PMICS, July 2025

CSE 807

Information Security Management

Instructor:
Md. Faisal Hossain

faisal.csedu@gmail.com
faisal.pmics@cse.du.ac.bd

INFORMATION & CYBER SECURITY

Disclaimer:

This material is designed & owned by the course instructor for the PMICS program of University of Dhaka. Use, copying, distributing, sharing, displaying, or reproducing the entire or any part of this material for any commercial purpose is strictly prohibited and illegal.

Critical Information Infrastructure (CII)

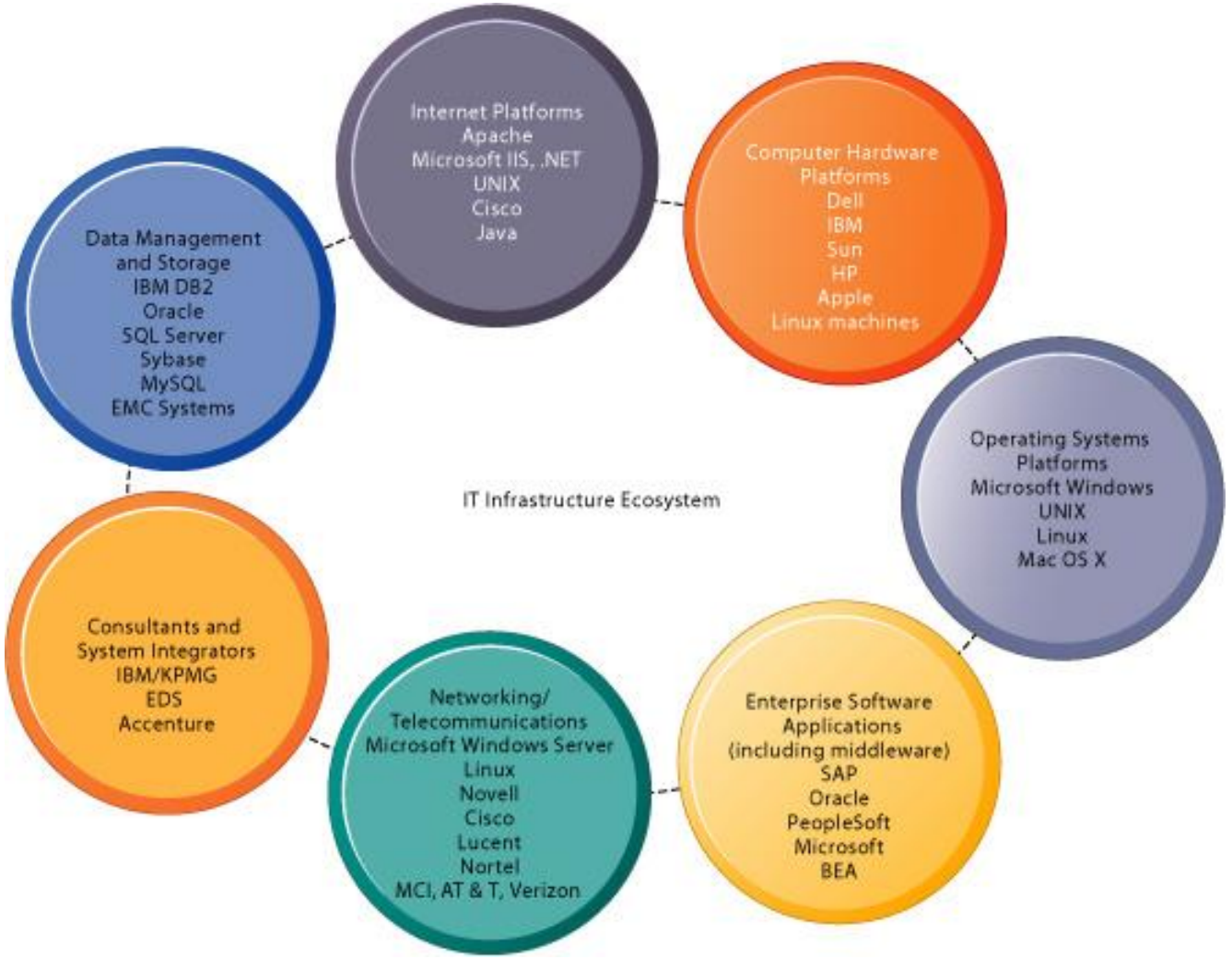
SL	Name of the Infrastructure	SL	Name of the Infrastructure
1	Office of the President	18	Immigration, Bangladesh Police
2	Prime Minister's Office	19	Bangladesh Telecommunication Company Limited (BTCL)
3	Bangladesh Bank	20	Bangladesh Power Development Board
4	National Board of Revenue	21	Power Grid Company of Bangladesh
5	Bangladesh Data Center Company Limited	22	Titas Gas Transmission and Distribution Company Ltd.
6	Bridge Division	23	Central Depository Bangladesh Limited
7	Department of Immigration and Passports	24	Bangabandhu Satellite Company Limited
8	National Data Center, Bangladesh Computer Council	25	Bangladesh Securities and Exchange Commission
9	Bangladesh Telecommunication Regulatory Commission (BTRC)	26	Civil Aviation Authority Bangladesh
10	National Identity Registration Division, Election Commission Secretariat	27	Office of the Registrar General, Registration of Births and Deaths
11	Central Procurement Technical Unit	28	Dhaka Stock Exchange Limited
12	Sonali Bank Limited	29	Chittagong Stock Exchange
13	Agrani Bank Limited	30	Shurokkha Platform
14	Janata Bank Limited	31	BRTA
15	Rupali Bank Limited	32	Land Records
16	Ruppur Nuclear Power Plant Establishment Project	33	Police Headquarters
17	Biman Bangladesh Airlines	34	RAB

Elements of Critical Information Infrastructure (CII)

- Physical
- Cyber
- Human

IT Infrastructure

Component of IT infrastructure



Digital Transformation

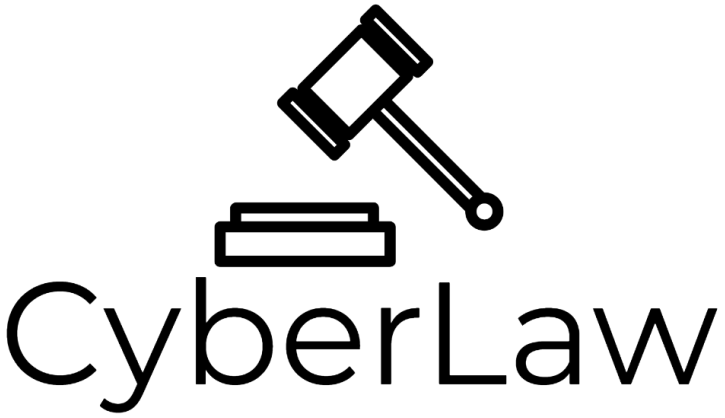
Laws, Legislations, Acts, Guidelines

- ISO/IEC 27001 — Information Security Management System
- ISO/IEC 27035 — Information Security Incident Management
- ISO/IEC 27032:2023 — Cybersecurity — Guidelines for Internet security
- ISO/IEC 31000 – Risk Management
- ISO 18788 — Security Operations Management System
- PCI DSS – Payment Card Industry Data Security Standard
- ANSI/TIA 942 – Data Center Security
- Health Insurance Portability and Accountability Act (HIPAA), 1996
- Sarbanes–Oxley Act (SOX) (Global)
- General Data Protection Regulation (GDPR), 2016/18 (EU)
- Copy Right Act, 2000 (BD)
- National ICT Policy, 2018
- Cyber Security Act 2023 (Amendment of Digital Security Act 2018)

Cyber Law

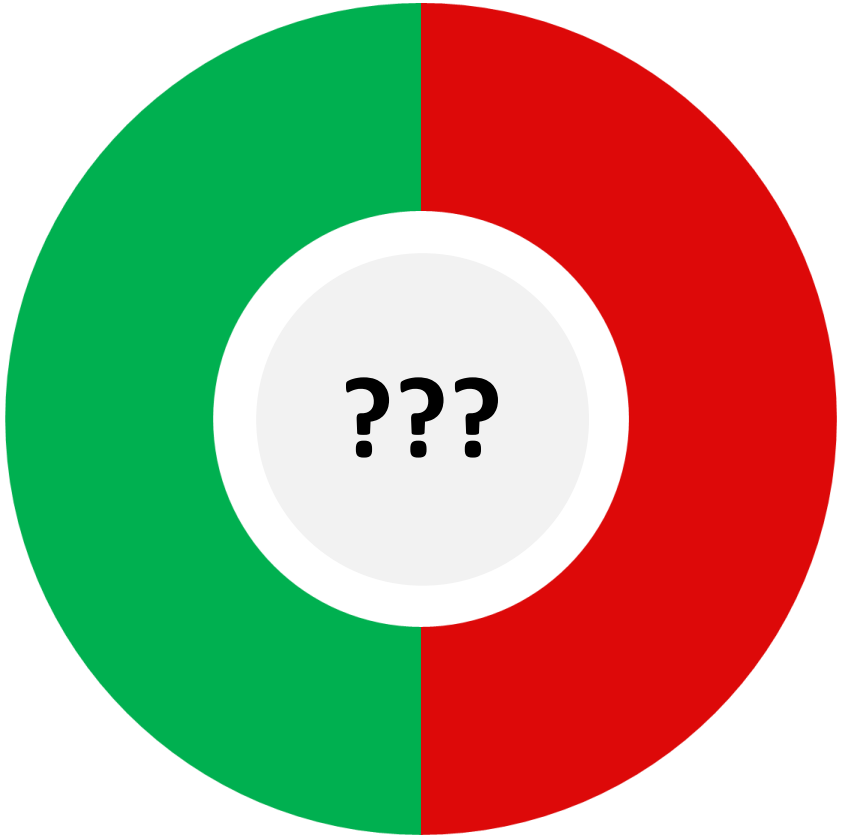
Cyber law, also known as Internet Law or Cyber Law, is the part of the overall legal system that is related to legal informatics and supervises the digital circulation of information, e-commerce, software and information security.

- Data Protection
- Fraud Prevention
- Online Harassment and Stalking
- Contracts and Employment Law
- Reduce or prevent cybercrime

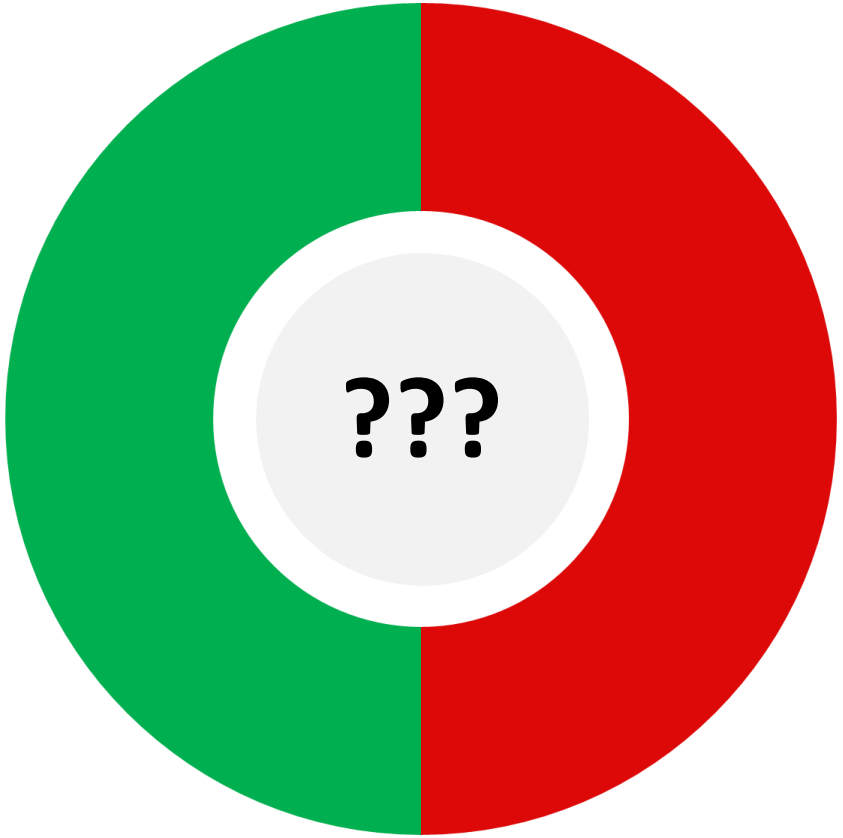


What is the most valuable object in the world?

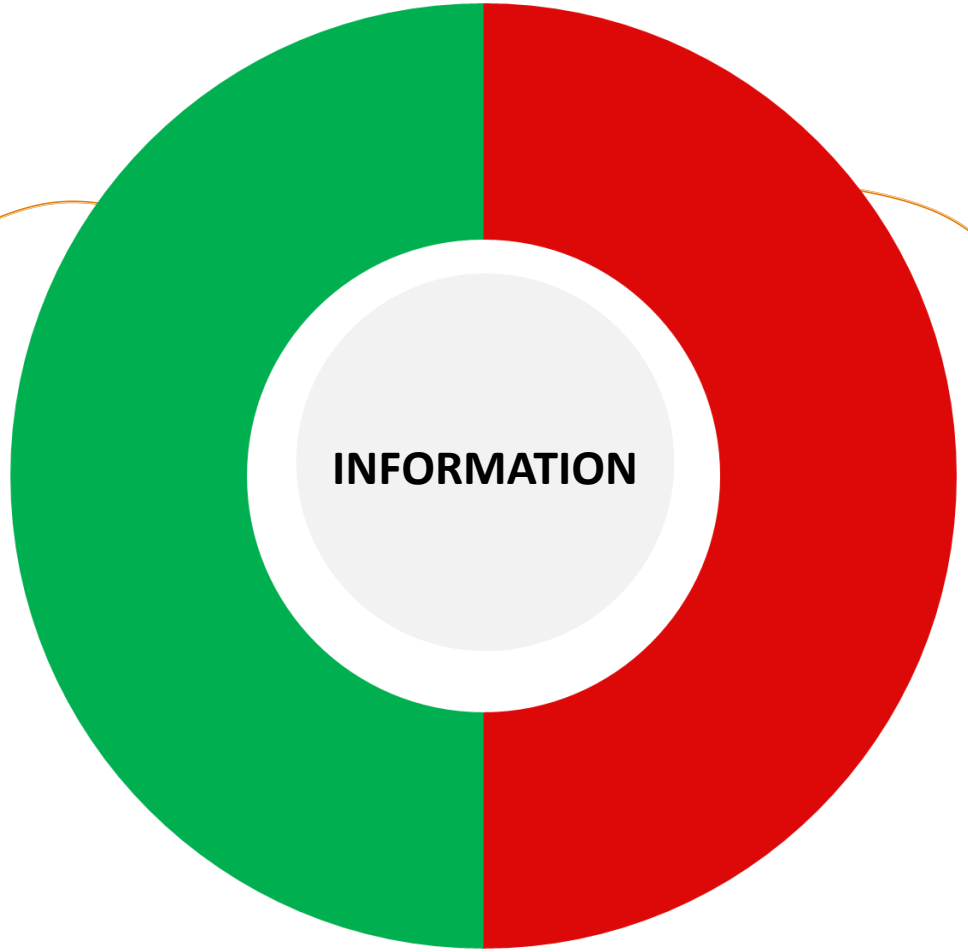
What is the most valuable asset in the world?



What is the most vulnerable asset in the world?



MOST VALUABLE ASSET



MOST VULNERABLE ASSET

Asset & Information

Asset - Anything of value that is owned by an organization. Assets include both tangible items such as information systems and physical property and intangible assets such as intellectual property.

Information - Information refers to data that is organized, structured, and meaningful, providing insight, knowledge, or understanding to the recipient. It is a crucial aspect of communication and understanding in various fields, including science, technology, communication, and everyday life.

Why Information is the most valuable & vulnerable asset?

- In this 21st century, Information and Communication Technology (ICT) is the major resource for fueling business ideas and innovations.
- In-addition, the more businesses are driven and dependent on automated systems, the more ICT risks and threats are invited.
- Thus, information is treated as the most valuable asset like other important business assets as well as vulnerable asset in today's highly competitive as well as cyber threatened environment.

The Most Important Concern of the World

SAFETY OF THE ASSET

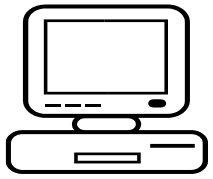
The Most Important Concern of the World

SECURITY OF THE INFORMATION

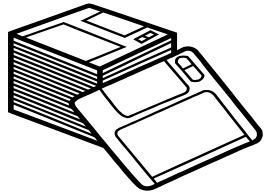
Information Systems (IS)

Information System is a coordinated and structured arrangement of people, data, processes, and technology designed to collect, process, store, and disseminate information for supporting decision-making, coordination, control, analysis, and other organizational activities. It involves the use of various components, including hardware, software, data resources, procedures, and people, all working together to manage and utilize information effectively within an organization or context.

Components of Information Systems

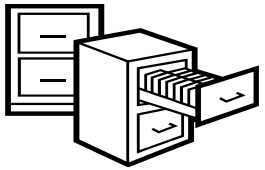


Hardware



Software

People



Data

Procedures

Safety of the Asset: The Information Security

Regardless of the nature of the business, organizations amass a great deal of confidential information about their customers, employees, products, services, research and financial status and people makes relation with the organization based on entrust and reliability and believes the organization as convergent entity for safe keeping the information and other assets.

