

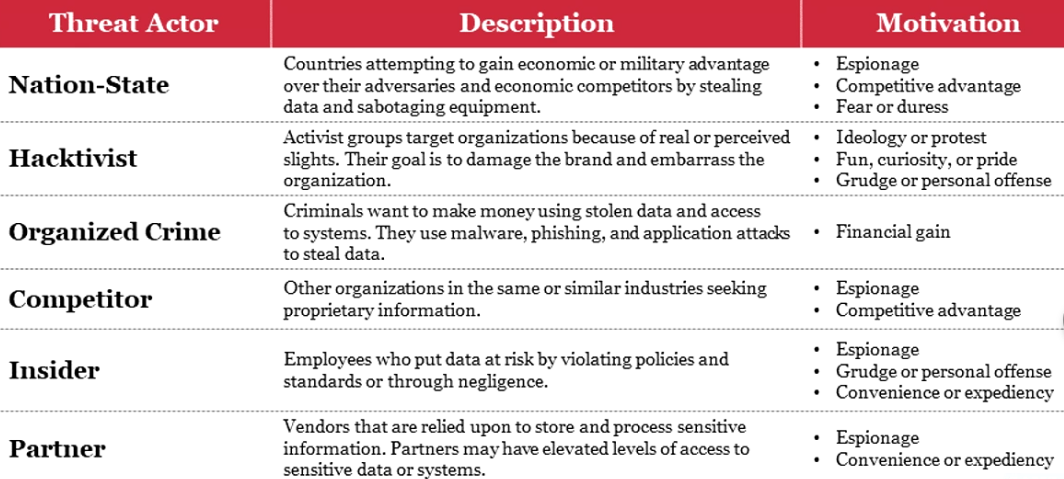
**Decipher the business** :-

* Historical analysis: Major periods of change, Security history, Technology risk graph, etc.
* Stakeholder management: A person or a group | 3 steps: identify, understand, manage
  + To manage stakeholders: 3 steps :-
    - Understand motivations, power/interest grid, prioritize relationships
    - 3 levels of Power: veto, vote, voice
    - 3 levels of Interest: High, Medium, Low
  + Use **SIPOC** tool (Suppliers, Inputs, Processes, Outputs, Customers)
* Values and Culture:
  + Business models: Direct sales, Franchise, Freemium, Subscription
    - Bundling and Unbundling
    - Vertical vs Horizontal business models
  + Business model (what we do for revenue) vs Business strategy (how we compete)
  + **Porter’s five forces**: Analyze competition in the industry to develop business strategy
    - Power of customers
    - Substitute products
    - Power of Suppliers
    - Threat of new Entrants
    - Competitive Rivalry
* Strategy maps:
  + Highlights gaps in strategy implementation
* Asset analysis:
  + Most valuable to the organization and most valuable to the attacker
  + Tangible assets | Intangible assets
  + Crown jewels: changes based on -> industry, business model and strategy, time horizon

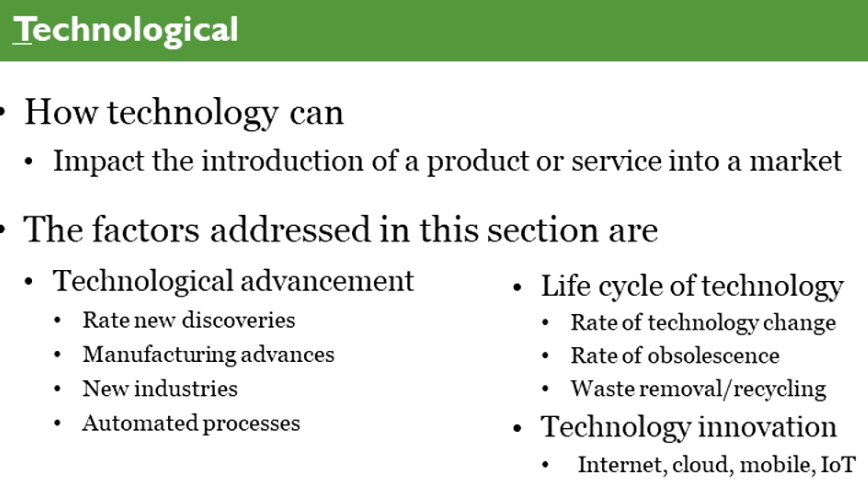
**Decipher the threats**:-

* Threat actors
  + **VERIS**: **V**ocabulary for **E**vent **R**ecording and **I**ncident **S**haring
    - Schema and metrics to describe security incidents in structured manner
    - Used by Verizon DBIR
    - **VCDB**: Veris Community Database: Free repo for reported security incidents
      * <http://veriscommunity.net/> and <http://veriscommunity.net/vcdb.html>
      * External | Internal | Partner



