

Cybersecurity Challenges in Indonesia

Affan Basalamah

Indonesia Internet Governance Academy 2024

whoami

affan

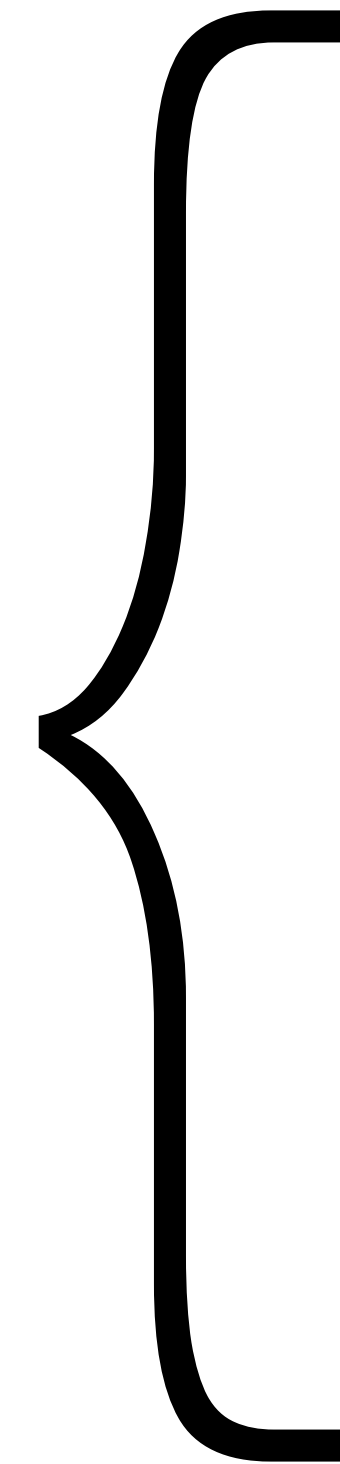
- **Affan Basalamah**
- APNIC Community Trainer
- Previous: Head of IT Infra @ ITB
- **@*affanzbasalamah***
- affan@salamahsystems.com



Sebenarnya apa ini semua?

Komponen pembangun Internet

- Cybersecurity on every level



APPLICATION LAYER
(HTTPS, SMTP, ETC)

PROTOCOL LAYER
(TCP/IP, DNS, BGP, ETC)

