**Lab 8 – Identity and Access Management**

**1) Research and describe the concept of non-repudiation.  How does it apply to electronic authentication, particularly to this situation?**

Non-repudiation refers to the ability of a system to counter repudiation threats. Repudiation refers to users who deny performing an action – the opposing party has no evidence to counter the claim. Electronic authentication supports the first probative value of non-repudiation – an example would be a digital signature to verify an account. In the case of the unauthorized access to the CEO’s healthcare account - the jilted party used the same authorized login to delete all of their Open Enrollment information, so it may be difficult to prove that any wrong-doing occurred from a third party.

**2) How could the system be modified to use biometrics to ensure non-repudiation?**

Because digital signatures and “secure” access to online accounts cannot always guarantee total security, biometrics are now being introduced into technology to help provide an additional layer of security. An example of biometrics system currently in place is the fingerprint scanner already present in many non-repudiation systems. Requiring a fingerprint scan in addition to providing login credentials can help to prevent unauthorized access and fight against repudiation threats. If a fingerprint scan was a required security measure to access the healthcare account, the CEO could argue that this biometric was not given at the time.

**3) Besides biometrics, what other suggestions for authentication methodologies, technical or non-technical, would you offer to help ensure non-repudiation?**

Secure Sockets Layer (SSL) provides authentication, data encryption and enforces data security by utilizing a public key infrastructure. SSL uses the exchange of certificates that are verified by trusted certificate authorities to provide authentication. SSL uses digital certificates (X.509 v3) and a public/private key to authenticate users within that system. The SSL protocol is one of the most-used encryption practices to date.

Public Key Infrastructures (PKI) utilizes multiple-step authentication protocols and security. Many companies now require a PIN or smartcard to log into their internal network. This would help deter unauthorized account access because the attacker would need to have multiple forms of authentication to get past the authorization stage in a PKI environment.

**4) As companies move more and more towards telecommuting, what other situations could arise in which a simple login and password would not be enough to ascertain the employee’s identity and prevent fraud?**

Telecom providers utilize large-scale network infrastructures to manage voice and data transmission. Stored communicative data is a vulnerable target for attackers due to the potential sensitive nature of the shared information. Denial-of-service or DDos attacks occur when multiple systems flood the bandwidth or resources of a targeted system. The telecom industry is an exceptionally vulnerable target for DDos attacks - telecom devices that are designed for security have been turned into attack vectors. Intrusion Prevention Systems (IPS) which are designed to prevent attacks fell victim to a DDos outage.