master@notes
by
Shubham Kumar Gond

* What is Cyber Security?

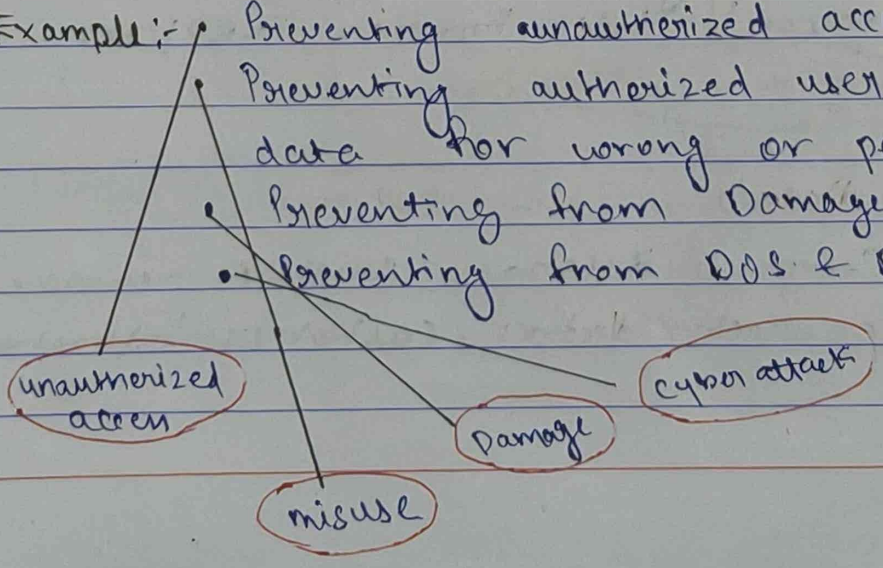
Ans:- Cyber Security is the process or practice of protecting Computers, networks, Server, application, data and all types of digital device from unauthorized access, damage misuse and cyberattack (attack by hacker)

- Cybersecurity is the defense system of digital world that protect individual, Buiness, government and industry from cyberattack.

→ Goals/importance of cybersecurity :-

- Reduce the risk of cyber-attack
- maintain the CIA (Confidentiality, Integrity, Availability) Triad.
- Protect organization and individual from intentional and unintentional exploitation of system, network, Server and technologies

Example:-
- Preventing unauthorized access to a banking system.
- Preventing authorized user uses the system or data for wrong or personal purpose.
- Preventing from Damage data (Delete, Corrupt, encrypt)
- Preventing from DOS & DDOS attack.



⊙ In Cyber security involves the implemention of PPT :-

People → Process → technology

• People :-
USER, EMPLOYEE, SECURITY PROFESSIONAL, SOC ANALYST
(right people with right skills and awarness)

• Process :-
SECURITY MANAGEMENT, INCIDENT RESPONSE, POLICY
(Systematic steps and rules that ensure security)

• technology :-
FIREWALL, IDS/IPS, EDR, VPN, PROXY, SIEM
(Security tools that support people and process)

* Cyber Security covers multiple domain such as :-

1. Network Security :- (Network devices)
Routers, Switches, firewall IDS/IPS, VPN server, Network Hub etc.

2. Application Security :- (Apps, web app)
Banking App, E-Commerce website, mobile app (like paytm, Amazon), web browser, ERP/CPM Software, API services

3. Information Security :- (Data)
Company database, employee records, financial documents, research data, customer information, Back up drives

4. Cloud security :- (online store)

Google drive, AWS (Amazon web services), microsoft Azure, Dropbox, cloud email (like outlook 365), virtual machine on cloud.

