Road to PIPA Week 13: DETERMING YOUR ORGANISATIONS RISK THRESHOLD

An organization’s risk threshold is the measure of ‘acceptable risk’ for an organisation – the severity of potential harm combined with the likelihood of an incident indicates a threshold above which a risk becomes unacceptable. Risk should be viewed from both an organisational and an individual perspective.

Information Security (organisational risk)

Risk is viewed with respect to potential damage to the organization and its assets – both tangible and intangible.

Data Privacy (risk to individuals)

Risk depends on the impact/harm on the individuals.

$$\text{Risk} = \underbrace{\text{Likelihood}}_{\textit{For example: vulnerabilities, exposure, threats, mitigating controls}} \times \overbrace{\text{Severity}}^{\textit{For example: critical functions, reputation, etc.}}$$