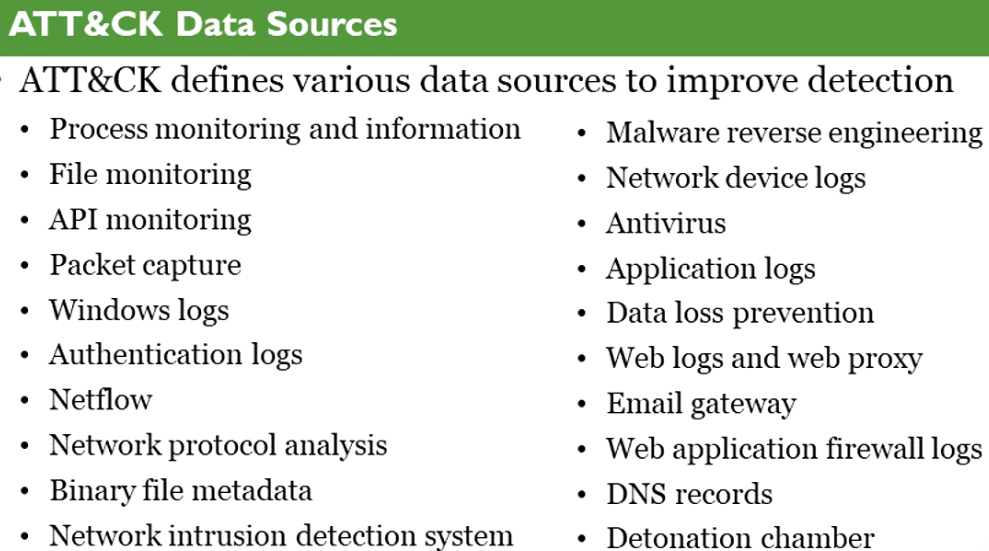




* Business threats (**PEST**)
  + 
  + 
  + 
  + 
* Analyze threats (MITRE **ATT&CK**)
  + Risk = Impact x Likelihood = Impact x (Vulnerability x Threat)
  + Intrusion **kill chain**: Recon, Weaponization, Delivery, Exploitation, Installation, C2, Action
  + **Pyramid of Pain**: Used to detect adversary activities

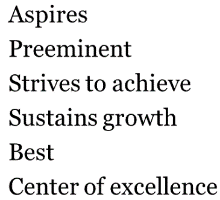


* + **ATT&CK navigator**: Free tool | Visualize and annotate (e.g. Color code) different techniques used by attacker
  + Sources to obtain ATT&CK data



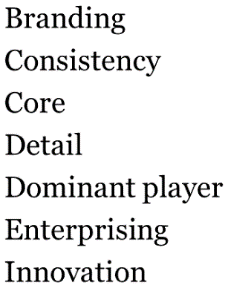
* **DeTT&CT**
  + Python based tool
  + Data source coverage | Visibility coverage | Detection coverage | Threat action map
    - => Detection coverage for specified threat actor
* **Cyber Threat Intelligence**: Collect, Classify, and use knowledge about adversaries
  + Share knowledge using frameworks: **STIX** (define) and **TAXII** (exchange)
* Possible action to take on adversaries:
  + Detect | Deny | Disrupt | Degrade | Deceive | Destroy

**BOOK-2: Strategy Roadmap development**



Define the state:

* **Vision**: “Why” the company exist | noble | seems like unachievable goal
  + **DRIVE** the vision: **D**irectional, **R**elevant, **I**nspirational, **V**ivid, **E**xtremely bold
* **Mission**: “What” the company does | what we are and what we do today



* + Cybersecurity mission statement:

*“To advance company’s mission by securing, defending, and monitoring our most important assets.”*

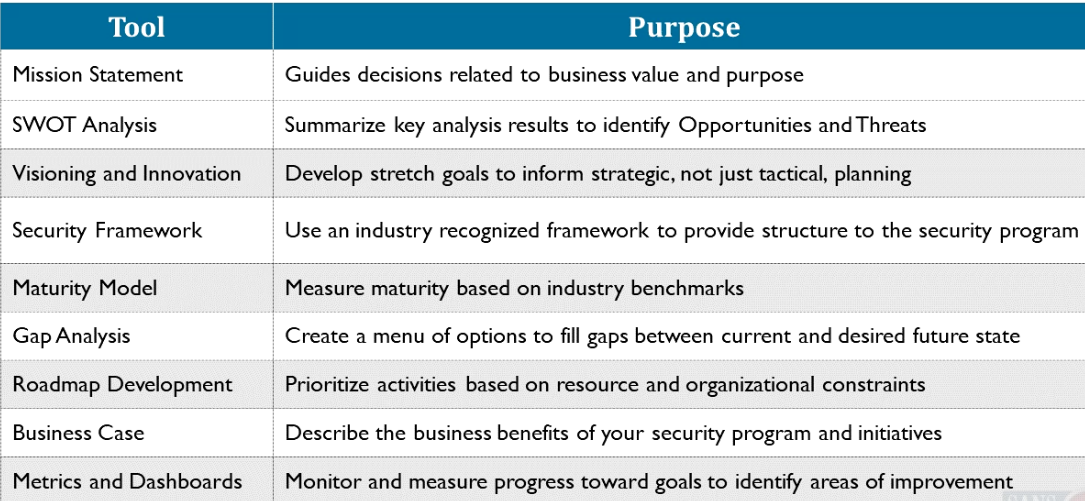
* **4 steps to create a mission statement**
  + Step-1: Tell a story
  + Step-2: Highlight keywords (circle, draw, underline)
  + Step-3: Group the big ideas
  + Step-4: Draft the mission
* **SWOT**: key questions to ask <- look at slides in the book!

