Made in partnership with orrick

US DATA PROTECTION LAWS OVERVIEW

If you're doing business in the US 2022 and have access to people's personal information, you need to know about data protection law (or "cyber-security law").

WHAT ARE DATA PROTECTION LAWS?

These are laws that govern what companies need to do to *protect personal information or systems*.

- There is no uniform standard federal legal requirement for cyber security.
- Instead there are about **30 different state laws** and a patchwork of **federal laws and regulations** that apply based on *industry* and the *type of data* a company processes.

FTC ACT

The main federal law. Prohibits unfair trade practices.

- The FTC Act passed in 1914, so they *probably* weren't thinking about cyber-security.
- But since then, the FTC has interpreted unfair trade practices to include "unreasonable security practices."

REASONABLE OR APPROPRIATE SECURITY

This is what many state laws require, it involves:

- **Risk Analysis**: companies should assess their potential *risks*, the *cost* of mitigations, and thus the value of mitigation options
- **Industry Customs**: what other companies in the industry are doing

HOW BUSINESS ADDRESS THESE RISKS

by building out a security program that is tied to a **recognized industry framework**- which addresses key security controls, like

- Encryption
- Monitoring
- Authentication
- Training

THIS DOESN'T *GUARANTEE* LEGAL COMPLIANCE

But it is a great start. There are also many other, more specific cybersecurity laws:

- **Defense Federal Acquisition Regulation Supplement (DFARS)**
- **HIPAA-** Healthcare
- **GBLA-** Finance
- **NERC CIP-** Energy and utility companies

All of these sectors have more rigorous cyber-security requirements that address issues like *encryption, monitoring, and authentication.*