Quinn Doak **11/14/2024**

The Human Factor in Cybersecurity

Trying to balance a small budget between training additional cybersecurity professionals and improving cyber technology is hard. It requires serious consideration, and you need to consider risks, existing security protocols, and the fact that cybersecurity is always evolving. Here's is how I would allocate the funds and my reasoning behind it.

---

1. **Prioritize training**

   According to Verizon, 74% of breaches involve a human element, this includes things like phishing attacks or credential thefts. (Verizon, 2023) On top of this, the average data breach will cost a company $4.45 million dollars, but breaches caused by phishing attacks are significantly reduced when employee training is implemented. (IBM, 2023).

---

2. **How to implement training**

   As seen above, active training is crucial. So how do we go about implementing it? Here's a few ways that I think could help benefit all employees and prevent the number of breaches.

   - Implement regular cybersecurity training sessions
   - Provide more specific training for IT teams, focusing on building a strong incident response team
   - Implement simulated phishing campaigns; this helps test your company and gives you an idea on who to focus your training on.

---

3. **Investing in technology**

   On top of training, investing in technology is also very important. Certain tools can help you automate very tedious tasks and overall free employees' time to work on other projects. In general, technology forms a critical layer of defense; being able to detect things humans wouldn't be able to. In addition to this, many industries such as healthcare or finance require specific technologies to be in place in order for them to be compliant.

4. **The trade off**

   A saying that has been said 100 times but worth bringing up is that your security is only as strong as your weakest link. All it takes is one person to interact with a phishing attack and bring your company down. This is why it's so important to have proper training for everybody in the company. However, the trade-off is you might have less money to invest into technologies.

5. **Conclusion**

   In conclusion, balancing a limited budget is a hard but important task that requires careful thinking. By focusing on training employees, companies can address the human element that contributes to majority of breaches, which can help reduce overall vulnerabilities. At the same time, investing in the proper technologies helps provide a crucial layer of defense, and can save employee time by having processes done through automation.

References

1. Verizon. (2023). *2023 Data Breach Investigations Report*. Retrieved from Verizon Report.
2. IBM Security. (2023). *Cost of a Data Breach Report 2023*. Retrieved from IBM Report.