Prospectus/Needs Assessment

Design Problem and Goals

This overview section will include difficulties that might emerge throughout the design and implementation of the interactive system.

Cybersecurity attacks effect users both professionally and personally. It has become evident with the increase in data breaches that Personal Identifiable Information (PII) has become a sought-after commodity for thieves. This can be costly for an individual, but for an organization, it can lead to lack of trust, impact future business, and possibly lead to bankruptcy. This is why it is critical to train employees on how to spot and prevent security breaches at work.

The goal is to design, develop and implement an elearning course to train employees on how to spot and avoid cybersecurity attacks before they penetrate the organization, which in turn will help secure client data. Elearning was chosen for a few reasons; it allows employees to take the training easily and conveniently regardless of their physical location, it is the preferred method of instruction when conducting compliance training in organizations, and is easily deployed for conducting annual training and knowledge checks throughout the year with very little overhead.

Design challenges include; how to design for varying technical skills levels, incorporating design elements that are engaging and motivating to employees, and creating activities that employees can participate in to aid in job transfer and continued engagement throughout the year.

Needs Analysis

The needs analysis consisted of an anonymous online survey sent to 6 individuals on the Executive Committee to measure their confidence in cybersecurity practices within the organization. Additionally, it was communicated that for compliance reasons, all employees were required to participate in a security training based on the confidentiality of client data and contractual obligations.

Five questions were included in the survey with a Likert Scale from 1-5 (1 = STRONGLY AGREE and 5=STRONGLY DISAGREE). A majority is defined as 90% or higher of the employee population. The following questions were included in the survey:

1. I am very confident that a majority of employees know how to spot and prevent a cybersecurity attack.

2. I am very confident that a majority of the employees know how to exercise safe data security practices.

3. I am very confident that a majority of the employees know how to handle confidential data and follow the organization's processes.

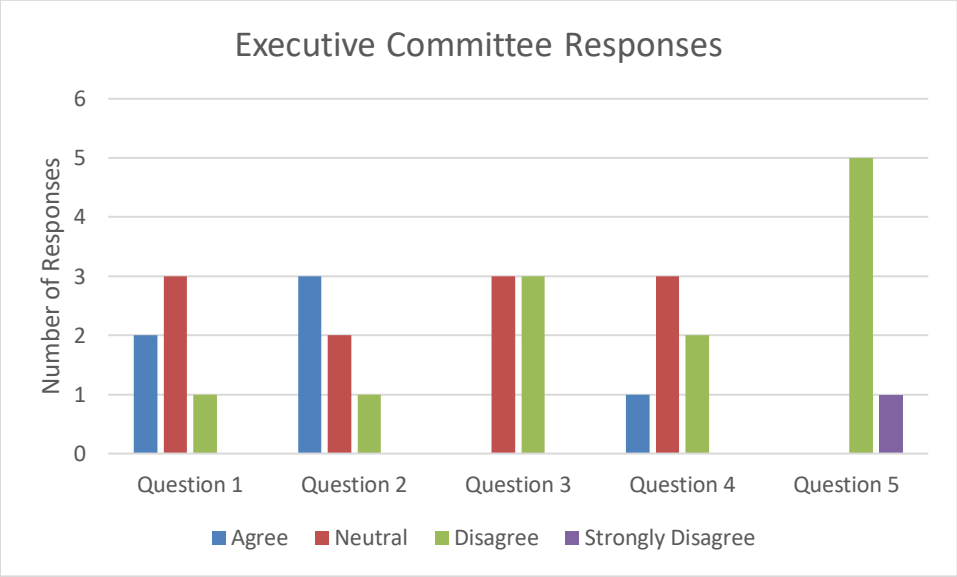
4. I am very confident that the organization will not suffer a major cybersecurity attack as a result of an employee's negligence.

5. I am very confident that the organization could withstand the financial impacts of a major cybersecurity breach.

Prospectus/Needs Assessment

Figure 1 illustrates leadership was not very confident in the overall knowledge and skills of employees regarding cybersecurity and showed no confidence that the organization could withstand the financial impacts of a cybersecurity attack. A comments section was included in the survey and 4 of the 6 respondents stated that the confidence threshold of 90% or higher was a determining factor in their scores. Compliance and contractual obligations require that 100% of employees pass an annual security training, thus the reason for the high threshold. However, it cannot be determined if there is a direct correlation between an employee passing the security training and having the prerequisite skills to prevent an attack; but it will do no harm and is already a required intervention based on contractual agreements and compliance.

Figure 1



Ten employees were sent an anonymous online survey focusing on employee compliance training. Specifically, modality preferences, their technological skill level, and overall confidence in preventing cybersecurity attacks.