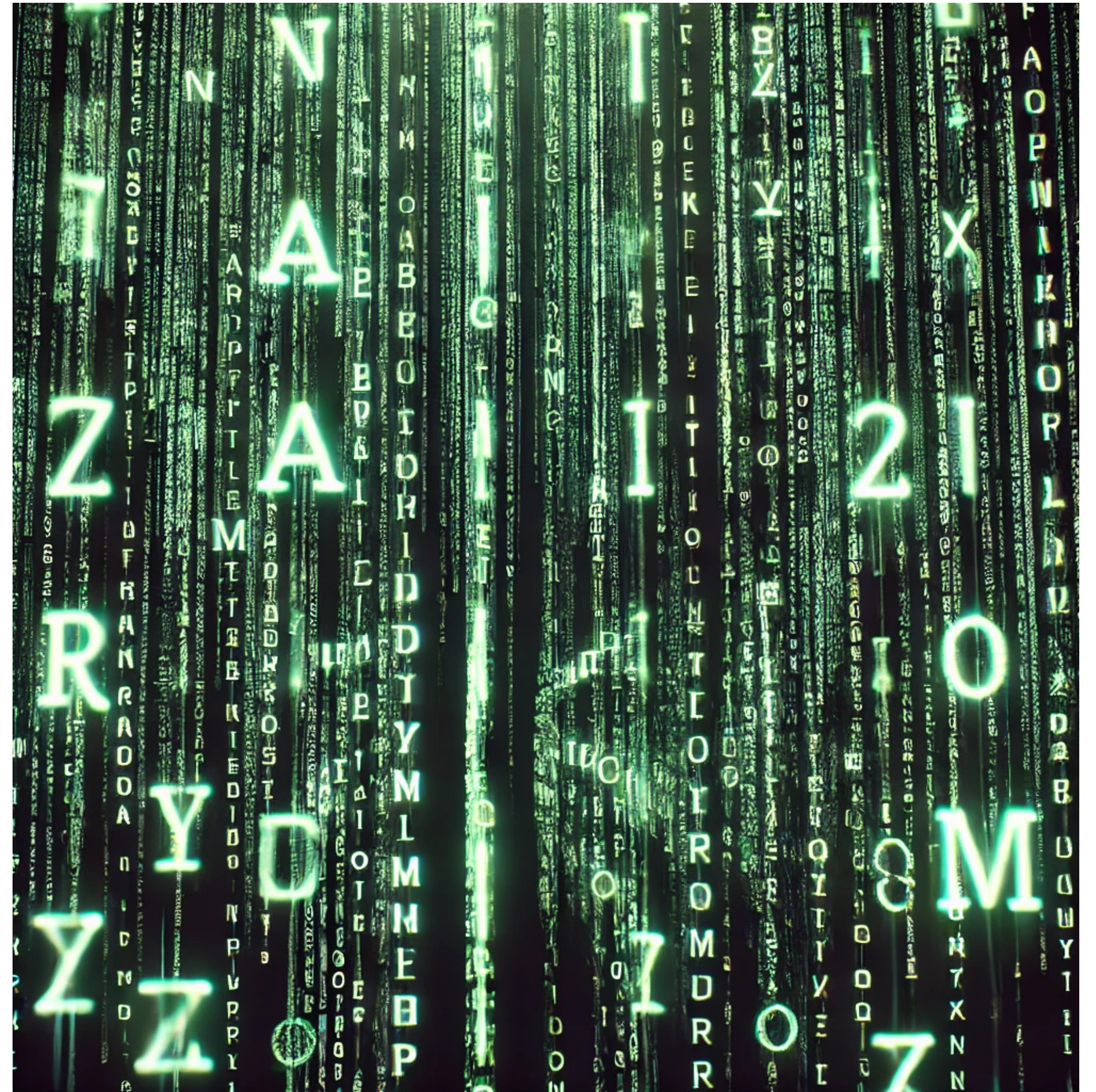
INFRASTRUCTURE LAYER
(FIBER, 4G/5G FREQUENCY, SATELLITE)

shodan.io

Status Cybersecurity di Indonesia

- Status cybersecurity di permukaan di Indonesia
- Prompt: country:ID
- Prompt: port, product, os
- Prompt: Universitas Indonesia, Institut Teknologi Bandung

Wisdom of Cybersecurity



*I've spent the **first half, 15 years** of a career trying **to make communications easier** because I could tell that something like the internet could become humanity's collective digital nervous system, and I thought that was a cool thing and I thought that would be great.*

*I've spent roughly the **second half, another 15 years** trying **to make communication harder** or at least more selective and safer, because of **all of the criminals and spammers that we brought with us** when we create humanity's collective digital nervous system*

Paul Vixie, the creator of the BIND DNS software

Cybersecurity Usual Suspects

- Unpatched vulnerabilities
- Security misconfiguration
- Weak, leaked, and stolen credentials
- Social Engineering
- Insider Threats

Threats & Countermeasures: CIA Triads

No, not that CIA

- **Confidentiality** - preventing unauthorized people or processes from accessing the data
- **Integrity** - maintaining and assuring the accuracy and completeness of data. Data cannot be modified in an unauthorized or undetected manner.
- **Availability** - ensuring information is available when needed, within expected bounds*
 - Example: it is expected that tape backups will be slow to recover data



Confidentiality

Threats: Disclose protected information intended to be kept private

- Confidentiality is attacked through A server may be compromised to extract the database of personal information.
 - Example: Ashley Madison is a cheating/dating site that had its customer information very publicly exposed
 - Sometimes the goal is password databases that can be decrypted and exposed (see: haveibeenpwned.com)

Integrity

Threats: modifying information to point to different information

- Integrity is attacked through.
 - A common example here is web site defacements, where the primary motivation for the attacker is to change the homepage of a web site (see: www.zone-h.org/archive)