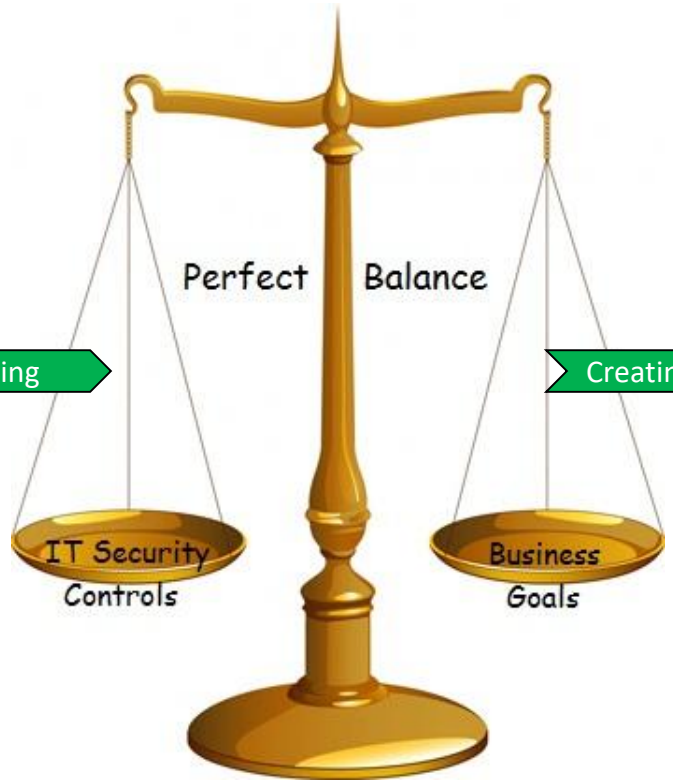
Therefore, Information Security has become the finger of the pulse of any organization.

Hence information and related technology inevitably needs to be suitably protected by ensuring an acceptable level of Information Security to ensure **business continuity (BC)**, **minimize business risk (BR)**, **maximize return on investments (ROI),** and help business gain a competitive edge/advantage and opportunities.

Information Security Objectives

✓Creating
✓Delivering
✓Communicating
Best IT Security Controls

Ensuring



Creating

✓Value of IT
✓Customer Confidence
✓Effective Awareness
✓Acceptable IT Risk
✓More Prevention
✓Sustainable Operations

Information Security

Information Security is not only about securing information from unauthorized access.

Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be physical or electronic one.

Information Security Triad

Availability-Protection from disruptions in access (reliable).

Confidentiality-Protection from unauthorized access (limit).

Integrity-Protection from unauthorized modification (trustworthy and accurate).

Confidentiality

The characteristic of data or information when it is not made available or disclosed to unauthorized persons or processes.

Confidentiality is the protection of sensitive information (personal/proprietary) from **unauthorized access or disclosure** by individuals, entities, or processes.

Sensitive information is information that if improperly disclosed (confidentiality) or modified (integrity) would harm an organization or individual. In many cases, sensitivity is related to the harm to external stakeholders; that is, people or organizations that may not be a part of the organization that processes or uses the information.

Confidentiality (cont.)

It relates to permitting authorized access to information, while at the same time protecting information from improper disclosure. To avoid those difficulties, security professionals must regulate access, permitting access to authorized individuals, for that protecting the data that needs protection.

Data that needs protections is also known as PII or PHI.

PII stands for Personally Identifiable Information.

PHI stands for Protected Health Information.

Related to confidentiality is the concept sensitivity a measure of the importance assigned to information by its owner, or the purpose of denoting its need for protection.

Examples of Confidential Information

Full Name
Date of birth
Addresses
Contact details
Personal bank details and credit card information
Images of staff, pupils or clients that confirm their identity and can be linked to additional personal information.

Why Confidentiality is Important?

What are the common threats related to Confidentiality?

- Wiretapping
- Dumpster diving
- Eavesdropping
- Snooping
- Social Engineering

Common Threats to Confidentiality – Definitions

Wiretapping is the electronic version of eavesdropping, the best way against that is by using encryption to protect the communication.

Dumpster diving looking for sensitive materials, but in the dumpster, a paper shredding protects against it.

Eavesdropping occurs when someone secretly listens to a conversation, and it can be prevented with rules about sensitive conversations.

Snooping involves gathering information that is left out in the open. Clean desk policies protect against snooping.

Social Engineering is the set of tactics used to manipulate, influence, or deceive a victim into divulging sensitive information or performing ill-advised actions to release personal and financial information or hand over control over a computer system.

Impact of Loss of Confidentiality

Financial Loss, Loss of public confidence, loss of credibility

Why Customers Quit?

Standard Measures to Establish Confidentiality

- Password
- 2FA, MFA
- Biometric verification
- Security tokens
- Data encryption

How Confidentiality can be Maintained?

- Access Controls
- File Permissions
- Encryption
- User Awareness

Forms of Sensitive Data

- physical to digital, such as written documents, photographs, videos or audio recordings

Regulated & Unregulated Data

Sensitive???

Confidential???

Private???

Sensitive Unregulated Data

- Customer surveys
- Job applications
- Employee contracts

Sensitive Regulated Data

- National Identity Numbers/Social Security Numbers
- Bank account numbers/information
- Healthcare information

Confidential or Non-Confidential Data

- A first and last name in a public record is harmless.
- A first and last name in an organization's database should be treated as confidential, as it could be tied to payment card data, home addresses, Social Security numbers, and more.

Is it possible for confidential data to become public in a different time or context?

Privacy

- Privacy concerns people. It’s a right of any person.
- Privacy restricts the public from accessing the personal details of a person.
- There are regulations, laws to protect privacy.

Confidentiality vs Privacy

Privacy concerns people. Example: Browsing History
Confidentiality concerns data. Example: Password

Privacy talks about a person. It’s a right of any person.
Confidentiality is about information.

Privacy restricts the public from accessing the personal details of a person.
Confidentiality protects the information from a range of unauthorized persons.

Privacy has certain acts, laws, etc.
Confidentiality has no act, law, etc.

The common thing is User Awareness.

Kevin David Mitnick (August 6, 1963 – July 16, 2023)

An Infosec Legend, American computer security consultant, author, and convicted hacker.

Confidentiality

Confidentiality is the protection of sensitive information (personal/proprietary) from **unauthorized access or disclosure** by individuals, entities, or processes.

Some examples of Confidential Information:

- Full Name
- Dates of birth
- Addresses
- Contact details
- Personal bank details and credit card information
- Images of staff, pupils, or clients that confirm their identity and can be linked to additional personal information.

Some measures to ensure confidentiality:

- User IDs and passwords
- 2FA, MFA
- Biometric verification
- Security tokens
- Data Encryption

Integrity

It is the property of information whereby it is recorded, used and maintained in a way that ensures its completeness, accuracy, internal consistency and usefulness for a stated purpose, which can be applied to information or data, system and process for business operations, organizations, people and their actions. Furthermore, restrict to data integrity, it is an assurance that data has not been altered in an unauthorized manner, covering data in storage, during processing, and while in transit.

Integrity

- Integrity is the protection of information from **unauthorized modification**. Integrity ensures that data is edited by only authorized persons and cannot be modified in an unauthorized or undetected manner and remains in its original state when at rest.
- It maintains and assures the accuracy and completeness and consistency of data over its entire life-cycle in accordance with business values and expectations.
- For example, if a bank transfers $10,000 to another financial institution, it is important that the amount does not change to $100,000 during the exchange. The concept of integrity also applies to electronic messaging, files, software and configurations.

- Any violation of integrity is significant because it may be the first step in a successful attack against system availability or confidentiality. Contaminated systems and corrupted data must be dealt with immediately to assess the potential for further violation or damage.
- The integrity of digital assets can be ensured by version control, checksums/cryptographic checksums and verified by logging, digital signatures, hashes, encryption and access controls.

How Integrity can be Controlled and Verified?

- Logging
- Digital signatures
- Hashes
- Encryption and
- Access controls

What are the common threats related to Integrity?

- Unauthorized modification attacks/Data Tampering
- Impersonation attacks
- Man-In-The-Middle (MITM) attacks
- Replay attacks
- SQL Injection
- Business Email Compromise

Common Threats to Integrity – Definitions

- **Data Tampering** – Unauthorized modification of files, databases, or system configurations. Unauthorized modification attacks make changes without permission. The best way to protect against that is the least privilege principle.
- **Impersonation attacks** pretend to be someone else. User education protects against impersonation attack.
- **Man-In-The-Middle (MITM) Attacks** – Intercepting and altering communication between parties. MITM attacks place the attacker in the middle of a communication session, monitoring everything that's occurring.
- **Replay attacks** eavesdrop on logins and reuse the captured credentials.
- **Malware (e.g., Trojans, Rootkits)** – Modifying system files or injecting malicious code.
- **Ransomware with Data Manipulation** – Encrypting or altering data to make it unusable.
- **Insider Threats** – Employees or contractors deliberately changing data for personal or financial gain.
- **SQL Injection** – Manipulating databases by injecting malicious queries.
- **DNS Spoofing (Cache Poisoning)** – Redirecting users to fraudulent websites by altering domain name system (DNS) records.
- **Fake Digital Certificates** – Forged or compromised certificates used to impersonate trusted entities.
- **Configuration Changes** – Unauthorized modifications to security settings or access controls.
- **Business Email Compromise (BEC)** – Attackers altering financial transactions through fraudulent emails.

Impact of Loss of Integrity

- Fraud
- Inaccuracy
- Erroneous decisions
- Failure of hardware
- Loss of compliance

Consistency

All instances of the data be identical in form, content and meaning.

Top Mobile Malware Infected Countries

Integrity vs Consistency

- Integrity ensures that the data is correct.
- Consistency ensures that the data format is correct, or that the data is correct with respect to other data.

Availability

It means that systems and data are accessible at the time users need them. It can be defined as timely and reliable access to data & information services only by the authorized users and the ability to use it.

The core concept of availability is that data is accessible to authorized users when and where it is needed and in the form and format required. This does not mean that data or systems are available 100% of the time. Instead, the systems and data meet the requirements of the business for timely and reliable access.

Some systems and data are far more critical than others, so the security professional must ensure that the appropriate levels of availability are provided.

Availability (cont.)

Availability ensures the **timely and reliable access** to and use of information and systems.

This includes safeguards to make sure data are not accidentally or maliciously deleted. This is particularly important with a mission-critical system, because any interruptions in its availability can result in a loss of productivity and revenue. Similarly, the loss of data can impact management's ability to make effective decisions and responses.

Availability is a business concern (investment) and aim is to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades.

Some types of security attack attempt to deny access to the appropriate user, either for the sake of inconveniencing them, or because there is some secondary effect. For example, by breaking the web site for a particular search engine, a rival may become more popular.

Availability can be protected by the use of redundancy, backups and implementation of business continuity management and planning.

What are the common threats related to Availability?

- DoS/DDoS
- Hardware Failures
- Power Outages
- Natural Disasters
- Zero-Day Exploits/Malware/Ransomware

Common Threats to Availability – Definitions

- **Distributed Denial-of-Service (DDoS) Attacks** – Overwhelming a system with traffic to make it unavailable.
- **Hardware Failures** – Malfunctioning servers, storage devices, or network components.
- **Software Bugs & Vulnerabilities** – Unpatched flaws that can crash systems or allow attackers to disable services.
- **Insider Threats** – Employees or contractors intentionally or unintentionally disrupting operations.
- **Natural Disasters** – Floods, earthquakes, fires, and other events causing system downtime.
- **Power Outages** – Loss of electricity affecting data centers and critical infrastructure.
- **Supply Chain Attacks** – Disrupting third-party vendors or service providers that impact availability.
- **Zero-Day Exploits** – Newly discovered vulnerabilities used before a fix is available.
- **Malware** – Viruses, worms, or other malicious software that corrupt or delete critical data.
- **Ransomware** – Encrypting files or systems and demanding payment for restoration.

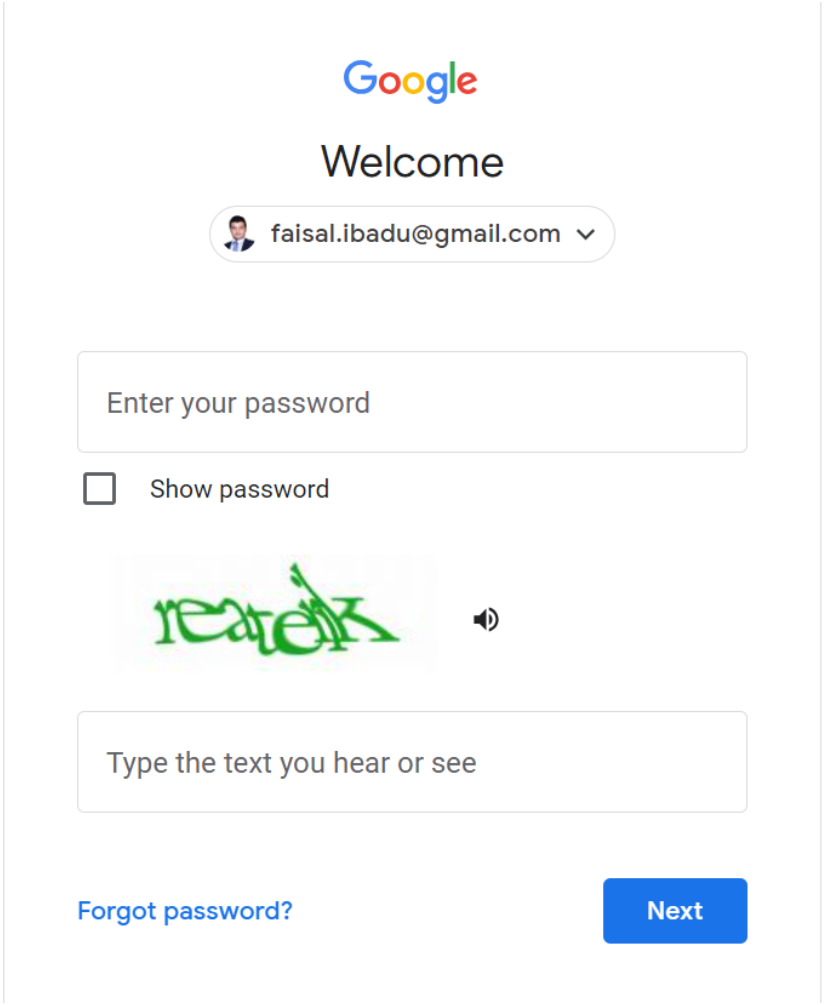
How Availability can be Maintained?

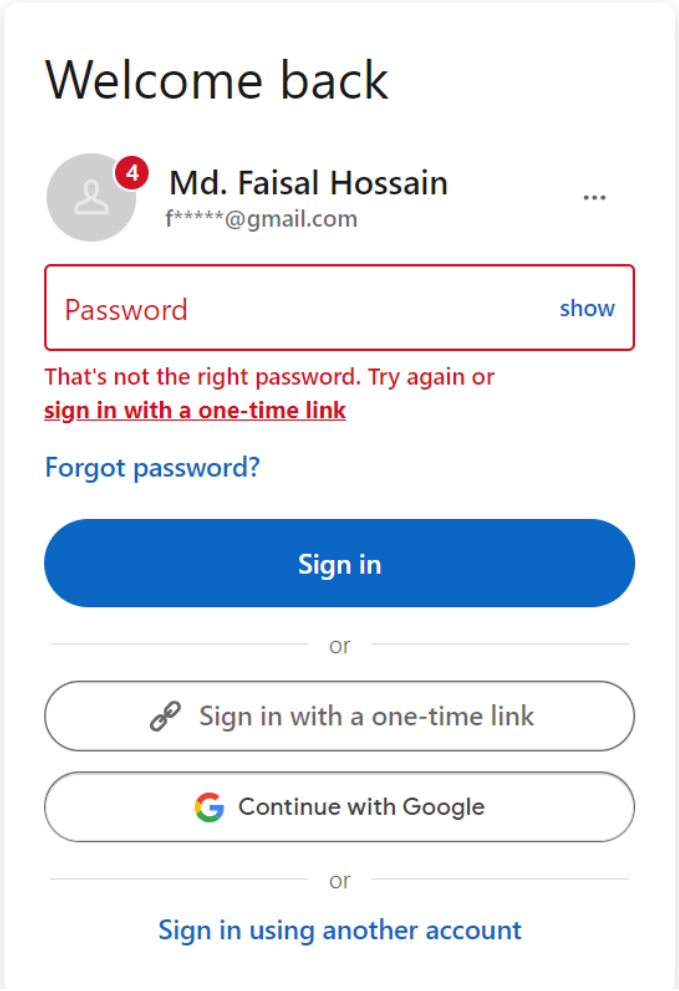
1. Denial of Service can be mitigated using firewalls to block unauthorized connections.
2. Power outages can be mitigated using redundant power and generators.
3. Hardware failures can be mitigated using redundant components.
4. Destruction can be mitigated using backups.

What is the basic property of an information?

