Trey Pennix

CYSE 200T

Prof. Duvall

11/18/25

Write Up - The Human Factor in Cybersecurity

BLUF: To maximize risk reduction with a limited cybersecurity budget, I feel like prioritizing a balanced approach: invest 30–40% in employee training to reduce human error, 40–50% in essential security technologies to defend against unavoidable technical threats, and 10–20% in automation tools that minimize reliance on perfect human behavior.

Foundational Human Training

Humans remain the top attack liability with phishing, misconfiguration, password reuse, and poor data handling causes a large percentage of breaches. Even expensive technology can’t compensate for consistently unsafe behavior.

I would invest in:

✔ Role-based training

- Basic cybersecurity awareness for everyone.
- Deep-dive secure coding and cloud security training for developers.
- Privileged access training for admins.

✔ Phishing simulations + feedback

Measurable, adaptive training reduces click rates dramatically.

✔ Clear, simple security policies and job aids

Training is ineffective if employees can’t remember how to do secure actions; cheat sheets and embedded guidance help.

Training is extremely important and reduces the likelihood of incidents across the entire workforce. With 30–40% of the budget, the organization can significantly minimize human error without overspending.