Develop the plan:

* 5 steps in developing a plan
* **Visioning**: How the world will be in the future | stretch the strategic planning | Tactical plan (w/o vision)
  + Praise to criticism ratio (5.6/High, 1.9/medium, 0.36/low) on ideas
  + **Hedgehog concept**: focus on doing one thing extremely well
  + **BHAG**: Big Hairy Audacious Goal: visionary goal, envisioned future
* **Innovation**: Anything new and useful | if not useful, then it is **invention**
  + Three types: Business model | Process | Product or service
  + *Sustaining* (evolves existing technology or process) vs *Disruptive* innovation (create new)
  + **Jobs to be done theory**: customers don’t buy products, they hire solutions to needs
  + Key questions:
    - How do we create value to customers?
    - How do we innovate?
    - Why does anyone need us?
* **Security Framework**:
  + Blueprint for building security programs, managing risk, communicating security
  + ISO27000:- 27001:ISMS | 27002:code of practice | 27003:impl guideline | 27004:measurement | 27005:risk management
  + COBIT, ENISA evaluation framework, ISF standard of good practice, NIST cyber f/w
  + NIST Cyber Sec Framework (CSF):
    - Identify, Protect, Detect, Respond, Recover
      * Has *Category*, *sub-category*, *Informative references* on the above
      * Has Tiers: 1 (Partial), 2 (Risk Informed), 3 (Repeatable), 4 (Adaptive)
    - 3 parts: Core, Implementation tiers, Profiles
  + **Maturity models** in cybersecurity framework implementations:
    - CMMI: Initial, Repeatable, Defined, Managed, Optimised
    - Enterprise security group (ESG) maturity model :- Basic, Progressive, Advanced
    - Gartner ITScore
    - C2M2 (Cybersecurity Capability Maturity Model)
    - BSIMM (Spider-chart): Access control, Awareness &Training, Data Security, Process/Procedures, Maintenance, Protective technology
    - OpenSAMM
    - CIMM (Capability Immaturity Model)
  + Assessing the maturity model:
    - FFIEC **C**ybersecurity **A**ssessment **T**ool (maturity lvl for domain Vs. inherent risk)
  + **Security Controls**:
    - NIST SP 800-53 | CIS Critical Security Controls | Australian Signals Directorate (ASD) mitigation strategies
      * CIS controls: **18** categories | **154** Safeguards (57/Group1, 131/2, 154/3)
    - Map controls to framework:
      * CIS mapping, NIST Informative References Program, Secure Controls F/w
  + **Third-party certifications**:
    - SOC2 Type II report (SOC = System and Organization Controls)
      * Privacy, Security, Availability, Processing Integrity, Confidentiality
    - ISO27001
    - FedRAMP
  + **Security Roadmap**:
    - **Gap analysis**: Identify future state -> Analyze current state -> Bridge the gap
    - **Decision matrix analysis**: tool to rank initiatives and inform decisions
      * **MCDA** (Multiple Criteria Decision Analysis): Cost, Ability to execute, stakeholder support, threat defense, Total
  + **Business case development**:
    - Reason for effort v| cost vs benefits
    - *Approaches*: Cost | Industry comparison | Business innovation (gain)
    - Where we get comparable data?
      * **ISAC** (Information Sharing and Analysis Center) | FS-ISAC, REN-ISAC
      * Community projects: BSIMM, OpenSAMM
      * Research & Consulting orgs: Gartner, Big Four, security services firms
    - ALE = ARO x SLE
    - Elements of a business care:
      * Exec summary, Introduction, Analysis, Appendix

Deliver the program:

* Security metrics program
  + CIS controls has **measures** that serves as metrics
  + Metrics have to be:
    - Properly designed
    - Economical to collect
    - High leverage
    - Encompass a feedback mechanism
  + Security Dashboard:
    - Financial, Customer & stakeholder satisfaction, Business processes, Security metrics
    - Should have:
      * Analysis and trends
      * Highlight anomalies, variations
      * Illustrate progress towards goals
  + **Gemba board**: Security, Quality, Delivery, Cost, People
  + Tips on metrics:
    - Discuss visualization strategy with marketing team
    - Avoid busy-looking graphs and charts that appear cramped or confusing
    - There is an element of art and design in this work
  + Executive metrics = Balanced Scorecard
  + Operational metrics = Security Dashboards
  + Technical metrics = Charts and graphs
  + **Pitfals to avoid** / mistakes in reporting:
    - Not getting leadership support
    - Too much information / too soon
    - Wrong information
    - Inaccurate, misleading, incomplete information
* **Marketing** & Executive communication
  + **SNAP**: Specify, Niche, Audience, Promote
  + Making ideas **STICK**:
    - Simple, Unexpected, Concrete, Credible, Emotional, Stories
  + Inbound content marketing (blogs, whitepapers, websites, online talks/videos) and Outbound marketing (ads, promotional videos)