Availability

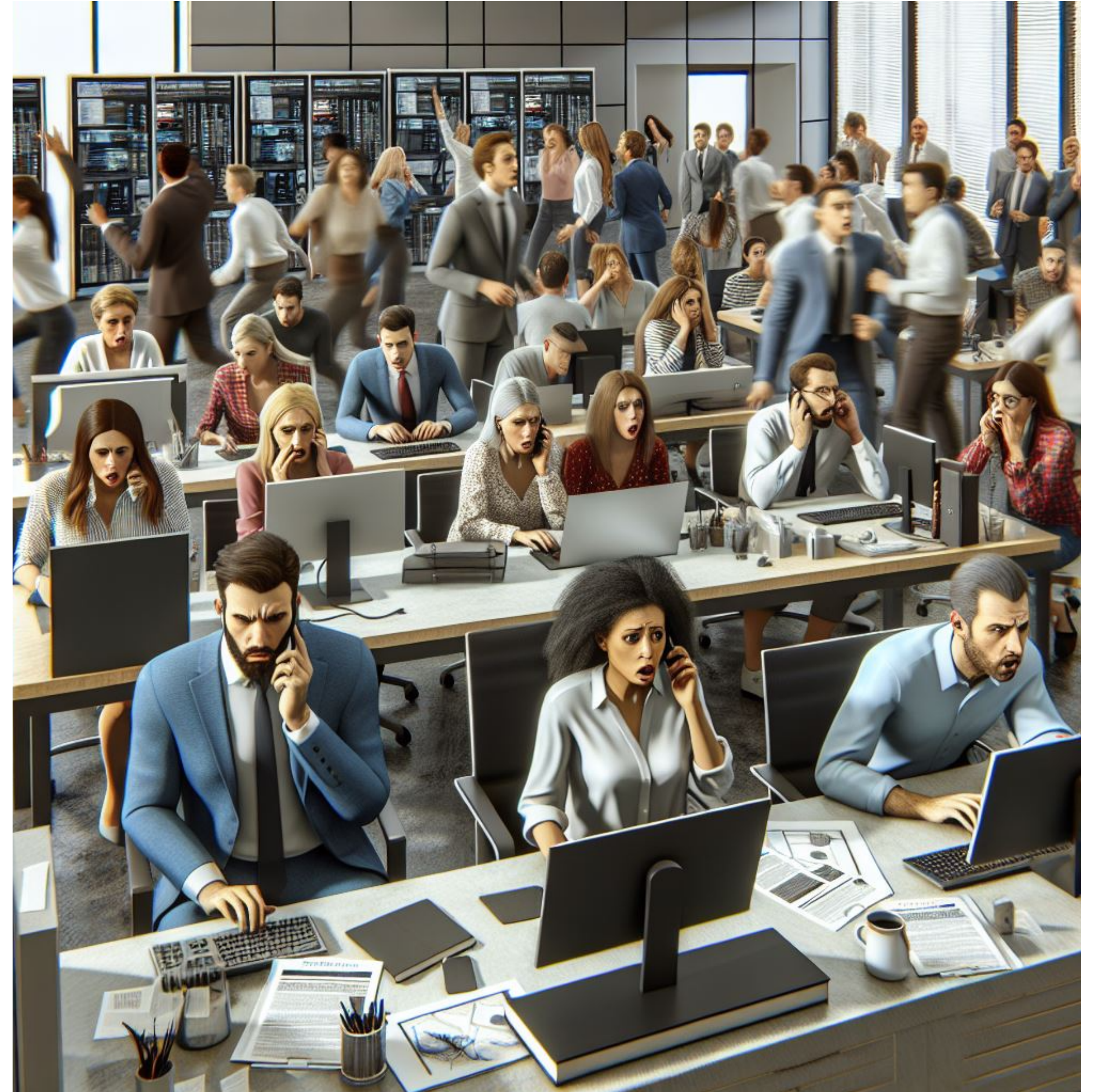
Threats: taking the systems or services offline

