Write Up - *The Human Factor in Cybersecurity*

As a chief information security officer, it most definitely will be challenging to balance a limited budget for additional cybersecurity technology and employee training. This is the plan overview that will be implemented: conduct an assessment of current technology and employee training, review assessment and allocate resources based on priority, then monitor and adjust resources accordingly.

ASSESSMENT…

Conducting an assessment will set the foundation. The assessment will cover the current cybersecurity technology used and employee training which will reveal areas that require immediate attention. Interestingly this strategy is similar to the NIST framework. Cybersecurity technology will be assessed for any holes, outdated systems, and software that need to be upgraded or replaced. This should decide if new technology would significantly improve security or if it's sufficient. The next important step is to evaluate employees' cybersecurity awareness and skills. A few examples that would be focused on is the awareness of phishing scams, which are messages that appear to come from legitimate sources but are malicious attachments. An extremely important one is having weak passwords, this simple thing could easily compromise their device or network. Once the assessment of training and technology is concluded, you can look at the state of each and see the current level.

PRIORITIZE…

Even knowing the level of employee training and current technology utilized, doesn't mean you can easily make a decision for fund allocation. There's a lot of variables to consider when you look at it based on what is priority. To determine the priority, you would look at the likelihood of security incidents based on historical data and recent threats of technology and training. Then assess the financial impact of those recent and previous threats. This data should provide a good overview of what should be prioritized. Unfortunately this still does not determine the budget allocation because organizations will have specific needs based on long or short term goals. What I mean is that what's a priority now could be a short term solution that wouldn't get you to the long term goal. So by evaluating the cybersecurity technology and employee training data acquired, you would prioritize based on your organization's unique needs and goals. This will ultimately lead to making the final decision to allocate the limited budget effectively and provide a solid foundation to solve similar future decisions.

MONITOR AND ADJUST…

The decision for budget allocation will change, so to account for this I would continuously improve how cybersecurity resources are used. Technology rapidly evolves and so do people so you have to monitor and re-assess the current levels overtime. The main steps taken will include figuring out how well employee training programs are working, figuring out how well investments in cybersecurity technology are working and staying up-to-date on new threats. I would use employee surveys/tests or Possibly simulate an attack as an exercise to figure out the current state of things.This could mean changing how the budget is spent on training and technology. By putting in place continuous monitoring and adjustments allows for an effective way to manage a limited budget.

CONCLUSION…

To summarize, the best way to determine a balance of funds between training and technology is to assess, prioritize based on goals/ needs, then monitor and adjust accordingly. This will provide the solution for determining budget allocation for employee training and cybersecurity technology.

By: Adrian Galvan