



# SEC-202: Secure Start-Up

## Lecture 1 – Secure Start-Up Strategy and Fundamentals

Instructed By:

**Dr. Charnon Pattiyanon**

Assistant Director of IT and Instructor  
**CMKL University**

Artificial Intelligence and Computer  
Engineering (AICE) Program

# Start-Up Development Phases



## Where is the place for Security?



Talent	Ideating	Concepting	Committing	Validating	Scaling	Establishing	Organization
	Entrepreneurial ambition and/or potential scalable product or service idea for a big enough target market. Initial idea on how it would create value. One person or a vague team; no confirmed commitment or no right balance of skills in the team structure yet.	Defining mission and vision with initial strategy and key milestones for next few years on how to get there. Two or three entrepreneurial core co-founders with complementary skills and ownership plan. Maybe additional team members for specific roles also with ownership.	Committed, skills balanced co-founding team with shared vision, values and attitude. Able to develop the initial product or service version, with committed resources, or already have initial product or service in place. Co-founders shareholder agreement (SHA) signed, including milestones, with shareholders time & money commitments, for next three years with proper vesting terms.	Iterating and testing assumptions for validated solution to demonstrate initial user growth and/or revenue. Initial Key Performance Indicators (KPI's) identified. Can start to attract additional resources (money or work equity) via investments or loans for equity, interest or revenue share from future revenues.	Focus on KPI based measurable growth in users, customers and revenues and/or market traction & market share in a big or fast growing target market. Can and want to grow fast. Consider or have attracted significant funding or would be able to do so if wanted. Hiring, improving quality and implementing processes	Achieved great growth, that can be expected to continue. Easily attract financial and people resources. Depending on vision, mission and commitments, will continue to grow and often tries to culturally continue "like a startup". Founders and/or investors make exit(s) or continue with the company.	

Startup Development Phases - from **idea to business** and **talent to organization**.

Version 3.6 - [www.startupcommons.org](http://www.startupcommons.org)



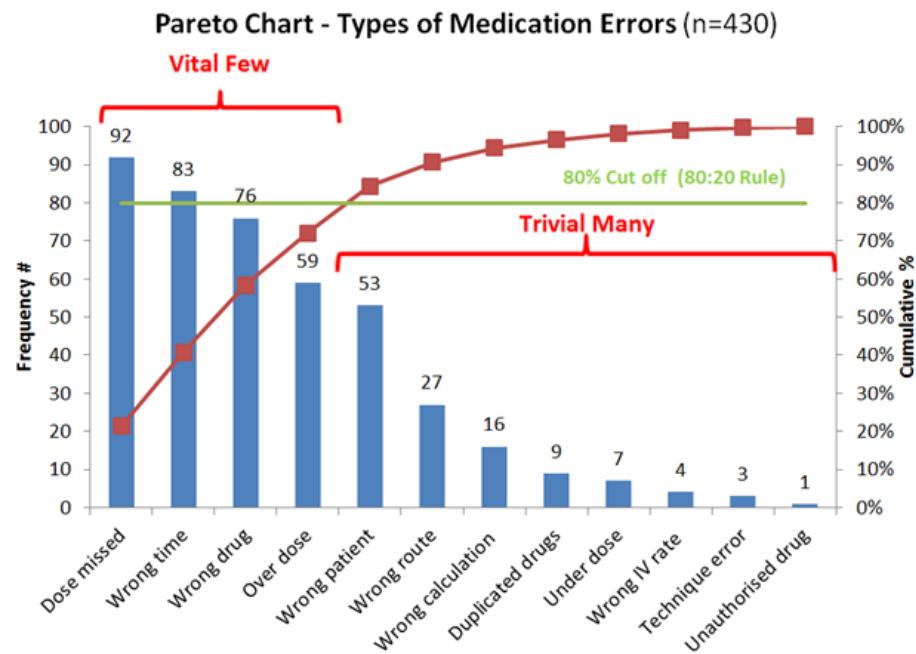
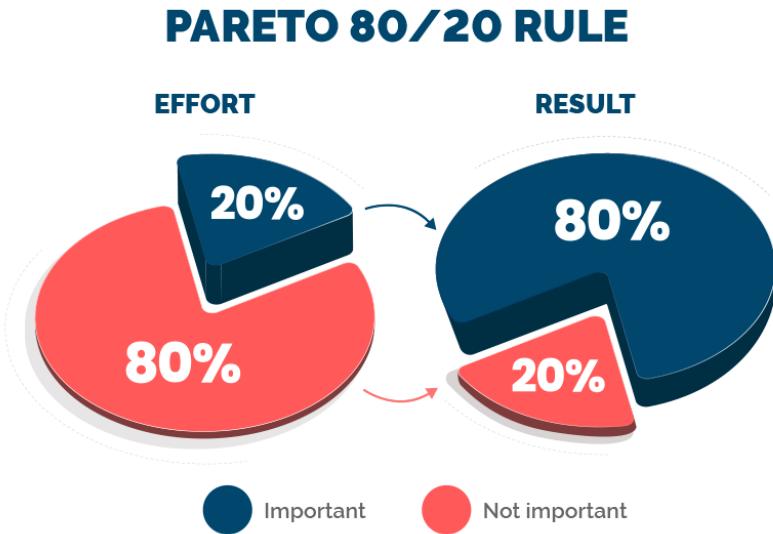