- Denial of Service (DoS) attacks typically target vulnerabilities in the application or operating system with small specially crafted packets.
- The network can be made unavailable by flooding the upstream connections with an excessive volume of data to fill the limited bandwidth.
- Attackers may also send an excessive number of small packets in order to fill up the router's connection tables.
- Server software can be made unavailable through exhausting the server resources (CPU, RAM, connection tables) through sending either legitimate or forged excessive connections

CIA Defences or Countermeasures:

- Confidentiality
 - Access control, encryption
- Integrity
 - Hashing, encryption, digital signatures
- Availability
 - Redundancy, high-availability, patching, increasing resources, backups, disaster recovery and business continuity plans (DR / BCP)

Cybersecurity Case in 2024



Use Case: National Data Center

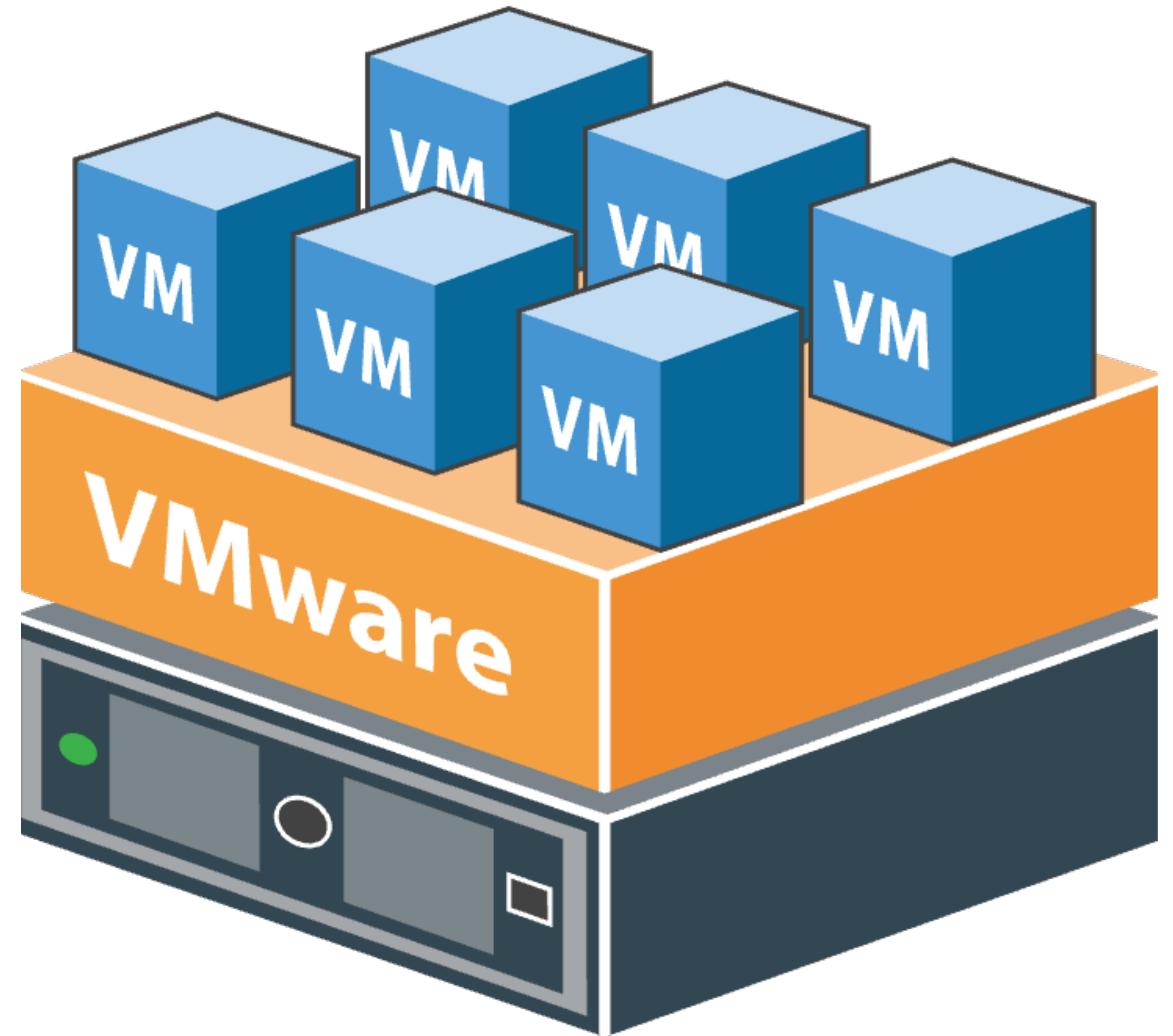
On a country located in Southeast Asia

- I wouldn't try to assume anything
- National Data Center host thousands of government applications and information systems
- Let's talk about the technology & security background

Virtualization

Datacenter Technology

- The idea: Resource Consolidation
- Rather than having 50 servers with:
 - 4-core CPU, 8GB RAM, 20GB disk, 1GE ethernet
- Can be consolidated into 1 server with:
 - 96-core CPU, 512GB RAM, 4TB disk on storage network, 100GE ethernet



Servers

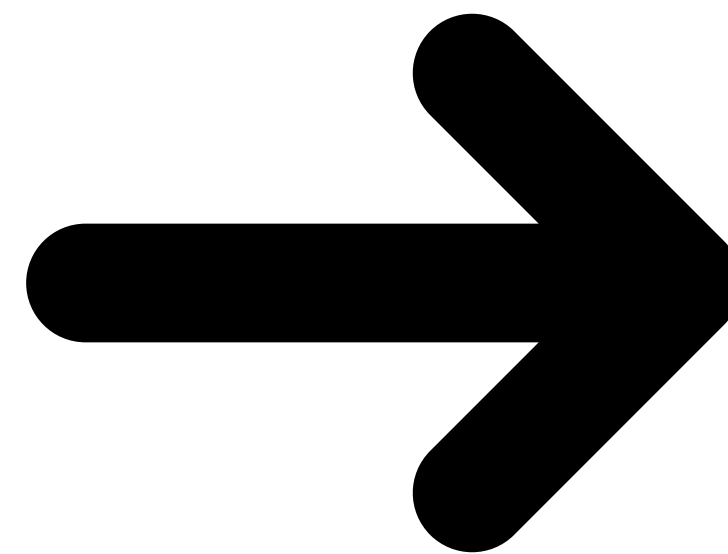
The ingredients of Data Center

- Consist of Rack Unit (RU) measurement
- 1RU, 2RU, and Blade enclosure (between 7-10RU)
- One datacenter rack usually 42RU, there are 45RU