THIS PAGE INTENTIONALLY LEFT BLANK

Identify C-I-A

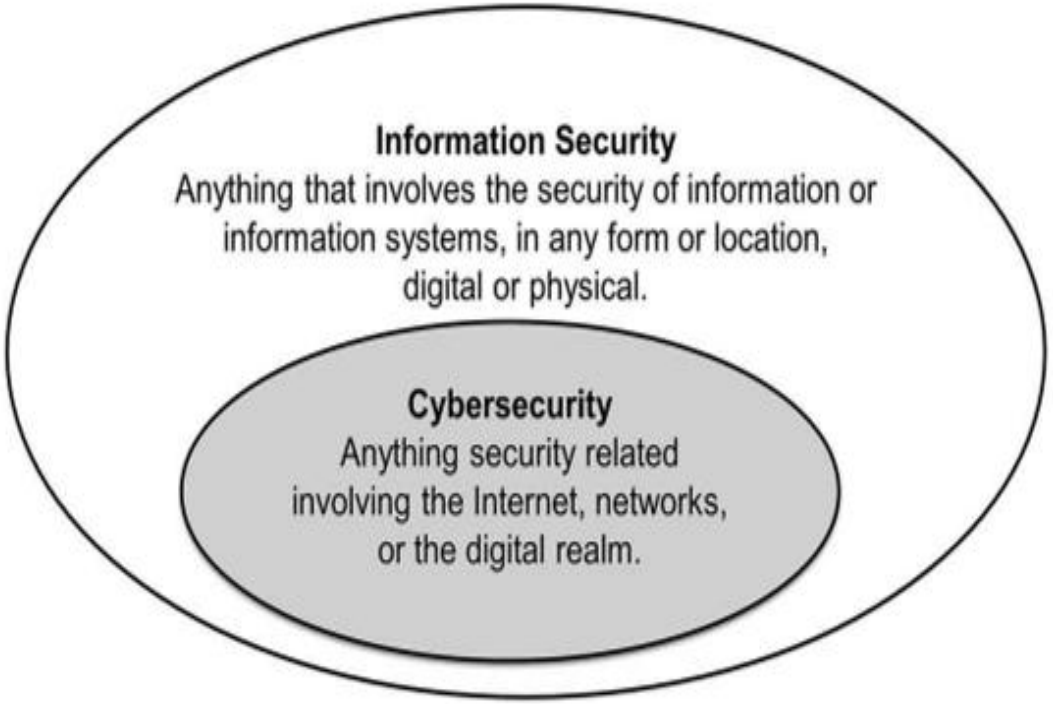




Information Security & Cyber Security

The terms “cybersecurity” and “information security” are often used interchangeably, but in reality, cybersecurity is a part of information security.

More specifically, cybersecurity can be defined as the protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems.



Information Security & Cyber Security (cont.)

Information Security	Cyber Security
Information Security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (CIA).	Cyber Security is defined as the ability to protect or defend the use of cyberspace from cyber-attacks.
Information security focuses on protecting a business as a whole. It doesn't just focus on technology, networking, and security. It has its foundations on protecting the business assets, including anything that would be considered intellectual property and data that should remain private.	The goal is to secure the internet as a whole. It doesn't just focus on private data, focus on protecting public data as well.

Information Security & Cyber Security (cont.)

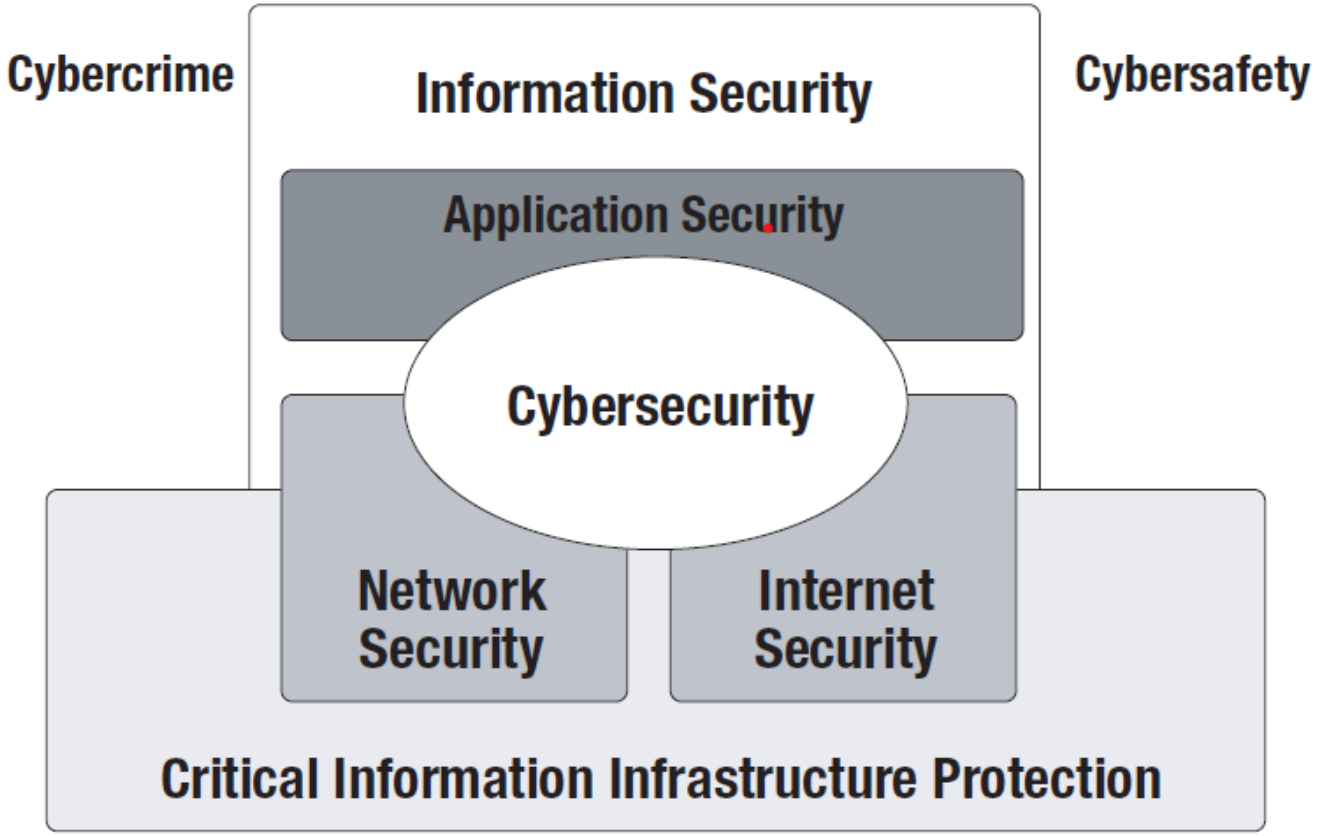
Unlike information security, cyber-security does not include **natural hazards, personal mistakes or physical security**.

To put it even simpler, if we remove offensive and adversary human behavior threats coming through interconnected systems, cyber-security would not be an issue, and information security alone would be sufficient.

Now, the whole confusion about terms is because most of the information today is saved electronically and most of the cyber-attacks are executed to disclose confidential information, harm the integrity of it or deny access to authorized users.

Cyber Security

The complex relationship among cybersecurity and other security domains, as described in International Organization for Standardization (ISO) 27032.



Information and Assets Privacy, Safety & Security

Security

Privacy

Safety

Identification

Consist of making a claim of identity.

Authentication

When users have stated their identity, it is necessary to validate that they are the rightful owners of that identity. This process of verifying or proving the user's identification is known as authentication, which means in another terms access control process validating that the identity being claimed by a user or entity is known to the system, by comparing one (single-factor or SFA) or more (multi-factor authentication or MFA) factors of authentication. Simply put, authentication is a process to prove the identity of the requestor.

- There are three common methods of authentication:
- Something you know: Passwords or paraphrases
- Something you have: Tokens (NISTIR 7711), memory cards, smart cards
- Something you are: Biometrics, measurable characteristics

Authentication (cont.)

Access control process validating that the identity being claimed by an entity is known to the system, by comparing one or more factors of identification.

Access control process validating that the identity being claimed by a user or entity is known to the system, by comparing one (single factor or SFA) or more (multi-factor authentication or MFA) factors of identification.

Methods of Authentication

There are two types of authentication. Using only one of the methods of authentication stated previously is known as single-factor authentication (SFA). Granting users access only after successfully demonstrating or displaying two or more of these methods is known as multi-factor authentication (MFA).

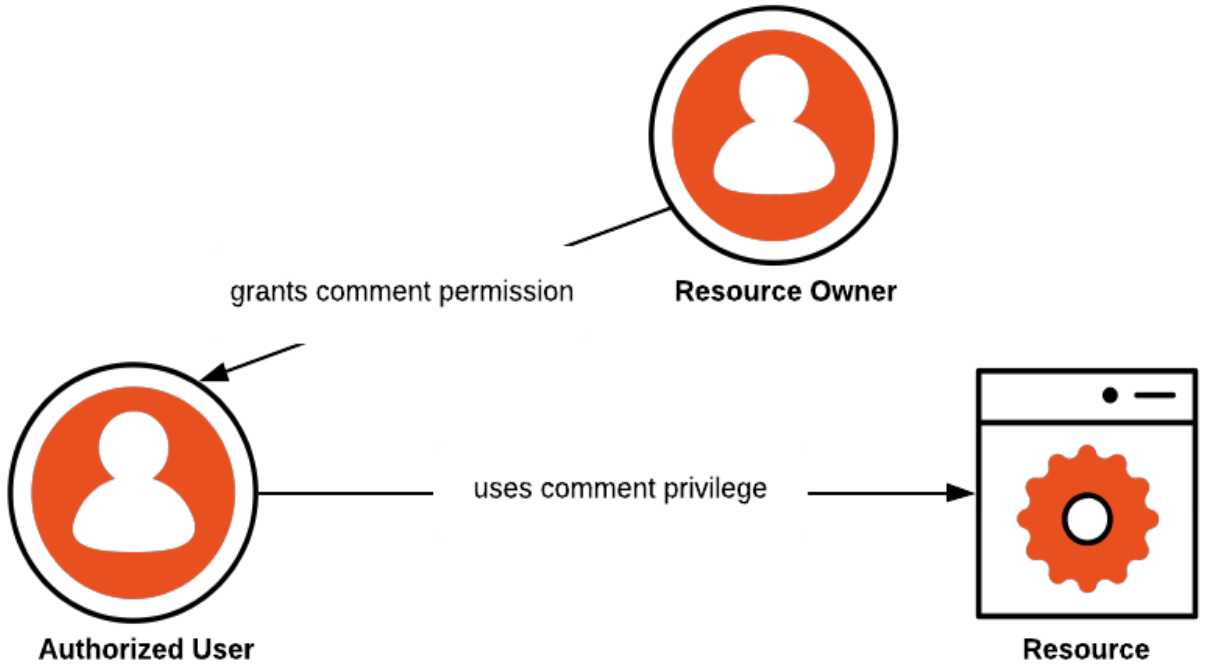
Common best practice is to implement at least two of the three common techniques for authentication:

- Knowledge-based
- Token-based
- Characteristic-based

Authorization

Ensure that an action is allowed.

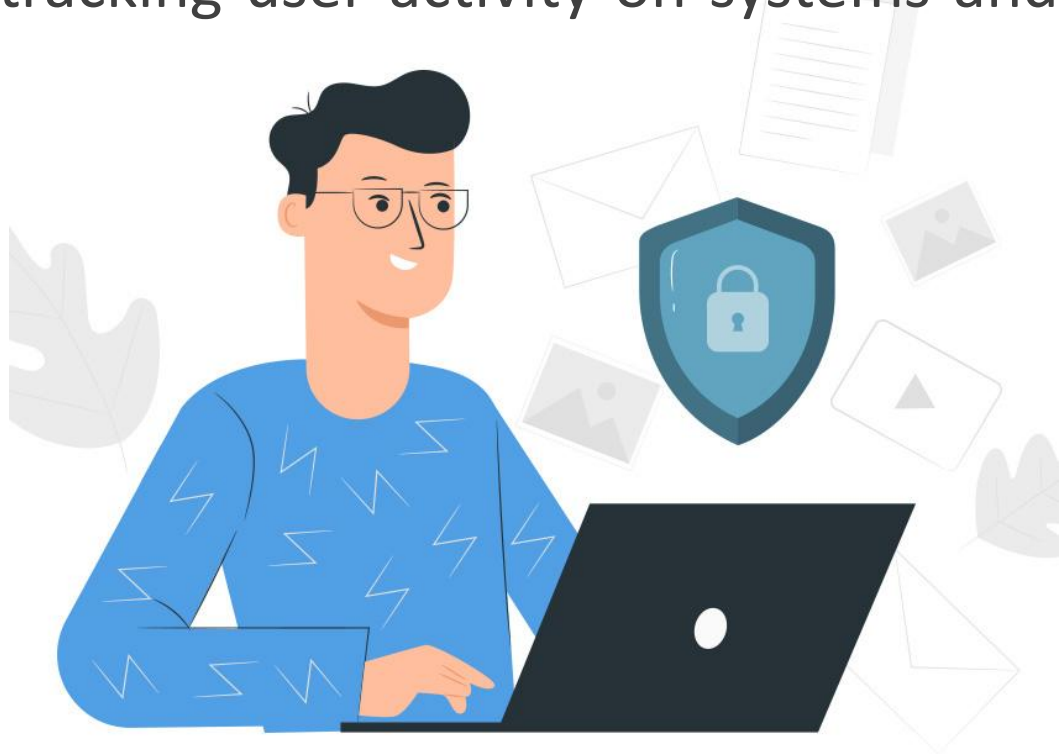
The right or permission that is granted to a system entity to access a system resource.



Accounting

It maintains logs of activity.

Functionality that allows administrators to track user activity and reconstruct that activity from logs. This may include tracking user activity on systems and even logging user web browsing history.

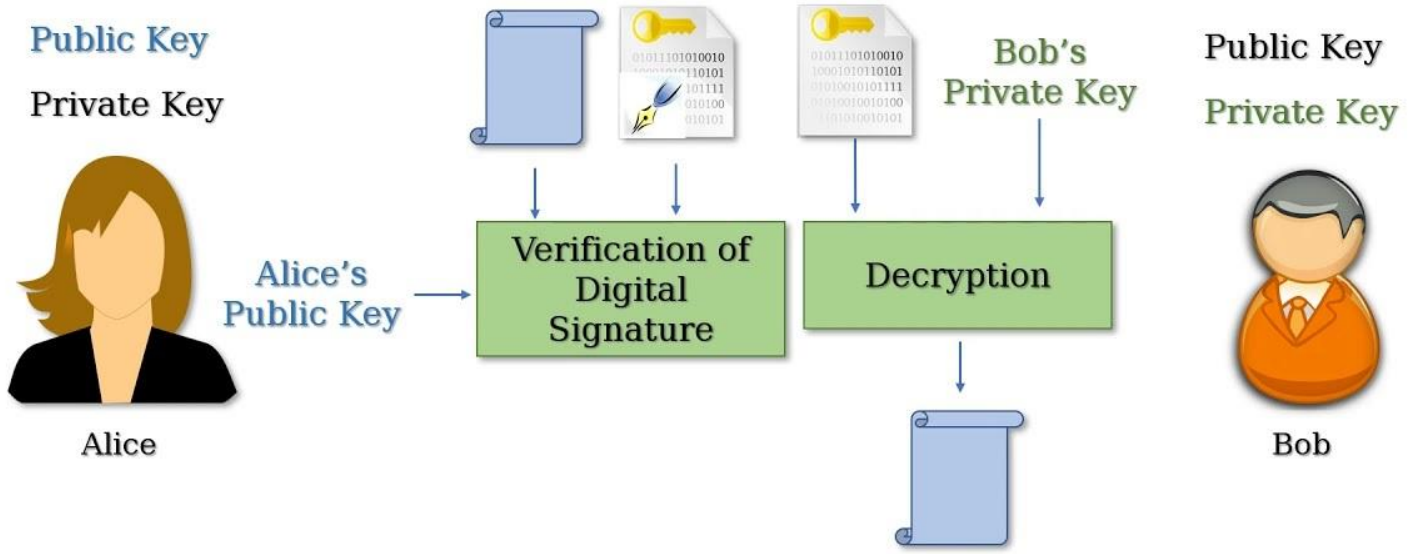


Non-repudiation

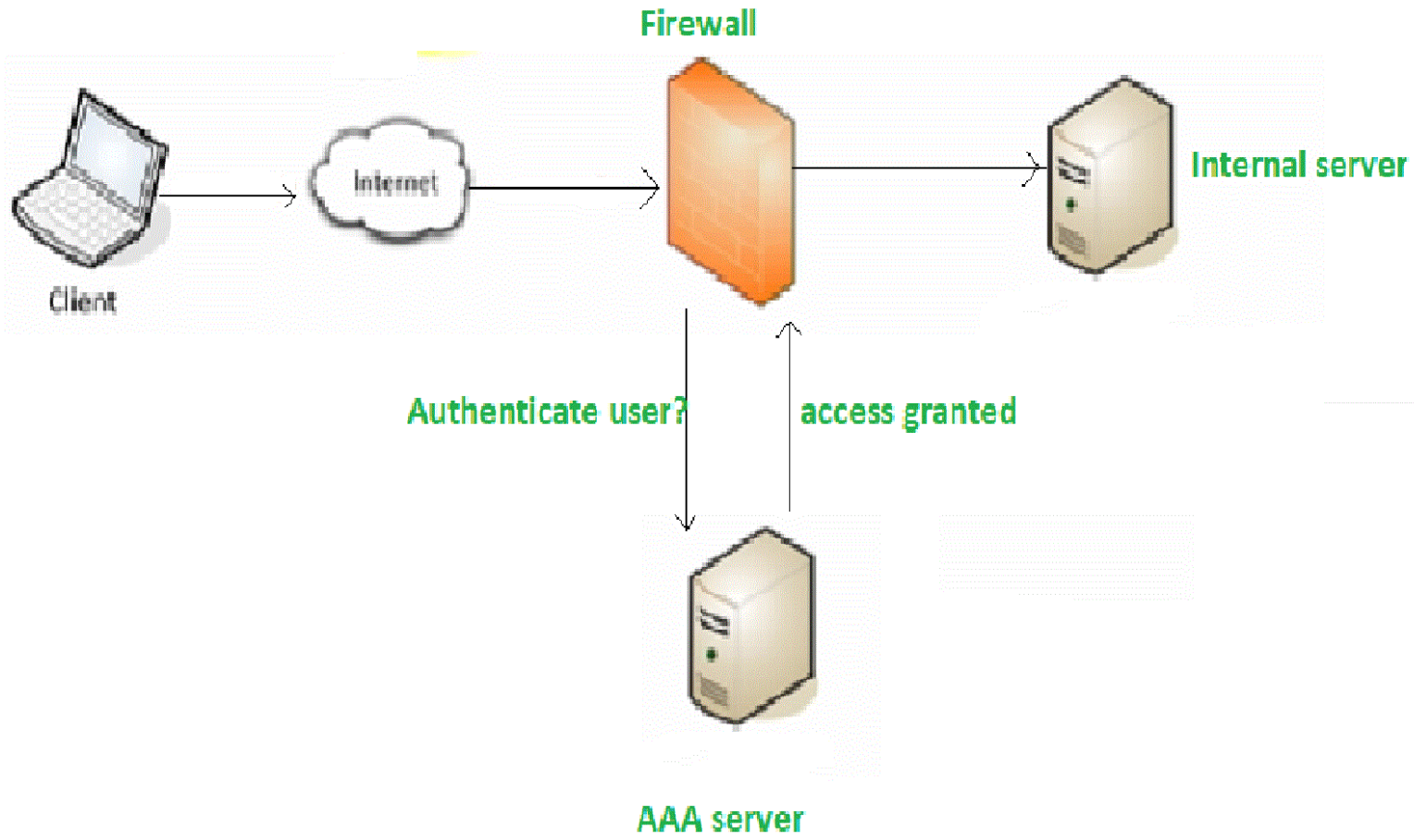
It is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that's widely used in information security and refers to a service, which provides proof of the origin and integrity of data.