# Discussion Time!

If a startup has **a limited budget**, why might it be strategic to invest in  
**'Minimum Security'** rather than striving for perfection immediately?

At what point does '**minimum**' become '**negligent**'?

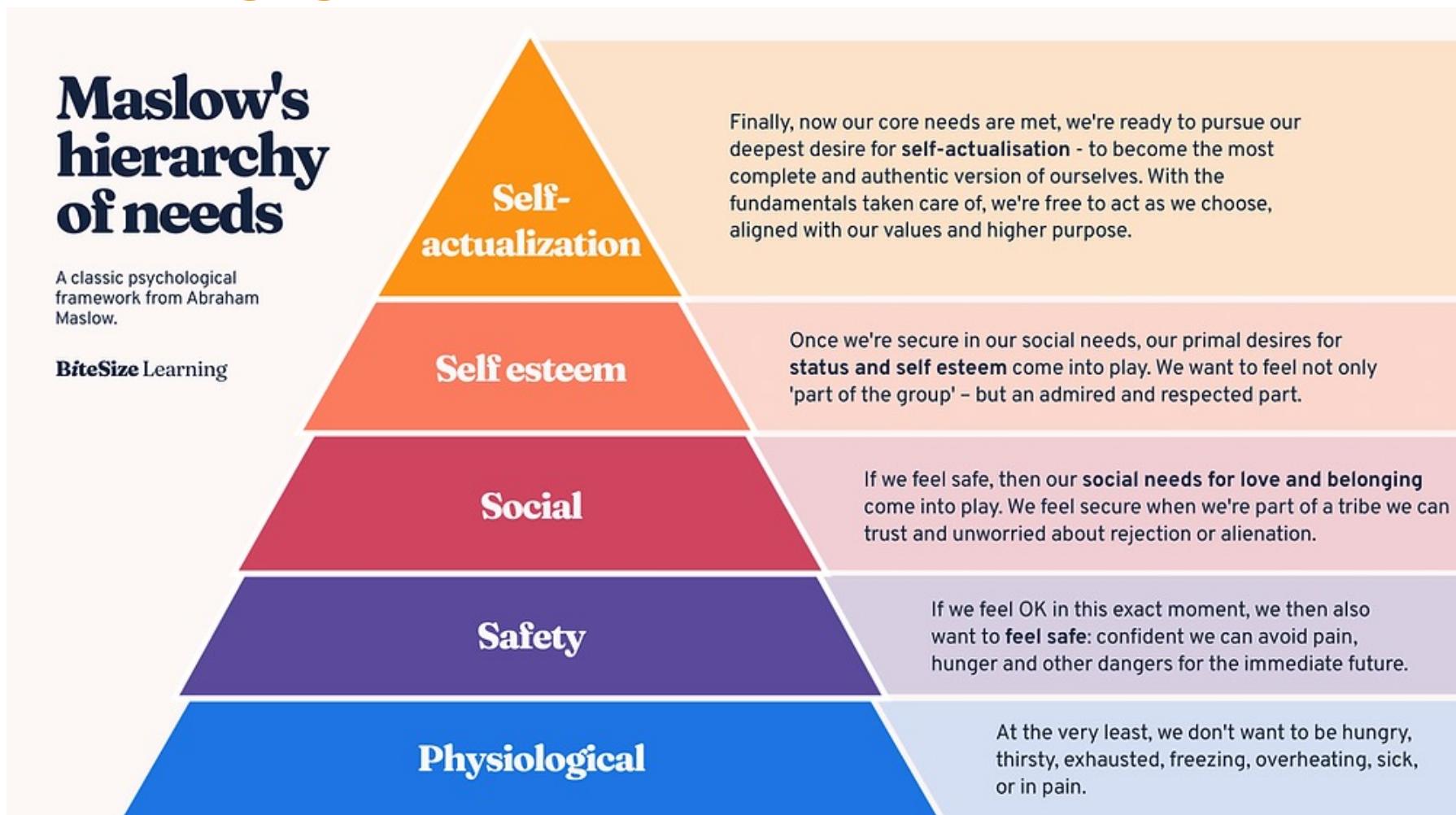
# Minimum Investment, Maximum Reduction



## ■ The Reality of Security:

- **Perfection is impossible:** You cannot eliminate 100% of risk without shutting down the business.
- **The Goal:** Increase the cost of attack for the hacker until it is no longer profitable for them to target you.
- **The "Minimum" Mindset:** It is not about being lazy; it is about being efficient. We focus resources on the controls that stop the most common attacks.

# The Low-Hanging Fruits (The Basics)



# The Low-Hanging Fruits (The Basics)

## What about Security?

### AI Defense | Antivirus and Endpoint Protection

- Advanced AI detection tools that could adapt to various kinds of threat to the organizational system.

### SaaS Security

- Myth:** "The cloud provider handles everything."
- Reality:** Shared Responsibility Model. You are responsible for who can access the data (Identity).