- 8 servers:
- 4-core CPU
- 8GB RAM
- 20GB disk
- 1GE ethernet



- 1 servers:
- 64-core CPU
- 256GB RAM
- 4 TB disk
- 100GE ethernet



Datacenter Operation

Resource Consolidation

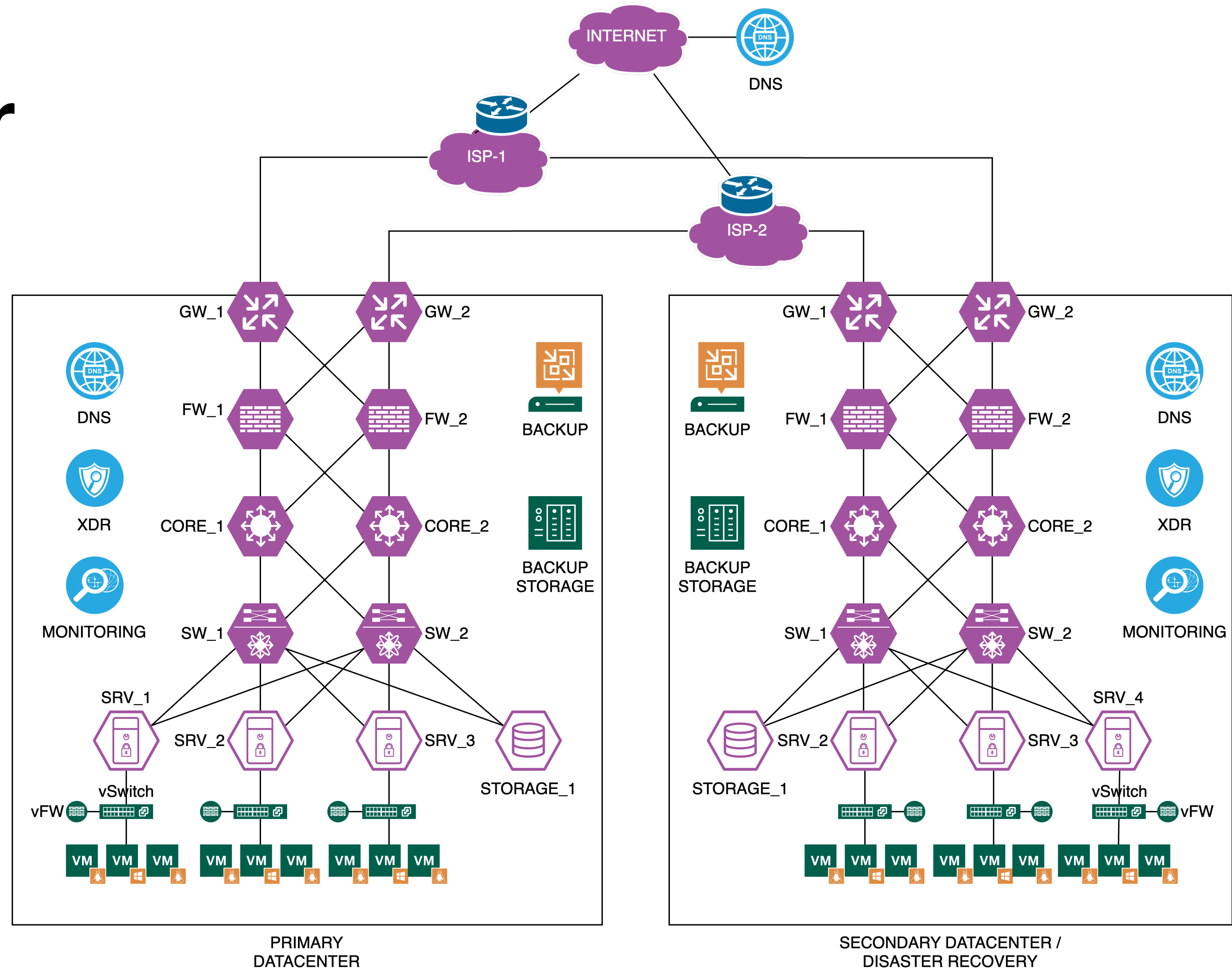
- Space
- Power
- Cooling
- Operational management



