CYBER SECURITY

Dr. N. Rukma Rekha

University of Hyderabad

Outline

- Introduction to CyberSecurity
- Cyber Security Threats
- Cyber Criminals
- Cyber Security Solutions
- Blockchains in Cyber Security
- Is Blockchain the future of CyberSecurity?
- Use cases - Government Perspective

Introduction to Cyber Security

Security

- Security is “the quality or state of being secure”
  — to be free from danger

- Protecting Money Vs Information

- Weakness of a system
  - **Vulnerability**
  - **Threat**
  - **Attack**

- Attacks
  - Interception – unauthorized party gains access - may / may not detect
  - Interruption – asset of system becomes lost/ unusable / unavailable
  - Modification – access the data & tamper it
  - Fabrication – un authorised party create fabrication of counterfeit objects

- Attacker must have a MOM
  - Method – skills, knowledge to pull off the attack
  - Opportunity – time & access to accomplish attack
  - Motive - reason to perform the attack against a system

What is Cyber Security?

- "The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks such as theft, damage, modification or unauthorized access."
  - Cyber refers to the technology that includes systems, networks, programs, and data.
  - Security is concerned with the protection of systems, networks, applications, and information.

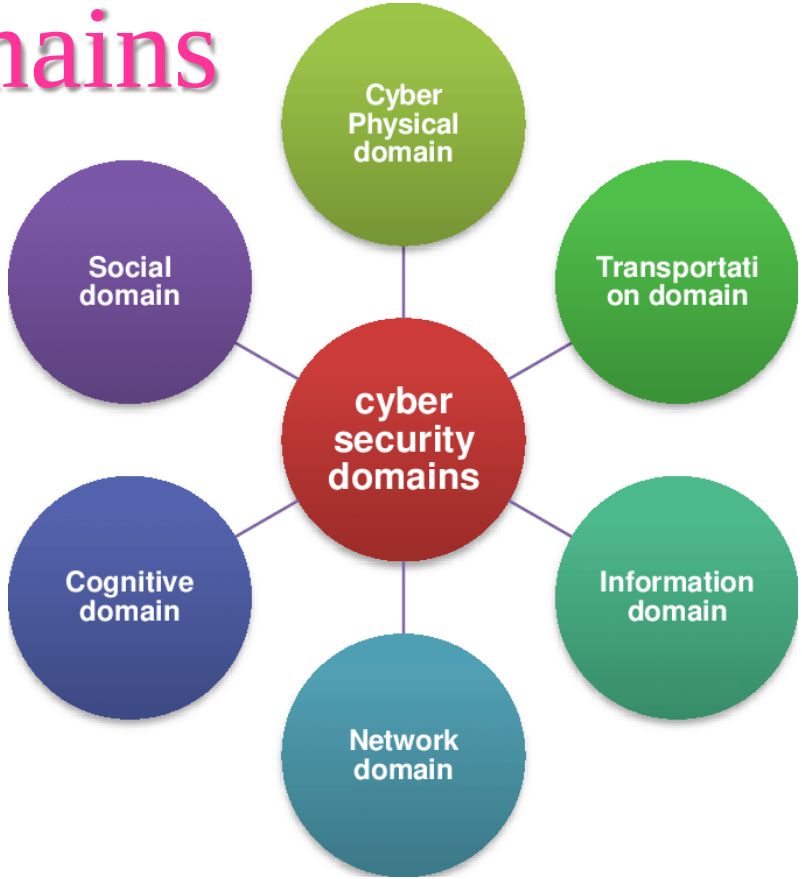
- Aim is to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks and technologies.

5W's of Cyber Security

- **Where**
  - Banking system, healthcare, financial institutions, governments, and manufacturing industries use devices connected to the Internet.
- **What**
  - Information, such as intellectual property, financial data, and personal data, can be sensitive for unauthorized access.
- **Who**
  - Intruders and threat actors
- **How**
  - Cyber-attack is now an international concern that hacks the system.
- **Why**
  - financial gain, extortion, political or social motives, or just vandalism.

Cyber Security domains

- Physical
- Information
- Cognitive
- Social



Zachary A. Collier, Igor Linkov, James H. Lambert, "Four domains of cybersecurity: a risk-based systems approach to cyber decisions", Environ Syst Decis (2013) 33:469–470

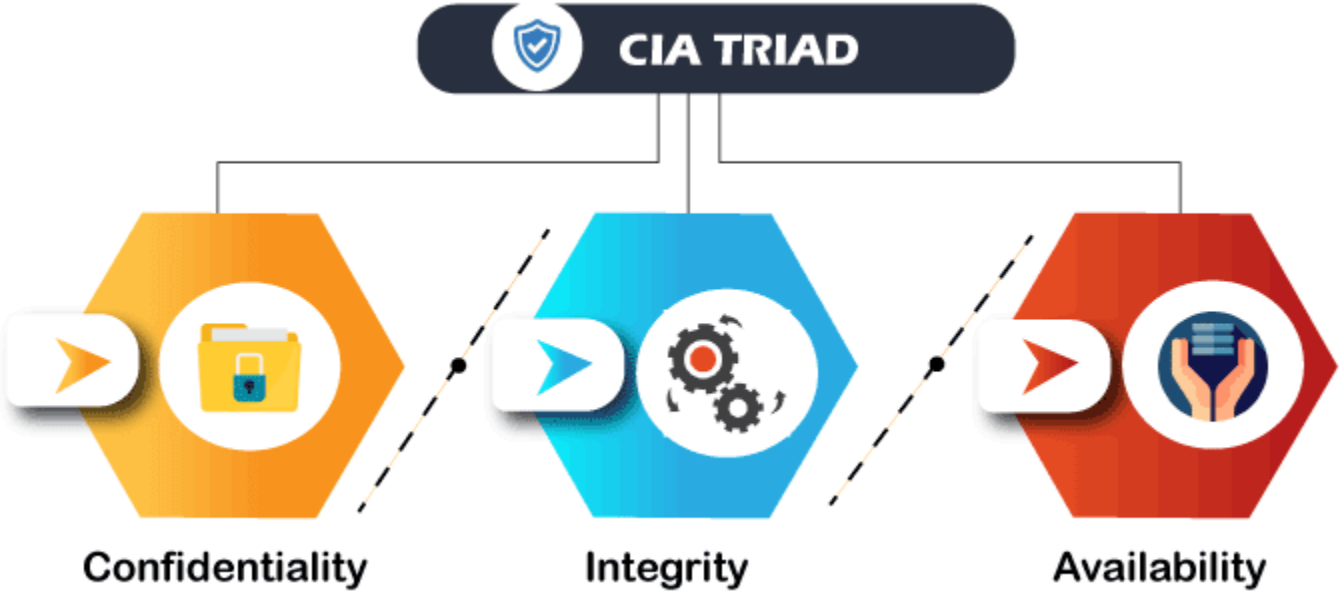
Then what is Information Security?

- "The protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information."
    - Broad areas – information security management, computer and data security, and network security.

- The CIA model of information security.

