26 October 2025

Human Factor in Cybersecurity

I would balance the training so that each employee is at least trained on how to use any new cyber equipment and how to avoid common attack vectors. This means that if the cost to implement a new technology was around $1 million, I would spend around $200k on ensuring all employees know the basics of the software and how to be safe with it. This may seem like a large sum of money, but compared to the cost in time for the IT department solving simple issues, or the much larger sum of money that would be paid to fix damages caused by vulnerabilities or exploits, this may even be a low amount to spend.

An example of this is if a company introduced a new VPN and wanted to train employees on it. I would have the employees learn how to connect to and use the VPN, and most likely some common issues and how to fix them. I would also train them on how to avoid issues, such as making sure the VPN is connected at all times, telling them not to share their login, and telling them some other company specific limitations. This ensures that most bases are covered, and helps limit the human error in cybersecurity, as informed users are much less likely to cause problems than ones who know nothing, especially when it comes to how to use the technology. Introducing new technology can improve the lives of employees, as well as allowing them to do faster and better work, but it is critical that employees are trained on how best to avoid pitfalls and security issues.