Data Center

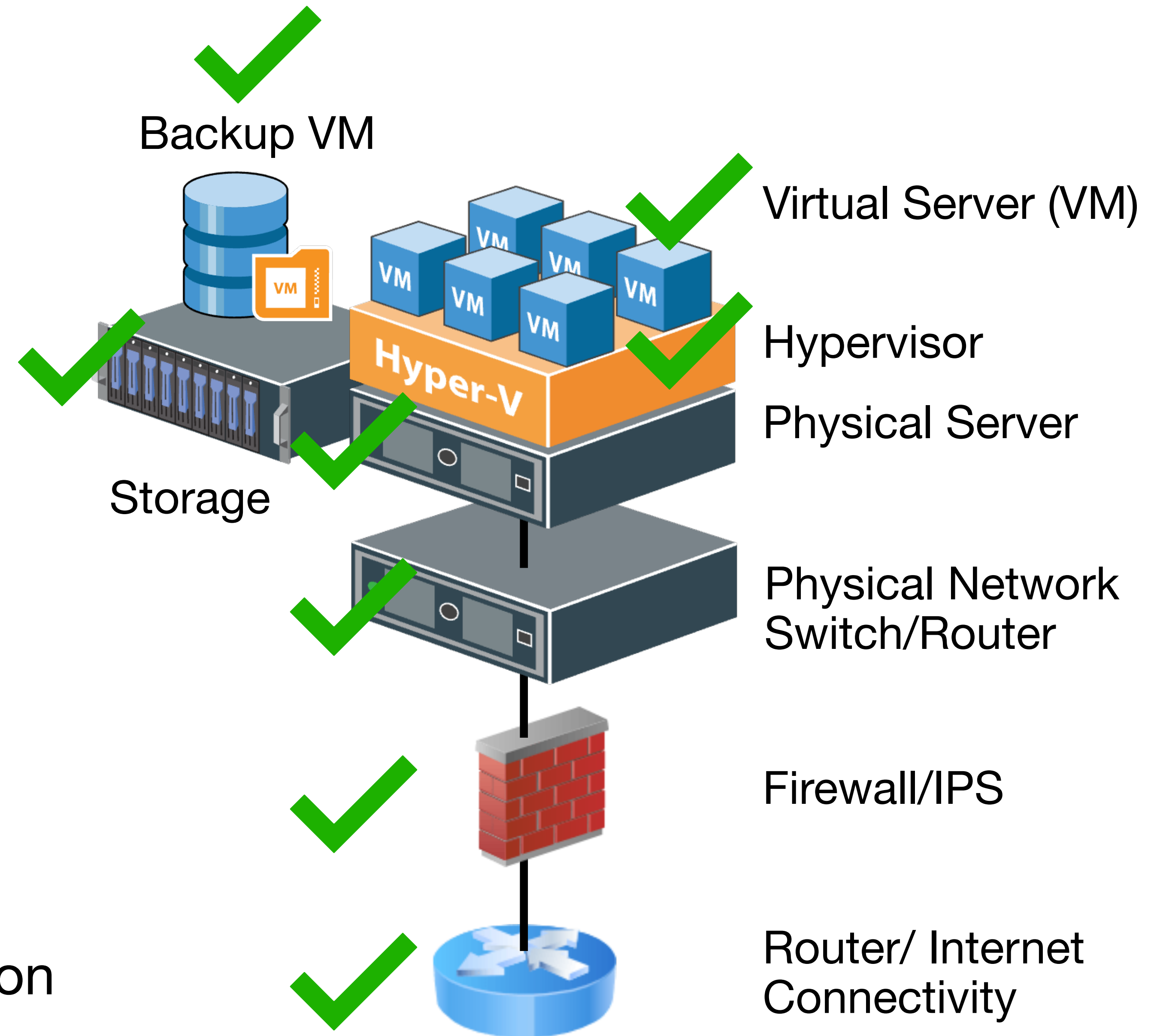
Sebuah contoh

- Physical Infrastructure:
 - Building, power, networks, servers
- Data infrastructure:
 - Application, data, archive
- Supporting infrastructure:
 - Hypervisor, network virtualization
 - Network monitoring
 - Security measures & monitoring
 - Data backup