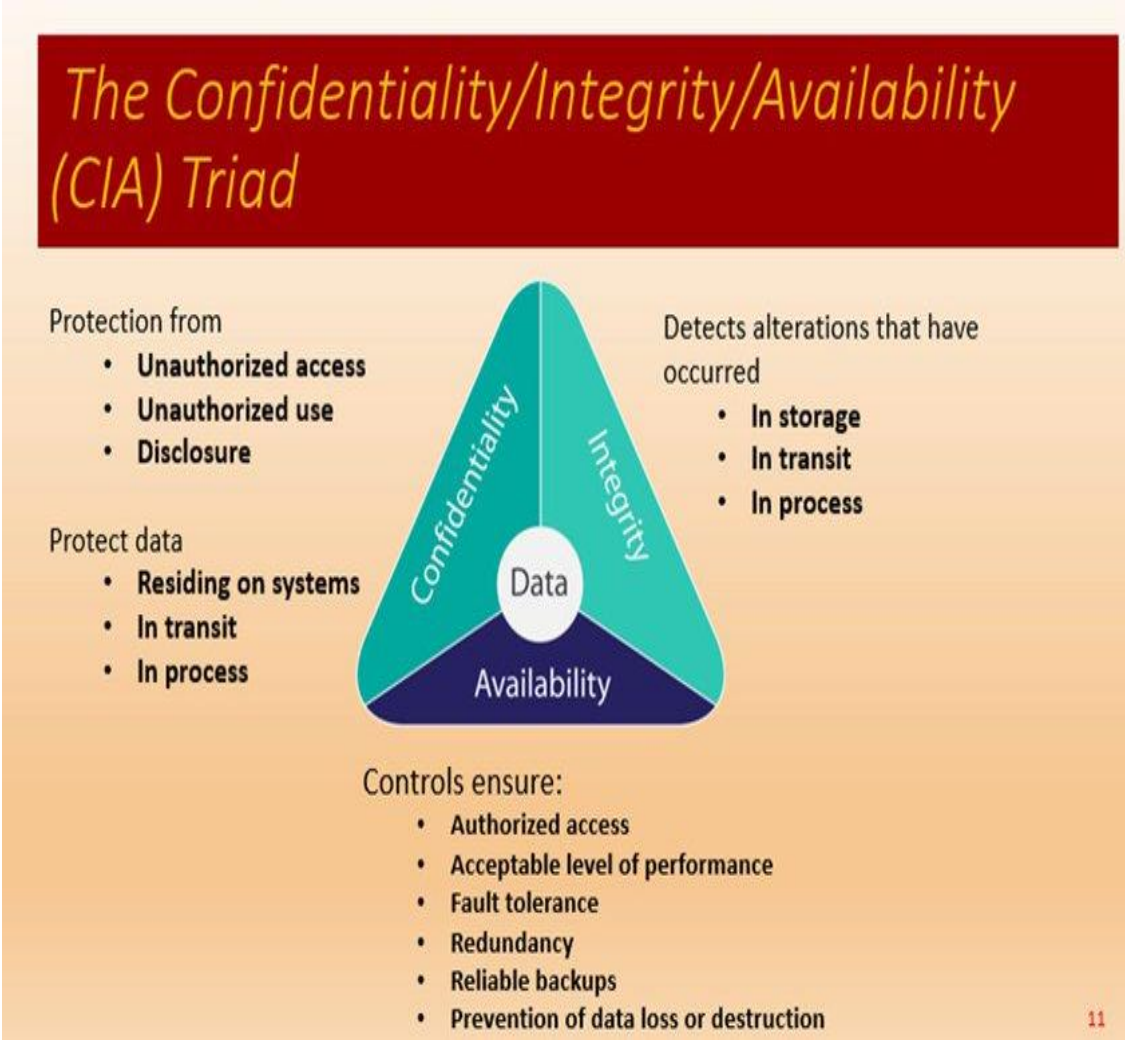
Security Parameters

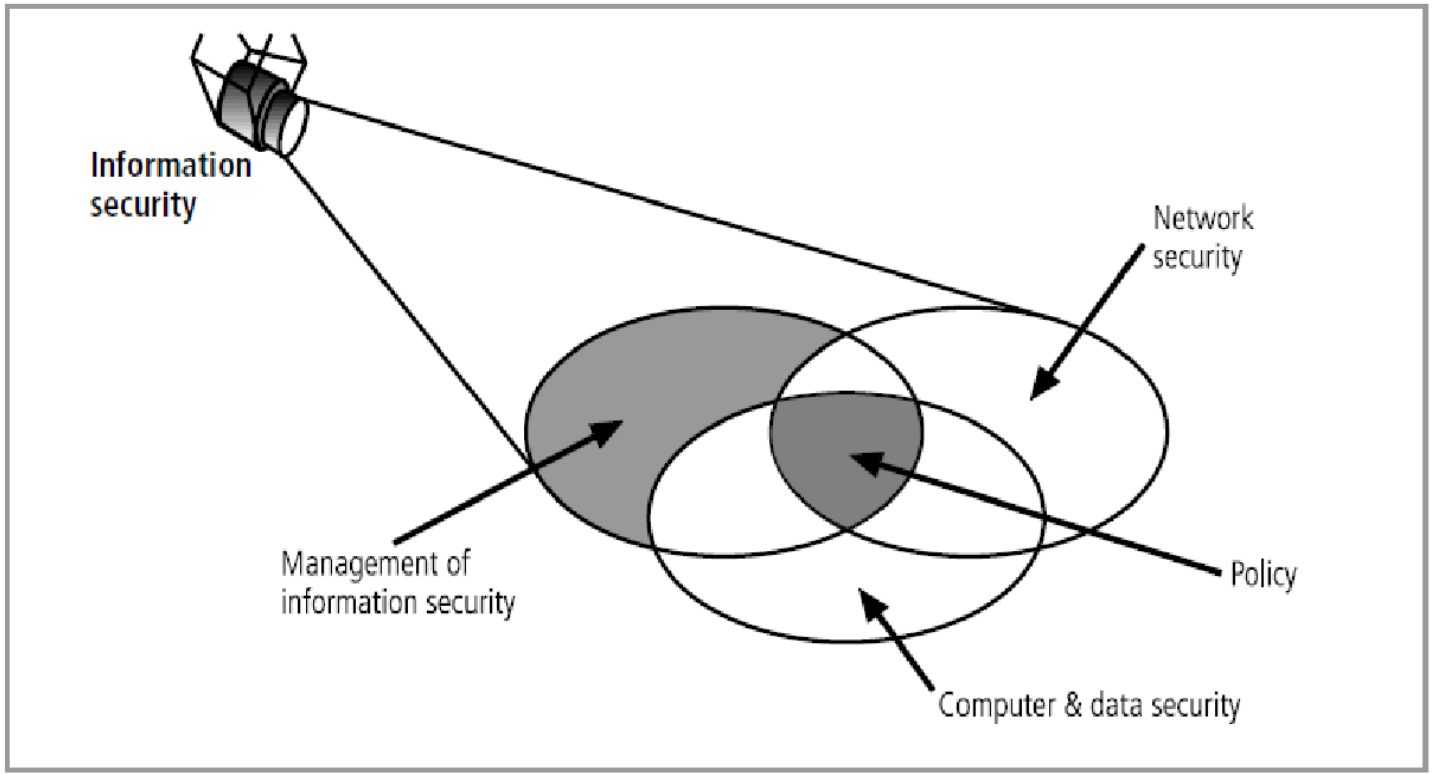
- CIA triad

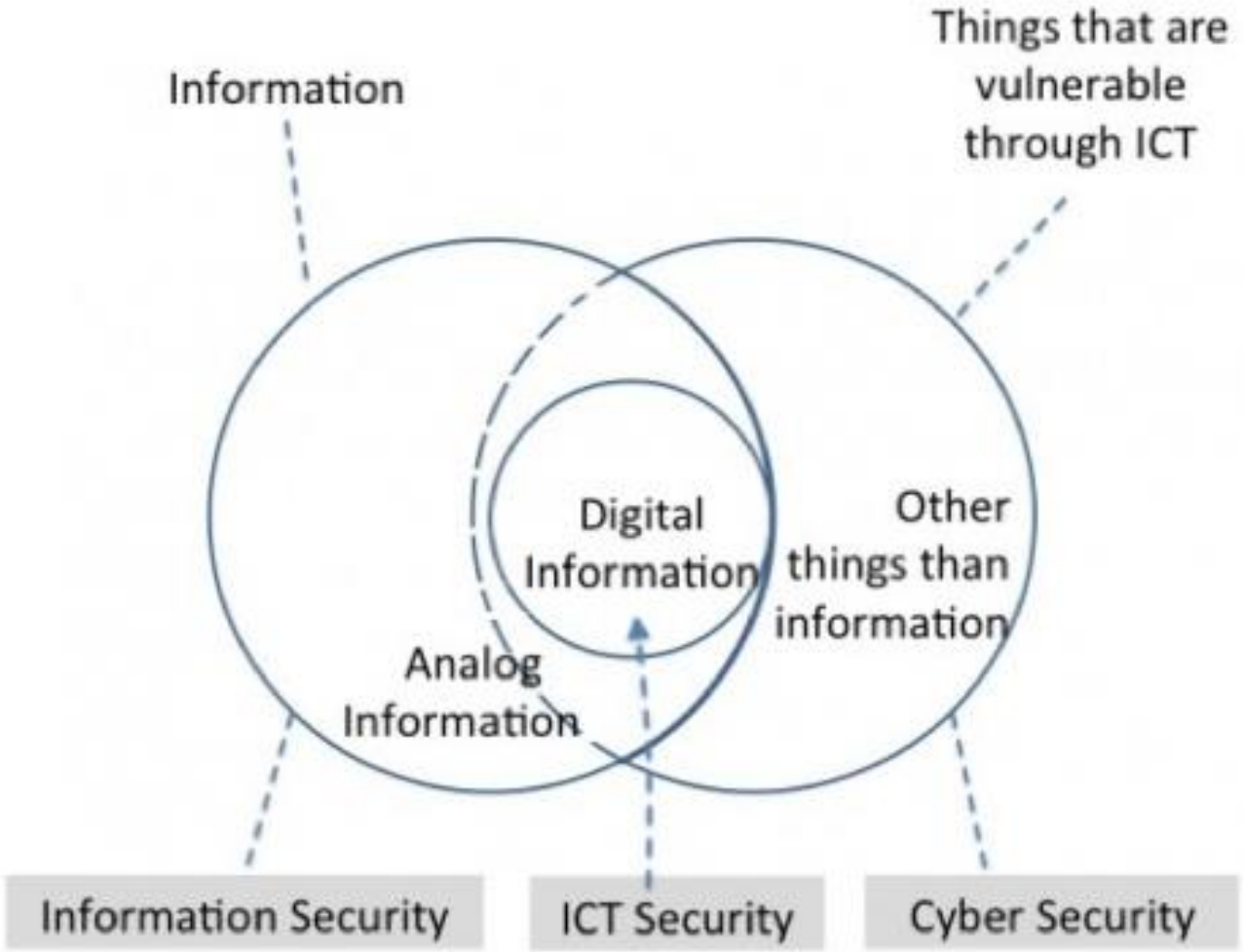

CIA TRIAD
Confidentiality
Integrity
Availability

Tools for CIA

- Confidentiality
  - Encryption / Access control
  - Authentication / Authorization
  - Physical Security
- Integrity
  - Backups
  - Checksums
  - Data correcting codes
- Availability
  - Physical Protections
  - Computational Redundancies




Information security
Network security
Management of information security
Policy
Computer & data security


Information
Things that are vulnerable through ICT
Digital Information
Other things than information
Analog Information
Information Security
ICT Security
Cyber Security

Cyber Security Goals

DATA PROTECTION

- CIA triad

Is that all?

Confidentiality	Integrity	Availability	Accountability	Accuracy
Authenticity	Awareness	Completeness	Consistency	Control
Democracy	Ethics	Legality	NonRepudiation	Ownership
Physical Possession	Reassessment	Relevance	Response	Responsibility
Risk Assessment	Security Design & Implementation	Security Management	Timeliness	Utility

How to achieve Cyber Security?

- Policy : CIA
- Threat Assumption
- Mechanism : H/W, S/W, System

Cyber Security Threats

Example

- Password Reset (Gmail)

- Alternate Email Id (me.com)
  - Password Reset
  - Address + Last 4 digits of Credit Card

- Amazon
  - Add new credit card
  - Password Reset – Give any credit card information

Vulnerabilities

- Gaps in application
- Inadequate border protection
- Remote Access Servers with weak access controls
- Misconfigured systems
- Systems with default configurations

- Example 1
  - Apple’s Cloud
  - Find my phone interface had no bound on Password guessing attempts

- Example 2
  - Citi bank – login password—Bank account
  - Xyz.com/acct?id=1234

- Example 3
  - Android Bitcoin
  - Seed -0000

Is this fine?

Vulnerable Code:

```
int read_req(void)
{
        char buf[128];
        int i;
        gets(buf);
        i = atoi(buf);
        return i;
}
```

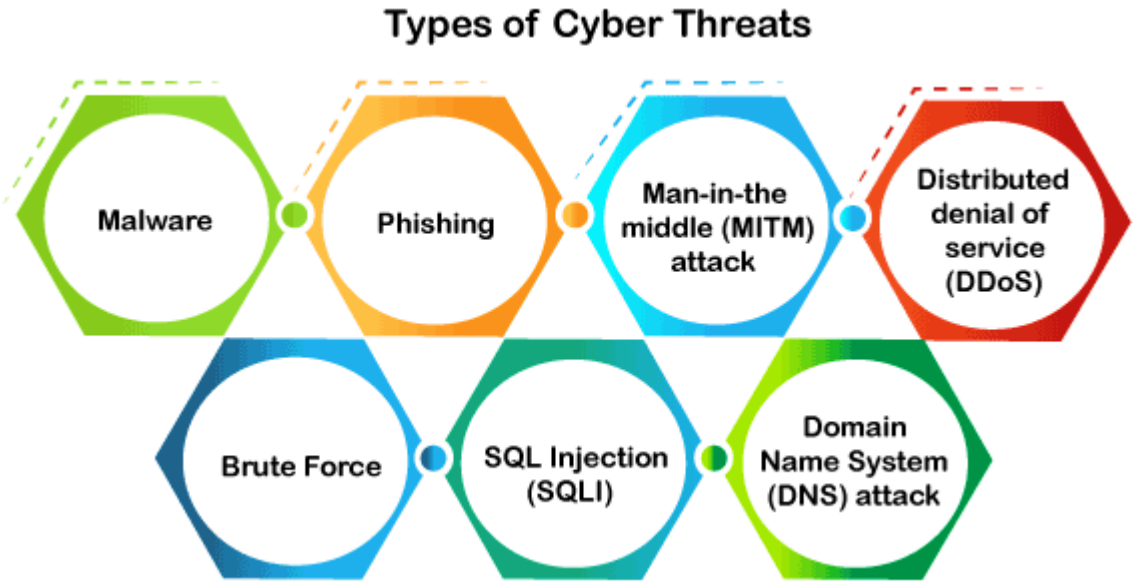