**BOOK-3: Security Policy Development & Assessment**

**Purpose of Policy**

Security Policy -> Statement of goal from senior leadership (documented approach)

Policy Set -> group of related docs | planned, documented, managed security controls |

* Policies, standards, guidelines, procedures, baselines

Policy protects people and organization

**Reasonable Person Rule**: When is it acceptable to not follow the policy?

* Foreseeable risk of harm actions vs utility of actions, extent of risk so created, likelihood, alternatives to lesser risk and costs associated

Protect technology policy, Protect PII policy, etc.

**PCI DSS** -> 12 specific requirements

**HIPPA** (e-PHI)

**SOX**: Ethical and honest accounting policies: 11 major elements like **PCAOB** , etc.

**CCPA**: applies to business with revenue >25m$

**GDPR**: appoints a data protection officer (DPO)

**EU-US Privacy shield**: prohibiting spam emails

EU: **NIS Directive**: Network and Information Systems: Designate CSIRT at EU member states

**China Cybersecurity law**: Important data must be stored in China

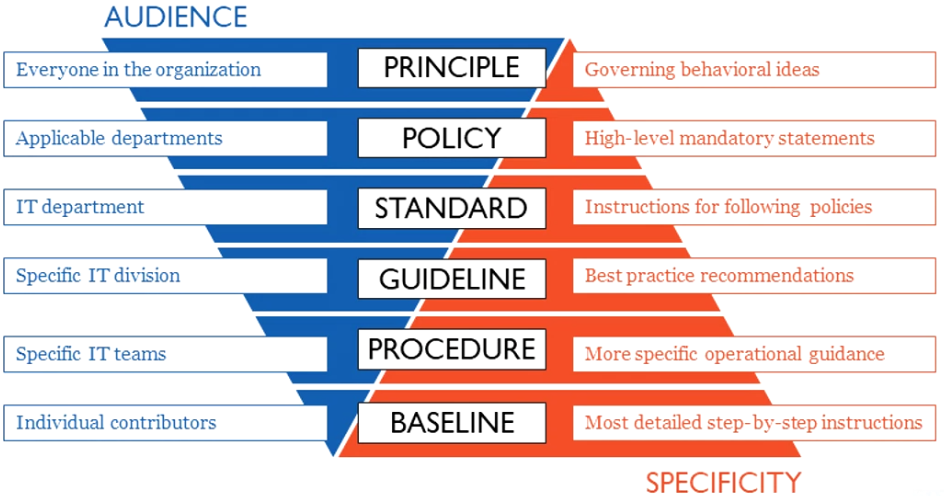
**Russian Data Protection law**: Personal Data Protection Act: Must store Russians data in Russia

Vendors and Third-parties

Policies should be enforced as ‘*Compliance by design*’

Policy lifecycle 🡪 DEVELOP -> SOCIALIZE -> MEASURE -> ACCESS

**Policy Pyramid**:



Creating policy rules:

1. Create policies that reduce risk
2. Socialize and educate employees about policies | Organizational adoption
3. Measure and enforce compliance by publishing results on security dashboard | **SMART**
4. Regularly assess and update policies | Report the results

**Types of Policies**: Governance | Operational | Security | Acceptable Use

RAS (**Risk Appetite Statement**): Highest level of policy in organization | Acceptable risk to do business

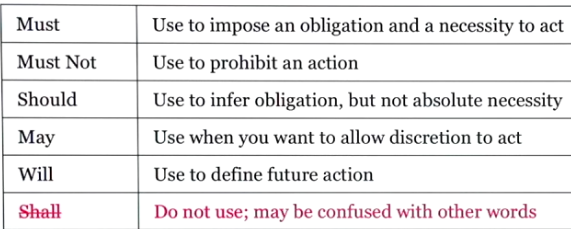
<https://www.occ.treas.gov/publications-and-resources/publications/banker-education/files/risk-appetite-statement.html>

**Risk Profile**: Organization’s risk at a point of time

**Risk capacity**: Absolute maximum risk the organization can incur

**Risk appetite**: Level of risk acceptable to conduct business

**Risk tolerance**: Thresholds that allocate risk appetite to certain types of risks



**Develop Policy**

*Language*: MUST and MUST NOT -> mandatory

SHALL, SHOULD, MAY -> optional

For acceptable behavior -> “must not”

To do the right thing -> “must do”

*Policy Structure*: 1.5 page is ideal

Component of a policy document:

Overview or background | Purpose | Scope | Policy statement | History (publish date, expiration, version) | Enforcement (penalty for violation) | Responsible parties (RACI) | Related documents

*Policy & Culture*: Organizational **ABV**s (Assumptions, Beliefs, Values)

**Management style**: Collaborate | Charismatic | top-down / Authoritarian

*Define Requirements*: Gather data (interviews, industry trends/PEST, Gap analysis/SWOT, Audit findings, Review of security program and activities)