Five questions were included in the survey with a Likert Scale from 1-5 (1 = STRONGLY AGREE and 5=STRONGLY DISAGREE). The following questions were included in the survey:

1. I am very confident in my skills to prevent a cybersecurity attack related to my account and passwords.

2. I am very confident in my skills for safe data security practices outlined by the organization.

3. I am very confident in my skills on how to handle confidential data following the organization's processes.

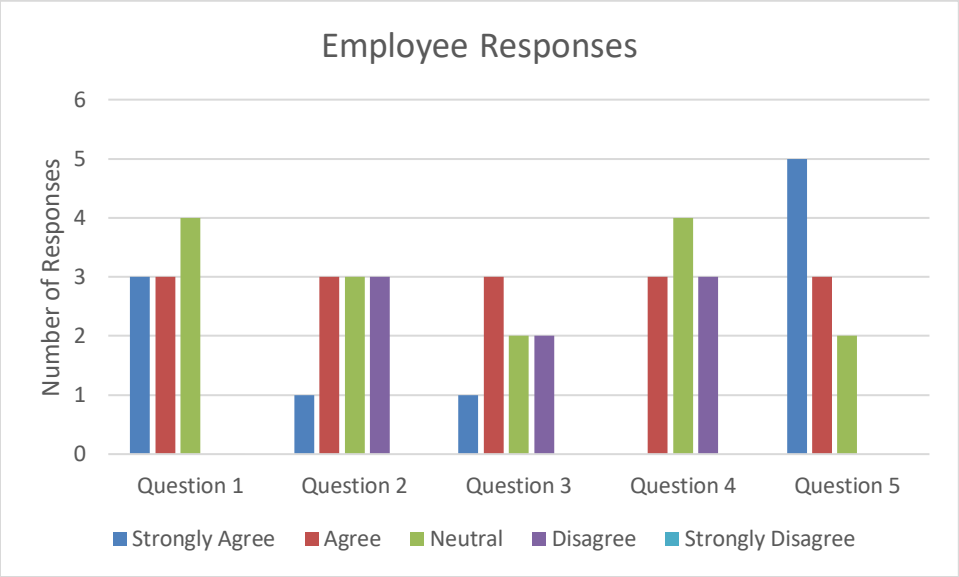
4. I believe elearning is the best way to deliver annual security awareness training.

5. I am very confident that my technological skill level is intermediate or advanced.

Prospectus/Needs Assessment

Figure 2 is a representation of responses from employees. Respondents felt the most confident in the modality of the training and their overall technological skills. However, they felt less confident in their cybersecurity skills, but not as much as the Executive Committee respondents. Confirmation of knowledge and skills in this subject matter area could be achieved through a knowledge assessment.

Figure 2



Learning Objectives

Based on the needs analysis results, the following training objectives have been developed for both the organization and employees:

- Employees will correctly recognize and report phishing attacks 95% of the time.
- Employees will model safe data security practices 100% of the time.
- Employees will demonstrate how to handle confidential client data 100% of the time.
- At the end of training, employees will demonstrate competency by achieving a score of 90% or higher on the knowledge assessment.
- The organization will demonstrate compliance by reducing the number of cyber breaches originating with employees by 80% annually.

Prospectus/Needs Assessment

What's Been Said

1. Merrill outlines and discusses in detail his 4 principles of instruction; problem centered, activation, demonstration, and application. He summarizes in each section the critical components to meet the criteria for each of these supported by additional research in this field. These principles can and should be applied to all learning regardless of the modality. (Merrill 2002)

2. In this paper, an exploratory study of 954 workplace learning professionals was conducted and analyzed. Results from the study revealed that elearning was the most useful in areas of company updates to products and compliance training. Elearning was not as suitable for employee development programs. (Rossett and Marshall 2020)

3. This study examines corporate training programs and the application of learning and development strategies that are applied both in elearning and classroom modalities. Specifically, there was an absence of implementing strategies that promote training transfer (after training strategies) in both settings, more so with elearning than classroom settings. (Beinicke and Kyndt 2020)

4. This study focuses on the training of retail employees and the use of games to increase engagement. The group that was allowed to participate in games as a post training exercise proved to be more engaged than the control group. Incorporating games in corporate training can help with the engagement of employees. (Kapp, Valtchanov, Pastore 2020)

5. This article examines adult learning and employee training through the use of UDL (Universal Design for Learning) formerly reserved until now for K-12 education. This allows the designer to develop and implement training and design for all learners not just the average learner. In addition, technological uses of UDL are recommended for all steps in the training and development process. (Gronseth and Hutchins 2020)

References

Beinicke, A., & Kyndt, E. (2020). Evidence-based actions for maximising training effectiveness in corporate E-learning and classroom training. Studies in Continuing Education, 42(2), 256–276. https://doi.org/10.1080/0158037X.2019.1608940

Gronseth, S. L., & Hutchins, H. M. (2020). Flexibility in Formal Workplace Learning: Technology Applications for Engagement through the Lens of Universal Design for Learning. TechTrends: Linking Research and Practice to Improve Learning, 64(2), 211–218.

Kapp, K. M., Valtchanov, D., & Pastore, R. (2020). Enhancing Motivation in Workplace Training with Casual Games: A Twelve Month Field Study of Retail Employees. Educational Technology Research and Development, 68(5), 2263–2284.

Merrill, M. D. (2002). First Principles of Instruction. Educational Technology Research and Development, 50(3), 43–59.

Rossett, A., & Marshall, J. (2010). What Corporate Training Professionals Think About e-Learning: Practitioners' Views on the Potential of e-Learning in the Workplace. Journal of Asynchronous Learning Networks, 14(2), 19–27.