5. Endpoint security :- (Endpoint System)

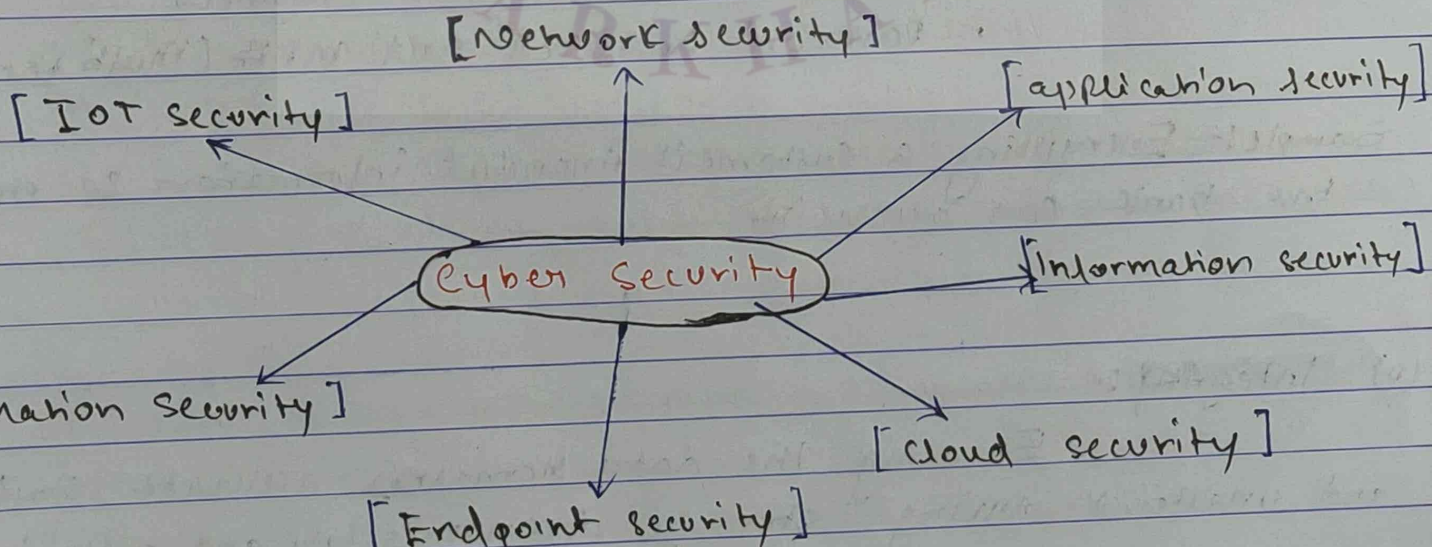
Laptop, Desktop PC, smartphone USB drive, Printers (network-connected)

6. Operations Security (OPSec) :- (Internal control)

user account, Access logs, admin dashboard, Data centerss, Back servers, Incident oresponce, file permission managment, Audit trails

7. IOT Security :- (Smart device)

Smartwatch, IP CCTV camera, Smart Door lock, Smart light/AC, Home assistant (Alexa), Smart refrigerator, washingmachine etc.



* CIA - TRIAD :-

The foundational model of cyber security consist three key principle :-

(1) Confidentiality (Protected) (2) Integrity (Reliable) (3) Availability (Accessible)

→ Three pillars holding up cyber security.

(1) Key principles :- (CIA)

(a) Confidentiality :-

Protecting sensitive information from unauthorized access, disclosser, exposure

goal :- Only authorized user can accss the data : other should be denied & restricted

How it's achived :

- Data Encryption (AES, RSA, SSL/TLS)
- Access control & Authentication
- use of VPN and secure channels
- Password Protected and MFA (Multi Factor Auth)

Example :- Encrypting a customer's financial information so only the bank can accss it.

(b) Integrity :-

Ensuring the data remains accurate, consistent and unaltered during storage, transmission and processing.

goal :

goal :- To prevent unauthorized modification or deletion of data.

- How it's Achieved :
  - Hashing algorithm (SHA, MD5 for validation)
  - Digital signatures
  - checksums and Hash verification
  - file permission & monitoring

Example: when a sending a file, hashing ensures that the file recieved is exactly same.

(c) Availability :

Ensuring the data & resources are accessible for authorized users whenever needed.

goal :- To maintain continous operation without interruption.

How it's achieved :

- Backup & Disaster recovery
- Load balancer & redudancy
- DDOS protection
- Regular maintainance & patch update
- High availability system (failover clusters)

Ex :- An online banking website must be available 24x7 for customer accers.

- If Amazon/flipkart are not available for some times then big business loss.

* **Extended Security Goals** : (CIA+)

Besides the primary CIA Triade, modern Cybersecurity adds three extended goal to ensure the complete protection and trustworthiness of information system.