Vulnerable Data:

- https://www.youtube.com/watch?v=QTX1h8zb8MI

Types of Cyber Security Threats

- Malicious activity by an individual or organization

- To corrupt or steal data, gain access to a network, or disrupts digital life



1.Malware - Disrupts or damages a legitimate user's system.

Virus	Spreads from one device to another. Infect files, stoles information, or damage device.
Spyware	Secretly records information about user activities on their system.
Trojans	Corrupt or steal data from our device or our network.
Ransomware	Encrypts a user's data and demands monetary ransom.
Worms	Steal or damage the data.
Adware	Unwanted program that is installed without the user's permission to generate revenue for its developer.
Botnets	Collection of internet-connected malware-infected devices to get data and access without the user's permission.


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/17/2017 16:59:56
Time Left
02:23:59:15
Your files will be lost on
5/21/2017 16:59:56
Time Left
06:23:59:15
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt

2. Phishing

- They contact a target via email, phone, or text message with a link.
- To provide sensitive data such as personal information, banking and credit card information.
- Clicking on the link will also install malware on the target devices.

Policy Update: Communicable Diseases

Human Resources <hr@[[company_domain]]>

FAKE E-MAIL ADDRESS

Wed 3/18/2020 6:04 AM

To: John Smith

All,

TOO GENERIC

Due to the coronavirus outbreak, [[company_name]] is actively taking safety precautions by instituting a Communicable Disease Management Policy. This policy is part of our organizational preparedness and we require all employees to read and acknowledge the policy before [[current_date_1]].

URGENCY

If you have any questions or concerns regarding the policy, please contact [[company_name]] Human Resources.

Regards,
Human Resources

CHECK FOR FRAUDLENT LINKS

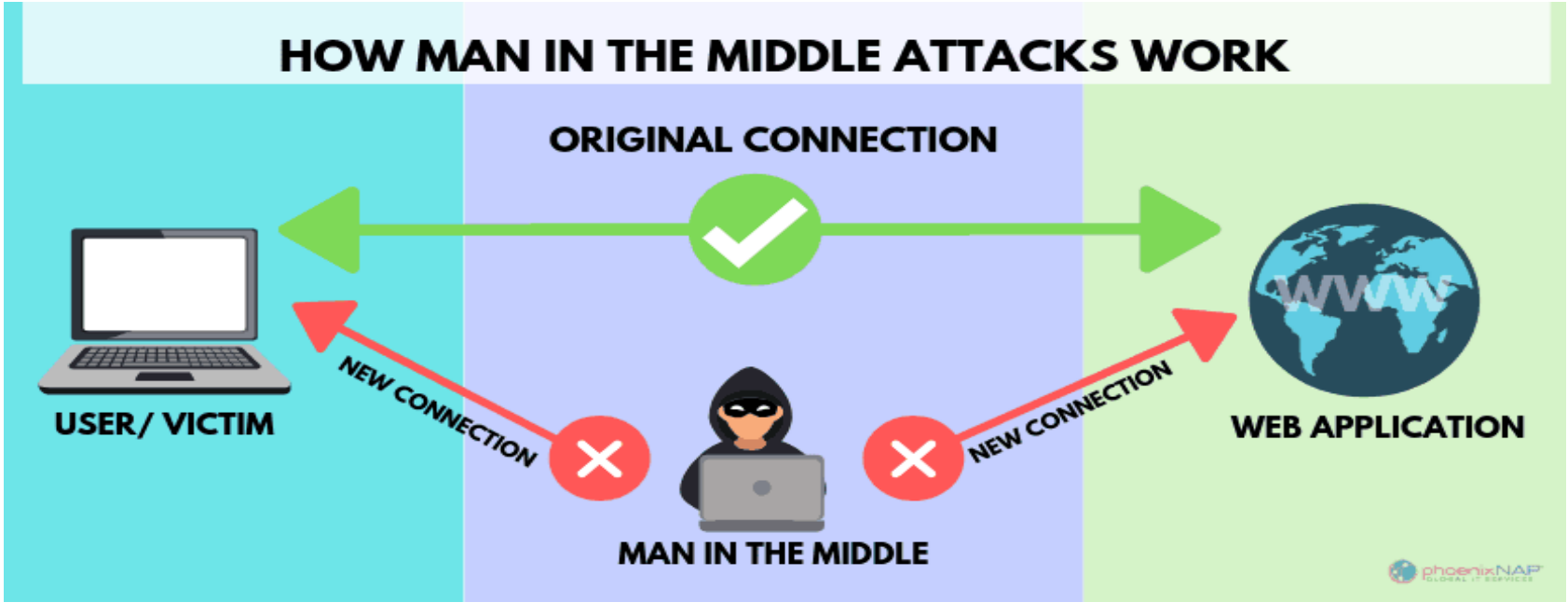
Make sure company details are correct but also standard verbiage for your organization.