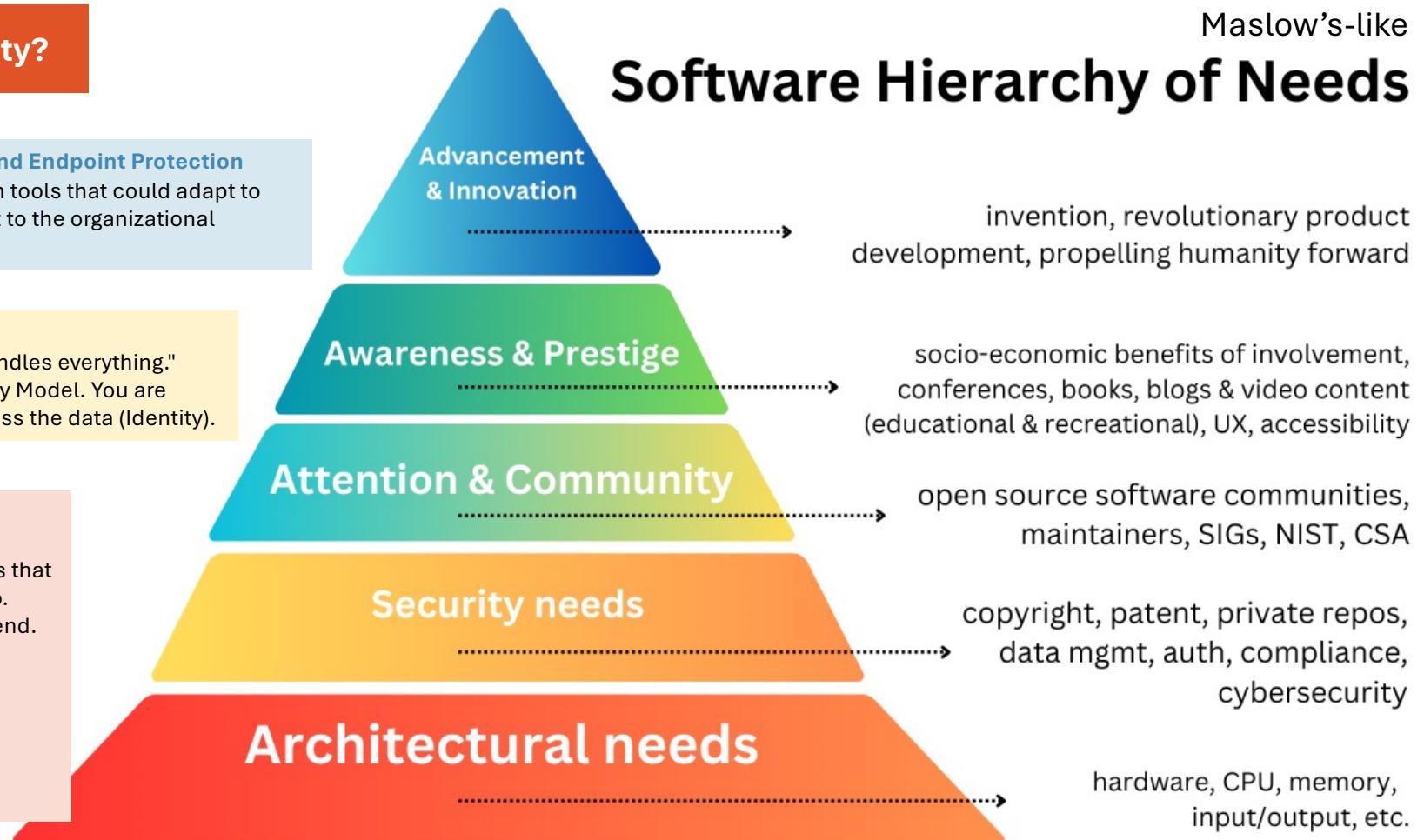
### Patching:

- The unglamorous truth:** Most breaches exploit vulnerabilities that were fixed months or years ago.
- Policy:** Auto-update is your friend.

### Email Security:

- ~90% of attacks start with a phishing email.
- Technical controls:** Filtering, SPF/DKIM/DMARC (brief intro).

## Maslow's-like Software Hierarchy of Needs



# Business Context – "What Type of Business Is This?"



A Bank



A Coffee Shop

What are their top risks?



A Hospital

## ▪ Context Dictates Strategy:

- **Fintech:** High regulation, target for direct theft. Priority = Integrity & Fraud prevention.
- **Healthcare:** High privacy requirement (HIPAA), life-safety issues. Priority = Availability & Confidentiality.
- **Retail/E-commerce:** High volume of transactions. Priority = PCI Compliance & Uptime.

## ▪ Management Vision:

- **The Board:** Cares about reputation and stock price.
- **The CFO:** Cares about financial loss and budget.
- **The CTO:** Cares about system speed and developer friction.

