Mark Migdal 11/16/2025
CYSE200T

Human Factor Within Cyber Security

In this paper we will cover the human factor within cyber security. We also cover what should be prioritized, cyber security technology or training for employees.

What is the “Human Factor” of Cyber Security?

The Human Factor refers to how humans or employees affect cyber security. You can have a flawless cyber security system, but it can be easily messed up by one person. An example of this is phishing. With just one click of a link, an attacker can be in a system. The Human Factor is the biggest risk to a company and their security. Employees being educated on the risks can be a major way to eliminate some of that risk. The other way to help eliminate this risk is upgraded security. This does eliminate the whole human factor risk, but it can be much more expensive.

Upgrading Security

Upgrading security seems like the best option at first glance but I believe that it might not be that simple. While upgrading security is always important, and there likely should be some upgrades, it is not very cheap. Although it's not cheap, there are some simple things that can make a major difference. Things like password expiration, MFA, and no trust policies can make for major protection upgrades.

Training Employees

Training employees can be a simple, and fairly inexpensive, way to keep an organization safer from attackers. There's a couple of ways to do this. The first is using outside people or programs to trainer employees. While this is the best and most effective way to train, it can be expensive if you choose the best programs out there. The other option is in-company trainers. Using cyber security employees to help train can cut down on cost a lot. Employees may not take it as seriously because their co-workers, and the people who teach this may not be the best at it which could cause for some subjects to be missed.

Conclusion

After looking at both of the options, I believe that a bit of both are needed to ensure the safety of an organization. Without good security, it won't matter how much training is done, attackers will be able to enter the systems. But without training, all the upgrades could be bypassed because of employees misunderstanding of security.