This can be solved with:

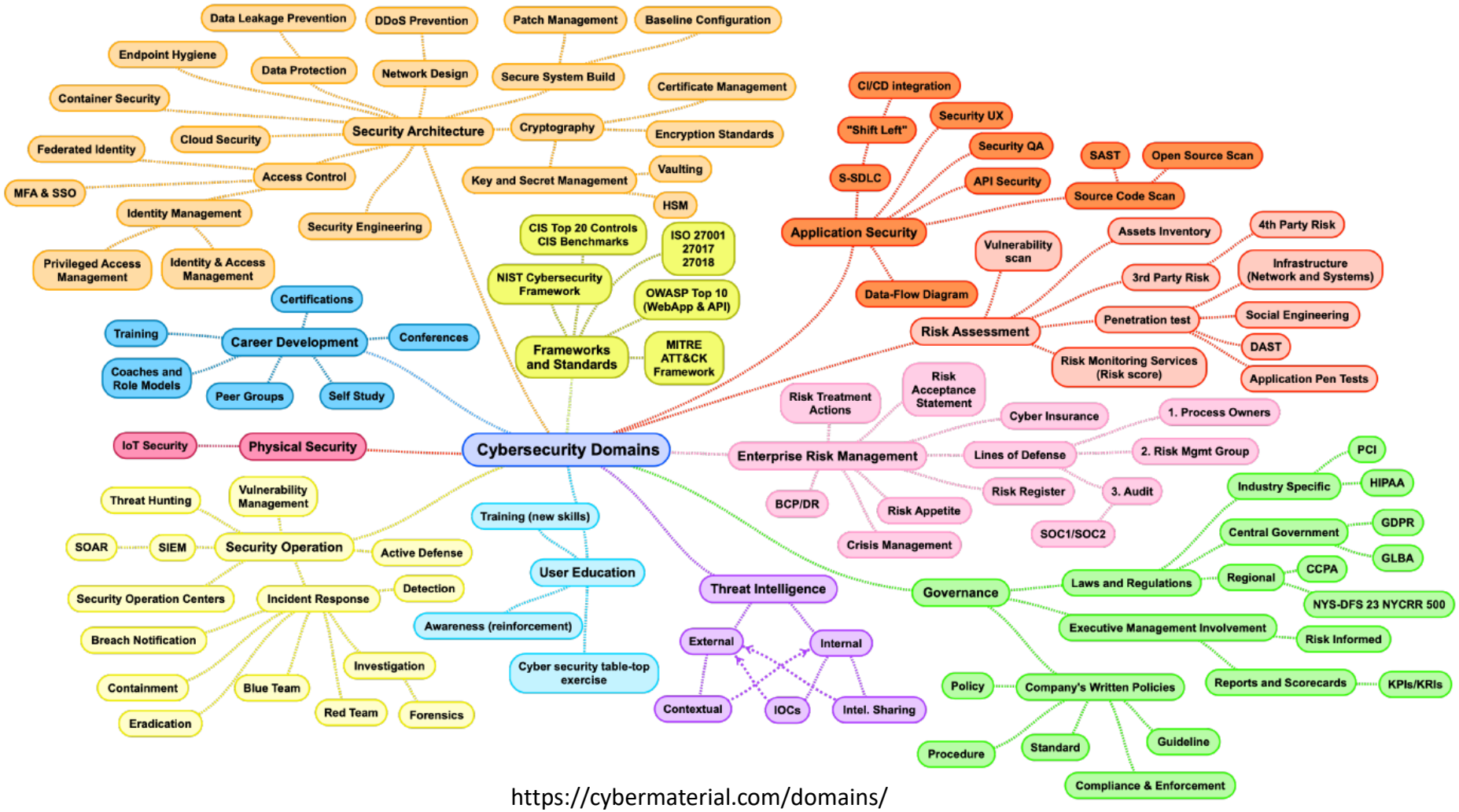
1. Signed contracts
2. Digital signatures
3. Video surveillance



AAA (Authentication, Authorization, Accounting)

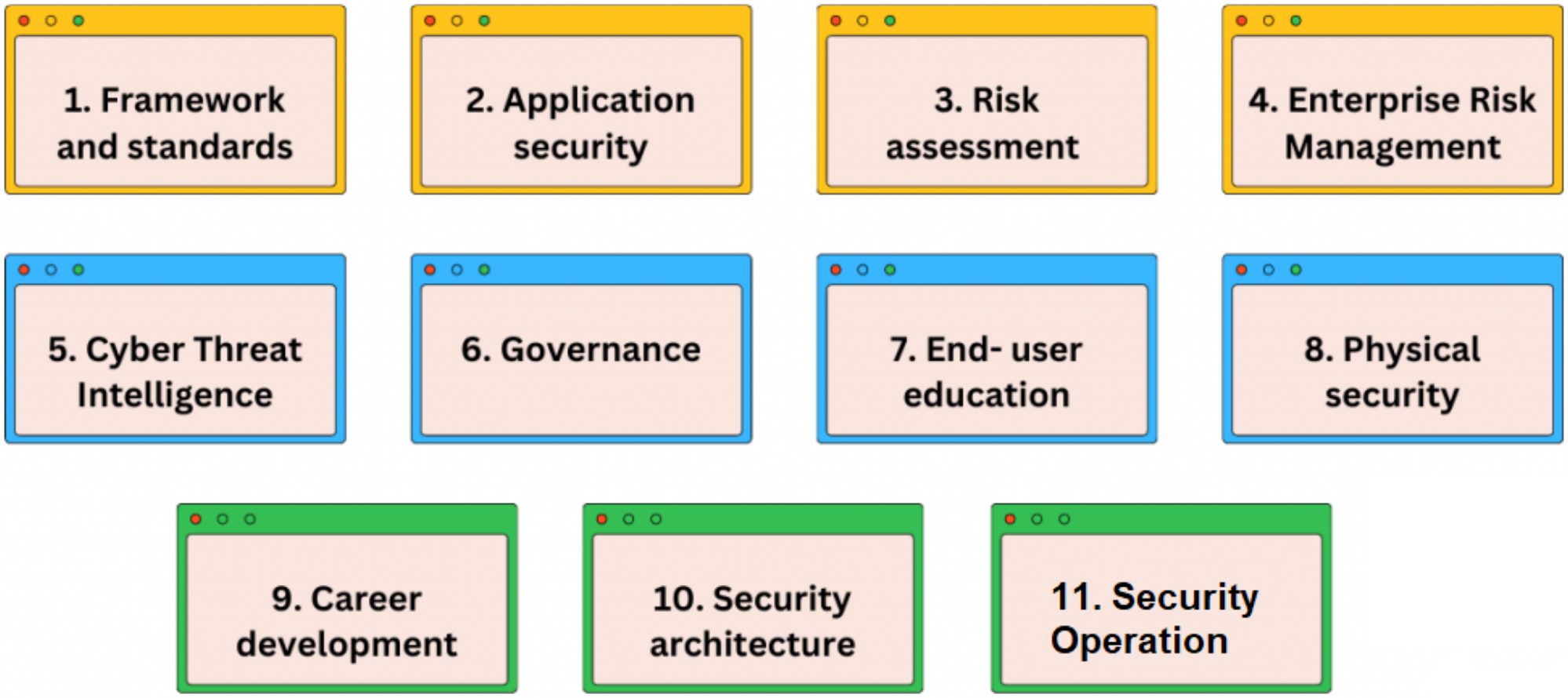


Domains in Cyber Security



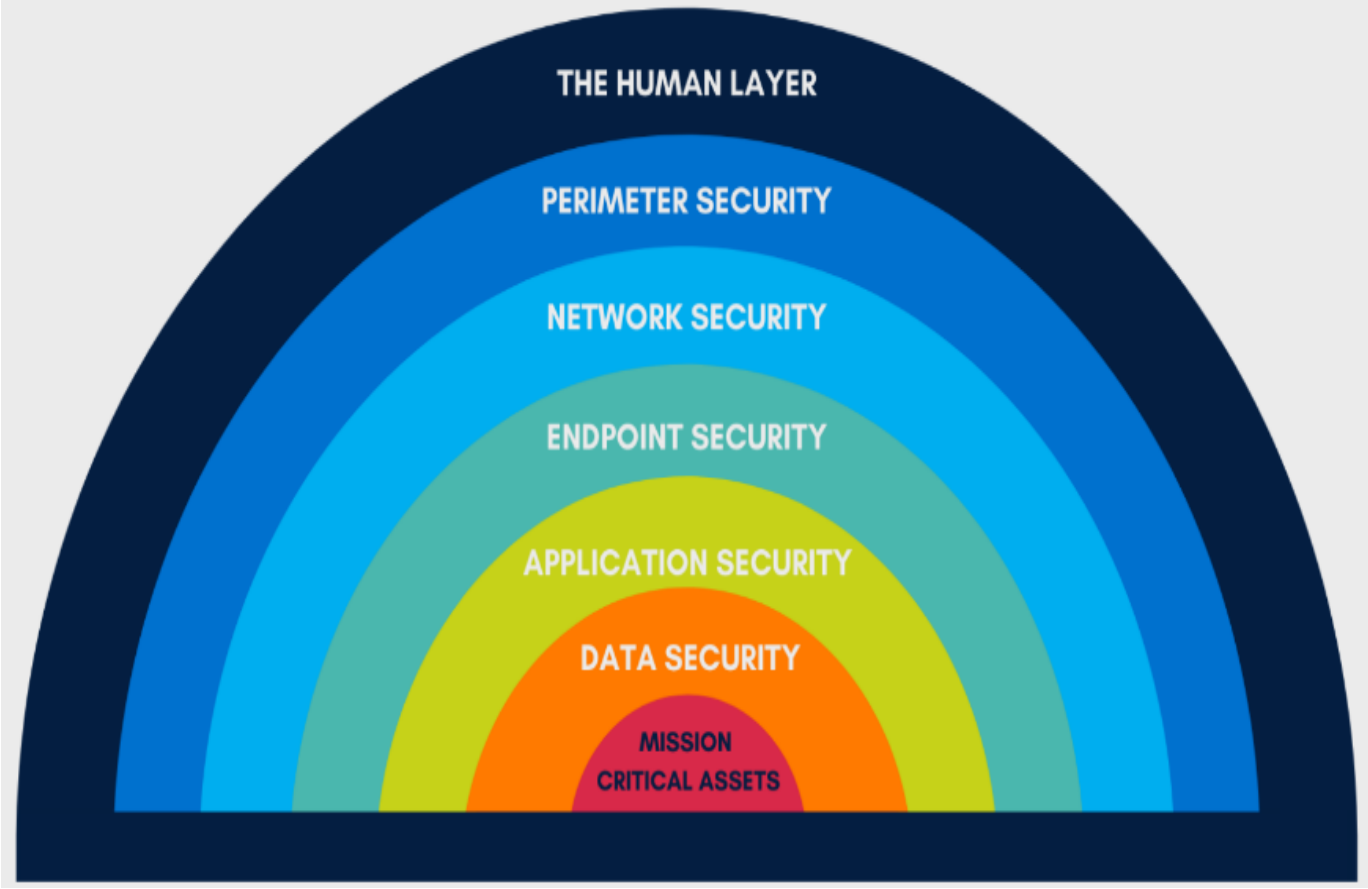
https://cybermaterial.com/domains/

Domains in Cyber Security (cont.)



THIS PAGE INTENTIONALLY LEFT BLANK

Cyber Security Layers



A layered approach to cybersecurity, also known as "defense in depth," involves implementing multiple security measures at different levels to protect against cyber threats, making it harder for attackers to breach the system.

Cyber Security Layers (cont.)

1. Mission Critical Assets – This is the asset you must protect/safeguard.
This layer focuses on protecting the most critical assets and data within an organization and without the assets an organization cannot function.

Mission-critical assets are systems, data, or infrastructure (e.g. computers) that are essential for an organization's operations, security, and business continuity. If these assets are compromised, the consequences can be severe, including financial losses, operational disruption, or reputational damage.

Importance:
Prioritizing security measures for these assets is essential to minimize the impact of potential cyberattacks.

Examples:
Implementing robust security measures for sensitive data, critical systems, and business operations. Physical security like security cameras, RFID key card door locks, burglar alarms and onsite security guards, etc. prevents direct access to your computer systems and therefore minimizes your risk of theft or damage.

Cyber Security Layers (cont.)

2. Data Security – This layer safeguards data both in transit and at rest, ensuring confidentiality, integrity, and availability. It aims to prevent unauthorized access, data breaches, and loss.

Importance:
Key components include data encryption, access controls, data loss prevention (DLP) tools, frequent backups, and two-factor authentication.

Examples:
- Encrypting sensitive data to protect it from unauthorized access.
- Creating regular backups to guard against data loss.
- Enforcing access controls to limit data exposure.
- Using DLP tools to monitor and prevent data leakage.
- Applying policies for secure data erasure and device reuse.

Data security is critical, as it forms the foundation of an organization's cybersecurity. Strong policies and proactive strategies are essential to defend against cybercrime targeting data.

Cyber Security Layers (cont.)

3. Application Security – Application security focuses on protecting software and devices from cyber threats by identifying, fixing, and preventing vulnerabilities in application code and configuration. Application security involves designing, developing, and maintaining software in a way that protects it from cybersecurity threats.

Objectives:

- ❑ Protect application access and internal processes
- ❑ Safeguard application access to mission-critical assets
- ❑ Ensure secure development and update practices
- ❑ Secure access to applications
- ❑ Control application access to critical assets
- ❑ Maintain internal security of applications
- ❑ Secure application access and internal operations
- ❑ Control application access to sensitive assets
- ❑ Prevent exploitation through vulnerabilities

Key Security Measures/Components:

- ❑ Application Firewalls (e.g. WAFs)
- ❑ Secure Coding Practices
- ❑ Regular Vulnerability Assessments & Scanning
- ❑ Authentication & Authorization Mechanisms
- ❑ Encryption & Secure Data Handling
- ❑ Security Logging & Monitoring
- ❑ Regular Updates & Patch Management

Security Strategy:

- ❑ Keep applications updated to address known vulnerabilities
- ❑ Regularly test and enhance security features to prevent exploits
- ❑ Implement solutions to detect and block threats like SQL injection and XSS

Best Practices:

- ❑ Conduct regular testing and patch vulnerabilities
- ❑ Follow secure software development lifecycle (SSDLC)
- ❑ Update applications frequently to mitigate known exploits

Examples:

- ❑ Using WAFs to prevent SQL injection and XSS attacks
- ❑ Performing code reviews
- ❑ Implementing role-based access controls (RBAC)
- ❑ Conducting regular security assessments & penetration testing
- ❑ Implementing secure authentication and access controls

Cyber Security Layers (cont.)

4. Endpoint Security – Endpoint security focuses on protecting individual devices (endpoints) such as laptops, desktops, smartphones, and tablets that connect to a network, and other network-connected devices from cyber threats, ensuring threats do not spread from compromised endpoints.

Purpose:

- Secure access points to prevent malware, unauthorized access, data breaches & threats from spreading across the network
- Monitor, detect, and block malicious activities on endpoint devices
- Safeguard connections between devices and the network through endpoint protection
- Prevent endpoints from becoming entry points for threats

Key Measures:

- Antivirus & Anti-malware Software
- Endpoint Detection and Response (EDR) Tools
- Device Management Policies
- Web Content Filtering & Application Controls
- Endpoint Encryption

Security Strategy:

- Ensure all endpoints & network-connected devices are monitored and secured
- Use EDR solutions to monitor, detect and respond to threats in real-time
- Use encryption and access controls to ensure safe device environments & operations
- Enforce policies for secure device usage, encryption to protect data and regular updates

Cyber Security Layers (cont.)

5. Network Security – Network security focuses on protecting an organization's network infrastructure and data flow from unauthorized access, misuse, disruption and cyber threats.

