Security Awareness Program Overview

2024

Prepared by: Taylor Rouleau

Program Objectives

1. Ensure all staff are trained in security upon hire and annually
2. Instill a culture of continuous security– it's everyone's job!
3. Create, maintain, and measure adoption of Trust / Security portal

Program Components

1. 30-day annual training campaign (suggest September, leading into Cybersecurity Awareness month in October)
    a. Gamify where possible, engage managers

2. Feature the Security Awareness Program in October company-wide All Hands meeting

3. Prior to the above, create and socialize an internal Security portal that includes learning materials, basics about Security posture at Everlaw, and a transparent roadmap

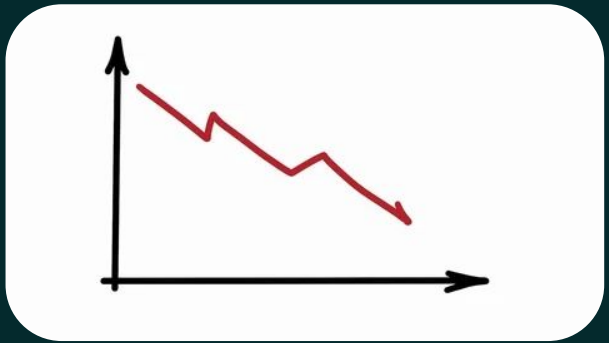
Training campaign details

1. Recognizing cyberattacks
    a. Phishing, social engineering, sharing of info (including on social media)
2. Physical security– clean desk policy, tailgaiting, securing company assets
3. Passwords & authentication– how and why to use strong passwords and mfa
4. Remote working– dangers of public wifi, use of VPNs, anti-virus software, secure use of cloud computing
5. Data privacy trends– basics of GDPR, CCPA

Metrics for measuring objective success

1. Metric: 95% completion rate for security awareness training across the organization

2. Metric: Measure baseline occurrence of security incidents & policy violations and track the trend over time (it should decrease if we're being effective!)



Suggested Tools

1. KnowBe4 or similar security awareness platform
    a. Offers updated training annually including addressing recent trends, automated reporting, phishing tests
    b. Would need a technical security staff member to review content and ensure it covers org's use cases

2. Confluence or a similar knowledge base for Security / Trust portal
    a. Include an executive overview of Security Program and posture

Questions?