Cybersecurity *Awareness* Month

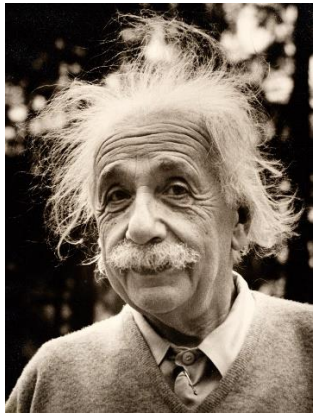
Do Your Part and Be Cyber Smart

By ***Hud*** *Seidu Daannaa*

www.daannaa.space | https://www.linkedin.com/in/hudsec

Please don’t judge the hair, our thoughts evaporate through the skin pores of our heads, *and our hair reacts accordingly*. **We are just too busy trying to save the world**, patting it down will take time.

Thank you all for understanding…



Snr. Manager - Cybersecurity Eng./Architect *(R&D)*
Lead *(Big Data & SOC Specialist)*

Cloud Solutions Architect

MSc| CEH| AWS-SAA| AZ-500| GCHQ| EC-Council-CS-Career-Mentor

www.daannaa.space |
https://www.linkedin.com/in/hudsec

Agenda

- **Early days**
- **Modern day** *(the cyber world & other worlds)*
- what is **cybersecurity**
- Importance of **cybersecurity**
- Impacts of **crimes** & threats crime in our lives
- Scenario
- **Phishing**
- Mitigations

Q&A

- Computers can be hacked, but is it possible for the human brain to be hacked as well ?
- Are we semi machines ?

Early Days

In the early days we solely relied on:

- **Grocery shops**
- **Bookshop**
- **Post Office**
- **Shops** *(Shopping)*
- **Banks**
- **Cinemas** *(Movies)*
- **Schools**
- **Work**
- **Conference Meeting**

The **Computer** *and its* **Evolution**

Computers make our lives easy, so we want to have access to that ease everywhere

This draws us to technology both physically and mentally

In **Modern Days** *(Today)*

- **Cyberworld**, the **Future** & the threats *(Easy of life)*
- The **other** Worlds *(Threats to life)*

Threats to the Cyber world

Health *(unauthorized access to patient records, tampering with medical devices leading to incorrect diagnoses or treatments,) , e.g. WannaCry attack ransomware*

Education *(data breaches involving student information, disruptions in online learning, or theft of academic research) e.g Blackbaud Data Breach (2020)*

Mental Health*(Cars could be remotely hijacked, lead to accidents, have their functions altered maliciously) e.g., social media, etc.*

Financial Sectors *(theft of funds, unauthorized transactions, manipulation of financial records, and a loss of trust in financial institutions)*

Government *(unauthorized access to classified information, disruptions in public services, manipulation of election systems, and undermined public trust)*

Social Life *(unauthorized access to personal messages, spreading of misinformation, stalking, or other forms of cyber harassment)*

Threats to the Cyber world *(Future)*

Metaverse *(rampant identity theft, unauthorized access, fraud, manipulation of virtual assets)*

Cryptocurrencies *(Vulnerabilities could lead to theft of funds, unauthorized transactions, manipulation of the blockchain)*

Smart Cars *(Cars could be remotely hijacked, lead to accidents, have their functions altered maliciously)*

Smart Cities *(hackers could cause traffic chaos, power outages, interfere with emergency services, or steal citizen data)*

Military *(Vulnerabilities could lead to unauthorized access to defense systems, misinformation campaigns)*

Neuro link *(there's potential for unauthorized brain data access, manipulation of a user's neural device)*

Artificial Intelligence *(compromised AI can make wrong decisions, be used maliciously)*

