6.8: Legal and Compliance Requirements

The increase in consumers' concerns over their privacy has led to new legal and compliance regulations.

Here is a brief overview of some key legal and compliance regulations related to information security that are relevant to businesses:

- PCI DSS (Payment Card Industry Data Security Standard) - Sets security requirements for any organization that processes, stores or transmits credit card data. Ensures secure handling of payment information.
- HIPAA (Health Insurance Portability and Accountability Act) - Requires protection and limited disclosure of patient health data by healthcare providers, insurance companies, and related businesses.
- GDPR (General Data Protection Regulation) - European Union data privacy regulations that govern how personal data is collected, stored and shared. Impacts any company dealing with EU citizens' data.
- CCPA (California Consumer Privacy Act) - Gives California residents rights over the personal information that businesses collect about them. Affects any company with CA customers.
- FERPA (Family Educational Rights and Privacy Act) - Governs access to student educational records; applicable to any educational institution receiving US federal funding.
- NIST Framework - Cybersecurity guidance for US federal agencies and contractors working with the government. Widely adopted as best practices.

Adhering to these regulations is mandatory, not optional, for any business that falls under their jurisdiction.

Fun Facts: What was the impact of GDPR to Google and US businesses?

The EU's General Data Protection Regulation (GDPR) came into effect in 2018 and imposed strict new requirements around data privacy and security. As one of the first major cases enforcing GDPR, Google was fined €50 million euros (~$57 million USD) that same year by French regulators for lacking transparency and consent controls for ads personalization.

GDPR has compelled many US companies to overhaul their data collection practices and security measures if they have any customers in the EU. Violations can lead to fines up to 4% of global revenue. Even for small to mid-sized US companies, GDPR prompted significant investment in consent management, data minimization, breach notification procedures, and other areas to avoid facing similar non-compliance penalties.

Do you remember that in that time frame, when we visited websites and received new prompts such as "by clicking Agree', you consent to us...", or "manage your preferences," etc.

It was not cheap to implement GDPR either. It could cost small businesses with less than 500 employees, around $9000.00 to meet compliance. It could be up to millions for large global companies!