LEGEND

- FAKE E-MAIL ADDRESS
- TOO GENERIC
- BAD LINKS
- URGENCY

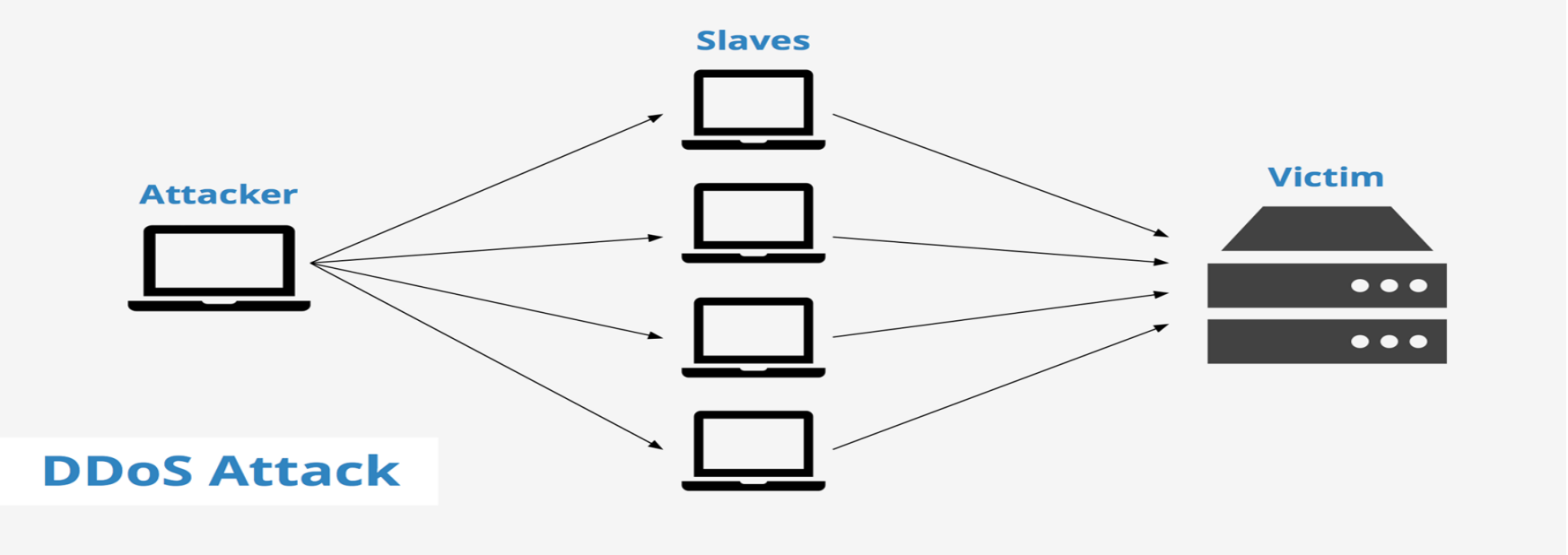
3. Man-in-the-middle (MITM) attack

- Cybercriminal intercepts a conversation or data transfer between two individuals.
- The main objective is to gain access to our business or customer data.
- A cybercriminal could intercept data passing between the target device and the network on an unprotected Wi-Fi network.



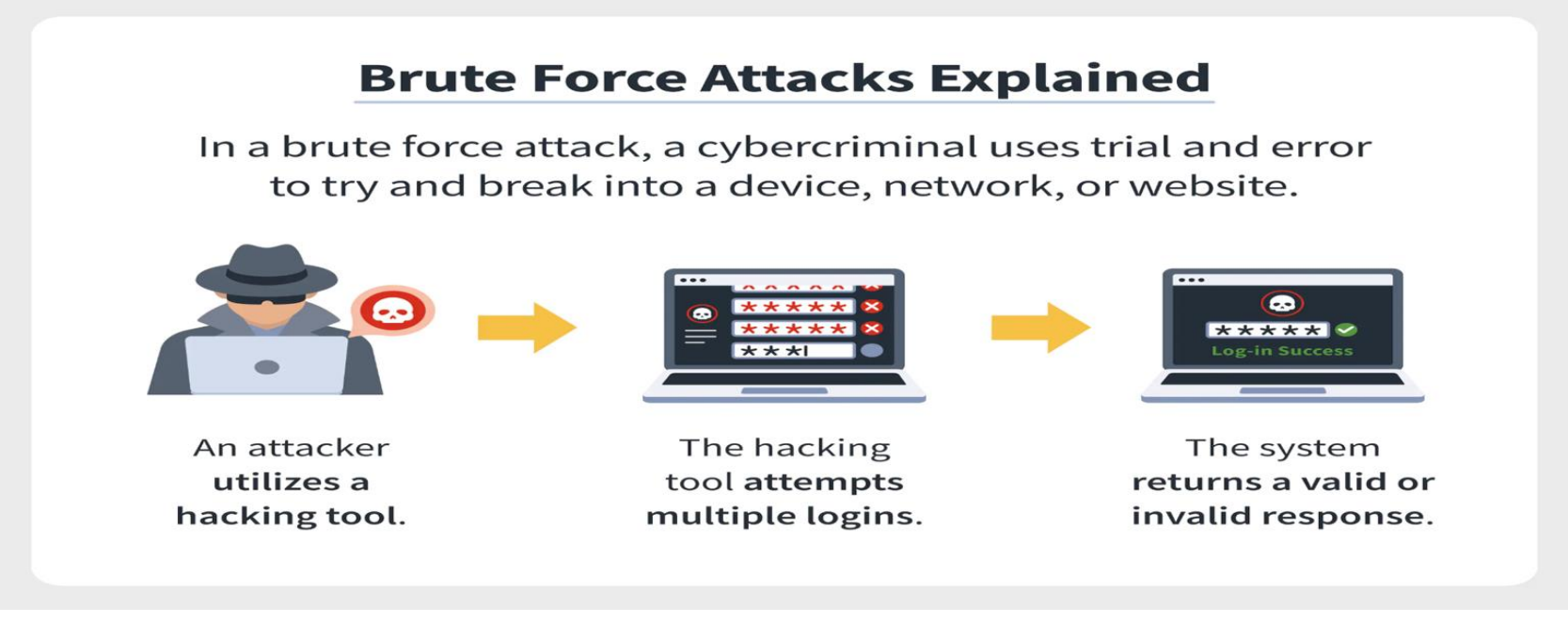
4. Distributed denial of service (DDoS)

- Requests come from several IP addresses that can make the system unusable.
- Overload their servers, slowing down significantly or temporarily taking them offline, or preventing an organization from carrying out its vital function