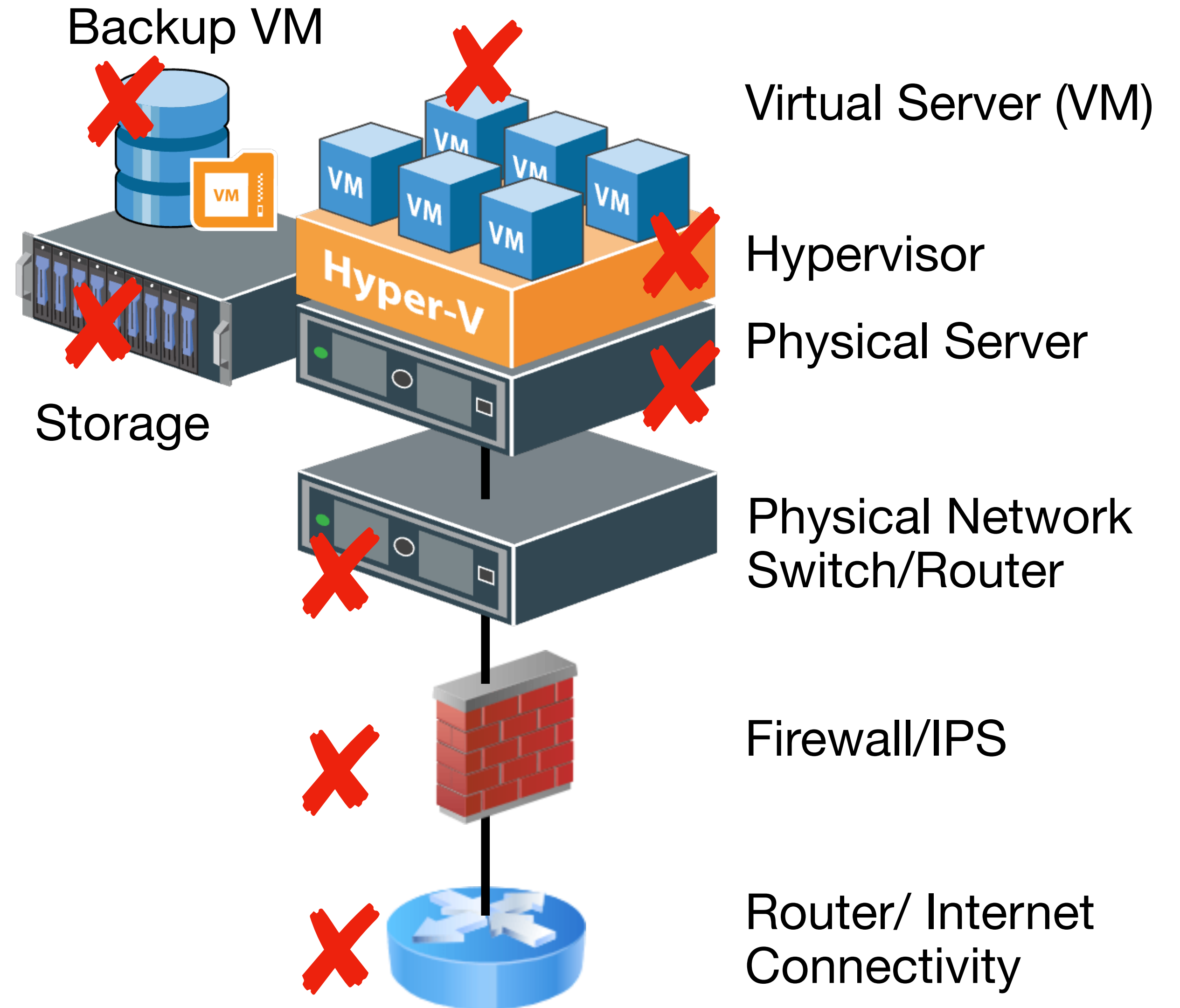
Level of Protection

- Internet connectivity protection
- Network security protection
- Server protection
- Hypervisor protection
- Storage protection
- VM protection
 - OS, Application, Data protection



Level of Protection

- Disrupted internet connectivity
- Datacenter network security breach
- Server not available
- Hypervisor cannot start -> VM cannot start
- Storage not available -> data, VM loss
- VM unprotected:
 - Can't access data -> availability loss
 - Data changed -> integrity loss
 - Data breach -> confidentiality loss



Actionable Items



Actionable Items

- End-users
- IT Architect and Implementation
- Government as regulators

End Users

Actionable Items

- Keep Software and Devices Up to Date
- Be Wary of Phishing and Suspicious Links
- Back Up Important Data with 3-2-1 rules
- Use Secure Networks and Encryption
- Use Strong, Unique Passwords and Enable Multi-Factor Authentication (MFA)

IT Architect and Implementation

Actionable Item

- Implement the CIA triads
- Patch all of your software
- Prevent malware installations
- Implement Incident Response
- Adhere to some security frameworks
- Commit to mandatory compliance regulations

Government as Regulator

Actionable Item

- Develop and Enforce Cybersecurity Laws and Standards
- Create National Cybersecurity Agencies and Promote Information Sharing
- Provide Adequate Funding and Support for Cybersecurity Research
- Raise Public Awareness and Promote Cybersecurity Education
- Coordinate International Cybersecurity Efforts

Terima Kasih!