Notes 1
Zero Trust presentation

In a world where everything is mutating and evolving at a faster rate, it is hard to see what is really changing. Even in the cyber world people are getting smarter and creating new ways to get access into places. One major advantage the hackers have is trust, they use trust that the systems have in the users and the accounts to give them access into a system without any doubts that the person they granted access to will do anything bad. But at this point in time we need to take away that advantage they have over companies, with this new model of security “Zero Trust”. The Zero trust model in simple terms makes the system trust no one, no matter how long you've been working, no matter what level of trust everyone has with you. We need validation and proof that you are who you say you are. With new ways to validate yourself to the system this would allow less attacks and less time an attack could last.

For the Zero trust model to work there needs to be an implementation of a protocol called IAM. IAM stands for Identity and Access Management, this protocol allows us to manage authentication of who is the user and the authorization of a user to what they can execute. For authentication of a user there are a few ways to secure against data breaches resulting from password compromises. Such as multi-factor authentication, Role based access control, and attribute based access control. They all work well in their own ways for MFA one common way is used is that if you were to sign into an account before you are given access to your account you would have to verify by 2 factors that it is you signing in, they send a randomly generated pin to your phone then you would have to enter the code. With MFA the 2 factors in this situation is 1st the password being sent which is something you know, and the 2nd is your device the password is being sent to which is something you have. This is one of the best because if it's not you logging into your account you now have knowledge that someone is trying to gain access, but on the other hand if the attacker has your device then the defense is flawed. Another good defense is attribute based access control or ABAC. This gives the system a base of knowledge such as attributes of the user for what time they normally login and logout, what they do on a daily basis, and if any attributes seem suspicious then it will take action to prevent an attack from happening.

Now in the present time there are ways to eliminate the entry of manual passwords in a system. The most common solutions are FIDO2, security keys, and biometric ID which include face ID and touch ID. “ A FIDO2 security device allows the generation of a cryptographic private/public key pair. Unlike password-based systems where a shared secret (password) is held by both users and the website, the private key never leaves the user’s possession. The user proves their identity to the website by creating a signed message, the message is signed using the user’s private key. The website validates the signature on the message using the user’s public key which has been passed to the website during registration. The security is further enhanced by requiring the user to be validated by the FIDO2 device, using a PIN or biometric or PIN, before private keys can be generated or used.” “(2020, February 5). *What is FIDO2*. Oxford Computer Training. Retrieved February 5, 2020, from https://oxfordcomputertraining.com/glossary/what-is-fido2/ “ This article from this website gives

great detail about FIDO2 and how it can be implemented in a system to eliminate password entry by using public and private key. Another solution that can be used to eliminate manual password entry is biometrics. Biometrics include face ID and touch ID, each of this solutions tracks the users physical evidence of identity to a scanner–placing their finger on a fingerprint scanner for Touch ID and placing their face to the camera to scan facial features of a user for Face ID.

By having these solutions to replace manual entry of a password this would cause reduction of audit findings and improve compliances. Such as being able to know that the private key was only given/ created by the user which would limit entry access, and by having biometric scanners you would know who is trying to gain access by the face/ touch id that was given to try and gain access into the system.

With Zero Trust protocol in place it would reduce data breaches, which would reduce cost by either having to give money out to attackers, paying for forensic analysts, inhouse investigations. And in total can cost millions if companies don't have the best defenses.