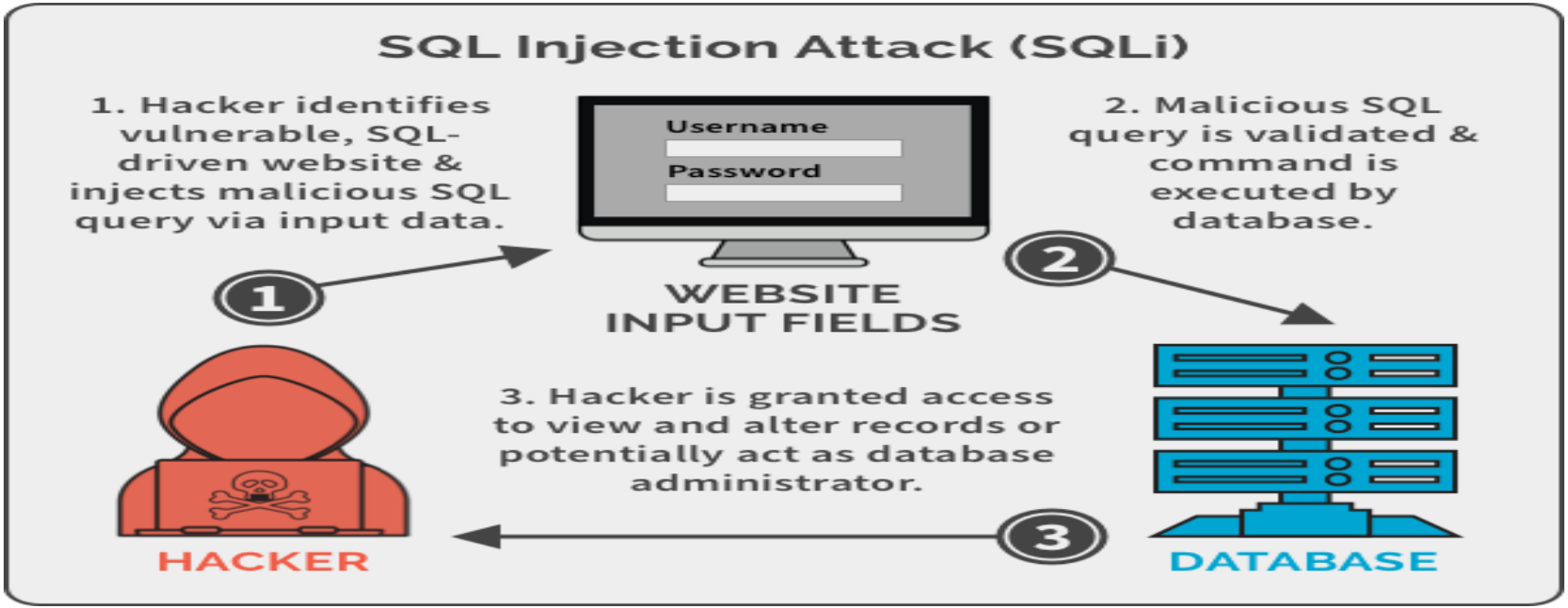
5. Brute Force

- trial-and-error method to guess all possible combinations until the correct information is discovered.
- Cybercriminals use this attack to obtain personal information about targeted passwords, login info, encryption keys, and Personal Identification Numbers (PINS).



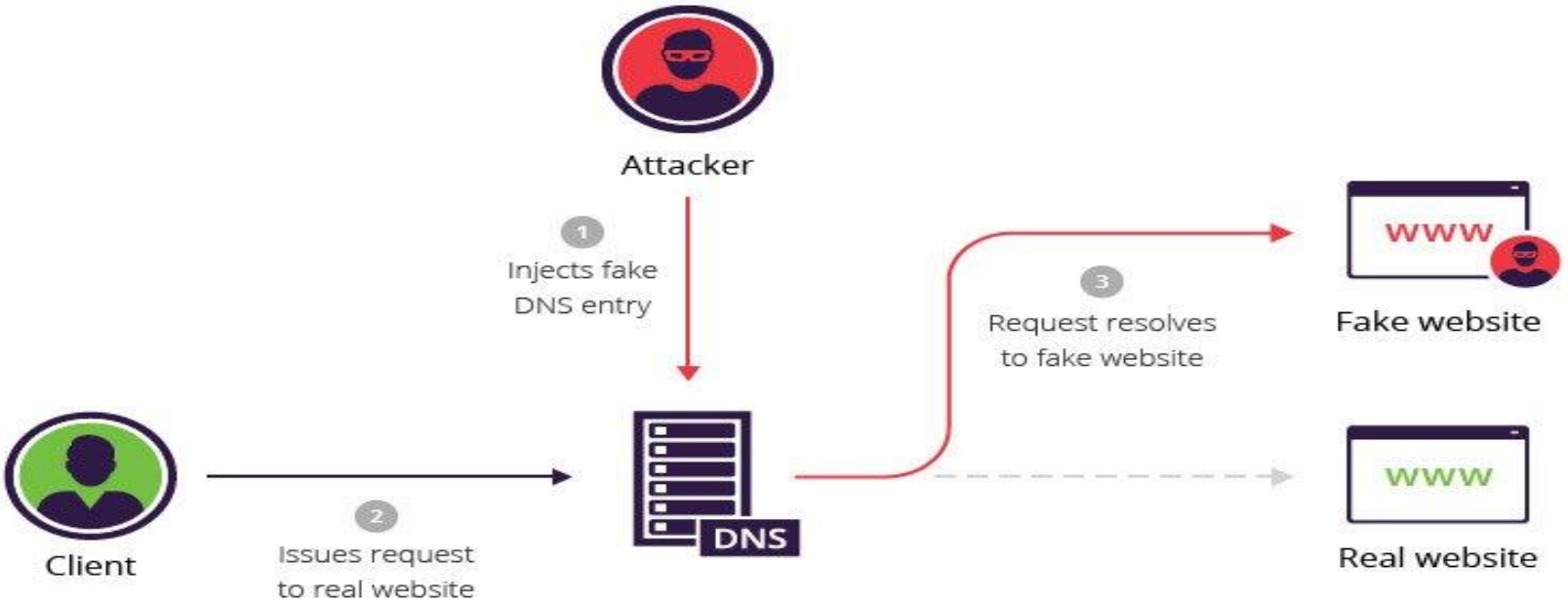
6. SQL Injection attack

- Cybercriminals use malicious SQL scripts for backend database manipulation to access sensitive information.
- Can view, change, or delete sensitive company data, user lists, or private customer details stored in the SQL database.



7. Domain Name System (DNS) attack

Cyber criminals take advantage of flaws in the Domain Name System to redirect site users to malicious websites (DNS hijacking) and steal data from affected computers.



Latest cyber threats

- Romance Scams:
  - U.S. government in February 2020.
  - Dating sites, chat rooms, and apps.
  - Dupe them to give away personal data.

- Dridex Malware:
  - U.S. in December 2019 - Financial Trojan malware
  - Phishing emails or existing malware to steal sensitive information for fraudulent transactions.
  - Devices are to be patched, anti-virus is turned on and up to date, and files are backed up to protect sensitive data.

- Emotet Malware:
  - Australian Cyber Security Centre identified this global cyber threat in 2019.
  - Seals sensitive data and also installs other malware on our device.

What about INDIA?

- Japan , Australia , India - Top 3 - The Internet Crime Report by the FBI
  - 20% -Access attacks
  - 11% - Ransomware (3.38million -2021)
  - 10% - Data Theft
  - 9% - Remote Access Trojans & Adware
  - 7% - Brute Force
  - 7% - Stolen Credentials

- Researchers from IBM's X-Force Threat Intelligence team
  - "Asian organisations are adept at identifying attacks quickly before they escalate into more concerning attack types."

Some Statistics

Govt.Data presented in Parliament	2020	1.16millioncases reported	Avg. is 3,137 cyber security issues
IBM - Data Breach Report	2020	Avg. cost of data breach - $2 million	9.4% increase from 2019
Inc42 - Indian media and information platform	After Covid-19 in India	4000% increase - phishing emails	400% spike in Policy Violations
Inc42 - Indian media and information platform	After Covid-19 in India	66% of Organisations - at least one data breach	Because of shifting to remote working model in Pandemic

Types of Cyber Attacks

Web based Attacks	System Based Attacks
Occur on a website or web applications	Intended to compromise a computer or a computer network
Injection Attacks	Virus
DNS Spoofing	Worm
Session Hijacking	Trojan horse
Phishing, BruteForce, Dictionary Attack	Backdoors
Denial of Service, Man in the Middle Attack	Bots

Cyber Criminals

Who are these Cyber criminals?

- **Hackers: Attention seekers**
  - Script kiddies
  - Scammers
  - Hacker groups
    - Black Hat/White Hat/ Grey Hat

Crackers(Outsiders): Non attention seekers

- Phishers
- Hacktivists
- Advanced Persistent Threat (APT) Agents or State-sponsored Attacker

Crackers(Insiders): Non attention seekers

- Employees
  - They may only be 20% of the threat, but they produce 80% of the damage.
  - considered to be the highest risk.
  - To make matters worse, they often reside within an organization.
  - Malicious/Accidental/Negligent

As G.I. Joe says, “Now you know, and knowing is half the battle!”