(i) Authenticity (ii) Accountability (iii) non-repudation

(a) **Authenticity** : (Ensuring Genuine ; Verification)
Ensure the data, communication and user identities are genuine and not forged.

Keypoint :- verify the senders or source information is real

Ex :- Username & password verification, Digital certificate (SSL/TLS), OTP (one time password), biometric authentication

Tool & techniques use :- Digital signature, certificate & Encryption, Authentication protocol (Kerbos, radius etc)

(b) **Accountability** :- (User responsibility + traceability)
Ensures that every user's actions are recorded and traceable so that individuals can be held responsible for their activities.

Keypoints :
- Track user activity within system
- Support incident investigation and awaiting

Ex :- Audit logs showing "who did what and when"

Tools and techniques we :-

log monitoring system (SIEM)
Audit trails & activity reports
user access control list (ACL)

(c) Non-repudiation :- (can't deny action, proof of action)

Ensures that a sender or user cannot deny the authenticity of their performed action or sent message.
(user can't deny their performed operations)

Keypoint :-

- Provides undeniable proof of origin and delivery
- maintains trust in digital communication
- Support legal evidence in disputes.

Ex :- Digitally signed emails or documents
Blockchain transaction records

Tool & techniques :-

- Cryptographic hash function
- Digital signature
- Secure timestamping services

Authenticity (A)	identity verification	user/data is genuine
Accountability (A)	Activity tracking	Every action is recorded and traceable
Non-repudiation (N)	Proof of action	user can't deny their performed operations

* Threat :-

It is any potential/possibility/future danger/cause or event that can harm a system, network or data

- Threat expdoit the vulnerability in the system., resulting damage the CIA Toiad

Threat can be deliberate (hacker or malware) or accidental (user mis

- Based origin threat :-

(a) External threat (outside the organization
(b) Internal threat (employees, contractor)

→ External threat :-

It orginate outside the organization and target public facing or network assets using attack vectors.

(1) Malware :- malacious software (virsus, trogans, ransomware, rootkits, Keylogger, spyware etc) delivered from outside via emails, web downloads, or infected devices

(2) Phising & social engineering : trick the user/empdoyee into revealing sensitive data via phising email.

(3) Denial-of-service (DOS/DDOS) Attacks :- (traffic/packet send huge) Attackers outside the network flood system or application with traffic for disruption.

(4) Man-in-the-middle (MitM) attack :-

External attack intercept or altered communication between parties (perform. Snifling & Spoffing)

(5) SQL/NOSQL injection :-
Outsider(hacker) inject malicious code into database.

(6) Password attack :-
External hacker attempt to crack or steal password through various means.

(7) Drive-by-download :-
malware install from external malicious websites, pop-ups.

(8) Zero-day Exploits:
hacker exploit the vulnerability which unknown by the vendor and organization.

(9) Session Hijacking :-
hacker can take control of legitmate sessions between user and servers.

(10) Supply chain attack :-
Compromise of external vendors or partners leading to risk for primary target organization.

(11) Cloud attack :- Exploit vulnerability in cloud platforms or misconfiguration

(12) IOT/mobile threats :- Targeting weakness in connected device to the network.

→ Internal threats :-

It originate within the organization and involve with legitmate or unauthorized accss to systems, data, or network assests.

(i) malicious insiders :- Employee or contractor misuse the access privileges, leak data for personal & financial gain,

(ii) Accidental insider activities :- Employee unintentionaly cause data breach, system compromise by negligance or lack of training (e.g. clicking malicious link, misconfiguring sys)

(iii) Malware deployment :- Sometimes insiders knowingly or unknowingly introduce malware into internal systems (eg via infected USB device/drive, go malacious website)

(iv) Policy violation :-

Internal actor bypass security controls, like disable antivirus software, or engage with unauthorized activities.

* Vulnerability :-

A vulnerability is a weakness or flaw in system, process and human behaviour, that can be exploit by a threat actor to gain onauthorized accss or cause harm

- Vulnerability are the entry points that allow threat to succed. they can exists in software code, system configuration, security policy and user activities.

→ Types of vulnerabilities :-

1. technical vulnerabilities :-
Software bugs, coding errors, unpatched system, outdated application, or weak encryption

2. Configuration vulnerabilities :-
Misconfigured firewalls, open ports default passwords, insecure permission that expose systems unnecessarily.

