Personally "no one is safe" is the way that I always thought that all security should be treated. Regardless of whether the user is connecting from within a secured network or from home. Every connection and every user should be verified before access to a system is granted and if that user needs to access a different sub-system within that system then the user would be authenticated again.

Whether it be within a banking system or just my personal email, I feel that zero trust would be beneficial to all parties included, users and business. If I want to access my bank account or email, ask me security questions, send me a secured SMS, or whatever means you need, to prove I am allowed to have access and then grant me access. I would feel much more secured and safer with my personal data if it were on a zero-trust basis.

When it comes to developing a system to encompass zero trust I would imagine that setting up a zero-trust platform and setting it as coding standard would be much easier than not having any security or even just leaving it till the end of the SDLC. They could simply add a protocol that trusted no-one or sent users to a 2FA to verify that user before access was granted to a system not only could they increase the overall security of their systems but their clients and users as well. And when it comes to clients and users, if they feel safe with you they are more likely to continue to be your client and not move to a competitor.

Implementing zero-trust would essentially and potentially save a company time and money if implemented correctly. If a company were to instruct their developers to envelope zero-trust into their normal coding standards and protocols so that they were to use a zero-trust within each application or set of code. That company could ensure that their users and data were safe and secure allowing their users more freedoms and allow the clients to have peace of mind when working with their company.

Secured data ensures less malicious information getting into the system and thus making it easier for developers to find any paths that attackers are using and either block or delete those paths saving that company money that would have been used to secure those path ways after a breach.