* Policy requirements can come from: Unexpected events | Anomalous events | Security incidents

**Levels of Policy**: Regulation/Law, Enterprise-wide, Division-wide, Local, Issue-specific, System-specific

**CEO-fraud**: business email compromise | targeting executives for wire transfer

**Mobile device Risks**: misconfigured devices | insecure mobile apps | devices without security controls

**One-sentence Policy examples**: Acceptable use, Remote access, Physical security, etc.

**Secure Development policy**!

**Manage Policy** (Approve, Socialize, Measure)

Identify key stakeholders | Solicit feedback during development | Define approval process | socialize the approval policy (distribute, communicate) | Policy awareness and training | measure adherence to policy | enforcement of policy (who?) | consequences of non-compliance | **policy** **Exception requests** (business justification, assessing risk, compensating controls) | Expiration date (1 year for exception) (*soft expiration date* <- bad)

**Assess Policy and Procedure**

**SMART** approach: **S**pecific, **M**easurable, **A**chievable, **R**ealistic, **T**ime Based

* General or Specific?
* Measure helps bridge gap between policy and procedure

**Policy Assessment Key questions**:

1. Is the policy fragment clear and concise?
2. Does it meet SMART objectives?
3. Does it outline responsibility and compliance?
4. Does it designate required actions?
5. Does it provide enough guidance to develop a procedure?

**BOOK-4: Leadership & Management competencies**

**Why choose leadership**:

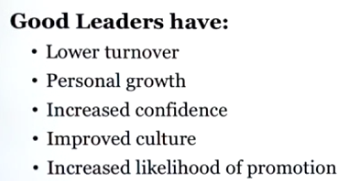


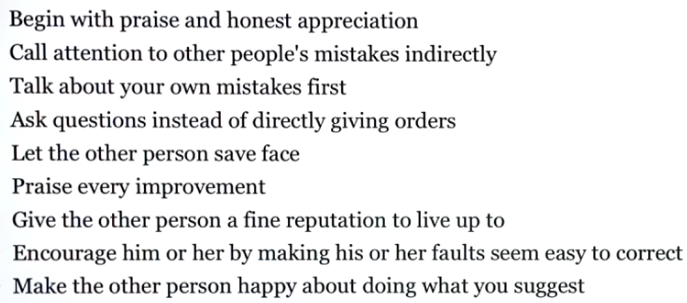
McGregor **Theory X and Theory Y**.

Why people become leaders 🡺 Trait theory | Great events theory | Transformational leadership theory

