**Zero Trust Deloitte Document Summary**

Zero Trust is an approach to cyber security that help organizations defend against the innovations hackers are making. Now, attackers are more organized, better networked and have more access to tools, so businesses have to be more prepared. Also, due to rigid cybersecurity constraints, if a hacker can gain entry to one system, they may be able to get access to many. Furthermore, cloud computing and digital collaboration software opens up holes in cybersecurity.

In all verity, Zero Trust is a framework that is based on the principle of “never trust, always verify”. I think this requires both internal and external keys to be validated consistently. Apparently, this is transformative. I think users, IoT devices and regular computers write to the cloud and other similar applications.

The benefits of switching to Zero Trust include: enabling trust in the modern workplace by allowing people to securely work remotely, supporting digital goods and services, mitigating risk and cost as well as making businesses more agile.

Zero trust makes enterprise architecture move from static, complex and reactive to a more simple and dynamic system. It allows users to use public rather than private networks, and from disparate identity stores to consolidated identity stores. Beyond this, it sounds like users would be able to use more types of devices, and store data using org wide classes. Security would also become more organization consistent, rather than siloed but department.

To adapt to Zero Trust, people star from frustration when they realize their current systems all need to change. Slowly, as people see improvement and modernity in new systems, acceptance, trust and love are fostered. Taking the first step seems daunting, but it does not require starting completely from scratch. You can take the pieces of existing org security, shuffle them and add new and next generation technology.

Some benefits of Zero Trust include reducing the blast radius of cyberattacks, making user authentication easier, allowing for users to bring their own devices to work, being industry 4.0 ready, and adaptive cybersecurity.

Some challenges in adopting zero trust can be encouraging organizations to adopt the new tech, integrating with legacy systems, building a complete end to end solution, and allowing for updates and changes that the future will bring.