Purpose:

- Manage and secure communication between devices, systems and applications
- Prevent unauthorized access, monitor traffic and mitigate internal/external threats
- Secure communication between devices Control and monitor access within the network
- Prevent interception, disruption, or manipulation of data
- Prevent unauthorized access Enforce control over user and device access within the network

Key Measures:

- Firewalls & Intrusion Detection/Prevention Systems (IDS/IPS)
- Network Segmentation
- Access Control & Least Privilege Policy
- Secure Protocols (e.g., HTTPS, VPNs)
- Network Traffic Monitoring & Analysis
- Minimum User Privilege (Least Access Principle)

Security Strategy:

- Apply the principle of least privilege to users and devices - limit internal movement to only what's necessary
- Segment networks to isolate sensitive assets/systems
- Use automated tools to detect, block, and respond to threats in real-time
- Use encryption and secure protocols to protect data in transit
- Continuously monitor and analyze network traffic for anomalies and intrusions
- Implement policies to define and enforce secure network behavior

Cyber Security Layers (cont.)

6. Perimeter Security – Perimeter security protects the boundary of an organization's network, preventing unauthorized access from external sources through physical and digital controls.

Purpose:

- Act as the first line of defense against external threats
- Control incoming and outgoing network traffic
- Secure devices and data at the network edge

Key Measures:

- Firewalls (Hardware/Software)
- Intrusion Detection/Prevention Systems (IDS/IPS)
- VPNs for Secure Remote Access
- Data Encryption
- Antivirus Software & Device Management
- Network Access Control (NAC)

Security Strategy:

- Define and secure the network perimeter
- Filter traffic based on security policies
- Monitor data flow across gateways and external-facing devices
- Enforce encryption and access control on all edge points

Cyber Security Layers (cont.)

7: The Human Layer – The human layer focuses on the people within an organization—employees, contractors, and users—who can be both a vulnerability and a line of defense in cybersecurity depending on their awareness and actions.

Why It Matters:
Humans are the most common entry point for cyber threats like phishing, social engineering, and insider threats. Over 90% of data breaches involve human error. Humans are the most vulnerable link in cybersecurity, responsible for the majority of breaches.

Key Security Measures/Controls:

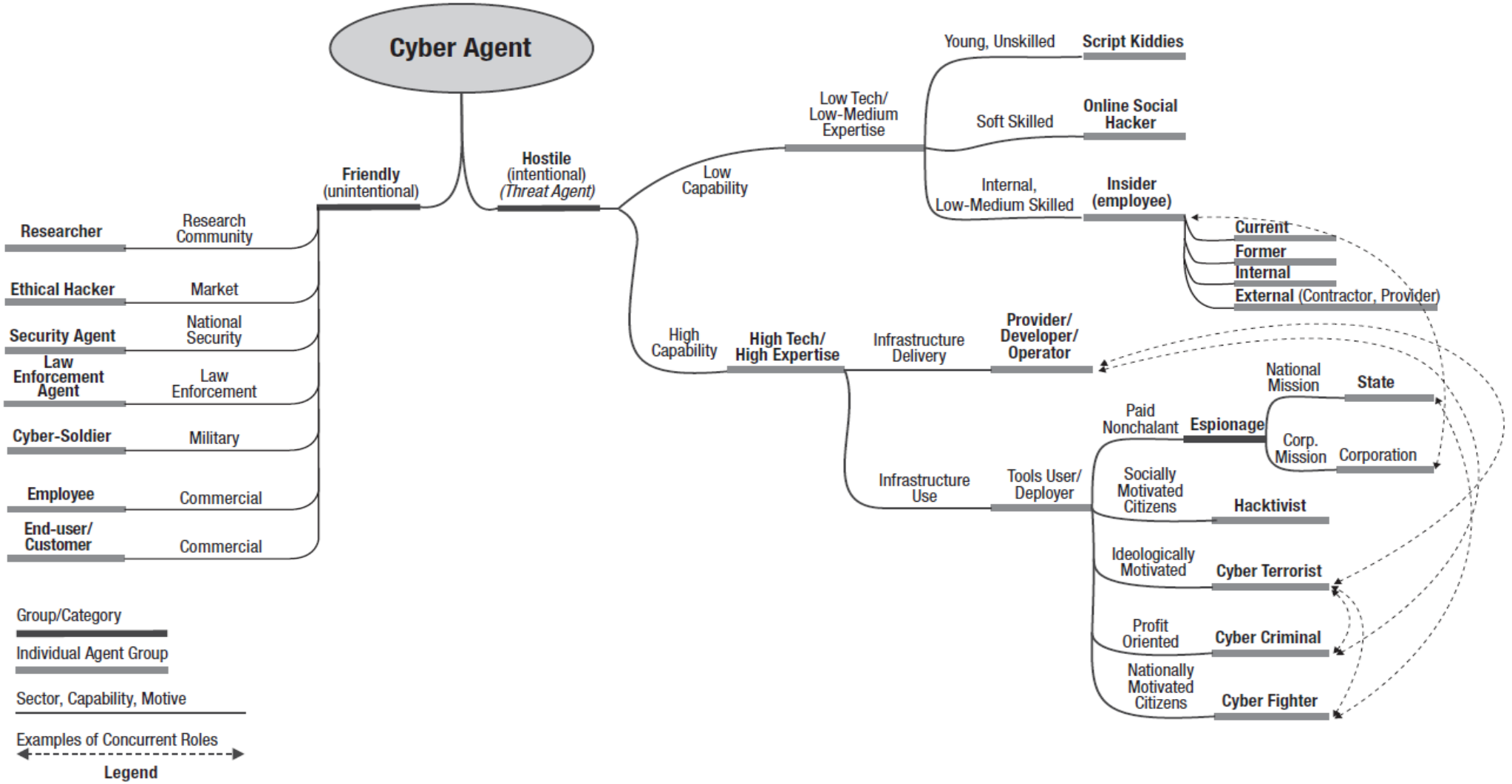
- Security Awareness Training
- Phishing Simulations
- Training on identifying phishing and social engineering attacks
- Clear Security Policies and Guidelines
- Defined procedures for handling sensitive data
- Strong Password Protocols, Policies & MFA
- Access Management Controls
- Incident/ suspicious activities Reporting Procedures

Security Strategy:

- Educate & encourage employees on cyber threats, identifying and reporting suspicious activity
- Regularly train employees to recognize phishing, social engineering attacks and safe practices
- Promote a culture of cybersecurity awareness
- Enforce strong password hygiene and access control policies, MFA
- Limit access to sensitive systems based on roles

THIS PAGE INTENTIONALLY LEFT BLANK

Cyber Actors & Vectors



Source: Marinos, Louis, A. Belmonte, E. Rekleitis, "ENISA Threat Landscape 2015," ENISA, January 2016, Greece

Cyber Attacks – Categories

1) Active Attack

Examples:

- Masquerade
- Session replay
- Message modification
- denial of service (DoS)/ distributed denial-of-service (DDoS)

2) Passive Attack

Examples:

- Eavesdropping
- Traffic analysis
- Malware attack

Cyber Attacks – Categories (other way)

1) Web-based attacks

Examples:

- Injection attacks
- DNS Spoofing
- Session Hijacking
- Phishing
- Brute force
- DOS
- MITM

2) System-based attacks

Examples:

- Virus/Malware
- Worm
- Trojan horse
- Bots

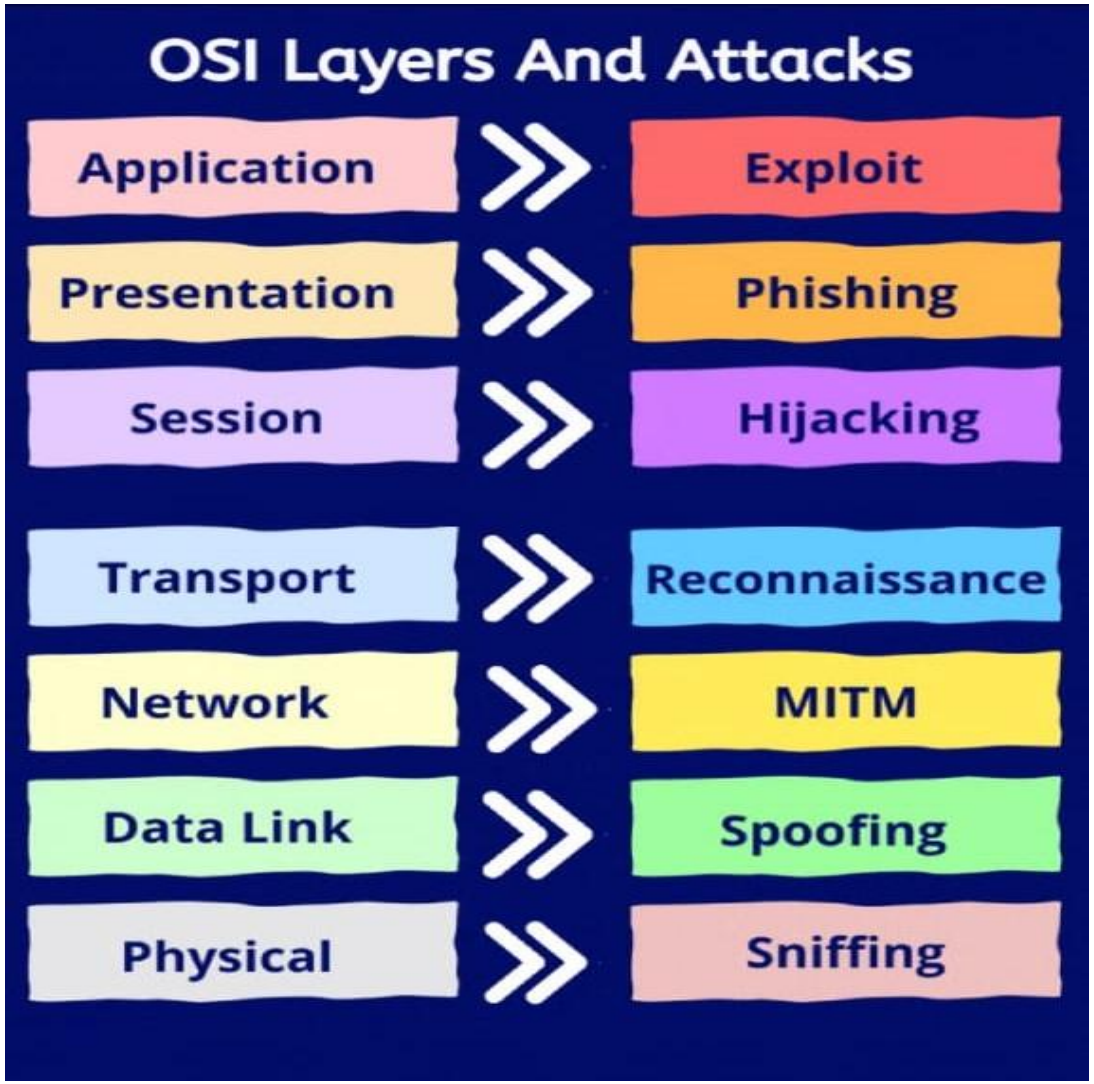
Cyber Attacks – CIA Wise

Confidentiality: Brute-force Attack

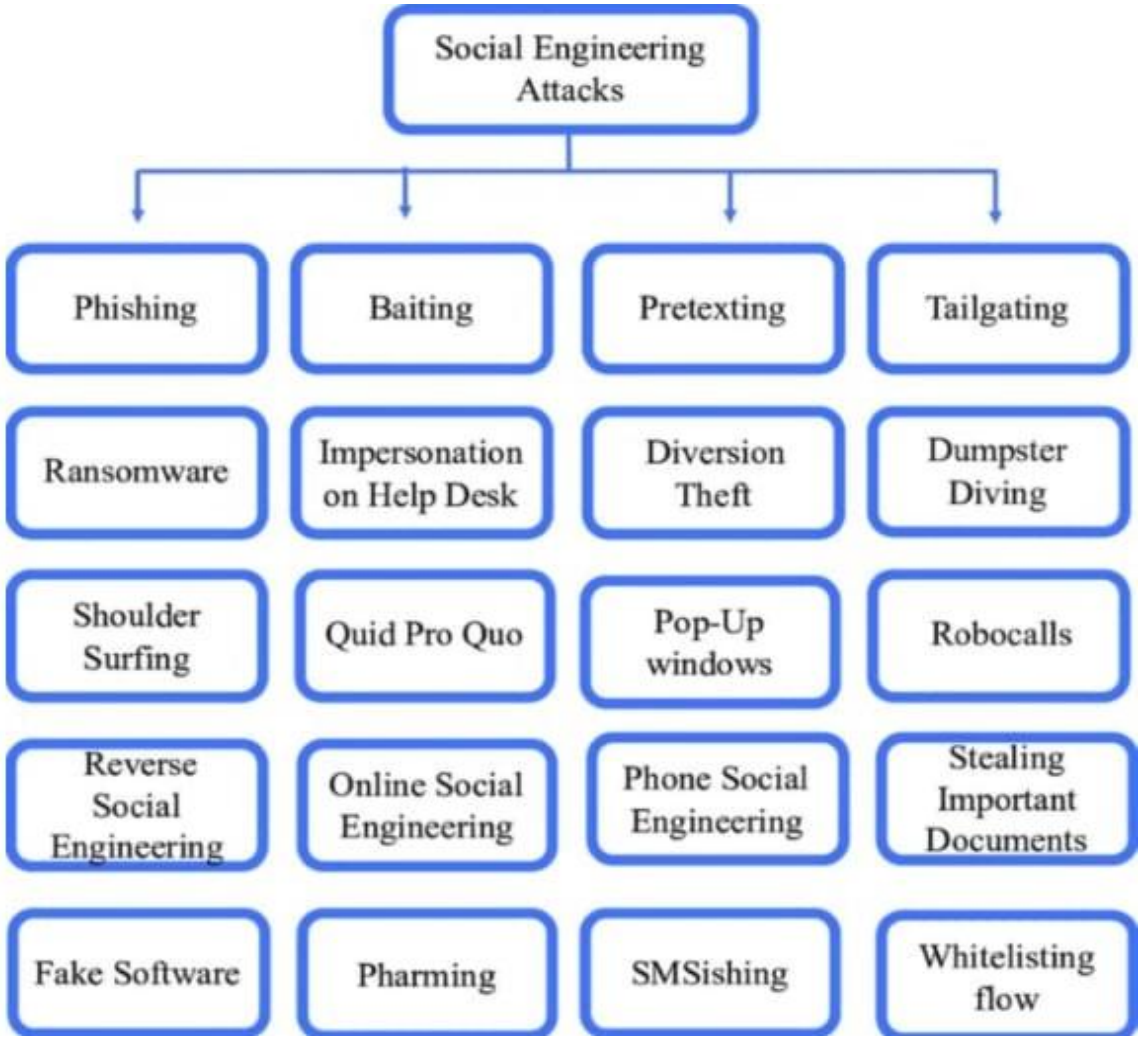
Integrity: Man in the Middle Attack

Availability: DOS/DDOS Attack

Cyber Attacks – OSI Layer Wise



Cyber Attacks – Social Engineering Types



Cyber Attacks – Domain Wise

- Malware
- Man In The Middle (MITM)
- Phishing
- DOS/DDOS
- Password Attacks
- Drive-by Download
- SQL Injection
- Cross-site Scripting (XSS)
- DNS Tunneling, DNS Poisoning
- IoT Attacks

Cyber Attack – Malware

Malware, also called malicious software/code, is designed to gain access to targeted computer systems, steal information or disrupt computer operations. Malware is often created by teams of hackers. Malware is one of the most common attack vectors used by adversaries/hackers.

Cyber Attack – Ransomware

Ransomware—also called “hostage code,” a class of extortive malware that locks or encrypts data or functions and demands a payment to unlock them.

This is the biggest cybersecurity threat and is happening very frequently in the whole world.
It may be spread through email, internet, falsified update of system, compromised auto update of the system, etc.

Phishing

The use of phishing attacks to target individuals, entire departments and even companies is a significant threat that the security professional needs to be aware of and be prepared to defend against. Countless variations on the basic phishing attack have been developed in recent years, leading to a variety of attacks that are deployed relentlessly against individuals and networks in a never-ending stream of emails, phone calls, spam, instant messages, videos, file attachments and many other delivery mechanisms.

Phishing attacks that attempt to trick highly placed officials or private individuals with sizable assets into authorizing large fund wire transfers to previously unknown entities are known as **whaling** attacks.

Social Engineering

Social engineering is an important part of any security awareness training program for one very simple reason: bad actors know that it works. For the cyberattackers, social engineering is an inexpensive investment with a potentially very high payoff. Social engineering, applied over time, can extract significant insider knowledge about almost any organization or individual.

One of the most important messages to deliver in a security awareness program is an understanding of the threat of social engineering. People need to be reminded of the threat and types of social engineering so that they can recognize and resist a social engineering attack.

Most social engineering techniques are not new. Many have even been taught as basic fieldcraft for espionage agencies and are part of the repertoire of investigative techniques used by real and fictional police detectives. A short list of the tactics that we see across cyberspace currently includes:

- Phone phishing or vishing:
- Pretexting
- Quid pro quo
- Tailgating

Phone phishing or vishing

Using a rogue interactive voice response (IVR) system to re-create a legitimate-sounding copy of a bank or other institution's IVR system. The victim is prompted through a phishing email to call in to the "bank" via a provided phone number to verify information such as account numbers, account access codes or a PIN and to confirm answers to security questions, contact information and addresses. A typical vishing system will reject logins continually, ensuring the victim enters PINs or passwords multiple times, often disclosing several different passwords. More advanced systems may be used to transfer the victim to a human posing as a customer service agent for further questioning.

Pretexting

The human equivalent of phishing, where someone impersonates an authority figure or a trusted individual in an attempt to gain access to your login information. The pretexter may claim to be an IT support worker who is supposed to do maintenance or an investigator performing a company audit. Or they might impersonate a coworker, the police, a tax authority or some other seemingly legitimate person. The goal is to gain access to your computer and information.

Quid pro quo

A request for your password or login credentials in exchange for some compensation, such as a “free gift,” a monetary payment or access to an online game or service. If it sounds too good to be true, it probably is.