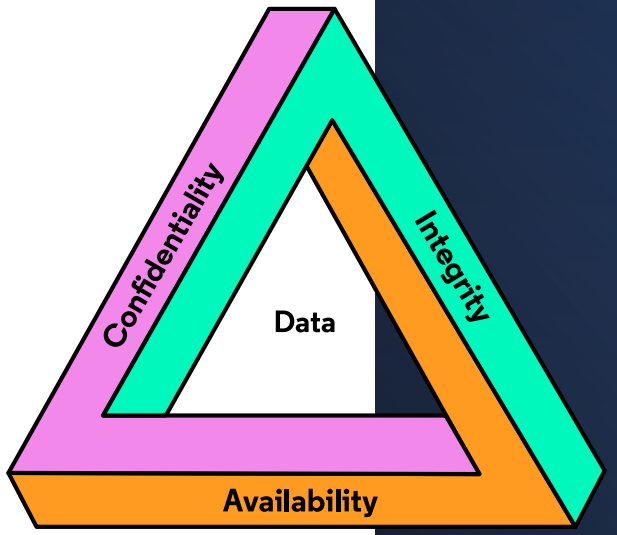
The way forward

- We cannot do without technology today *(we are tech)*
- *We have become so **dependent**, our lives depend on it*
- There is the need for **security** just like what we have in the real world
- A **cyberworld** calls for **cybersecurity**

We need to Stop **cyber attacks** *like these*

What exactly does Cybersecurity entail ?

- Cybersecurity refers to the practice of protecting *computer systems, networks, and data from theft, damage, disruption,* or *unauthorized access.*
- Aimed at ensuring **confidentiality**, **integrity**, and **availability** of data. The CIA triage

