Information Assurance

Domain 1

Information Security Governance

Part B

Information Security Strategy

Goals and Strategy

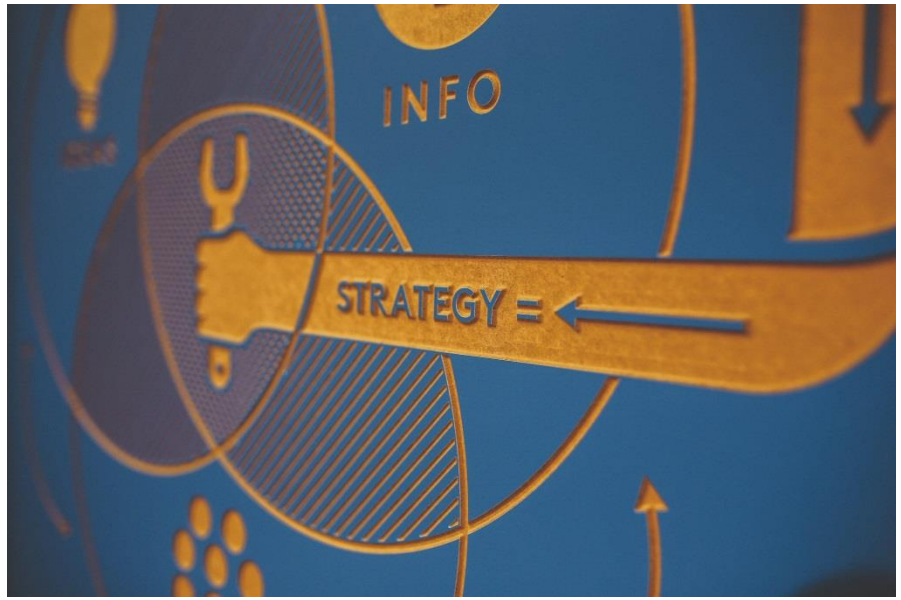
- Business goals are set by the board of directors
  - Senior management builds the strategy to achieve these goals
- Governance ensures business strategy remains consistent with business goals
- Information security governance provides strategic guidance for security
  - Information security strategy should be linked to the overall business strategy

Discussion Question

- Why is it important to have a formal process for accepting risk?

Pitfalls in Strategy Development

- Overconfidence/Optimism
- Anchoring
- Status quo bias
- Mental accounting
- Herding instinct
- False consensus
  - Confirmation bias
  - Groupthink



Strategy and Risk

- Purpose of information security strategy: Manage information risk to an acceptable level
  - Understand the risk profile
  - Understand risk exposure
  - Be aware of risk management priorities
  - Ensure sufficient risk mitigation to achieve acceptable consequences from residual risk
  - Risk acceptance based on an understanding of the potential consequences of residual risk

Start with the Goals

- What is the information security goal?
  - Typically to assure the reliability of information-related business processes
- Often unaware of what information exists within the enterprise, criticality, etc.
  - Impact cost-effectiveness (too expensive and inefficient)
- Goals help set objectives, which drive strategy
  - Should tie to enterprise goals

Asset Classification

- Initial classification can be time consuming
  - Does not get easier over time
- Best approach is to start as soon as possible
  - Classify new assets when they are created
  - Monitor for changes over time

Focus on Data

- Information security has traditionally centered on protecting IT systems rather than the data they handle.
- Business process owners view IT systems as mere tools, while data carries real business value.
- Emphasizing data protection makes it easier to align information security with corporate governance.

Valuation of Data

- Criticality of data can be derived from criticality of processes that use that data.
- Sensitivity can be derived by determining consequences of data leakage.
  - Sensitivity of data may be subjective.
  - Certain types of data may be considered sensitive by law or regulation.

Current Vs. Desired State

- Desired State
  - Ideal information security environment
  - Frameworks/standards helpful to identify outcomes
  - Defined desired state makes it easier to identify path from current state
- Current State
  - What is actually occurring
  - Help to identify where the environment falls short of the desired
- Gaps between current and desired state
  - Plans for achieving desired state

Building the Strategy

- Strategy provides a road map to the desired state
- Path could be long depending on distance between current and desired state
- Should identify:
  - Available resources
  - Available methods
  - Constraints

Thanks a lot