Cyber Criminals- Source /Target?

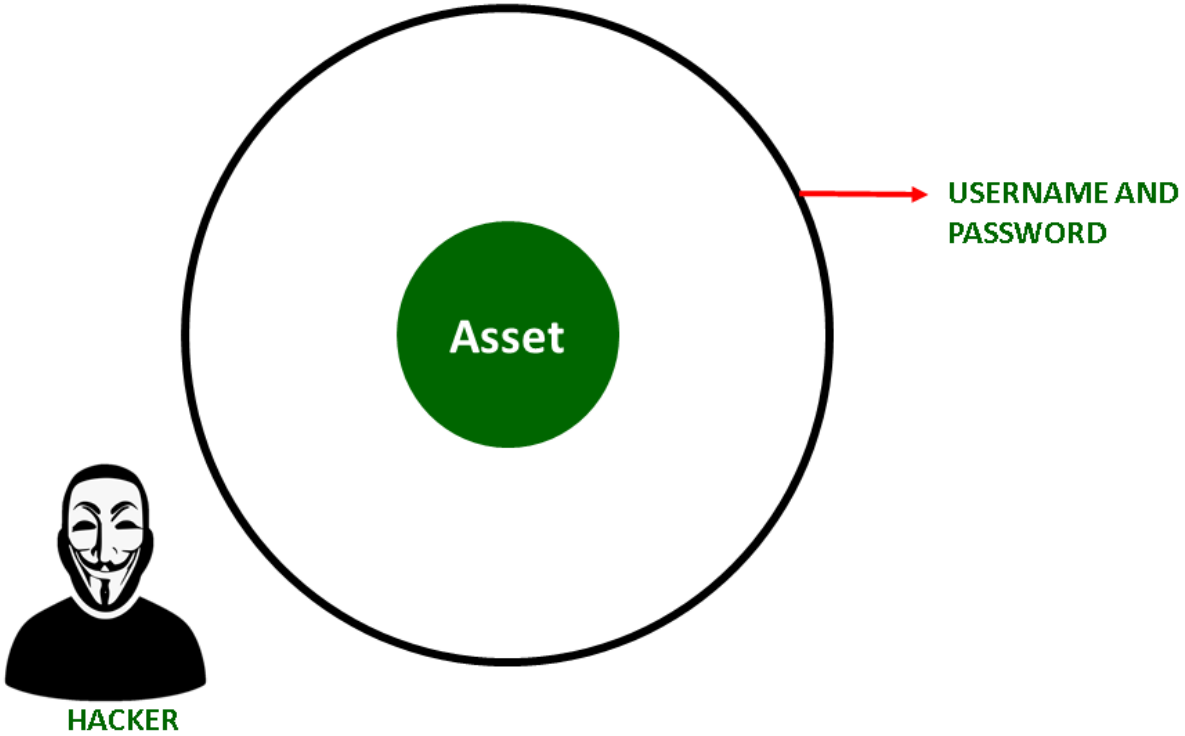
- Select computer as their target-
  - They attack other people's computers to do cybercrime, such as spreading viruses, data theft, identity theft, etc.
- Uses the computer as their weapon-
  - They use the computer to do conventional crime such as spam, fraud, illegal gambling, etc.
- Uses the computer as their accessory-
  - They use the computer to steal data illegally.