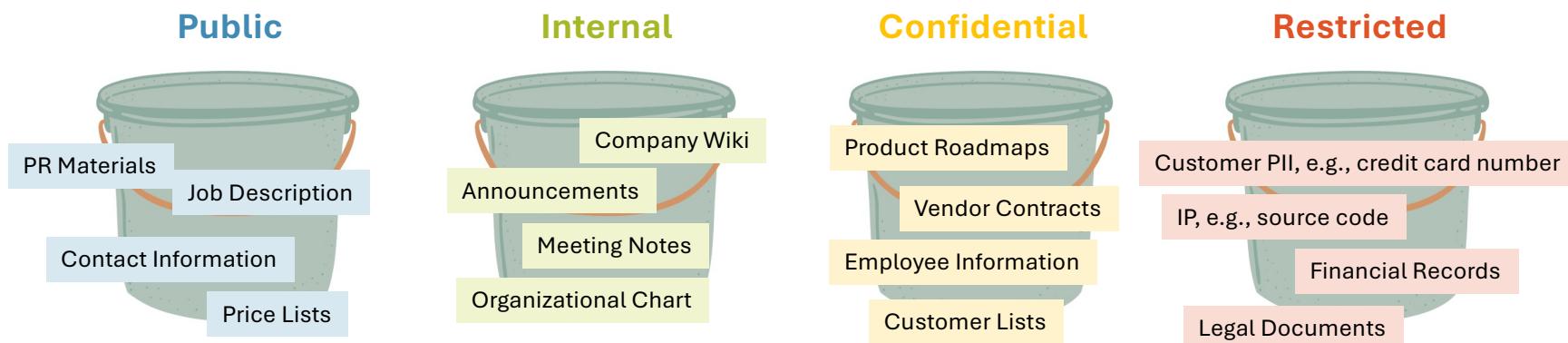
Who cares about security?

You must speak their language,  
not just "tech" language.

How about your startup co-founder?

# Data Classification

- We might know that the sensitivity of data in a system can be classified into multiple levels. But, the scope of data classification for start-up company is broader than that.



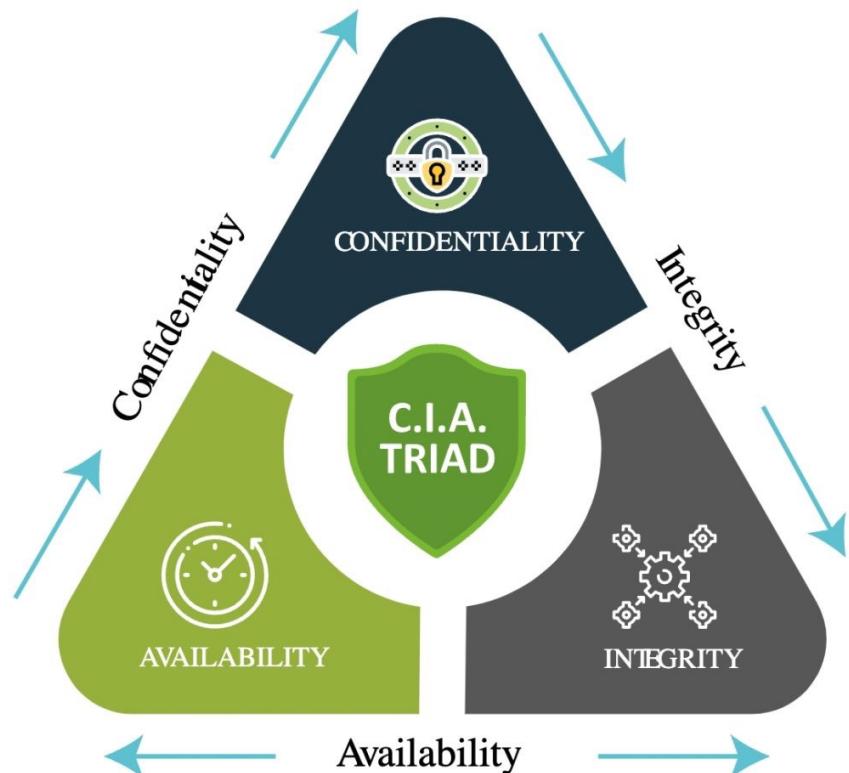
- Identifying the "Crown Jewels":
  - PII (Personally Identifiable Information):** Names, SSNs, emails (Regulatory risk).
  - IP (Intellectual Property):** Code, formulas, designs (Competitive advantage risk).
  - Financials:** Bank accounts, transaction ledgers (Direct fraud risk).