3. Human Vulnerability :-
Social engineering susceptibility, weak password or poor awarness among employees.

4. process Vulnerability :-
weak policies, poor incident respon plans, or lack of access control managment.

5. Physical vulnerability :-
Insecure data centers, lack of cctv unprocted hardware, or missing environental safeguards.

Ex :- If a web-application runs outdated software with a known sql injection flaw, the flaw represent a vulnerability. A hacker (threat) could exploit the weap steal and modify the database information.

[threat is the potential danger that can exploit a weakness]
[An attack is the actual taken to exploit that weakness]

* Risk :-

Cybersecurity risk is the potential impact (loss or damage) when a threat exploits the vulnerability successfully in a system, network, assets and process.

Risk = threat x vulnerability x impact

[Risk=0] ⇒ If factor is zero

Key terms in risk :-

- Impact :- Consequence of successful attack (e.g data breaches, downtime)
- threat :- Anything that can cause harm to assets.
- vulnerability :- weakness or flaw in system, assets, process, human,
- likelihood :- Probability or chance than threat exploit successfully

→ Types of risk :- Risk classified on nature, source, impact

* Based on source :-

- Internal risk :- (employee, system, policies)
  risk comes from within the organization
  (insider threat, human error, policy violation)

External risk :- (hacker, competitors, natural disasters)
outside the organization (e.g DDOS attack)
ransomware, data theft.)

#Based on nature :-

(I) Strategic risk :-

risk from poor wrong business or technology decision that affecting security.

Ex:- • Adopting new technology without security check.
• failing to invest in cybersecurity tool
• choose cloud vendor with poor security compliance.

(II) operational risk :-

Risk comes from internal process, System misconfiguration and human error.

Ex :- misconfigure firewall, poor patch managment, poor time respon

(III) Compliance risk :-

risk comes when organization fail to Comply with law, regulation and standards (like GDPR, HIPAA, ISO 27001)

Ex- leaking customer data → GDPR violation → heavy fines

(IV) technical risk :-

risk comes from hardware, software or network architecture failure.

Ex.- outdated hardware crash under load, weak encryption.

(V) Financial risk :-

Direct or indirect financial loss due to cyberattacks, damage.

Ex- ransomware payment, data loss, downtime, loss of customers. (fine)

Defence:- Cyber insurance, incident response planning, backup strategy.

- Reputational risk :-
  risk from when loss of trust or brand (goodwill) image after security breach.

Ex:- Public exposure of customer data - media backlash - Drop in sales

Based on ~~double~~ likelihood and impact :-

- likelihood :- The probability or chance that a cyber threat will actual occur

Ex:- Very likely, possible, unlikely [very likely - unpatched system]

- Impact :- damage or loss if threat become real.
  Ex:- Severe impact, moderate impact, low impact.
  [weak passwords - moderate impact]

[if chance high then loss or damage high : likelihood ↑ impact ↑]

* Risk Assessment process :-
  A systematic method to identify, analyze and prioritize risk to system, data and network to guide security decisions.

→ Helps to allocate resource effectively and prevent

key steps :-

(a) Identify risks :- list of potential threat & vulnerability
Tools - vulnerability scanned.

e.g> finding/spotting weakness or flaw in system, network, policy.

(b) Analyze risks :- Evaluate the likelihood or impact of each risk.
Assign scores or use qualitative method (1-5 for likelihood & 1-10 for impact)

e.g> A DDOS attack is likely (4/5) and has impact (8/10)

(c) prioritize risks :-
rank risks on the based of analysis to focus on the most critical ones.

e.g> Prioritizing zero day exploit over a major config mismatch,

(d) mitigate Risk :- Develop and implement plans to reduce risk as well as eliminate the risk

e.g> Apply the patch, train users, add more security firewall, updating software, replace technology tool which outdated.

Assessment process ⇒ Identify → Analyze → prioritize → ~~mitigate~~

* Risk managment :-

The proiess of identifying, assessing and reducing risks to protect systems, data and networks from threat and vulnerabilities.

risk managment = Assessment + mitigate + check (action)

Assessment is analysis phase; managment is the full proiess to analyze, mitigate and check.