Cyber Security Solutions

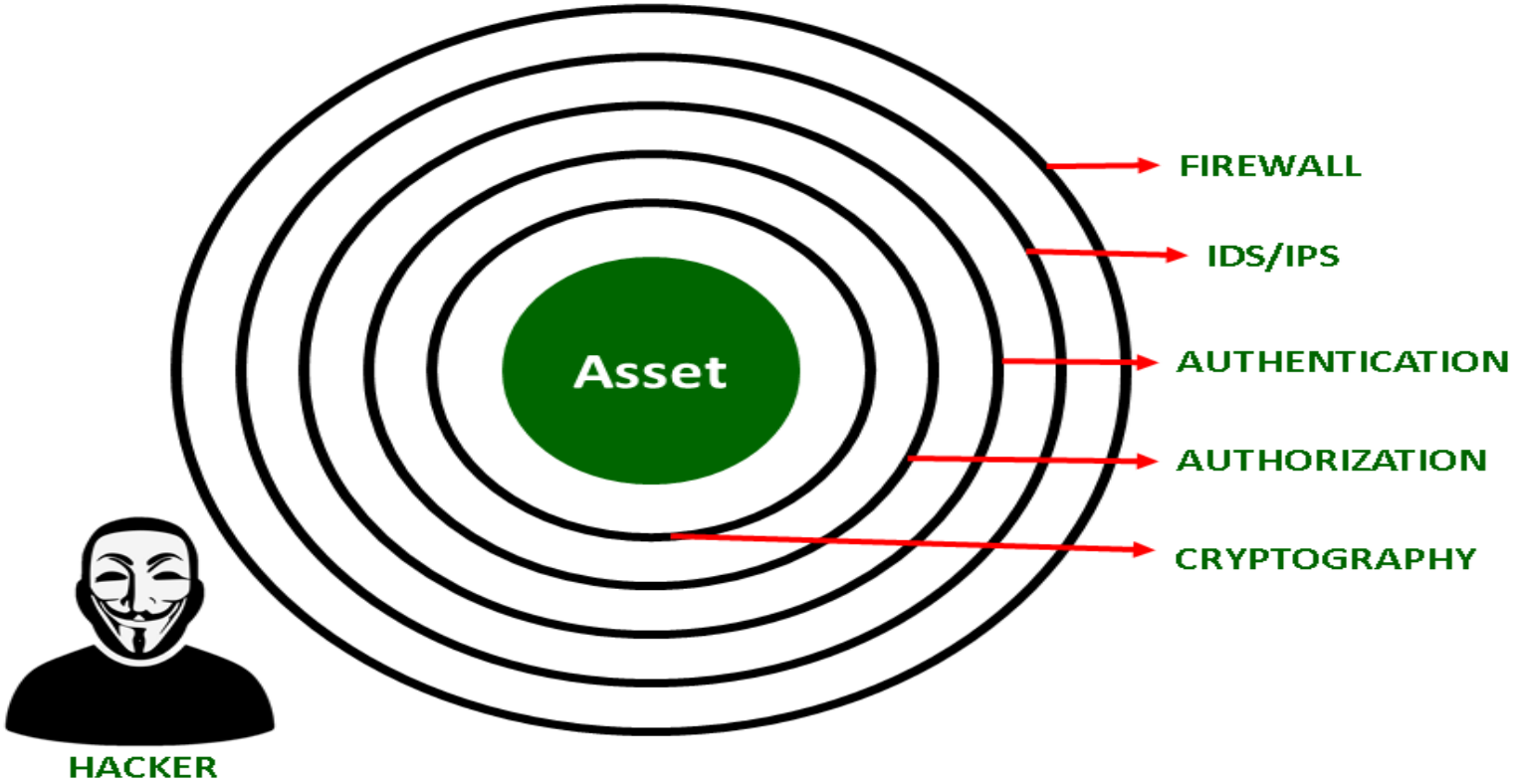
What’s the Defence Mechanism

- Fencing Approach
- Layered approach

LOLLIPOP MODEL

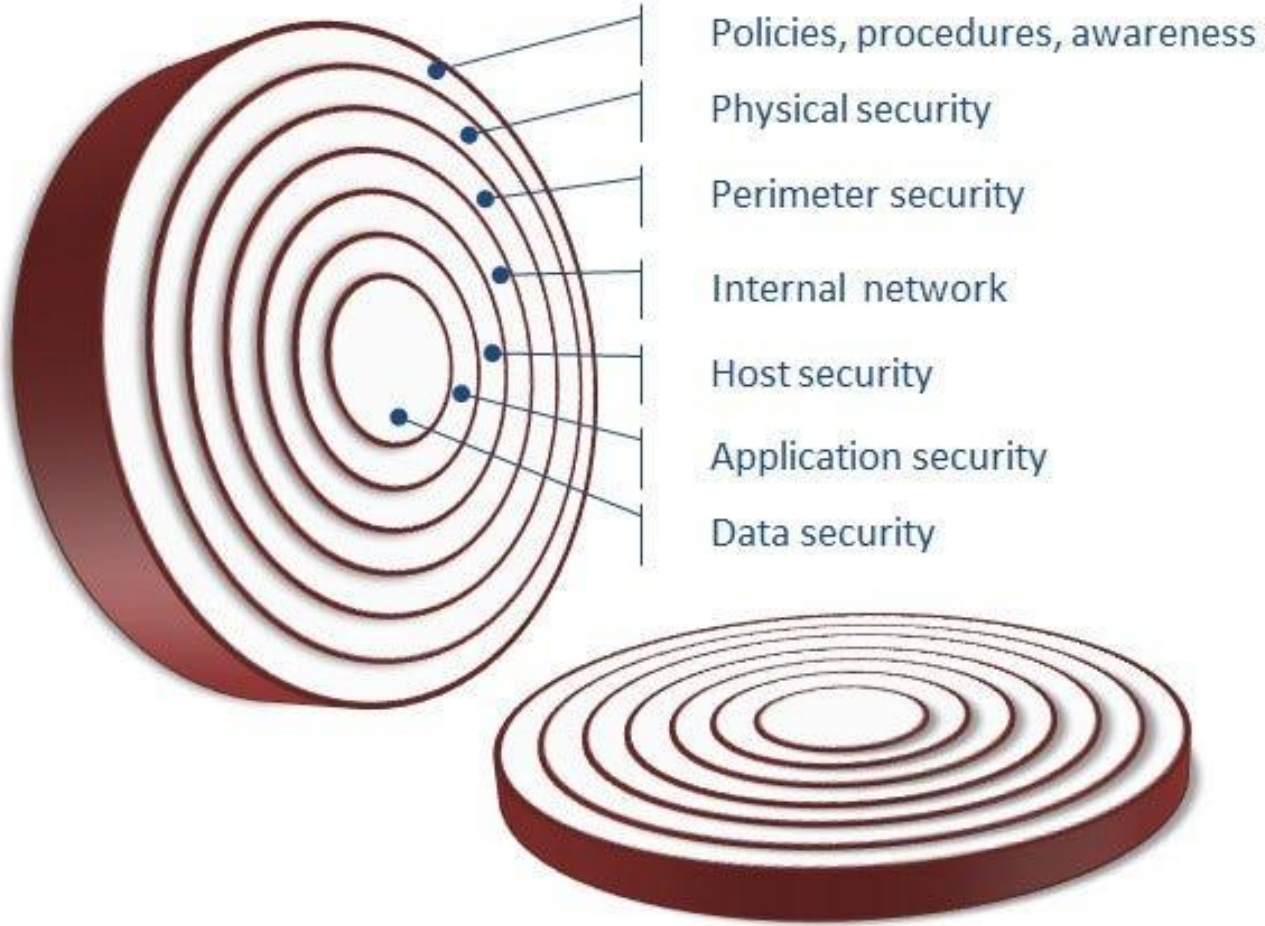


ONION MODEL


Asset
FIREWALL
IDS/IPS
AUTHENTICATION
AUTHORIZATION
CRYPTOGRAPHY
HACKER

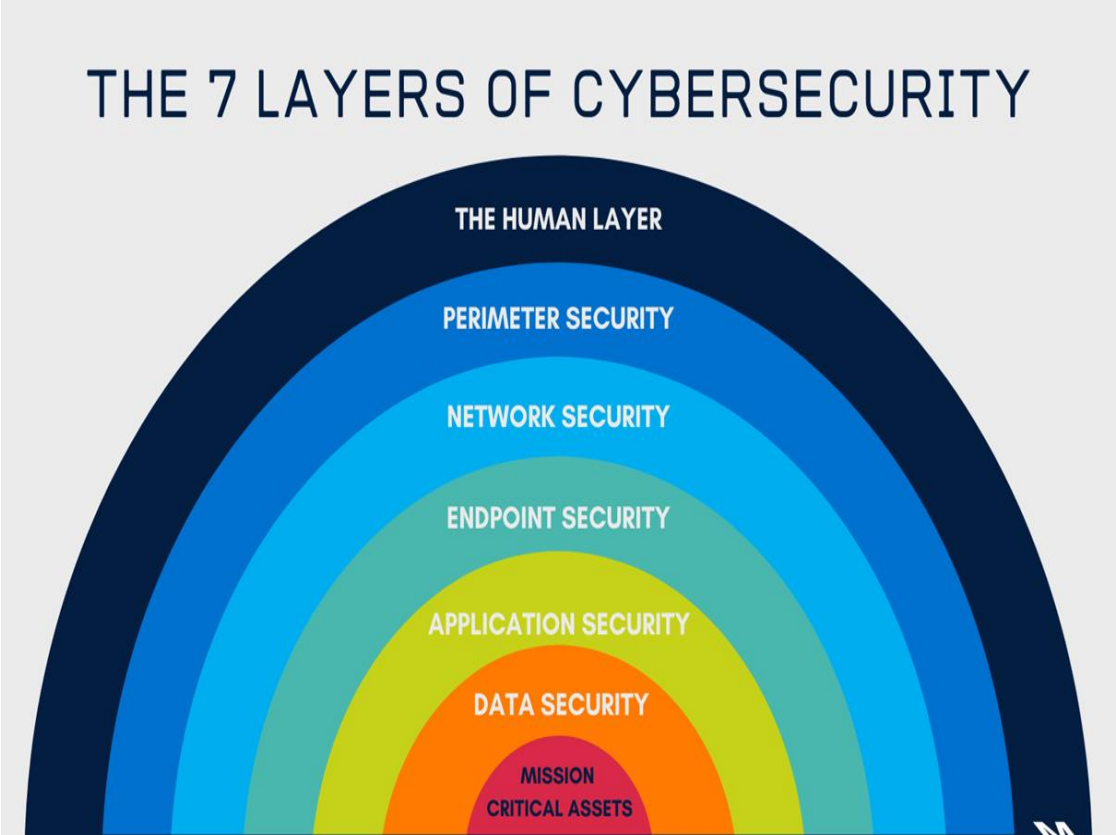
Authentication and Authorization

- Authentication is the means of verifying who a person is.
- Authorization determines what they’re allowed to do.
    - Authorized users get access to the appropriate computing resources


Policies, procedures, awareness
Physical security
Perimeter security
Internal network
Host security
Application security
Data security

Seven layers of Cyber Security

1. Mission Critical Assets
2. Data Security
3. Application Security
4. Endpoint Security
5. Network Security
6. Perimeter Security
7. The Human Layer



Layers of Cyber Security

- **Network Security:**
  - Secure a computer network from unauthorized access, intruders, attacks, disruption, and misuse.
- **Application Security:**
  - Protects software and devices from unwanted threats.
  - constantly update the apps to ensure they are secure from attacks.
- **Information or Data Security:**
  - mechanism to maintain the integrity and privacy of data, both in storage and in transit.
- **Identity management:**
  - Determines the level of access that each individual has within an organization.
- **Operational Security:**
  - processing and making decisions on handling and securing data assets.
- **Mobile Security:**
  - securing the organizational and personal data stored on mobile devices

- **Cloud Security:**
  - protects the information stored in the digital environment or cloud architectures.
  - Use cloud service providers such as AWS, Azure, Google, etc.

- **Disaster Recovery and Business Continuity Planning:**
  - Processes, monitoring, alerts, and plans to how an organization responds when any malicious activity happens.
  - Resuming the lost operations to the same operating capacity as before the event.

- **User Education:**

Data Security Consideration

- **Backups**

  Use the Backup 3-2-1 Rule.

  3 copies of our data

  2 different formats, i.e., hard drive+tape backup or DVD (short term)+flash drive

  1 off-site backup, i.e., have two physical backups and one in the cloud

- **Data Archives**

  protect the older information that is not needed in day to day operations but may have to be accessed occasionally.

