Reed Wilhelm

CYSE 200T

Professer Kirkpatrick

11/20/22

Dealing With The Human Factor in Cybersecurity

Cybersecurity is a complex issue that has always accompanied computers, and as hackers continue to come up with more creative ways to break security measures, the issue is only growing. However the biggest problem in cybersecurity isn't hackers, its users. In this paper I will discus the human impacts on cybersecurity and how I would mitigate those risks as a CISO.

The Human factor in Cybersecurity

In Jeff Capone's article, "The impact of human behavior on security," he starts by pointing out that its human nature to try and be as efficient as possible, and the most people will use the easiest and fastest way possible when accomplishing a task, this efficiency, however, is also our biggest problem when is comes to security. The issue is that when it comes to security, efficiency typically means shortcuts, and these shortcuts are what causes issues. Capones idea that humans are the weakest link in security is backed up in the article titled, "Why Is Cyber Security About Human Behavior?" The author of this article observes that many of the cyber threats around today originated from the 1960s-1980s, and that they've simple matured along with technology. The author goes on to mention how the reason that these same attacks are more successful now is because, while the concept is the same, the attack vector has changed to a more hybrid model. This hybrid form of attack means that the victim plays a part in their own downfall, the rise of

these hybrid attacks can be seen as “over 90% of successful breaches worldwide start with a phishing email,” (Why Is Cyber…).

Solving The Human Factor

Now the problems of the human factor in cybersecurity can’t be completely solved, however I have come across a few ideas that have been shown to mitigate the risks humans present. Recently I had the chance to speak with the CTO of organization that runs .org (The CTO gave me permission to reference our discussion, their position, and their organizations services, in any upcoming papers for my schoolwork, however they did ask me avoid directly naming them or their organization.) while I talking with them I had the chance to learn a lot about how they handle cybersecurity in their organization, and the point they stressed the most is how much training has changed in the last five years. They said that five years ago any cybersecurity training would’ve typically been an hour-plus meeting that happened once a year, however, training gradually evolved, cyber training went from once a year to once a quarter, the meetings also got shorter and more practical. The CTO said that now their training consists of two things, first is monthly meetings, theses are roughly 20 minute meetings that often consist of short vides from MimeCast, this is the example video they showed me. The second part of cyber training at their organization is a very short weekly meeting that the CTO referred to this as their “60 Seconds of Security” meeting. They described 60 Second of Security as a “short set of slides that covers things from basic internet hygiene, to the latest cyberthreat trends.” The CTO said that providing training through theses shorter more frequent meetings is both more effective and efficient for the organization.

The Tech Side

After I talked about training with the CTO, they said that no matter how much training they do its inevitable that eventually someone makes a mistake, so to help prevent this they essentially "baby proof," their environment. The two main things they use to do this both involve email. The first thing they do is any link that is received by a company email has to be checked and cleared before it opens. They do this by running links through a third-party program that rewrites the URL and checks to see if its on a "bad link list", this program also acts as an extra layer of defense if the link is deemed "sketchy." The second thing that they use to protect their emails is a program that checks the sending email address, they use this because of how easy it is to forge emails addresses that look like they're from within the companies. This program is also useful because it flags any addresses throughout the company that has potential to be fraud.

Conclusion

I think that the first things I would implement to mitigate to human factor would be the two email related things the CTO mentioned, the program to rewrite URLs and the fraudulent email flag system. I would also implement a similar cybersecurity training to what the CTO said. I personally, used to think that focusing on training was somewhat foolish as I figured the average employee probably wouldn't pay attention, however when they mentioned how their training has evolved into shorter a more digestible meetings, I quickly came around to their side of thinking. Overall I think the issues presented by the human factor can't be completely solved, however there are ways that have proven to be effective at mitigating the risks that we present.

Sources

Capone, Jeff "The impact of human behavior on security" May 25, 2018 https://docs.google.com/document/d/1J3v_V167mktbGVynbtHW8yHXW9onjaBzVASo-behDfY/edit

"Why Is Cyber Security About Human Behavior?" cyberbitsetc.org. https://docs.google.com/document/d/1QplIrfcKlmkSOuKt9i0Kte72kYrukFeCm1wj9DxpnGU/edit#

Interview with CTO. I know me using this person as one of my sources might seem questionable, they didn't want me to directly name them or their company in writing so that's why it looks a bit vague. If you have any doubts as to how legit this actually is feel free to shoot me an email and we can set up a time to talk about it. (Also here is another link to the example trying video they showed me.)