Risk managment steps :-

[Identify risks]

↓

[Analyze risks]

↓

[prioritize & evaluate risks]

↓

[mitigate risks]

↓

[check & monitor & review risks]

Continous track & check risks and update the plan as new plan-(threat emerge)

Monitor tool :- SIEM tool, logi checker

* What is hacker?

Any individual or group who use their skills and exploit/hack the computer system, network, application and digital devices. (Target)

"hacker" is neutral terms become good and bad depending on the intent, authorization, legal/ethical boundaries.
(motives)

(a) White hat hacker :- Ethical hacker who test system, network, application with permission to improve security.
→ protect organization, earn a living.

(b) black hat hacker :- Malicious hacker who hack the targeted system without permission for personal gain & financial gain

(c) Grey Hat hacker :- Hacker who hack the targeted system without permission but sometimes report issues.
e.g> individual who curious or seeking reward not always malicious

(d) Script Kiddies :- Amateur hacker using pre-written tools without deep knowledge.
e.g> motives :- fun, fame, or minor disruption.

(e) Hacktivists :- Hacker who targeted the system to promote a social or political cause
e.g> protest, awareness,

(f) State-sponsored Hackers :- Hackers hacked the target system for governments support about espionage or cyber warfare.

Espionage :- It means the act of secretly collecting confidential or sensitive data from organization, government or individual.

(g) Insider Malicious :- insider hacker, intentially steals or leaks the dates by employee, partners and contractors.

(h) Green hacker :- Inexperienced learners, not attacks - Curious to learn hacking.

(i) Blue hackers :- hackers hack the target for revenge who not part of Blue team.

(1) Red team :- (offensive team)
offensive security Experts (Ethical hackers) who simulate real cyberattack to find vulnerabilities.

→ Ethical hacker, penetration tester find the vulnerabilities in specific system and app & fix it, but otherhand
Redteamers simulates real cyber-attack (end to end) testing people, process and technology.

(2) Blue team :- Defensive team, Defenders
this team monitors, detects and responds to attacks in real time
(protects organization digital assets from real hacker)

(3) Purple team :- Hybrid team that combines red & Blue team efforts for collaborative defense.
> Red team testing, Blue team responding and purple team aligns strategic.

(4) Orange team :- managment or oversight team the plan & evaluate security exercise

e.g>
overseeing a red/Blue drill and assessing results.

(5) Yellow team :- neutral team that referense exercise & enforce rules.

e.g>
Seting boundaries for a Red/Blue team drill.

(Compromise the

Attack Vectors :-

An attack vectors is the method or path used by threat to gain credential and unauthorized access to a system, network, application and data.

In simple word, which path or method use that attack happend. (performed)

- Importance of attack vectors to know :- Identify the likely attacker vectors allow defenders to prioritize controls.
  identify → protect → fix vulnerability

→ Categories of attack vectors :- (initial phase)

Attack vectors can be grouped by the medium or technique used.

(1) Networks-based vectors : (remote networking protocol, open ports.)
eg RDP/SSH

(2) Application-based vectors : (web applications bugs, logic error, insecure design in web, mobile, desktop app)

(3) Social engineering vectors : (Phising, spear phising, vishing)
e.g. email phising

(4) Physical vectors : (device theft, USB insertion, hardware keyloggers)

(5) Supply-chain vectors : (Exploits third party software, hardware, services)

(6) Configuration & process vectors : (misconfiguration, weak policy)

(7) Cloud & virtualization vectors : (misconfigured cloud storage, insecure APIs)

(8) Wireless & IOT vectors : (wifi, IOT protocol, unpatched software)

(g) Drive by downloads & browser based vectors :- (user visit malicious website and malware download automatically)

(h) AI specific & AI Enhanced attack vectors :-

Attack target the AI/ML system by prompt injection, data poisoning and model extraction.

Note :- An attack is a chain of phases, Brute force attack may give initial access or later escalate accounts. malware can be dropper (initial access), back door (persistence) or ransomware (impact phase).

→ Commonly attack techniques used by attackers :-

(a) Phising :-

Deceptive email or message trick users into revealing credential or click malicious link or malware installation.

(b) Ransomware attack :- (impact phase attack)

Malicious software encrypts victim's data and demand ransom (money). Sometimes delivered by phising or exploit.