Where is data created?

Where is it live?

Where is it sent?

# Core Theory Revisit – The CIA Triad



- For start-up companies, the three pillars need to be balanced:
  - **Confidentiality:** Keeping secrets secret (e.g., preventing data leaks).
  - **Integrity:** Ensuring data hasn't been tampered with (e.g., preventing financial ledger hacks).
  - **Availability:** Ensuring systems are up and running (e.g., preventing Ransomware/DDoS).
- **The balancing act:**

High security often reduces availability (usability).

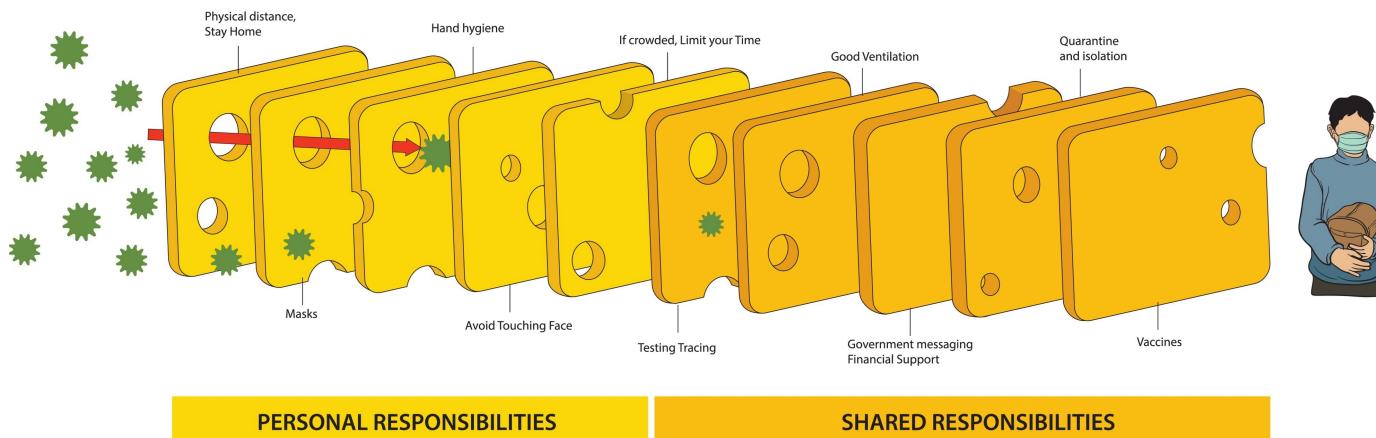
**Question:** Which letter of the CIA triad is most important for a Hospital? For a Bank?

**How about your start-up company?**

# The Concept of "Defense in Depth"

## THE SWISS CHEESE

The Swiss cheese model of Covid-19



- **The "Swiss Cheese" Model:** Every security control has holes.

- **Layering Controls:**

- If the **Firewall** misses the attacker, the **Endpoint Protection** should catch them.
- If that fails, **MFA** should stop the login.
- If that fails, **Data Encryption** renders the theft useless.