Tailgating

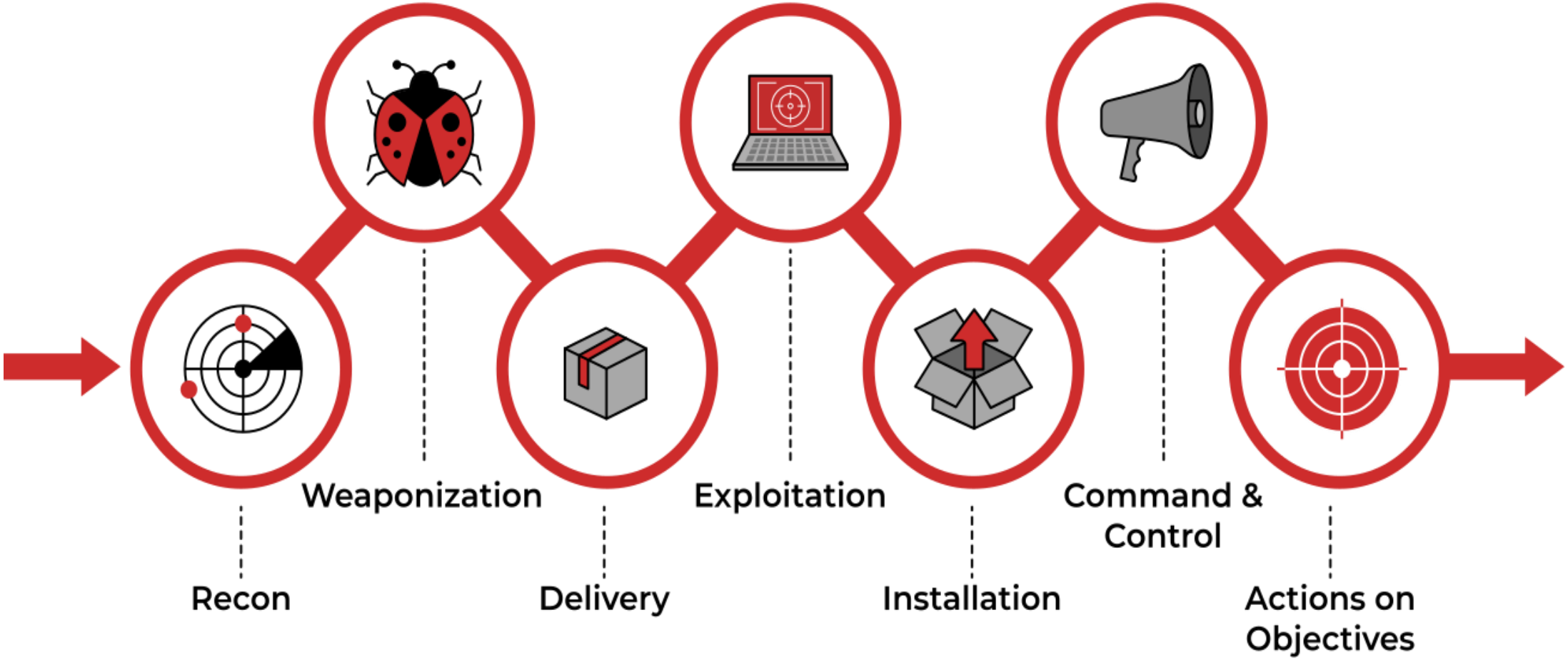
The practice of following an authorized user into a restricted area or system. The low-tech version of tailgating would occur when a stranger asks you to hold the door open behind you because they forgot their company RFID card. In a more sophisticated version, someone may ask to borrow your phone or laptop to perform a simple action when he or she is actually installing malicious software onto your device.

Zero Day Attack

“Cyber-attacks are the number one problem with mankind, even worse than nuclear weapons.”

_Warren Buffet

Cyber Kill Chain



Cyber Security Controls – Common Categories with Examples

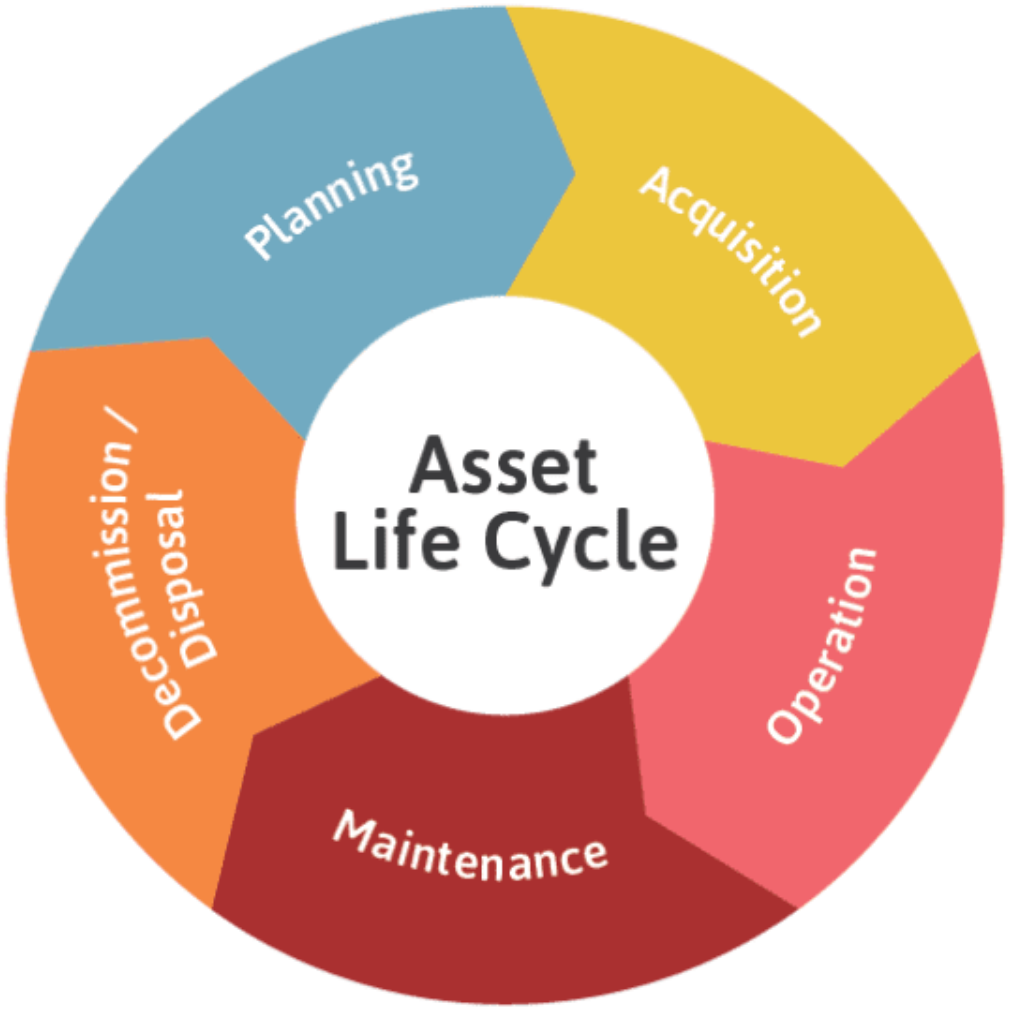
	PREVENTATIVE	DETECTIVE	CORRECTIVE
PHYSICAL CONTROLS	• Fences • Gates • Locks	• CCTV • Surveillance Cameras	• Repair physical damage • Re-issue access cards
TECHNICAL CONTROLS	• Firewall • IPS • MFA • Antivirus	• IDS • Honeypots	• Vulnerability patching • Reboot a system • Quarantine a virus
ADMINISTRATIVE CONTROLS	• Hiring & termination policies • Separation of duties • Data classification	• Review access rights • Audit logs and unauthorized changes	• Implement a business continuity plan • Have an incident response plan

THIS PAGE INTENTIONALLY LEFT BLANK

Asset Lifecycle

Five stages (classic):

1. Planning
2. Acquisition
3. Utilization
4. Maintenance
5. Disposal



Asset Lifecycle Calculation

Straight-line method for calculating depreciation:

- It is simple to calculate.
- It is the most commonly used.

This is calculated by dividing a fixed asset's depreciable base by its useful life. The depreciable base is the difference between an asset's all-in costs and the estimated salvage value/residual value at the end of its useful life.

There is no formula or universal mathematical model to calculate the useful life of an asset. Not least because the useful life of the asset depends on how often it is used, the conditions it is exposed to (humidity, temperature, among others), and the quality of maintenance throughout its useful life.

$$\text{Depreciation} = \frac{\text{Cost} - \text{RV}}{\text{Useful life}}$$

IT Asset Lifecycle Management

- Core process of IT Asset Management (ITAM)
- Comprehensive framework for managing an organization's IT assets throughout their entire lifecycle
- Ensure that organization is running at peak efficiency
- Helps to increase organizational productivity
- Help making informed decisions on IT needs and services
- Reduce costs
- Optimize asset utilization

IT Asset Management

- Inventory
- Classification
- Labeling
- Retention
- Destruction

IT Asset Management (cont.)

Inventory:

Making an inventory, catalog or registry of all the information assets is the first step in any asset management process. You can't protect what you don't know you have.

- ❑ Hardware Assets
- ❑ Subsystem and Software Assets
- ❑ Information Assets
  - Virtual Assets
  - Cloud based Information Assets
  - Customer information
  - Business operations information
  - Intellectual property

An inventory of information and other associated assets, including owners, shall be developed and maintained. In many organizations, this may prove difficult since there is often no comprehensive inventory of information-related assets.

IT Asset Management (cont.)

Classification:

The first step in the classification process is locating and identifying information resources. The identification process will include determining the:

- ✓ location of the data
- ✓ the data owners
- ✓ users and custodians

Classification is the process of recognizing the organizational impacts if the information suffers any security compromises related to its characteristics of confidentiality, integrity and availability. Information is then labeled and handled accordingly. For example:

Highly restricted: Compromise of data with this sensitivity label could possibly put the organization's future existence at risk. Compromise could lead to substantial loss of life, injury or property damage, and the litigation and claims that would follow.

Moderately restricted: Compromise of data with this sensitivity label could lead to loss of temporary competitive advantage, loss of revenue or disruption of planned investments or activities.

Low sensitivity (sometimes called "internal use only"): Compromise of data with this sensitivity label could cause minor disruptions, delays or impacts.

Unrestricted public data: As this data is already published, no harm can come from further dissemination or disclosure.

IT Asset Management (cont.)

Labeling:

Security labels/markings are part of implementing controls to protect classified information. It is reasonable to want a simple way of assigning a level of sensitivity to a data asset, such that the higher the level, the greater the presumed harm to the organization, and thus the greater security protection the data asset requires. This spectrum of needs is useful, but it should not be taken to mean that clear and precise boundaries exist between the use of “low sensitivity” and “moderate sensitivity” labeling.

Retention:

Data should be kept only for as long as it is beneficial, no more and no less. Certain industry standards, laws and regulations define retention periods, when such external requirements are not set, it is an organization’s responsibility to define and implement its own data retention policy.

Data retention policies are applicable both for hard copies and for electronic data, and no data should be kept beyond its required or useful life.

Security professionals should ensure that data destruction is being performed when an asset has reached its retention limit.

IT Asset Management (cont.)

Destruction

This can be done by one of several means:

- **Clearing the device or system**, which usually involves writing multiple patterns of random values throughout all storage media. This is sometimes called “overwriting” or “zeroizing” the system, although writing zeros has the risk that a missed block or storage extent may still contain recoverable, sensitive information after the process is completed.

- **Purging the device or system**, which eliminates (or greatly reduces) the chance that residual physical effects from the writing of the original data values may still be recovered, even after the system is cleared. Some magnetic disk storage technologies, for example, can still have residual “ghosts” of data on their surfaces even after being overwritten multiple times. Magnetic media, for example, can often be altered sufficiently to meet security requirements; in more stringent cases, degaussing may not be sufficient.

- **Physical destruction of the device or system** is the ultimate remedy to data remanence. Magnetic or optical disks and some flash drive technologies may require being mechanically shredded, chopped or broken up, etched in acid or burned; their remains may be buried in protected landfills, in some cases.

IT Asset Management (cont.)

In many routine operational environments, security considerations may accept that clearing a system is sufficient. But when systems elements are to be removed and replaced, either as part of maintenance upgrades or for disposal, purging or destruction may be required to protect sensitive information from being compromised by an attacker.

Data that might be left on media after deleting is known as **remanence** and may be a significant security concern. Steps must be taken to reduce the risk that data remanence could compromise sensitive information to an acceptable level.

THIS PAGE INTENTIONALLY LEFT BLANK

Data Management

Data Management Stages:

1. Data Collection
2. Data Entry
3. Data Access/Usage/Process
4. Data Transfer
5. Data Storing
6. Data Deletion

Data States

Three states:

1. Data at Rest (sometimes called data on storage)
2. Data in Transit (sometimes called data in motion or being communicated)
3. Data in Use (also known as data being processed)

Data States (cont.)

Data at Rest:
Any data stored on media such as system hard drives, solid-state drives (SSDs), external USB drives, storage area networks (SANs), and backup tapes.

Data in Transit:
Any data transmitted over an internal network using wired/wireless methods and data transmitted over public networks such as the internet.

Data in Use:
Data in memory or temporary storage buffers while an application is using it.

Data States (cont.)

Data at Rest:
Strong symmetric encryption protects data at rest.

Data in Transit:
A combination of symmetric and asymmetric encryption protects data in transit.

Data in Use:
Applications often decrypt encrypted data before placing it in memory. This allows the application to work on it, but it's important to flush these buffers when the data is no longer needed. In some cases, it's possible for an application to work on encrypted data using homomorphic encryption. This limits the risk because memory doesn't hold unencrypted data.

Data Handling – Roles & Responsibilities

Multiple people within an organization have different responsibilities for how data is handled, and those responsibilities can be classified by their role. Some of the common roles and responsibilities are

- **Management** Personnel in management and leadership positions define the data classifications and specify the requirements to protect data with different classifications. A data policy or security policy includes these definitions, and management personnel ensure the policy is available to everyone within the organization.
- **Data owner** Data owners have primary responsibility for protecting the data based on its classification and requirements stated within a security policy. When data owners create data, they identify the appropriate classification and mark or label the data according to requirements dictated in the data policy. They periodically review the data and modify the classification if necessary based on changes within the organization.
- **Custodian** In some cases, the data owner delegates various data-related tasks to a data custodian. For example, a data custodian could perform regular backups of the data based on requirements stated within a backup policy.
- **Administrator** Administrators use available access control mechanisms to provide access to the data to personnel that need access. For example, administrators assign permissions to personnel to grant access, typically by direction from the data owner.
- **User** Users access the data. Users are also responsible for protecting the data they handle.

Asset & Data Owner

The data owner (sometimes referred to as the organizational owner or senior manager) is the person who has ultimate organizational responsibility for data.
The owner is typically the chief executive officer (CEO), president, or a department head (DH).
Data owners identify the classification of data and ensure that it is labeled properly. They also ensure that it has adequate security controls based on the classification and the organization's security policy requirements.
Owners may be liable for negligence if they fail to perform due diligence in establishing and enforcing security policies to protect and sustain sensitive data.

Responsibilities of data owner:
■■ Establishes the rules for appropriate use and protection of the subject data/information (rules of behavior)
■■ Provides input to information system owners regarding the security requirements and security controls for the information system(s) where the information resides
■■ Decides who has access to the information system and with what types of privileges or access rights
■■ Assists in the identification and assessment of the common security controls where the information resides

Similarly, senior managers are ultimately responsible for other assets, such as hardware assets.
Consider an IT department that manages servers. The IT department owns these servers, and the senior management in the IT department is responsible for protecting them.

Data Custodian

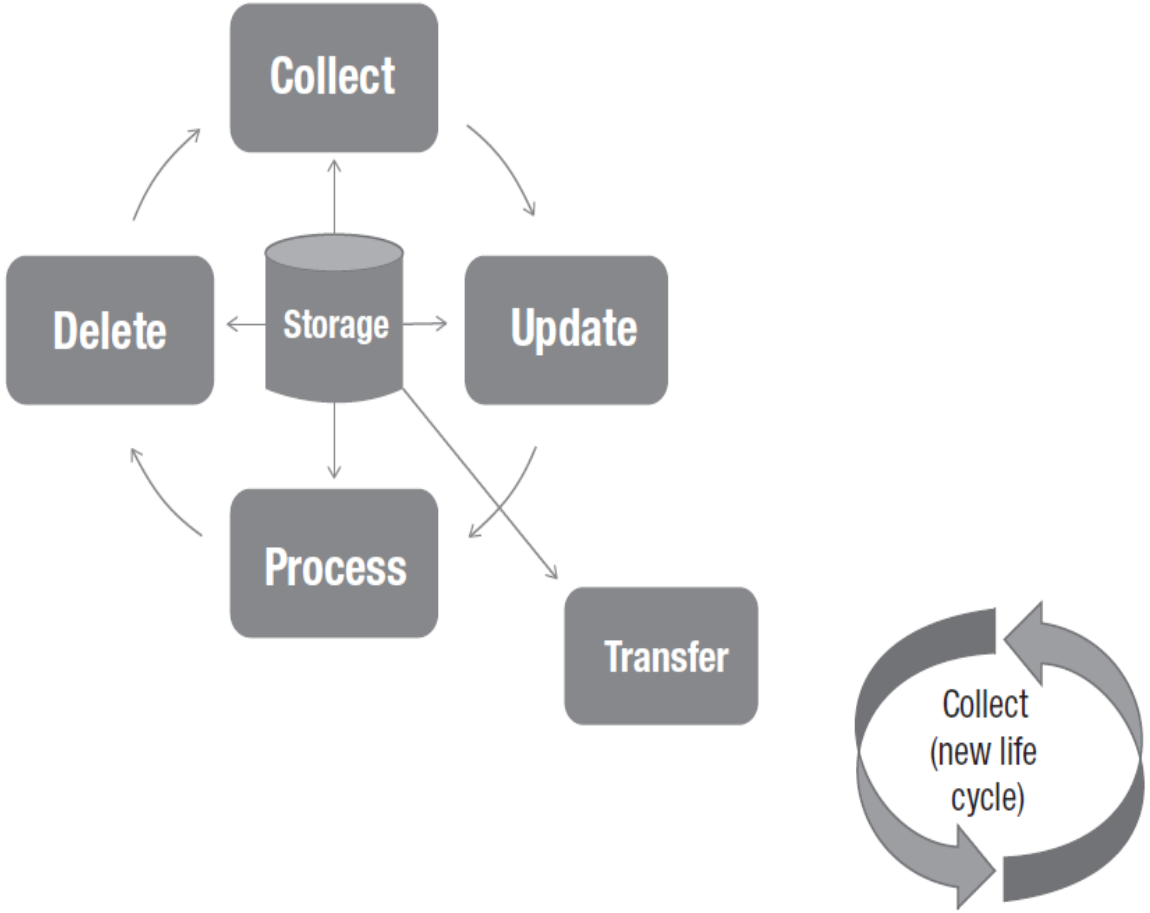
An individual with day-to-day responsibilities (often delegated by data owner) for protecting information asset. In practice, personnel within an IT department or system security administrators would typically be the custodians. They might be the same administrators responsible for assigning permissions to data.