(c) Brute force attack :- Attacker use the multiple username & password for try again & again until correctly guessing (to gain unauthorized access to user account & network.

(d) DOS/DDOS Attack :- flooding network or ~~traffic~~ services with traffic to cause outages, overload the system and network (huge no. packet send to target)

(e) Man in the middle (MitM) attack :- sniffing, spoofing

Intercepting and may be modification communication between two parties to steal data or impersonate users.

(f) SQL injection :-

Inject the malicious SQL queries into the input area to manipulate the database (read, modify or execute)

(g) Cross-site scripting :-

Attack inject the malicious script (code) Java at client side into trusted website to make pages viewed by others user. (enabling code execution in victims' browser.)

(h) Insider attack :-

malicious or accidental intent attacks by the internal people (employee, association) with access to systems.

(i) Zero-day attack :-

threat exploit the vulnerability which unknown by the developers & vendors or unpatched software by developer & vendor.

(j) Supply-chain attack & third party attack :-

Attacker attacks that those system which less-secure in the supply chain. e.g. Software updates, Hardware implants.

famous attack :- • (Morris worm) (1988) - Type - worm
impact - 10% of internet computer crash.
• (Wanna Cry ransomware) (2017) - Type (wormable, SMB exploit)
affected 2.3m computers across 150+ Countries.

* Malware :- (malicious code/script)

Malicious software designed to harm, exploit or gain unauthorized access to computer system, networks or data.

Purpose :- disruption, theft, espionage, persistence, monetization, ransomware, - cryptomining, ad-fraud).

* Classification by Intent, Behaviour, visibility

- Intent: Disruption, Destruction, Espionage, financial gain, steal data.
- Behaviour: Infectious (self-replicating) vs non-infectious
- visibility: persistence (resident) vs fileless/in-memory.

→ Types of malware :-

(1) Virus : malicious program attached to legitimate file or application and spreads when the infected file executed.
- require user action to spread, can corrupt, delete, modify system file.

(2) worm : self-replicating malware that spreads across the network without user action.

(3) Trojan (Trojan Horse) : Malicious software disguised as legitmate; often provides backdoor to hacker.

(4) Ransomware : Encrypt the file or lock the system and demand ransom (money) for recovery.

(5) Spyware / Keylogger : Secretly monitors user activity and steal credential, keystrokes or browsing data.

: Understanding different types of malware is essential to detect, prevent, respond effectively to cyber threat in any security environment.

- malware works on multiple phase : exploitation & post exploitation :

(6) Adware :- A malware design for display unwanted ads, in pop-ups, redirect often generating attackers revenue.

(7) Rootkit :- rootkit is dangerous malware which design for aquire high-level access (admin-level) and controling the network & system while hide it's presence. rootkit operates at kernal or firmware layer software.

(8) Botnet :- network of compromised (infected) computers (bots) infected by malware and controlled remotely by malicious actor (hacker) for further attack, DDOS attack, SPAM, Crypto-mining.
(botnet is types of malware design for infected system into remotely controlled bot by attack for further attack.)

(9) fileless malware :- operates directly from memory (ram) not writing - malicious file or disk. (run/write on main memory) for hard to detect.

(10) Logic bomb :- malicious code execute by specific condition or action (eg. date, event etc.)

(11) REXX/Macro malware : malicious macros in documents (office macros) or scripts.

[Exploit vulnerability — Executed payload — Etabliched control]

- ⊙ Exploit payloads - Small shell code that execute command.
- ⊙ Backdoors - Create secret access path bypassing authentication.
- ⊙ Trojan horse - disguised legitmate file or application but create backdoor.
- ⊙ Rootkits (initial variant) - Hide malicious activity rights after exploitation.
- ⊙ fileless malware (loader stage) - load and run in memory after exploitation.

how to do it ↓ — what to do must follow ↓

* Cybersecurity framework & standard —

→ what is cybersecurity framework?

Ans:- Cybersecurity framework is the structured guide (blueprint) that help organization protect their digital assets, manage risk and ensure compliance.

It's roadmaps or systmatic approach for building, managing and improving Cybersecurity in an organization.

