Juwon Brunson
CYSE 200T
Jbrun001@odu.edu

Allocation of funding for 2026 memo

The allocation of our funding for the year 2026 should be as follows: 90% available funds for the training of employees and 10% of funding into R&D of new technologies to combat cyber threats

Funding allocations

Good morning, I am requesting the available funding to be allocated on a 90/10 split for the training of employees and material required for training, and Research / Development. This allocation would allow us to primarily focus on the intensive training materials and regimen that we have planned for 2026 as cyberattacks increase. The IT department has stated that "employees are falling for classic phishing emails that do not have complexity," which is concerning to me and should be to you as well. The reasoning this should be concerning is that if employees are falling for the most basic cyber intrusion tactics at a rate of 34.3% then what is their failure rate for attacks, we cannot self-test for, like tailgating, vishing, spear phishing?

Examples

Examples of cybersecurity training being the most important asset that we can obtain would be from a recent 2025 report by the United States Cybersecurity Institute (USCS) states that "Human error is the weakest link (States)" with their research showing that most of the breaches occur through human error which consist of "clicking a malicious link, using a weak password, or mismanaging data. (States)" .

This is consistent with what we have seen throughout our company as well with employees clicking on malicious links that were generated by the IT team for training. Our improved cybersecurity training would be able to help reduce these clicks and keep our company safer. Employees would be able to

understand the importance of our training as not just a checkmark by HR, but as a way for them to serve the company and themselves by gaining knowledge.

Reasoning behind the allocation request

As shown above in the examples section, our reasoning for requesting the funds is imperative. We would reduce the rate of which employees are clicking on malicious links, reduce the amount of incident responses needed because of these clicks and access to our systems, reduce the man hours and funds needed to get back into compliance for the organization, and most importantly reduce the risk likelihood that we will be fined for violating compliance standards as outlines in PCI-DSS, HIPPA, GDPR, and other standards we work with.

References

- *PHISHING by INDUSTRY BENCHMARKING REPORT 2024 EDITION PAGE 2. 2024.*
- States, United. "Why Cybersecurity Training Is the Smartest Investment for Organization in 2026." *Https://Www.uscsinstitute.org/Cybersecurity-Insights/Blog/Why-Cybersecurity-Training-Is-The-Smartest-Investment-For-Organization-In-2026*, 2025, www.uscsinstitute.org/cybersecurity-insights/blog/why-cybersecurity-training-is-the-smartest-investment-for-organization-in-2026.