  Online, offline, or cloud storage

Other Security Considerations

- Firewall
- VPNs
- Intrusion Detection System (IDS)
- Access Control

Cyber Safety Tips

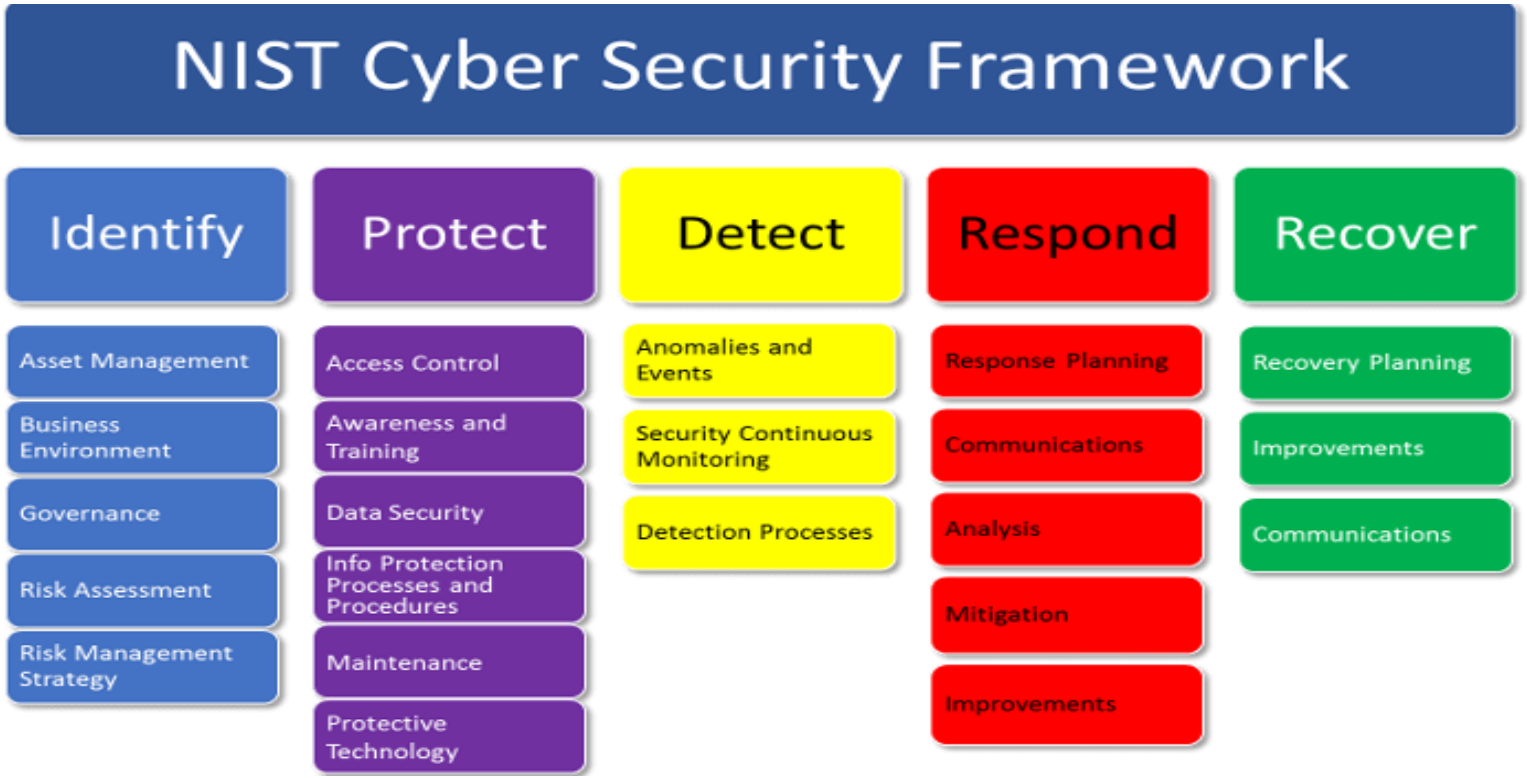
- **Conduct Cybersecurity training and awareness:** on cybersecurity, company policies, and incident reporting
- **Update software and operating system**: update the software and O.S. for latest security patches.
- **Use anti-virus software:** detect and removes unwanted threats from your device.
- **Perform periodic security reviews:** To identify security risks early in a secure environment.

- **Use strong passwords**: recommend to always use long and various combinations of characters and symbols
- **Do not open email attachments from unknown senders**: Because it could be infected with malware.
- **Avoid using unsecured Wi-Fi networks in public places**: they can leave you vulnerable to MIM attacks.
- **Backup data:** Every organization must periodically take backup of their data to ensure all sensitive data is not lost or recovered after a security breach.

Steps to follow

- Perform Basic Discovery
- Test, Analyze, And Repeat
- Assess Your Security Program And Compliance
- Strategically Build In Remediation And Controls
- And Yet – Prepare To Be Attacked

Cyber Security Framework



https://www.youtube.com/watch?v=J9ToNuwmyF0

Benefits of cybersecurity

- Cyberattacks and data breach protection for businesses.
- Data and network security are both protected.
- Unauthorized user access is avoided.
- After a breach, there is a faster recovery time.
- End-user and endpoint device protection.
- Regulatory adherence.
- Continuity of operations.
- Developers, partners, consumers, stakeholders, and workers have more faith in the company's reputation and trust.

Cybersecurity and Compliance – Secure Operations Map

Organization	Awareness	Security Governance	Risk Management	
Process	Regulatory Process Compliance	Data Privacy and Protection	Audit and Fraud Management	
Application	User & Identity Management	Authentication and Single Sign-On	Roles and Authorizations	Custom Code Security
System	Security Hardening	Secure SAP Code	Security Monitoring and Forensics	
Environment	Network Security	Operating System and Database Security	Client Security	

Blockchains in Cyber Security

Blockchains Defined

- Blockchain is a shared, immutable ledger for recording transactions, tracking assets and building trust.
- Shri Ravi Shankar Prasad, Hon'ble Union Minister of Law & Justice, Communications, Electronics and Information Technology (MeitY), inaugurated the Centre of Excellence in Blockchain Technology at Bengaluru, Karnataka on 18th January 2020.
- BCT will open new frontiers
  - governance, treasury management, excise operations etc.
  - like to see its use in the field - agriculture, health and primary education.

The Properties of Distributed Ledger Technology (DLT)

Programmable
A blockchain is programmable (i.e. Smart Contracts)

Distributed
All network participants have a copy of the ledger for complete transparency

Secure
All records are individually encrypted

Immutable
Any validated records are irreversible and cannot be changed

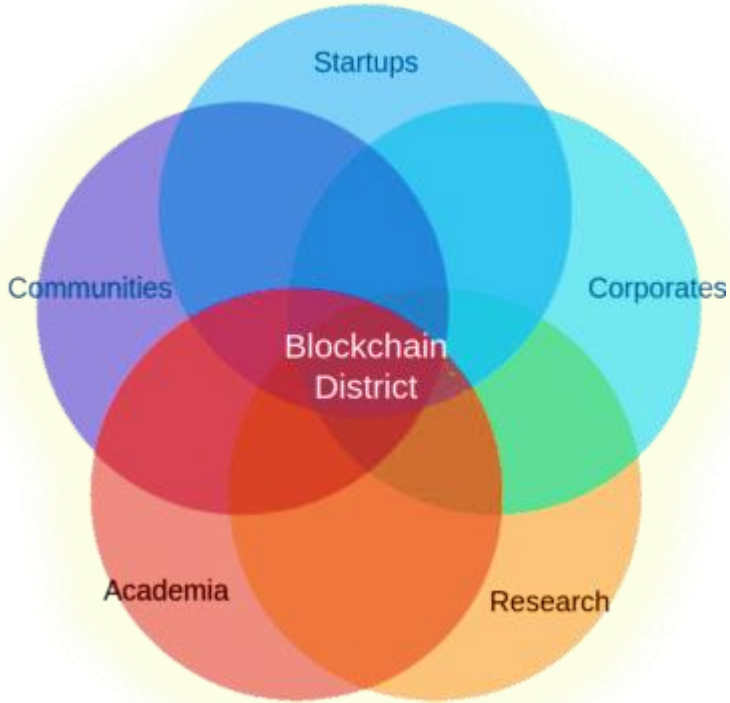
Anonymous
The identity of participants is either anonymous or pseudonymous

Unanimous
All network participants agree to the validity of

Time-stamped
A transaction timestamp is recorded on a block

Usecases - Blockchain District

- Government of Telangana - Centre of Excellence
- to promote the use of Blockchain technology in the state
- **Dharani,** an integrated land record management system.
- Telangana State Council of Higher Education (TSCHE) is initiating a pilot project to secure 10th and 12th-grade certificates issued to the students by the State.
- LegitDoc, a blockchain, is helping the Government of Maharashtra to issue 1 million tamper-proof diploma certificates



- MeitY has recommended the formation of a National Blockchain Framework
  - health, agriculture, education, and finance.

- “geographically distributed national-level shared infrastructure" is needed to “enable citizen services at large scale and enable cross-domain application development".

- “create trusted digital platforms through shared blockchain infrastructure"

Is Blockchain the future of Cyber Security?

- YES

- But, its not a silver bullet

Security is a Myth

THANK YOU

rukmarekha@uohyd.ac.in