### Single Points of Failure:

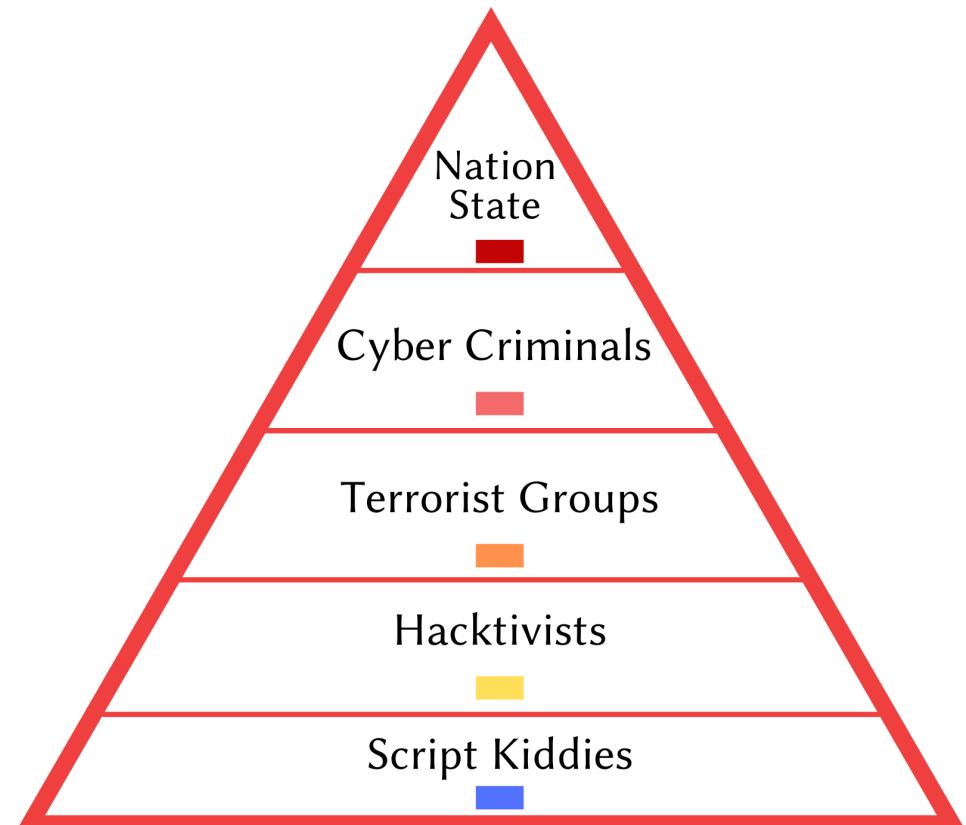
Relying on just one tool (like a firewall) is a strategy for failure.

# Understanding the Adversary (Threat Landscape)

## ▪ Who is attacking you?

- **Commodity Threats:** Automated bots scanning every IP address on the internet. (99% of noise).
- **Cyber Criminals:** Financially motivated (Ransomware gangs).
- **Nation States (APTs):** Spies. (Unless you are Defense/Gov/Infra, this is rarely your primary threat).

## ▪ Strategic implication: Don't buy "Nation State" defense tools if your biggest risk is a bot guessing passwords.



# The Cost of Security (Budgeting)

- **Security is a Cost Center:** We don't make money; we save money by preventing loss.

- **CAPEX vs. OPEX:**

- **Capital Expenditures (CapEx):**

Buying a \$50k firewall box (One time).

- **Operational Expenditures (OpEx):**

Paying \$2k/month for a SaaS security tool (Recurring).

- **ROSI (Return on Security Investment):**

$$\text{ROSI (\%)} = \frac{(\text{ALE} \times \text{Mitigation Ratio}) - \text{Cost of Security Solution}}{\text{Cost of the Security Solution}}$$

