# T-Mobile promises to try not to get hacked again

**Corporate Governance** – T-Mobile's Chief Information Security Officer will give regular reports to the board concerning T-Mobile's cybersecurity posture and business risks posed by cybersecurity. This is a foundational requirement for all well-governed companies. Corporate boards need both visibility and cybersecurity domain experience in order to effectively govern. This commitment ensures that the board's visibility into cybersecurity is a key priority going forward.

**Modern Zero-Trust Architecture** – T-Mobile has agreed to move toward a modern zero trust architecture and segment its networks. This is one of the most important changes organizations can make to improve their security posture.

**Robust Identity and Access Management** – T-Mobile has committed to broad adoption of multi-factor authentication methods within its network. This is a critical step in securing critical infrastructure, such as our telecommunications networks. Abuse of authentication methods, for example through the leakage, theft, or deliberate sale of credentials, is the number one way that breaches and ransomware attacks begin. Consistent application of best practice identity and access methods will do more to improve a cybersecurity posture than almost any other single change.

https://www.theverge.com/2024/9/30/24258763/t-mobile-fcc-settlement-cybersecurity-investment