*This document is intended to be used as a resource to help prepare a funding or approval request for phishing simulation at your organization. The information contained within this document should be incorporated into your organization’s specific funding format. The context of the text is from the point of view of you making a request for funding internally; this is not a sales proposal.*

**BUSINESS CASE:**

**IMPROVE SECURITY THROUGH PHISHING SIMULATION**

# EXECUTIVE SUMMARY

Social engineering, or the act of attacking the human element of security, poses a risk to our industry. To improve our overall information security posture, we recommend conducting simulated social engineering attacks to evaluate our employees’ susceptibility to such tactics.

This document provides support for obtaining a license to use a hosted software system, allowing us to easily conduct realistic, non-intrusive, social engineering attacks via phishing, which is the most common delivery tactic. Such testing will promote employee awareness of the threat and allow us to identify employees needing additional training.

We recommend a solution from PhishingBox. Their system will provide us with the ability to perform testing for all of our employees for an annual investment of $xxxx.

# SITUATION

Social engineering attacks are a significant threat to businesses. This is a concern for us as 82% of hacking attacks begin with social engineering and according to the Anti-Phishing Working Group, more phishing attacks occurred in 2022 than in any previous year, resulting in the highest average cost of data breaches in the organization’s history of tracking data.

As an organization, we need to maintain an adequate control environment. Our stakeholders, clients, and regulators expect it, and we need to protect our trade secrets and other business information. A data breach would be expensive and negatively affect our reputation. We have invested in security systems and software, such as firewalls and anti-virus software; however, we are not adequately prepared for social engineering attacks. As part of a layered defense, we need to improve and test the human link of our security chain.

The primary method to improving the human element of security is through training and testing. Using phishing simulation will do more to improve our security than upgrading our computers or increasing password complexity. We expect the following benefits from implementing phishing simulation training and testing.

**PHISHING SIMULATION BENEFITS**

# Increased Security

Phishing simulations provide quantifiable results that can be measured.

These measurements allow improvement to be identified and tracked. Initially, we expect a 33 percent failure rate. After subsequent training, we expect an ongoing failure rate of approximately 5 percent. We do not expect the success rate to be 100 percent due to employee turnover, forgetfulness, and other reasons. This fact is the reason for ongoing training and testing to mitigate risk as much as possible.

# Demonstrated Responsibility

As a responsible organization, we need to demonstrate to our stakeholders our understanding of the current threat environment and present the steps we’re taking to reduce our risk. By ignoring the threats from social engineering attacks, we could be exposing ourselves to litigation.

# Improved Training Retention

We can provide training on what to do and what to avoid, but until an employee experiences it, their actions are unknown. After seeing what is capable, employees understand and are more cyber aware.

# Net Reduced Training Cost

By pinpointing employees who are more susceptible, such as repeat failures, we can provide additional training to those employees without the cost and burden to other employees.

# ALTERNATIVES CONSIDERED

We considered several alternatives. These options included creating systems internally, obtaining a commercial phishing simulation system, and contracting for phishing as part of an external social engineering test. Below are key points relating to each of the alternatives.

|  |  |  |
| --- | --- | --- |
| Option | Pro | Cons |
| Internally Developed / Open  Source Systems | ~ Total control | ~ Resource Intensive  ~ Needed Expertise  ~ Install Software  ~ Support Software |
| Hosted Phishing Simulation  System | ~ Low cost  ~ Good controls  ~ Vendor support | ~ Vendor reliance |
| Outsource Social Engineering Testing | ~ Good expertise | ~ One-time  ~ Expensive |

# RECOMMENDED SOLUTION

We recommend the purchase of a license to use a web-based solution from PhishingBox LLC. We selected PhishingBox based on system methodology, affordability, general ease-of-use, and overall support and power.

The PhishingBox system will provide us the ability to perform testing for all of our employees for an investment of $xxxx annually. Their Investment Summary is detailed in the proposal.