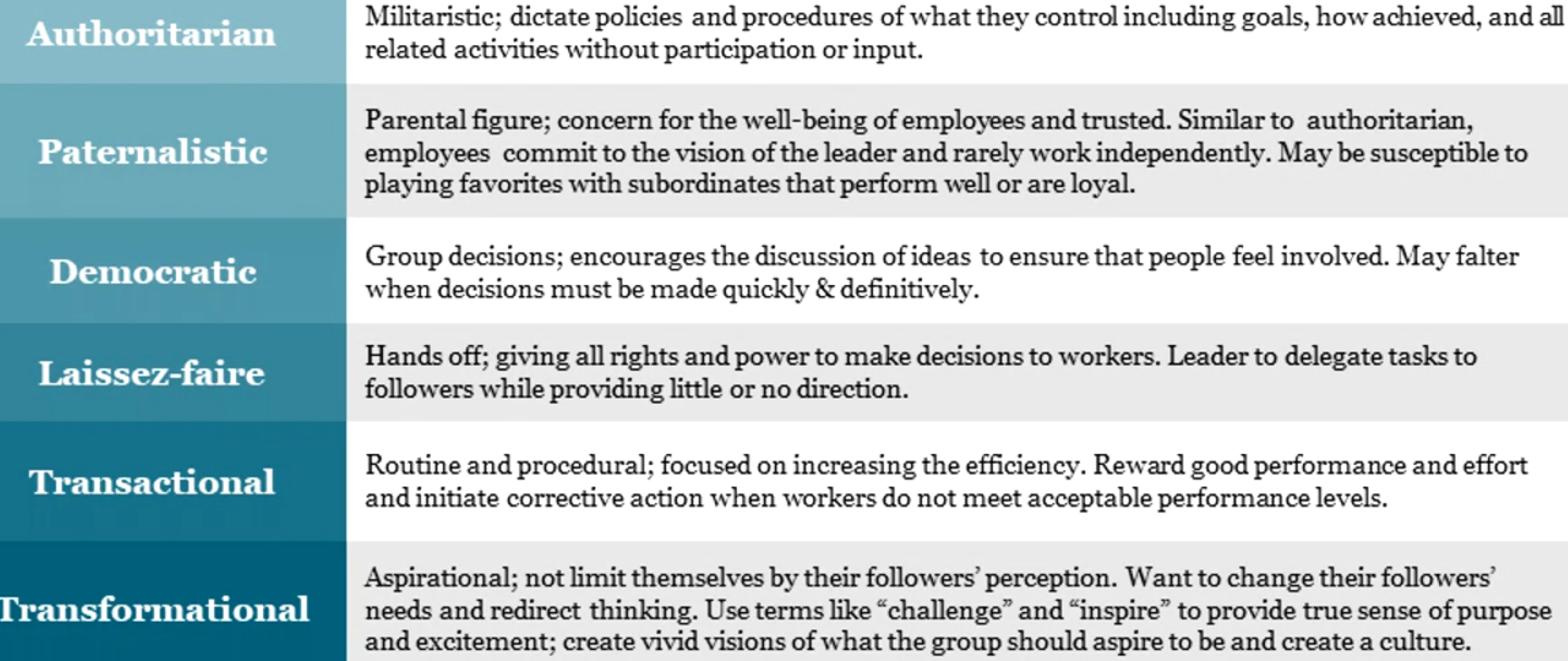
*Fundamentals on Handling people*

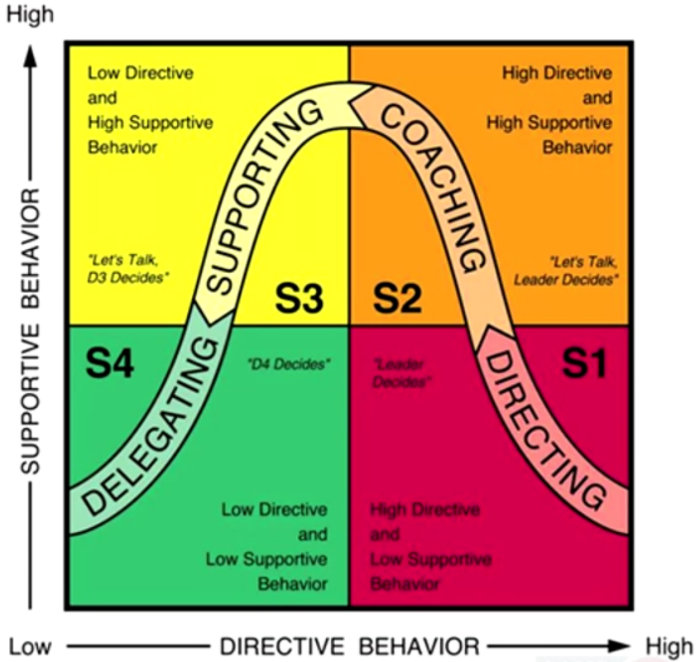
* Try to understand the other person
* Give honest and sincere appreciation
* Arouse in the other person an eager want

Change people without causing resentment:



**Leadership styles**:



Situational leadership model (adaptive): ===============🡺

Leadership behavior types:

* Telling (one-way)
* Selling (provide direction)
* Participating (share decision resp, focus on relationships)
* Delegating (focus on monitoring)

**Be your best**!

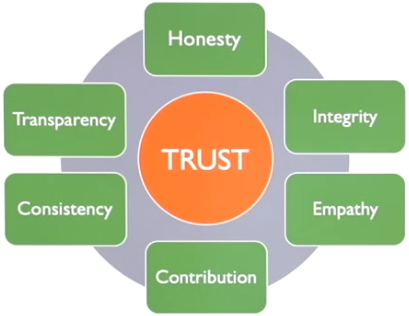
**Leadership essentials**:

Peer to Leader.

***Five dysfunctions of a team***

* No results
  + Avoidance of accountability
    - Lack of commitment
      * Fear of conflict
        + Absence of trust

**Circle of trust**:



**Servant leadership**: lifting others up!

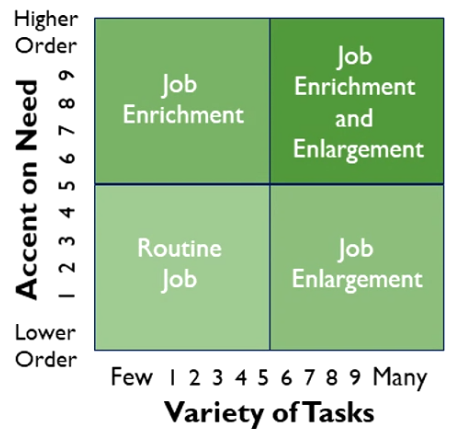
* 10 principles of servant leadership:
  + Listening, Empathy, Healing, Awareness, Persuasion, Conceptualization, Foresight, Stewardship, Commitment to the growth of people, Building community

**Maslow’s hierarchy of needs**:

* Self-actualization
  + Self-esteem
    - Social
      * Safety
        + Physiological

Motivational factors: Achievement, Advancement, Growth, Responsibility, Job challenge

**Job enlargement and Job enrichment**



Human capital model: Growth -> Skills -> Empowerment -> Creativity -> back to Growth