**ALE** = Average Loss Expectancy = Cost per incident times the # of incidents

**Mitigation Ratio** = Efficacy of solution at stopping attacks as a percentage

**Example:** Spending \$10k to stop a likely \$100k loss is a good investment.

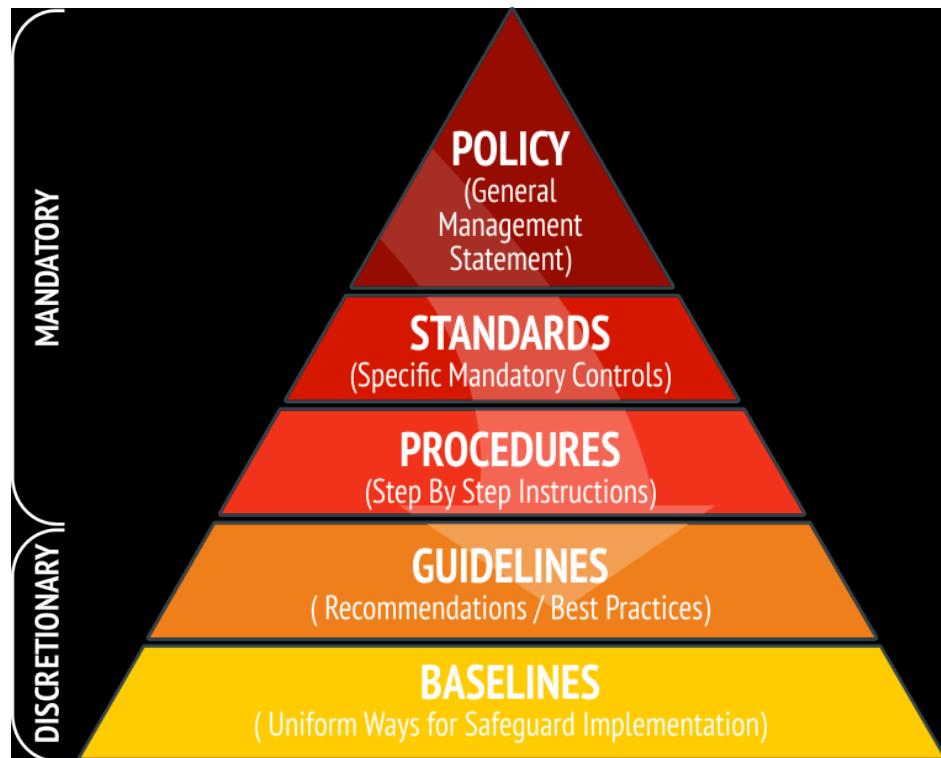
## CapEx Examples



## OpEx Examples



# The Governance Hierarchy (Documentation)



- **Policy (The "Why"):** High-level rules set by management.  
(e.g., "All employees must secure their accounts.")
- **Standard (The "What"):** Mandatory technical requirements. (e.g., "Passwords must be 12+ characters.")
- **Procedure (The "How"):** Step-by-step instructions. (e.g., "How to reset your password in Okta.")
- **Why it matters:** If it isn't written down, you can't audit it, and you can't fire someone for violating it.

# Building the Roadmap (Strategy vs. Tactics)



## ■ Tactics (The "Now"):

- Immediate fires that need putting out (e.g., "Turn on MFA today," "Patch the servers").
- Quick wins to demonstrate value to leadership.

## ■ Strategy (The "Future"):

- Where do we want to be in 12–24 months?
- Changing the culture, obtaining certifications (SOC 2, ISO), automating compliance.

## ■ Measurability:

- How do we define success?
- *Bad metric:* "We blocked 1 million firewalls hits." (Meaningless noise).
- *Good metric:* "Time to patch critical vulnerabilities dropped from 30 days to 48 hours."

# Key Takeaways

- We learned about the **start-up development phases** and how to infuse security into each stage.
- We explored aspects that should be considered for secure start-up companies, such as the **business context**, **data classification**, and **depth of defense**.
- We discussed the **cost** and **governance** of security in a start-up company.

## Homework 1:

- Group up with your friends (**Up to 3 students in a group**).
- Pick a hypothetical company and identify the minimum viable product of the company.
- Answer the following questions:
  - **Question 1:** What is the #1 data asset that would kill the company if leaked?
  - **Question 2:** What is the "Minimum Security Investment" for day one?
  - **Question 3:** Who is the key stakeholder they need to convince to spend money?

You don't have to submit it;  
just keep it for your  
assessment project.



# End of the Lecture

Please do not hesitate to ask any questions to free your curiosity,

If you have any further questions after the class, please contact me via email ([charnon@cmkl.ac.th](mailto:charnon@cmkl.ac.th)).