Security culture is where everyone in our organization knows their part in keeping valuable organization assets safe. It is much more than a set of Dos and Don’ts on a message board. It overrides ignorance and laziness because its not just everyone’s livelihood. It’s how we communicate. This is important because although we may install the most expensive IPS in the world, it can be rendered useless upon insecure behavior.

We need every machine facing employee to implement a Zero Trust Security mindset. Zero Trust Security is where everyone understands that any machine, website, or link that connects to a company asset immediately becomes an additional liability and vulnerability for our company. This mindset translates to anyone approaching an insecure behavior should feel the social pressure to do the right thing. It should have the levity of a game, but still be serious. Our employees have the knowledge and confidence to exert, expect and reinforce Zero Trust Security upon themselves and each other.

The next step is to implement administrative controls. This includes notifying the entire IT department of all security actions including testing and training. Security incidents are always reported to the CISO. If there is a breach of assets, a Crisis Manager should be appointed to hold all parties accountable and liaison with legal authorities for correct reporting and auditing procedures. Our HR and legal teams need to already be involved at a quarterly basis to test employee awareness of all security principles of weak points in our organization.