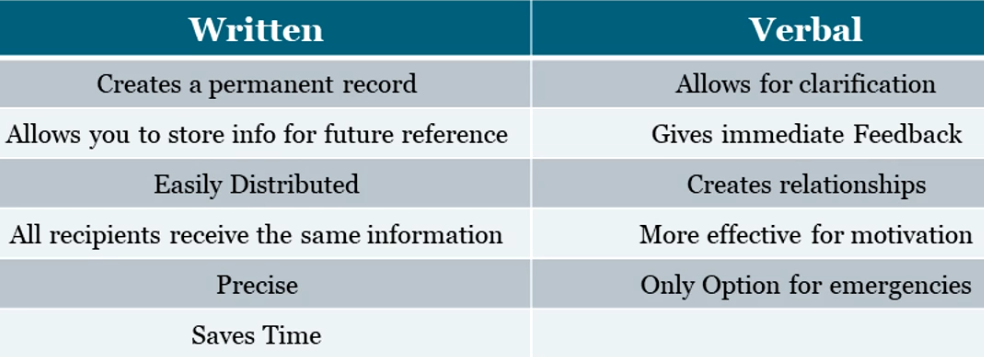
Evolve from **Formal Authority to Moral Authority**!

**Top-down vs collaborative**!

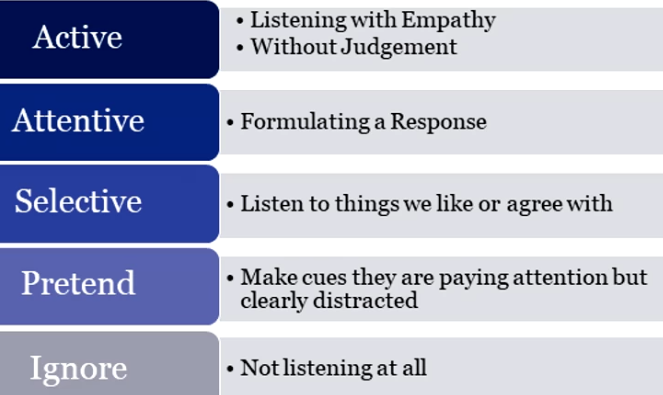
**Effective communication**:

Content and Context -> (page-68)

3 step process: IDEA -> ENCODING -> DECODING



Filters to communication:

* Culture, background, bias
* Ourselves
* Perception
* Stress

**Great presentation tips**

Active Listening (or empathetic listening)

* And Passive listening
* Hearing and Listening are not same!

Providing Feedback

* **FILE model**: **F**acts | **I**mpacts | **L**isten | **E**xpectations

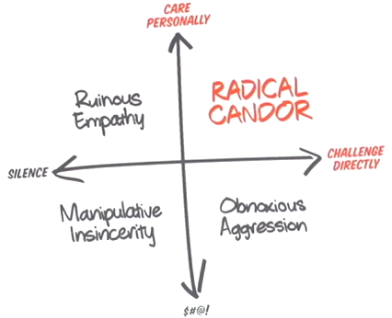
Receiving Feedback

* **ALCR model**: **A**pproachable | **L**isten | **C**larify | **R**espond

**Performance Analysis Quadrant (PAQ)**: Tool to identify root cause of performance issues

Challenging conversations

**Radical Candor**



**Conflict resolution styles**:

* Competitive (position of power) | Collaborative (variety of viewpoints) | Compromising (cost of conflict > cost of losing) | Accommodating (peace is more valuable than winning) | Avoiding (no one’s feelings hurt)

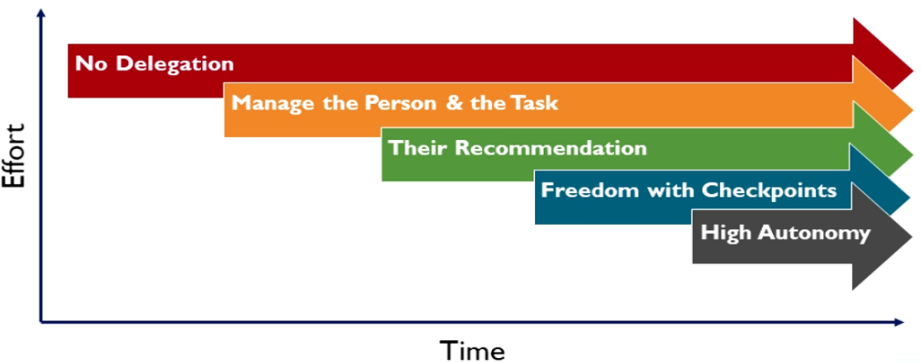


**Build effective teams**:

* Group vs Team
* Low performing teams (page: 112)
* High performing teams
* High-trust relationships
* Diversify team styles: (page-122)
  + Contributors
  + Collaborators
  + Communicators
  + Challengers

**Tuckman’s Teaming Model**:

* Forming | Storming | Norming | Performing | Adjourning (page-128)



