    - Follow-Up Quiz:
        - Conduct a quiz to ensure understanding of the material.
    - Manager Involvement:
        - Notify the employee's manager to discuss the importance of security practices.

- Tier 3: Third Failure and Beyond
    - One-on-One Coaching:
        - Schedule a meeting with the employee and the security team to discuss patterns and provide personalized training.
    - Intensive Training:
        - Require participation in an intensive cybersecurity awareness workshop.
    - Performance Review Consideration:
        - Include security awareness as a factor in performance reviews.
    - Potential Disciplinary Actions:
        - For continuous failures, consider further actions according to the company's disciplinary policies.

Board of Directors Training

Objective: Equip the Board of Directors with the knowledge and understanding necessary to oversee cybersecurity risk management effectively.

Components:

- Annual Security Briefing:
    - Overview of the current cybersecurity landscape, including threats and trends.
    - Summary of the organization's current security posture and major initiatives.
    - Review of legal, regulatory, and compliance requirements related to cybersecurity.
- Risk Management Training:
    - Discuss the role of the board in managing and overseeing cyber risk.
    - Provide an overview of risk assessment frameworks and how they apply to the organization.

- Incident Response and Crisis Management:
    - Explain the board's role in the event of a major security incident.
    - Walkthrough of the organization's incident response plan, including communication protocols.
- Data Privacy and Protection:
    - Training on data privacy laws and regulations that impact the organization.
    - Discuss the implications of data breaches and the board's responsibilities in such cases.
- Ongoing Engagement:
    - Regular updates on cybersecurity developments at board meetings.
    - Quarterly or semi-annual reports on security metrics and key performance indicators.

Obtaining Signatures on an Acceptable Use Policy (AUP)

Objective: Ensure all employees understand and agree to comply with the company's acceptable use policies regarding IT resources.

Components:

- AUP Creation and Distribution:
    - Develop a clear AUP that outlines the acceptable use of company assets, including:
        - Company devices and networks.
        - Email and communication tools.
        - Data handling and classification.
        - Remote work guidelines.
    - Distribution and Review:
        - Distribute the AUP during onboarding and annually.
        - Provide a review session during onboarding training to explain key points.

- Acknowledgment and Signature:
  - Require employees to sign the AUP, acknowledging their understanding and commitment to compliance.
- Digital Record Keeping:
  - Use a digital acknowledgment system to track signed AUPs for compliance purposes.