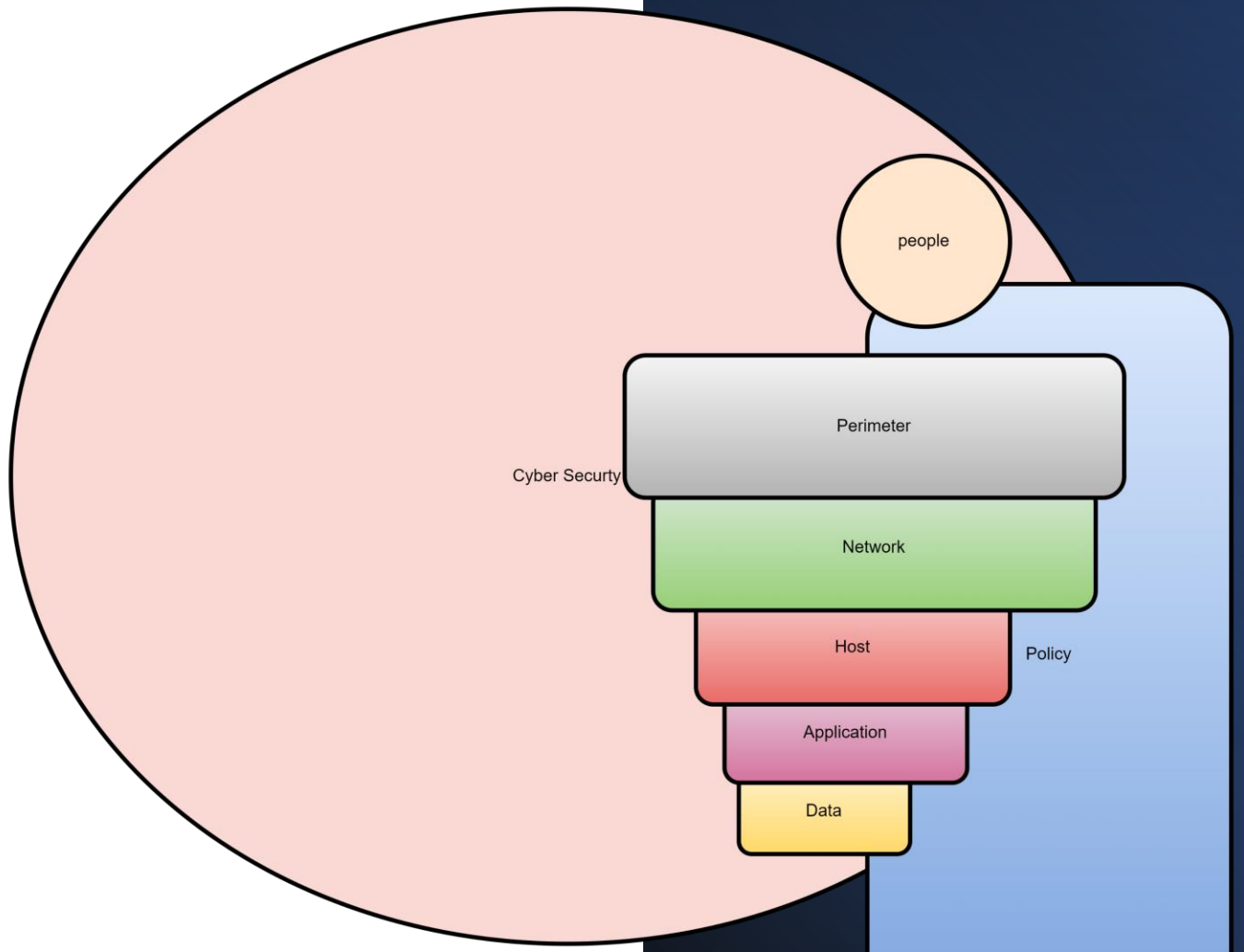


Importance Of Cybersecurity

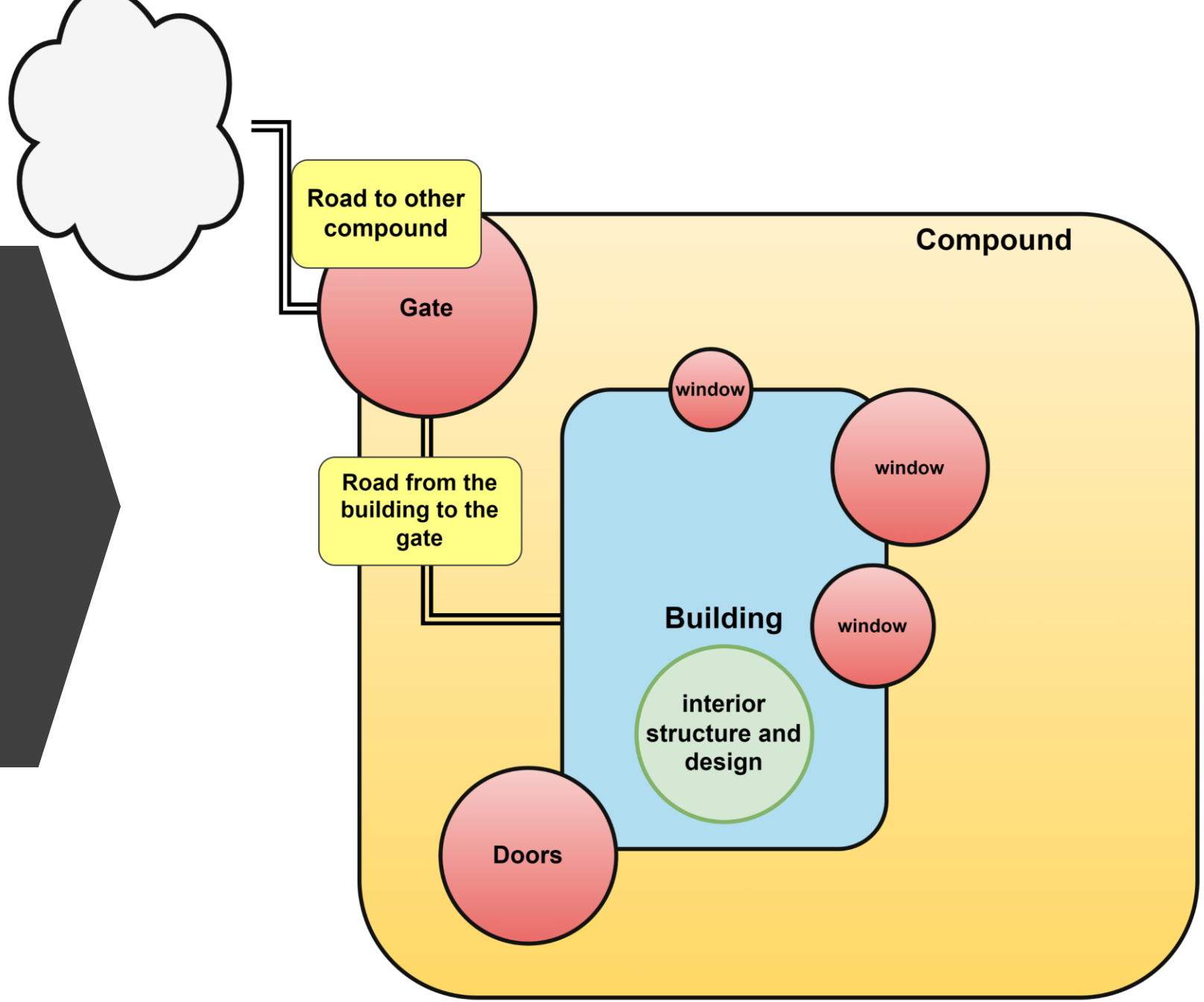
- **Protection of Data**: As data becomes more central to our lives and businesses, cybersecurity ensures that sensitive personal and business data is protected from unauthorized access and cyber threats.
- **Prevention of Unauthorized Access**: Cybersecurity measures prevent hackers and cybercriminals from accessing and misusing personal, financial, or business information, which could lead to identity theft or financial loss.
- **Maintaining Business Continuity**: For businesses, a cybersecurity breach can result in downtime and disruption. Implementing strong cybersecurity measures ensures uninterrupted business operations.
- **Boosting Customer Trust**: When customers know that their data is secure with a company, they are more likely to trust and engage with it. A secure online presence strengthens customer loyalty and trust.
- **Regulatory and Compliance Reasons**: Many industries have regulations requiring businesses to take certain cybersecurity measures to protect customer data. Non-compliance can result in hefty fines and legal repercussions.