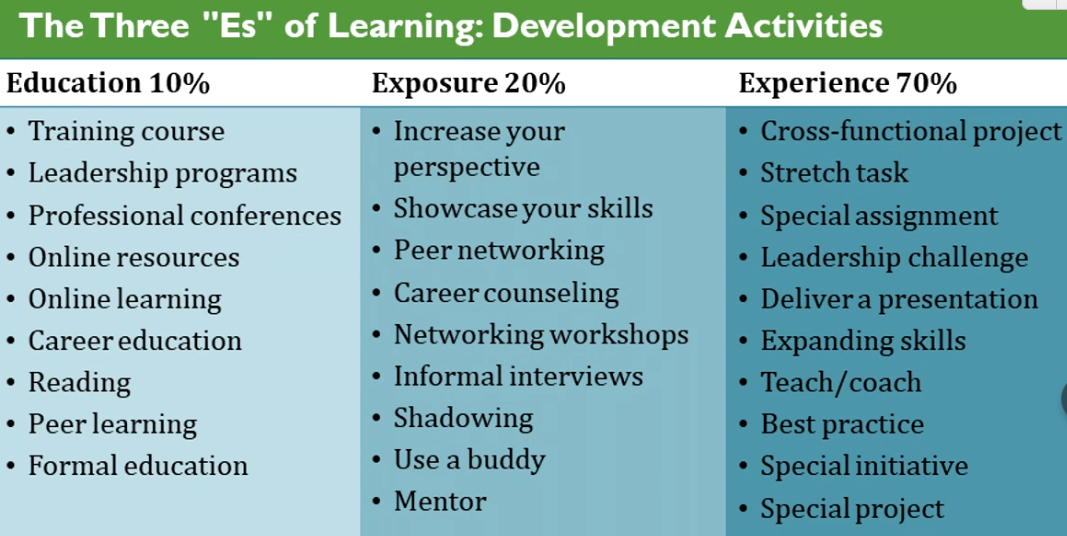
**Learning to Delegate**:

**ABC**s of Delegation:

* Assess | Break the news | Communicate

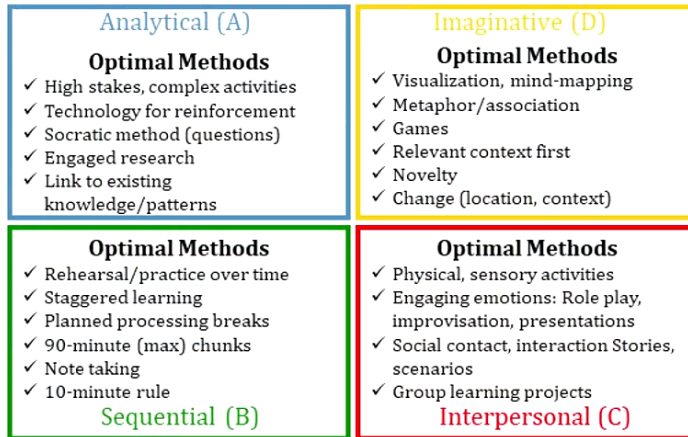
**Coaching, Mentoring, Sponsorships**:

* 3 E’s of learning
  + Education (knowledge and skills)
  + Exposure (feedback from peers, senior leaders, managers, etc. learning from others)
  + Experience (demonstrating the knowledge, skills, behaviour)



**Herrmann Brain Dominance Instrument (HBDI)**:

* Learning considerations
  + Analytical (A) | Sequential (B) | Interpersonal (C) | Imaginative (D)



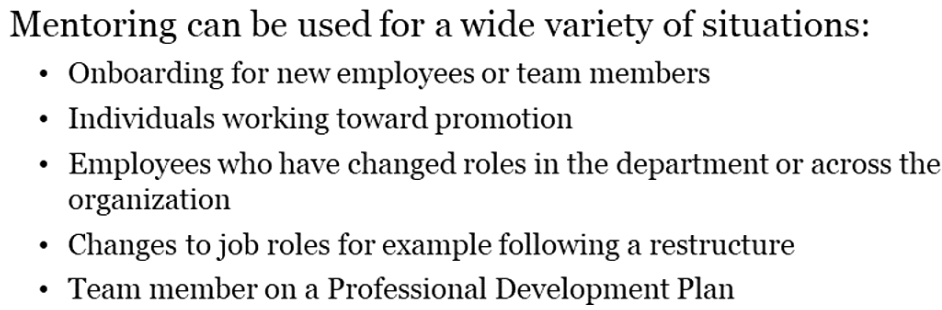
**Coaching:**

* **GROW** Coaching model:



**Mentor**:

* An experienced and trusted advisor
* Role as mentor:
  + Listen, Ask question, Understand the situation, Provide info and knowledge, share informal networks, Be a sounding board



**Sponsorship**:

* Able to guide and influence career
* Take interest in your advancement
* Necessary for executive and C-level position

Career management **PIE**:

* Performance (10%)
* Image (30%)
* Exposure (60%)

**Six Cs** of career management:

* Challenge | Chemistry | Commitment | Compensation | Contract | Commute

**Leading change**:

3 stages to change:

* Unfreezing | Changing | Refreezing

Stages of change!

**Behavioral economics**: **Bias** includes: Herd mentality | Status Quo | Availability heuristic

**Valence**: How happy is a person

**Arousal**: How excited is a person