A Cybersecurity framework is a blueprint of rules, standard and best practices that guide organization on how to identify, protect, deetect, respond and recovery.
- Ensure consistency across policies, process, tools
- Aligns security activities with business goals/objectives.

→ Major Cybersecurity frameworks :- [NIST CSF, ISO/IEC 27001, COBIT, CIS]

(a) NIST Cybersecurity framework (CSF)
developed by national institute and standard technology (U.S)
It framwork essential for incidedent handling lifecycle.
focus on continous monitoring, detection, response and recover.
(strategic risk management)

The NIST framework (CSF) is a structured set of five core function identify, protect, detect, respond and recover that guides organization to manage cybersecurity risk -
identify the assets, protect the assets, detect and respond the threat and ensure resilliant recovery of system and data.

Note:- Incident handling is the complete mangment (start to end) & incident response is imediate action to control or fix the incident.

[overall cyber security process]

[this approach widely use in an organization]

- Identify : Assets, system, Data, network, Risk, Vulnerability.
- Protect : firewalls, Access controll, Encryption, policies, training, Patching-Backups.
- Detect : monitoring logs, SIEM alerts, correlation, Anomalies, threat intel.
- Respond : Triag, Contain, remediation, communication, Collect Evidence, Mitigate, Playbook.
- Recover : System recover data, Post-incident Review, lessons learned, verify services, update controls.

- Identify : Know what assets are important and what risks exist.
- Protect : Apply security control (firewall, encryption, access control)
- Detect : Continous monitor for threats and suspicious activity.
- Respond : Take immediate action when an occur incident occurs.
- Recover : Restore system & data and operation back to normal.

ISO/IEC 27001 Framwork :

- An International information security standard that defines how to Creat/build, implemend and maintain an Information Security management system (ISMS) to protect data and systems

objective : maintain the CIA (confidentiality, Integrity, Avalaibility) of information through well-define policies and continous improvement.

- ISO 27001 framework helps organizations build a Complete management system to protect and Continously improve information Security.

main Components in ISO 27001 :

(a) Establish ISMS : build the Complete system (Policiy + People + Process + technology) that manages and protect organization information.

(b) Implement ISMS : Apply Security control from Annex A (93 controls) like encryption, access control, and backup etc.

(c) monitor & review - Conduct regular audits and risk assessments.

(d) Continous Improvement :- Update and enance control after every review & incident.

COBIT (control objectives for Information related technology) developed by ISACA.

COBIT is a governance and managment framework that guides organization How to align IT and Cybersecurity with business goal/objective

COBIT ensures that every IT and Security decision directly supports bussiness goals, like protecting revenue, maintaining trust or staying compliant

Ex- Reduce ~~bank~~ Customer data breaches and improve trust in online banking service.

How cant align IT & cybersecurity : Reduce data breach, Improve regulatory compliance, Ensure Service availability, Make IT decisions accountable. (role & responsibility)

IT, security are not just technical tasks but integral to achieving business objectives/goals.

CIS (Center for Internet Security Controls)
develop by CIS non-profit organization, Practice & Control framework to ~~CIS~~ defense from Cyber threat.
CIS framework offer practical and technical guidance for improving Cyber defense and reducing risk of organization digital assets, network, system, data.

CIS control :
The CIS control are the set of 18 prioritized security action (practice) designed to help organization ~~over~~ digital assets from cyber threats.

The 18 controls are divided in 3 implementation Group (IG_s) depend organizational resource & maturity.

IG_1 (Basic) - small organization ⇒ Essential Cyber hygiene
IG_2 (Foundational) - medium organization ⇒ more advance security practi
IG_3 (organizational level) - large organization ⇒ Comprehensive risk

- organizational level (IG_3) also include (IG_1 + IG_2) & foundational include (IG
Basic control (1 to 6) foundational control (7 to 16) organizational (17+1

→ list of CIS controls (version 8)

Basic (1 to 6)

(1) Inventory & Control enterprise assets :
Identify, track & manage all hardware connected to the network.