Typical responsibilities include the following:

- Adherence to appropriate and relevant data policies, standards, procedures, baselines and guidelines
- Ensuring accessibility to appropriate users, maintaining appropriate levels of data security
- Fundamental data maintenance, including but not limited to data storage and archiving
- Data documentation, including updates to documentation
- Assurance of quality and validation of any additions to data, including supporting periodic audits to ensure ongoing data integrity

For example, custodians would ensure that the data is backed up and data storage is maintained by following guidelines in a backup policy. If administrators have configured auditing on the data, custodians would also maintain these logs.

Data Life Cycle



Prior to Data Classification

When classifying data, the following requirements should be considered:

- Access and authentication—Determine access requirements including defining users profiles, access approval criteria and validation procedures.
- Confidentiality—Determine where sensitive data are stored and how they are transmitted.
- Privacy—Use controls to warn an affected user that his or her information is about to be used.
- Availability—Determine the uptime and downtime tolerances for different data types.
- Ownership and distribution—Establish procedures to protect data from unauthorized copy and distribution.
- Integrity—Protect data from unauthorized changes using change control procedures and automated monitoring and detection for unauthorized changes and manipulation.
- Data retention—Determine retention periods and preserve specific versions of software, hardware, authentication credentials and encryption keys to ensure availability.
- Auditability—Keep track of access, authorizations, changes and transactions.

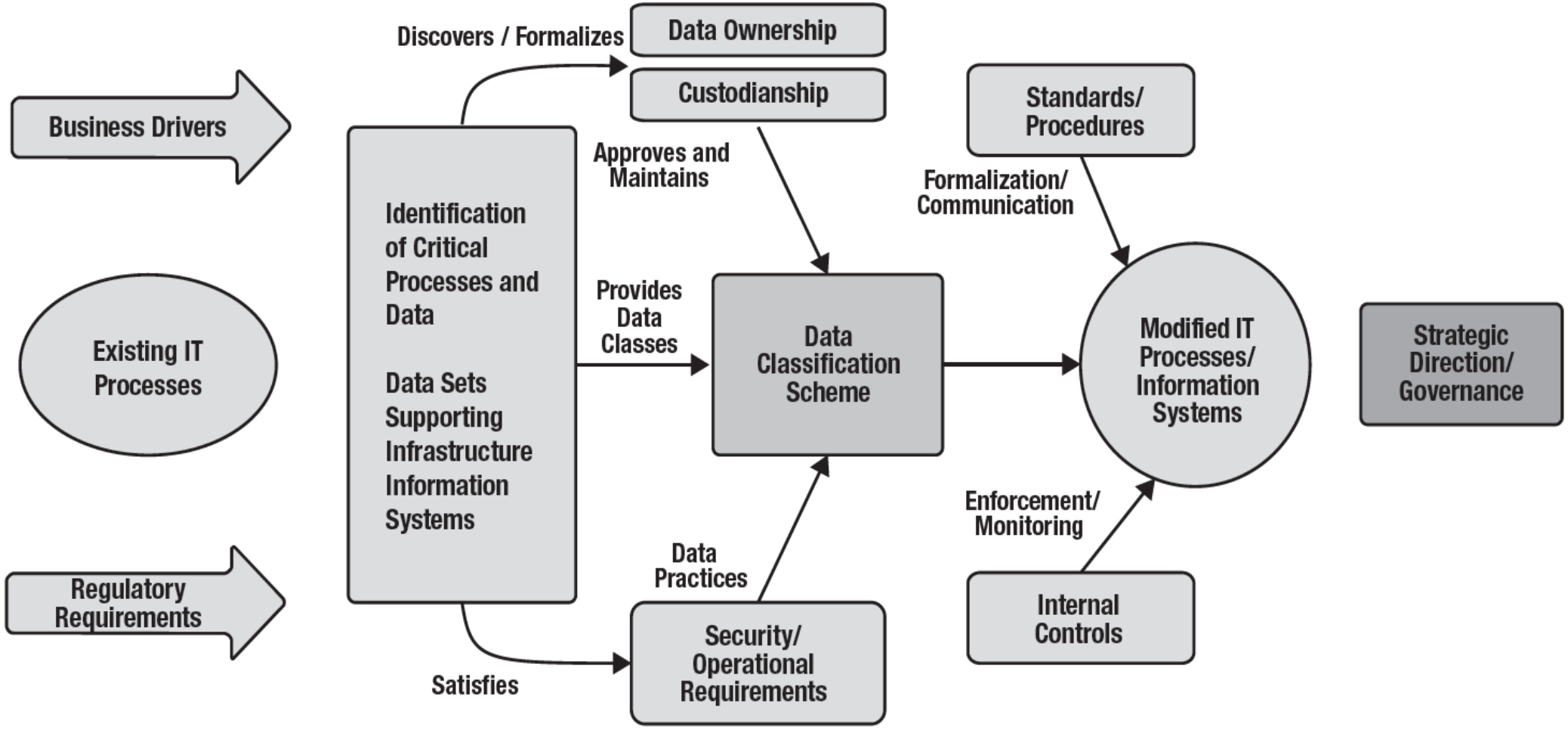
Data Classification – Considerable Items

- How many classification levels are suitable for the organization?
- How will information be located?
- What process is used to determine classification?
- How will classified information be identified?
- How will it be marked?
- How will it be handled?
- How will it be transported?
- How will confidential information be stored and archived?
- What is the life cycle of the information (create, update, retrieve, archive, dispose)?
- What are the processes associated with the various stages in the information asset life cycle?
- How will it be retained according to policy or law?
- How will it be safely destroyed at the end of the retention period?
- Who has ownership of information?
- Who has access rights?
- Who has authority for determining access to the data?
- What approvals are needed for access?

Post to Data Classification

After data classification has been assigned, security controls can be established such as encryption, authentication and logging. Security measures should increase as the level of data sensitivity or criticality increases.

Data Classification Process



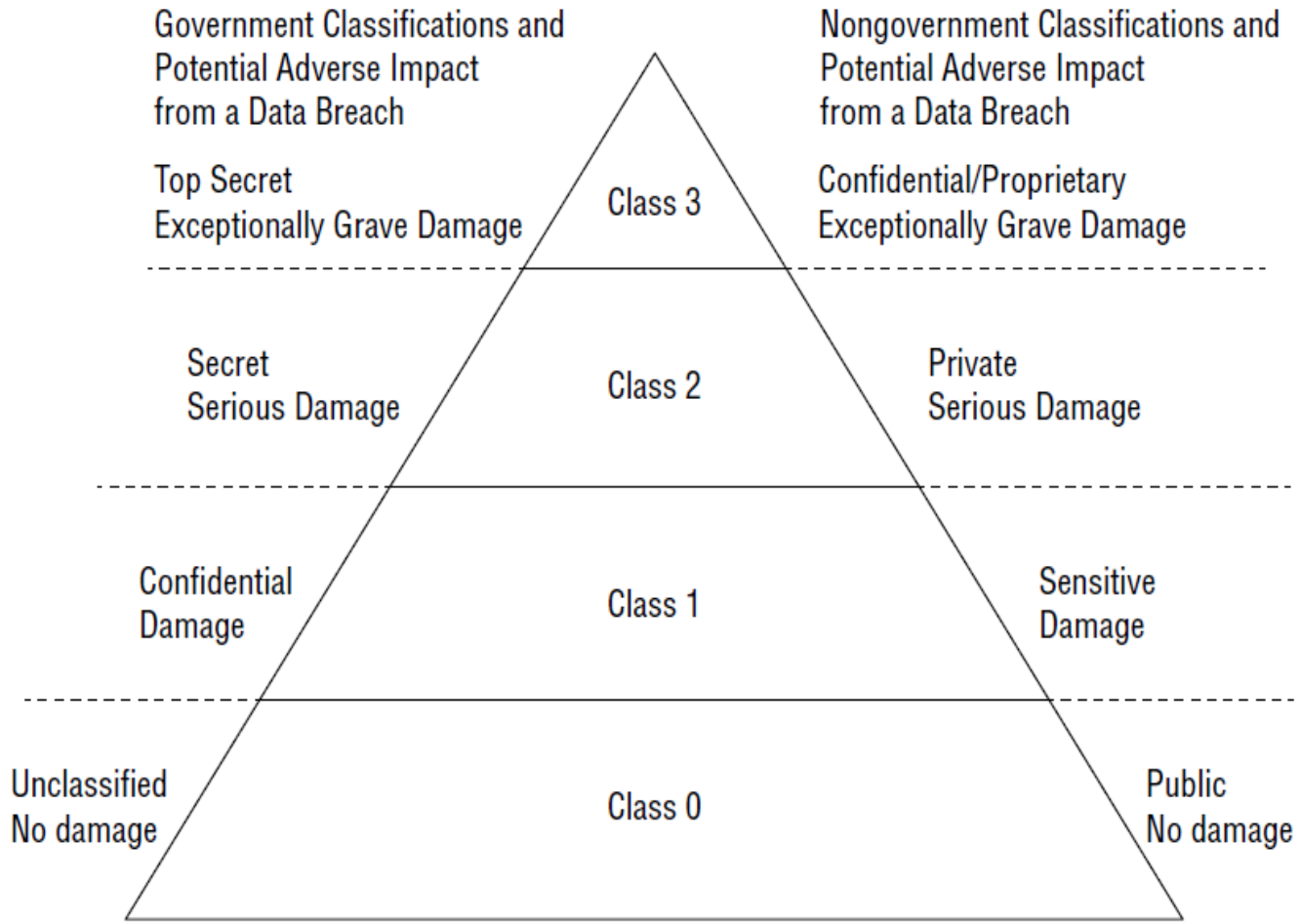
Data Classification – For Military

The U.S. government uses the following classifications for data, from highest to lowest:

- Top Secret
- Secret
- Confidential
- Unclassified

Classification	Definition	Example
Top Secret	If disclosed, it could cause grave damage to national security.	Espionage data, weapon blueprints
Secret	If disclosed, it could cause serious damage to national security.	Troop plans, nuclear facilities
Confidential	Unauthorized disclosure could cause serious effects.	Trade secrets, Health care information, company's competitive information.
Sensitive but Unclassified (SBU)	Minor secret. If disclosed, it could cause serious damage.	Medical data, Answers to test scores
Unclassified	Not sensitive or classified	Job Circular, Recruiting information

Data Classification – Pyramid



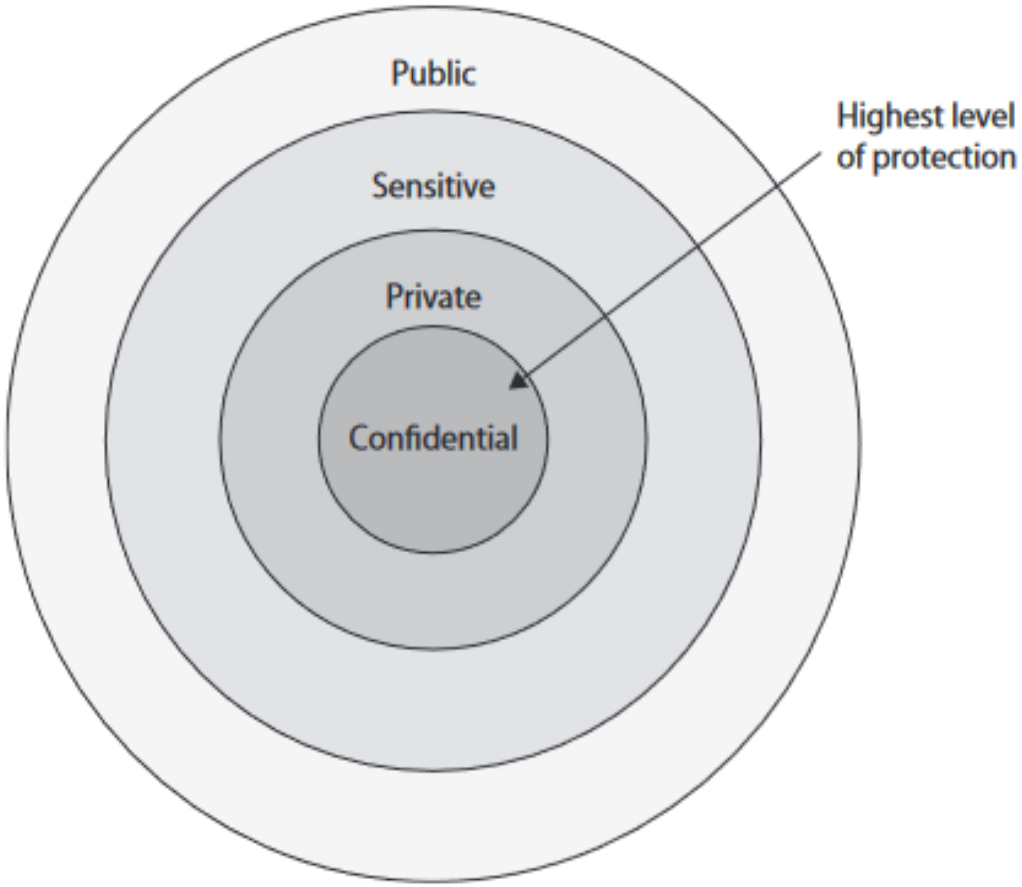
Data Classification – Sample for Non-Military

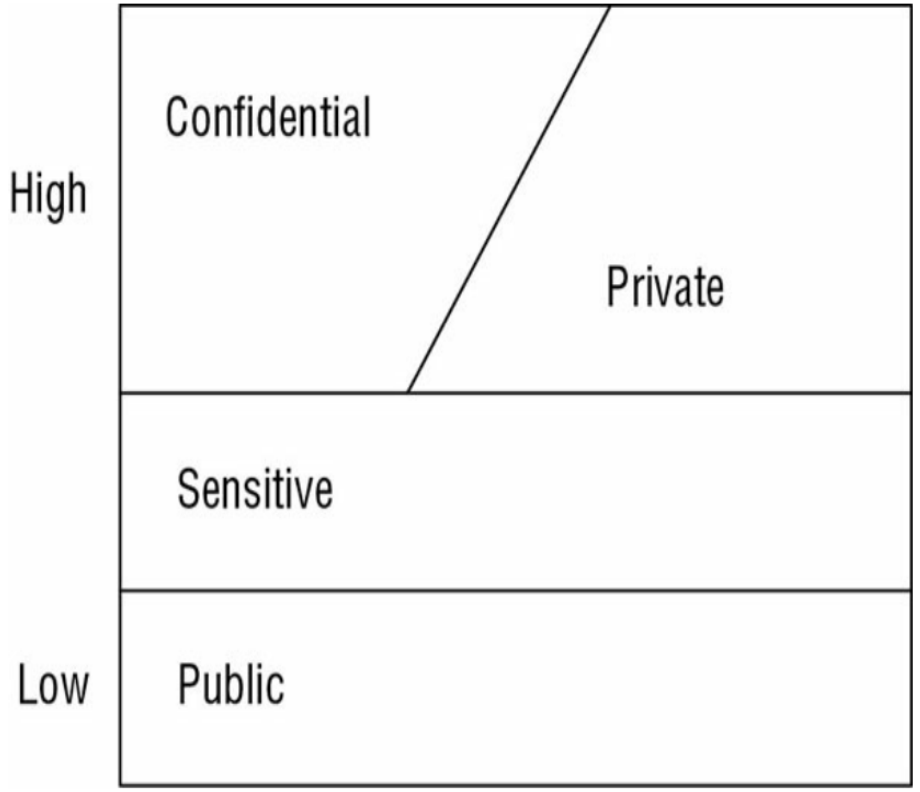
Organizations are free to create classification systems that best meet their own needs. it is typically best if the organization has enough classifications to distinguish between sets of assets with differing sensitivity/value, but not so many classifications that the distinction between them is confusing to individuals. Typically, two or three classifications are manageable, and more than four tend to be difficult.

