To: Internal Stakeholder Board

From: Juliano Alves de Souza

Date: 12/10/2023

Subject: Service Level Agreement Requirement Recommendations

I. Introduction

In response to the recent developments and the evolving cybersecurity landscape, it is imperative that we reinforce our commitment to information security and develop an effective Service Level Agreement (SLA) to meet the requirements of our partnership with Helios Health Insurance. This document outlines two selected sub-controls from the CIS Controls framework, justifies the control types and implementations, discusses the necessity for a training program targeting a specific social engineering threat, and outlines expected outcomes.

II. Selected Sub-Controls

1. **Control One**: Implement a Security Awareness and Training Program (Control 17)

Justification: A comprehensive security awareness and training program is essential to equip our workforce with the knowledge and skills needed to identify and respond to social engineering attacks effectively. By implementing this control as a policy, we establish a clear framework for ongoing training and awareness efforts.

2. **Control Two**: Train Workforce on Identifying Social Engineering Attacks (Control 17, Section 6)

Justification: This sub-control specifically addresses the need to train our workforce in identifying social engineering attacks, such as phishing, phone scams, and impersonation calls. By implementing this as a procedure, we create a structured approach to deliver targeted training and evaluate the effectiveness of our efforts.

III. Necessity for a Training Program

The necessity for a training program to address social engineering threats is evident in the increasing sophistication and prevalence of such attacks. Social engineering techniques prey on human psychology and can bypass even the most advanced technical controls. Without proper training, employees may inadvertently fall victim to these attacks, leading to data breaches and financial losses.

IV. Expected Outcomes of the Training Program

A well-structured training program aimed at addressing social engineering threats is expected to yield the following outcomes:

- Improved Awareness: Employees will gain a deeper understanding of social engineering tactics, enabling them to recognize suspicious communication or behavior.

- Enhanced Vigilance: The workforce will become more vigilant, exercising caution when handling emails, phone calls, or requests for sensitive information.
- Reduced Vulnerabilities: As employees learn to identify and report potential threats, the organization's overall vulnerability to social engineering attacks will decrease.
- Effective Incident Response: In the event of a social engineering incident, employees will be better equipped to respond promptly and mitigate potential damage.
- Compliance with SLA: Meeting the SLA requirements related to social engineering controls will demonstrate our commitment to information security and safeguarding our partnership with Helios Health Insurance.

V. Conclusion

In conclusion, implementing these sub-controls as policies and procedures within our SLA will ensure that we establish a robust framework for addressing social engineering threats through comprehensive training and awareness efforts. The expected outcomes will contribute to a more secure environment, reduce the risk of successful attacks, and demonstrate our dedication to maintaining a secure partnership with Helios Health Insurance.

References:

1. NIST SP 800-50 Infosec Awareness Training. https://csrc.nist.gov/publications/detail/sp/800-50/final
2. EDUCAUSE https://library.educause.edu/search#?q=security%20awareness%20and%20training