List of CIS control (v8)

Basic (1 to 6)	
(i) Inventory & control of enterprises assets.	identify, track, manage all hardware which connected to network.
(ii) Inventor & control of software assets.	Track all installed software and allow only approved software.
(iii) Data Protection	secure data during storing, transmission and processing.
(iv) ~~account manage~~ secure configuration of enterprises assets & software	Secure Configuration, reduce vulnerability
(v) Account management	manage account of user and secure.
(vi) Access control managment.	Give acces only authorized user. manage privilege.
Foundational (7 to 16)	
(7) Continous vulnerability management	regularly scan. system, network for weakness and patch them quickly.
(8) Audit log managment	Collect and review logs for detection
(9) Email & Browser protection	Block malicious email, link & Browser safe
(10) malware defenses	use antivirus, EDR and keep update
(11) Data recovery process	take regular backup & test it work
(12) Network infrastructure managment	secure router, switches, firewall use networks.

(13) Network monitoring and defense	use IDS/IPS and siem tool to detect & response
(14) Security awareness and skills training	train employee to regonize and prevent
(15) Service provider managment	Assess and monitor third-party vendors security practice.
(16) Application software security	secure application, apply secure coding & bug free.
Organizational (17 to 18)	
(17) Incident response managment	Develop and test incident response plans
(18) Penetration testing	Simulate attacks to test defenses and identify and fix them. (simulate real cyber attack).

Summary :

Basic (1 to 6) : Control hardware & software, Data protect, account & access management.

Foundational (7 to 16) : Vulnerability check, logs audit, malware, recovery, network monitor & management, Awareness, vendor, secure software.

Organizational (17 to 18) : Incident response, Penetration testing

prioritize approach to reduce cyber risk, improve defenses and Create strong security.

* what is cybersecurity standards?

Cybersecurity standard are set of rules and requirement that organization must follows to maintain a uniforms level of security.

[what must be done (Standard) by org.]

→ Common Cybersecurity standards :

(a) ISO/IEC 27001 & 27002

international standard for Information security management System (ISMS) developed by ISO/IEC

ISO/IEC 27001 is a standard ~~that~~ provides rules and regulations & requirements for building a secure management system for information.

[set policies, risk assessment and control data security]

(b) PCI-DSS (Payment Card ~~Interface~~ industry Data Security standard)

Protect Credit/Debit card data during storage, processing & transmission,

developed by PCI security standard council.

Ex- e-commerce website companies must follows this standard secure user/customer Card (visa, mastercard, American express etc.)

protect personal ... and ensure privacy rights of individuals

(c) GDPR (General data protection regulation)
Type: regulation (legal law in EU developed

purpose: Protect personal data and privacy right of individuals in the Europion union.

Goal:- To ensure that Companies Collect, store, and process personal data lawfully, transparently and securely.

Key principle:- Consent: clear permission before collecting personal data
purpose: Use data only for the reasons, it was collected
data minimization: collect only what necessary
Right access and deletion: User can request access or deletion of their
Data protection: secure data using encryption and other. data-
Breach notification: inform authorities and user if data breach.

(d) HIPAA (Health insulance portability and accountability act)
laws & regulations - standard developed by U.S (HHS)
→ protect patient all record (medical info personal info etc.)

To insure CIA (confidentiality, integrity, availability of protected
Health record (info) [PHI]

Summary:-

ISO/IEC 27001: How to build and maintain (I.S.M.S)
PCI-DSS: Protect payment card data.
GDPR: Protect personal data & privacy.
HIPAA: protect patient record.

Key term:

(a) Regulation (laws):
legal laws mandatory by government or authorities (Industries)
. Define laws what must be done to comply with regulation.
Ex- GDPR, PCI-DSS, HIPAA

(b) Policy (DIRECTION full):
organization principles (internal statement that defines management's intent, security objective and approach. what general approach the organization takes.
Ex:- All data must be encrypted and access restricted to users.

(c) Standard (specification):
Define consistent requirement, technical and operational. and best practice support policy.
Established mandatory criteria to meet policies.
Ex:- ISO/IEC 27001

(d) Procedure (steps): detailed step by step process describing how to meet standards

(e) Rule (Enforce): define what is allowed and prohibited eforceably. eg> lock the screen of p.c when leave their desk.

(f) Compliance (Prove):
Ensure the organization comply (adherance) to rule, regulation, policies, standard and laws that are set by government or organizations.

· follow the internal guidance (Company policy, procedures) and External guidance (Such a government laws and industry standards)