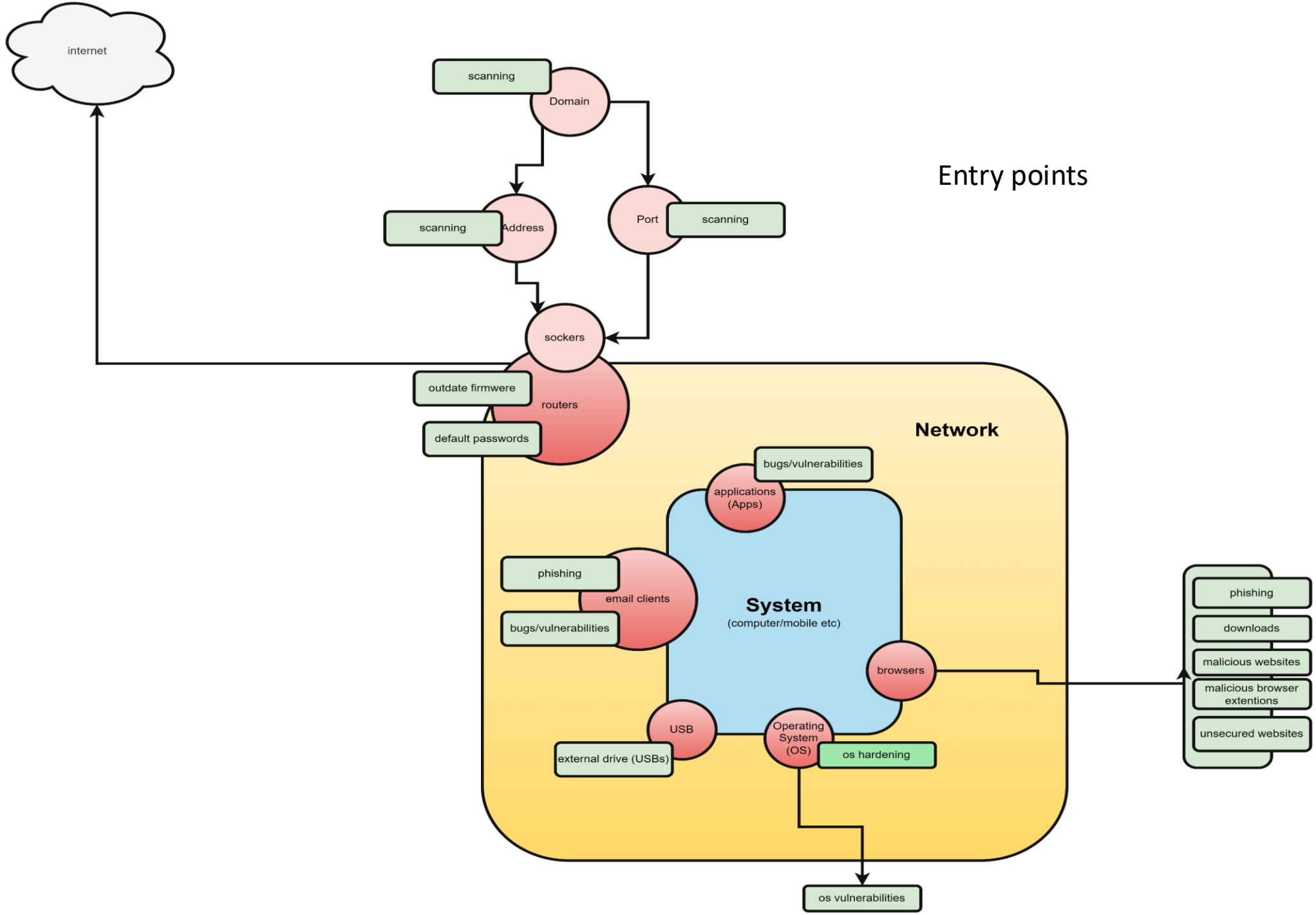
Breakdown Of Cybersecurity

- **People**
- Hardware
- Network
- Applications
- **Data**
- Procedures



The Breakdown





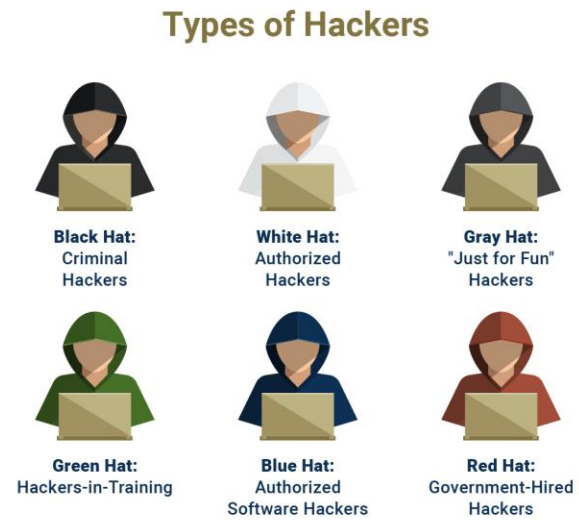
Entry points

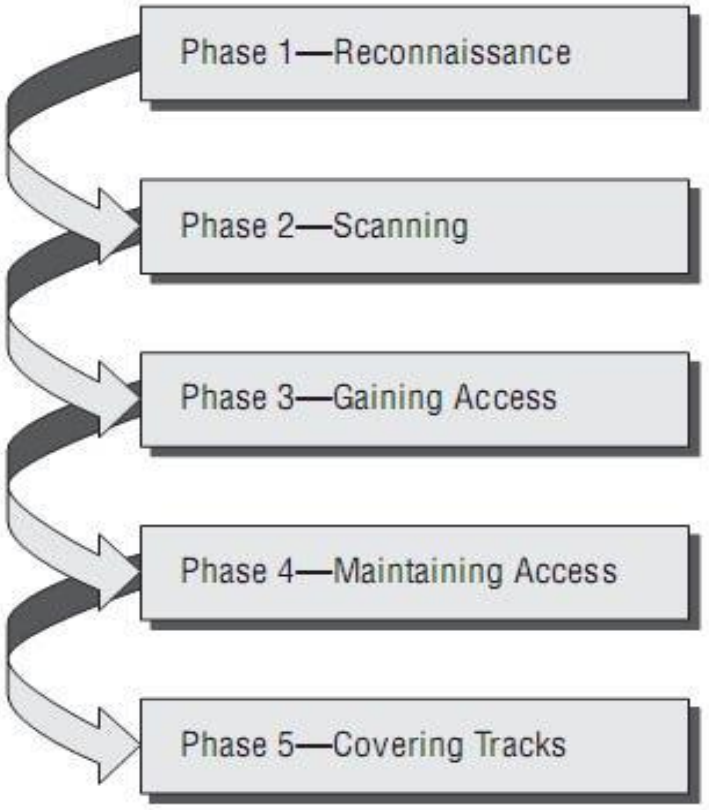
Cybersecurity frameworks

- Cybersecurity frameworks provide structured approaches and best practices to managing and securing an organization's information and technology assets

Threats	Functions & Safeguards				
	Identify	Protect	Detect	Respond	Recover
Out of Memory	-Inventory of IT systems	-Autoscaling instances -Increase instance sizes	- Infrastructure monitoring alerts on memory usage to trigger incident	-DevOps pipeline redeploys with new instance size -Restart Machine	-Change Configuration Settings to account for this threat
SQL Injection	-Identify web pages which require user input	-Sanitize input fields -Use cases which use SQL attacks -WAF/RASP	-SAST/DAST Scanner -IDS alert	-Block bad user accounts -Turn off API	-Post-mortem -Backups
Insider Threat	-List of users with Admin Privileges	-Require two person approval	-Log privileged activities	-Contact Security -Remove user access	-Legal Investigation

