Secure coding should be regarded as a requirement not a standard. Keep your programs secure and the data that it stores out of malicious hands is a must. To keep your programs secure, you should implement security throughout the entire production process. Types of securing methods include input validation and data type management. While both of these items seem simple, they are a firm way to interrupt a hackers ability to breach your program.

The secure coding standard I would like to adopt is Defense-In-Depth or DID for short. DID is a method for using multiple security layers to cover the flaws that each layer might present. This allows each layer to check and balance the other layers and keep the whole system cohesive and secure. While introducing DID into your system might be costly to setup up and maintain, the initial costs most definitely outweigh the potential data breach. Data breaches can effectively cripple a company, so securing your code to the best of your ability is a small price to pay. (Fortinet)

Zero Trust is a business model which is meant to secure data from anywhere and anyone in the world. According to Check Point Software Technologies, around 70% of data breaches are from compromised devices. These devices include mobile devices, IoTs, and computers alike. To help combat against data breaches, the Zero Trust model checks all login instances and authenticates whether that user is allowed access. While you yourself might not intentionally allow hackers to use your devices to breach a company’s network, the chance always existed for it to happen. Ignorance can lead to a massive amount of capital loss. (Check, 2019)

Overall, both DID and Zero Trust should be implemented into a company to ensure that all bases are covered inside and outside of the company. DID adds multiple layers of security to the companies programs. Zero Trust creates a better authentication platform for the company. Both strategies can work together to create a well built and maintainable security system which can stand up against even the best of hackers out there.

**Resources**

fortinet. (n.d.). What is defense in depth? defined and explained. Fortinet. <https://www.fortinet.com/resources/cyberglossary/defense-in-depth#:~:text=Defense%20in%20depth%20is%20a%20comprehensive%20approach%20that%20employs%20a,data%2C%20applications%2C%20and%20networks>

Check Point Software Technologies, Ltd. (2019, November 22). What is Zero trust security?. YouTube. <https://www.youtube.com/watch?v=1D5mg9an19o>