A **Cyber** **Attack** *(structure – A **hackers** mindset)*





Cyber *Crimes*

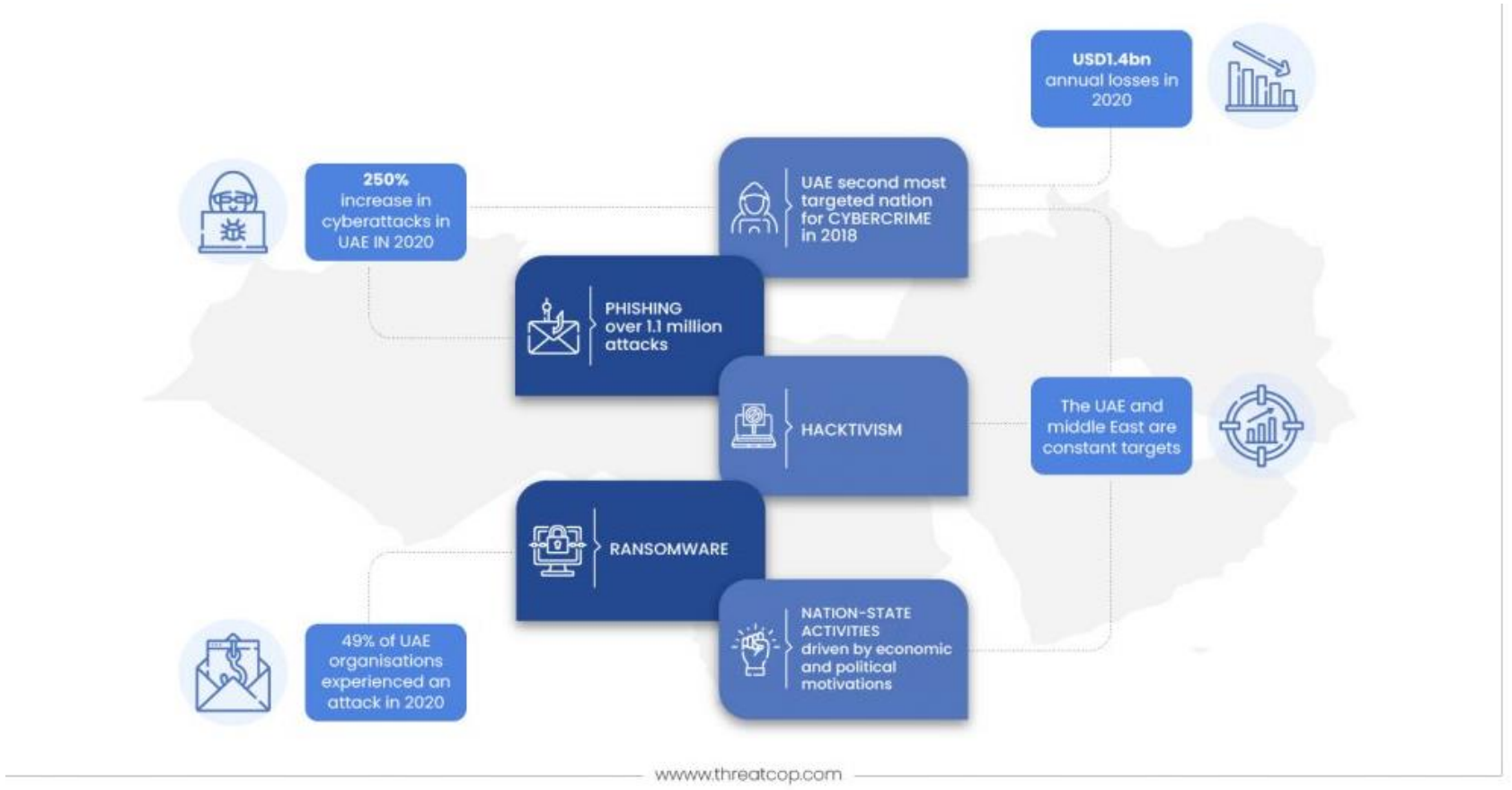
- **Malware:** Malicious software designed to harm or exploit devices, networks, or services.
- **Ransomware:** Malware that encrypts a victim's files, demanding payment to restore access.
- **Virus:** Malware that self-replicates by inserting its code into other programs
- **Phishing:** Deceptive attempts, usually via email, to steal sensitive information by posing as a trustworthy entity.
- **Denial of Service (DoS) Attack:** An attack aimed at making a service unavailable by overwhelming it with traffic.
- **Identity Theft:** Illegally acquiring and using someone's personal data, typically for financial gain.
- **Worms**: Malware that replicates itself to spread to other computers, often using network connections, without requiring human intervention.
- **RATs (Remote Access Trojans):** Malicious software that allows a hacker remote access and control over a victim's computer without their knowledge.

Statistics of *cyber attacks* in the **UAE**

- According to a blog by **Internation Security Journal**, there were 311 attacks in a week per organization **in 2021, while in Kuwait and Saudi Arabia, there were 409 and 392 attacks respectively**.
- It is believed that due to remote working, **cyber attacks in the UAE** **have increased by 190%. Brute force attacks were 15.8 million on RDP** (Remote Desktop Protocol).
- Not only in UAE, but the whole Middle East has reported over **2.57 million phishing attacks** in 2020.
- The UAE **experienced a 250% increase** in cyber attacks in 2020, led **primarily by phishing and ransomware attacks**.
- An article by **ITP.net** has revealed that, according to a report, **72% of the CISOs in the UAE feel unprepared to deal with a cyber attack**.
- In 2020, **UAE lost $1.4 billion** due to **cyber attacks**.

Cyber Attacks on Organizations *(UAE)*

Notable **Attacks** in the *UAE*



BREAK