An organization may classify information as per below 4 layers:

a. Restricted (only senior management have access)
b. Confidential (employees with designated roles have access)
c. Internal (all employees have access)
d. Public information (everyone has access)

Data Classification – Sensitivity & Population Circle





Data Classification – Definitions

Classification	Definition	Examples	Organization That Would Use This
Public	• Disclosure is not welcome, but it would not cause an adverse impact to the company or personnel.	• How many people are working on a specific project • Upcoming projects	Commercial business
Sensitive	• Requires special precautions to ensure the integrity and confidentiality of the data by protecting it from unauthorized modification or deletion. • Requires higher than normal assurance of accuracy & completeness.	• Financial information • Details of projects • Profit earnings and forecasts	Commercial business
Private	• Personal information for use within a company. • Unauthorized disclosure could adversely affect personnel or company	• Work history • Human resources information • Medical information	Commercial business
Confidential	• For use within the company only. • Data that is exempt from disclosure under the Freedom of Information Act or other laws and regulations. • Unauthorized disclosure could seriously affect a company.	• Trade secrets • Health care information • Programming code • Information that keeps a company competitive	Commercial business/Military
Unclassified	• Data is not sensitive or classified.	• Computer manual and warranty information • Recruiting information	Military
Sensitive but Unclassified (SBU)	• Minor secret. • If disclosed, it could cause serious damage.	• Medical data • Answers to test scores	Military
Secret	• If disclosed, it could cause serious damage to national security.	• Deployment plans for troops • Nuclear bomb placement	Military
Top secret	• If disclosed, it could cause grave damage to national security.	• Blueprints of new wartime weapons • Spy satellite information • Espionage data	Military

THIS PAGE INTENTIONALLY LEFT BLANK

Access Control – Subject

(Who)

A subject can be defined as any entity that requests access to our assets. The entity requesting access may be a user, a client, a process or a program, for example. A subject is the initiator of a request for service; therefore, a subject is referred to as “active.”

A subject:

- Is a user, a process, a procedure, a client (or a server), a program, a device such as an endpoint, workstation, smartphone or removable storage device with onboard firmware.
- Is active: It initiates a request for access to resources or services.
- Requests a service from an object.
- Should have a level of clearance (permissions) that relates to its ability to successfully access services or resources.

Access Control – Object

(What)
Anything that a subject attempts to access is referred to as an object. An object is a device, process, person, user, program, server, client or other entity that responds to a request for service.

Whereas a subject is active in that it initiates a request for a service, an object is passive in that it takes no action until called upon by a subject. When requested, an object will respond to the request it receives, and if the request is wrong, the response will probably not be what the subject really wanted either.

Note that by definition, objects do not contain their own access control logic. Objects are **passive**, not active (in access control terms), and must be protected from unauthorized access by some other layers of functionality in the system, such as the integrated identity and access management system.
An object has an owner, and the owner has the right to determine who or what should be allowed access to their object. Quite often the rules of access are recorded in a rule base or access control list.
An object:

- Is a building, a computer, a file, a database, a printer or scanner, a server, a communications resource, a block of memory, an input/output port, a person, a software task, thread or process.
- Is anything that provides service to a user.
- Is passive.
- Responds to a request.
- May have a classification.

Access Control – Rules

(How and When)

An access rule is an instruction developed to allow or deny access to an object by comparing the validated identity of the subject to an access control list. One example of a rule is a firewall access control list. By default, firewalls deny access from any address to any address, on any port. For a firewall to be useful, however, it needs more rules.

A rule might be added to allow access from the inside network to the outside network. Here we are describing a rule that allows access to the object “outside network” by the subject having the address “inside network.” In another example, when a user (subject) attempts to access a file (object), a rule validates the level of access, if any, the user should have to that file. To do this, the rule will contain or reference a set of attributes that define what level of access has been determined to be appropriate.

A rule can:

- Compare multiple attributes to determine appropriate access.
- Allow access to an object.
- Define how much access is allowed.
- Deny access to an object.
- Apply time-based access.

Access Controls – Physical

Examples of physical access controls:

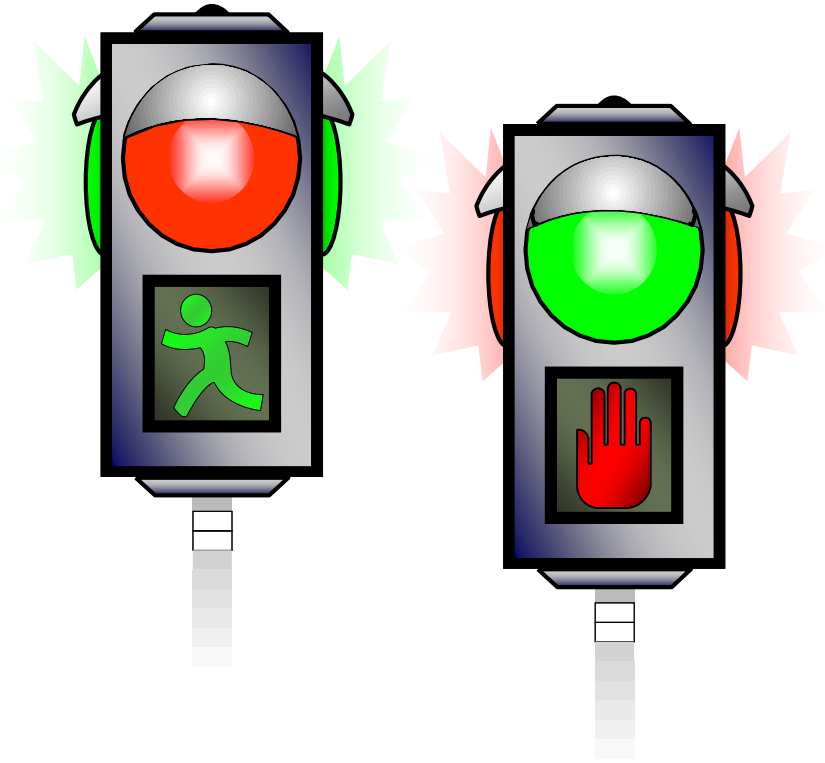
- Security guards
- Fences
- Motion detectors
- Locked doors/gates
- Sealed windows
- Lights
- Cable protection
- Laptop locks
- Badges
- Swipe cards
- Guard dogs
- Cameras
- Mantraps/turnstiles
- Alarms

Access Controls – Logical

Access control model is a framework that details how the system operates.
Common models are:

- ❑ Discretionary Access Control (DAC)
  - Identity-based access control

- ❑ Non-Discretionary Access Control (Non-DAC)
  - Mandatory Access Control (MAC)
  - Role Based Access Control (RBAC)
  - Rule-Based Access Control (RuBAC)
  - Attribute-Based Access Control (ABAC)
  - Risk-based Access Control (RAC)



DAC

Discretionary access control (DAC) allows the owner, creator, or data custodian of an object to control and define access to that object. All objects have owners, owners have full control over the objects and access control is based on the discretion or decision of the owner.

- DAC model is implemented using access control lists (ACLs) on objects.
- DAC model is very flexible, scalable and access to objects is easy to change.
- DAC model does not offer centrally controlled management system.
- Most information systems in the world are DAC systems.

For example, if a user creates a new spreadsheet file, that user is both the creator of the file and the owner of the file. As the owner, the user can modify the permissions of the file to grant or deny access to other users.

The New Technology File System (NTFS), used on Microsoft Windows operating systems, uses the DAC model to manage files and folders. The whole Unix family tree (including Linux) and iOS, use this type of data structure to make fast, accurate decisions about authorizing or denying an access request.

Non-DAC

In non-Discretionary Access Control (non-DAC) models, security administrators centrally control the access granted to users and can make changes that affect the entire environment.

Static Non-DAC:

- Multi Level Security (MLS)
- Attribute-Based Access Control (ABAC)
- Role Based Access Control (RBAC)

Dynamic Non-DAC:

- Separation of duty (SOD)

✓Non-DAC systems are centrally controlled and easier to manage (although less flexible).
✓Access does not focus on user identity.
Some operating systems implement non-DAC models for system file access. This prevents malware from taking ownership of any critical or sensitive system files or modifying permissions on any of these files. Users still own and manage their own files using DAC, but the non-DAC model methods protect system files.

MAC

A mandatory access control (MAC) policy is one that is uniformly enforced across all subjects and objects within the boundary of an information system. In simplest terms, this means that only properly designated security administrators, as trusted subjects, can modify any of the security rules that are established for subjects and objects within the system.

- ✓In MAC, it is mandatory for security administrators to assign access rights or permissions
- ✓MAC is the use of labels applied to both subjects and objects
- ✓MAC relies on the use of classification labels
- ✓MAC enforces the need to know principle
- ✓MAC is prohibitive rather than permissive, and it uses an implicit deny philosophy
- ✓MAC is more secure than the DAC model, but it isn't as flexible or scalable

Although MAC sounds similar to DAC, the primary difference is who can control access. With MAC, it is mandatory for security administrators to assign access rights or permissions; with DAC, it is up to the object owner's discretion.

For example, the U.S. military uses the labels Top Secret, Secret, and Confidential to classify data. Administrators can grant access to Top Secret data to users with Top Secret **clearances**. However, administrators cannot grant access to Top Secret data to users with lower-level clearances such as Secret and Confidential.

RBAC

Role-Based Access Control (RBAC), as the name suggests, sets up user permissions based on roles. Each role represents users with similar or identical permissions.

RBAC model is the use of roles or groups. Instead of assigning permissions directly to users, user accounts are placed in roles and administrators assign privileges to the roles. These roles are typically identified by job functions. If a user account is in a role, the user has all the privileges assigned to the role.

- ✓ RBAC enforce the principle of least privilege by preventing privilege creep.
- ✓ RBAC is useful in dynamic environments with frequent personnel changes because administrators can easily grant multiple permissions simply by adding a new user into the appropriate role.
- ✓ Many applications use the RBAC model because the roles reduce the overall labor cost of maintaining the application.

Microsoft operating systems implement RBAC with the use of groups. Some groups, such as the local Administrators group, are predefined. However, administrators can create additional groups to match the job functions or roles used in an organization.

RuBAC

A rule-based access control model uses a set of rules, restrictions, or filters to determine what can and cannot occur on a system.

✓A key characteristic of the rule-based access control model is that it applies global rules to all subjects.

✓Administrators create rules that determine access to resources.

One common example of a rule-based access control model is a firewall. Firewalls include a set of rules or filters within an ACL, defined by an administrator. The firewall examines all the traffic going through it and only allows traffic that meets one of the rules.

ABAC

Attribute based Access Control (ABAC) is a more sophisticated type of Rule-based Access Control. It evaluates subject and object attributes, and grants access through the use of policies which combine attributes together. The policies can use any type of attributes (user attributes, resource attributes, environment attribute etc.

ABAC characteristics:

- use policies that can include multiple attributes for rules.
- more flexible than a rule-based access control model
- allows administrators to create rules within a policy using plain language statements such as "Allow Managers to access the WAN using a mobile device."

Many software-defined networks (SDNs) use the ABAC model.

Access Control Models - Differences

Factors	DAC	MAC	RBAC	ABAC
Access Control to Information	Through owner of data	Through fixed rules	Through roles	Through attributes
Access Control Based on	Discretion of owner of data	Classification of users and data	Classification of roles	Evaluation of attributes
Flexibility for Accessing Information	High	Low	High	Very high
Access Revocation Complexity	Very complex	Very easy	Very easy	Very easy
Support for Multilevel Database System	No	Yes	Yes	Yes
Used in	Initial Unix system	The U.S. department of defense	ATLAS experiment in CERN	The Federal government

THIS PAGE INTENTIONALLY LEFT BLANK

Common Security Architecture Flaws and Issues

No security architecture is totally secure. Every computer system has weaknesses and vulnerabilities.

Common flaws are:

- Covert channels
- Design/coding flaws
- Rootkits
- Incremental attacks

Covert Channel

It is an unknown, unexpected, unauthorized, not designed (at least not by the original system designers), unmonitored, and uncontrolled method of data transfer.

Overt Channel:
It is a known, expected, authorized, designed, monitored, and controlled method of communication.

Covert Timing Channel

It conveys information by altering the performance of a system component or modifying a resource's timing in a predictable manner. Using a covert timing channel is generally a method to secretly transfer data and is very difficult to detect.

■■ Blinking a light visible outside the building so that if a reading is taken every two seconds when the light is on count it as a 1 and when the light is off count it as a 0. With an external camera linked to a recording system, a slow transmission of binary data can occur.
■■ Using a microphone to listen to the noise occurring in an area or related to a computer system. Then modify a case fan to spin faster (for a 1) or slower (for a 0) to force a change in the noise generated every 10 seconds.
■■ Monitoring utilization levels of an internet connection when an insider is artificially padding or restricting traffic every 30 seconds. When traffic is above 80 percent utilization, record a 1; when below 40 percent utilization, record a 0.

Covert Shortage Channel

It conveys information by writing data to a common storage area where another process can read it. When assessing the security of software, be diligent for any process that writes to any area of memory that another process can read.

■■ Writing data into **unallocated or unpartitioned space**, which may be accomplished using a hex editor
■■ Writing data directly into a **bad sector** of an HDD or a bad block on an SSD
■■ Writing data into the unused space at the end of a cluster, an area known as slack space
■■ Writing data directly into sectors or clusters without proper registration with the directory system, file container, or header

Design or Coding Flaws

Certain attacks may result from poor design techniques, questionable implementation practices and procedures, or poor or inadequate testing. Some attacks may result from deliberate design decisions when special points of entry, built into code to circumvent access controls, login, or other security checks often added to code while under development, are not removed when that code is put into production.

Rootkits

A rootkit is malware that embeds itself deep within an OS. The term is a derivative of the concept of rooting and a utility kit of hacking tools. Rooting is gaining total or full control over a system.
A rootkit can manipulate information seen by the OS and displayed to users. A rootkit may replace the OS kernel, shim itself under the kernel, replace device drivers, or infiltrate application libraries so that whatever information it feeds to or hides from the OS, the OS thinks is normal and acceptable. This allows a rootkit to hide itself from detection, prevent its files from being viewed by file management tools, and prevent its active processes from being viewed by task management or process management tools. Thus, a rootkit is a type of invisibility shield used to hide itself and other malicious tools.

Obviously, the best protection against rootkits is defense (i.e., don't get infected in the first place) rather than response.
There are often no noticeable symptoms or indicators of compromise related to a rootkit infection. In the moments after initial rootkit installation there might be some system sluggishness and unresponsiveness as the rootkit installs itself, but otherwise it will actively mask any symptoms. In some rootkit infections, the initial infector, dropper, or installer of the malware will perform privilege escalation.

A means to potentially detect the presence of a rootkit is to notice when system files, such as device drivers and dynamic-link libraries (DLLs), have a file size and/or hash value change. File hash tracking can be performed manually by an administrator or automatically by HIDSs and system monitoring security tools.

Incremental Attacks

Some forms of attack occur in slow, gradual increments rather than through obvious or recognizable attempts to compromise system security or integrity. Two such forms of incremental attack are data diddling and the salami attack.

Data diddling occurs when an attacker gains access to a system and makes small, random, or incremental changes to data during storage, processing, input, output, or transaction rather than obviously altering file contents or damaging or deleting entire files. Such changes can be difficult to detect unless files and data are protected by encryption or unless some kind of integrity check (such as a checksum or message digest) is routinely performed and applied each time a file is read or written. Encrypted filesystems, file-level encryption techniques, or some form of file monitoring (which includes integrity checks performed by file integrity monitoring [FIM] tools) usually offer adequate guarantees that no data diddling is under way. Data diddling is often considered an attack performed more often by insiders rather than outsiders (external intruders). It should be obvious that since data diddling is an attack that alters data, it is considered an active attack.

Information Security Models

- Bell-LaPadula
- Biba
- Clark-Wilson
- TCSEC
- Brewer and Nash Model
- Goguen–Meseguer Model
- Sutherland Model
- Graham–Denning Model
- Harrison–Ruzzo–Ullman Model

Bell-LaPadula

Bell-LaPadula model was published in 1976 as the first formal information security model.

It was the first mathematical model of a multilevel security policy used to define the concept of a secure state machine and modes of access and outlined rules of access.

In the 1970s, the U.S. military used time-sharing mainframe systems and was concerned about the security of these systems and leakage of classified information. This model was developed to address these concerns.

Its development was funded by the U.S. government to provide a framework for computer systems that would be used to store and process sensitive information.

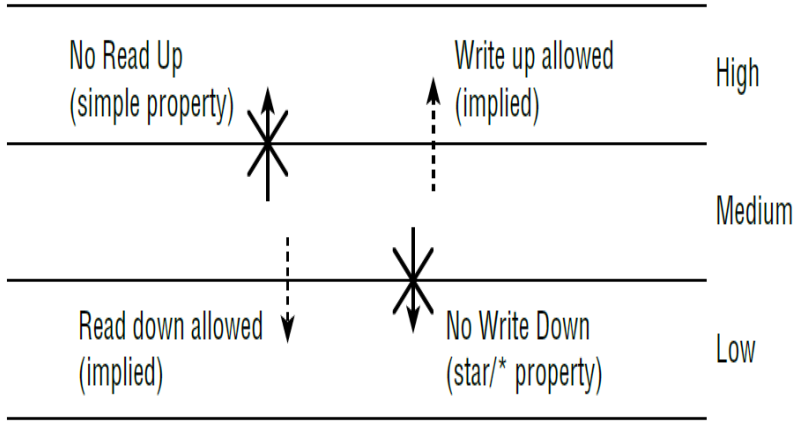
Example:

how you (subject) could read a data element (object) from a specific database and write data into that database.

Bell-LaPadula

The Bell-LaPadula model is used to provide confidentiality.
Three main rules are used and enforced in the Bell-LaPadula model:

- the simple security rule
- the *-property (star property) rule, and
- the strong star property rule



The **simple security rule** states that a subject at a given security level cannot read data that resides at a **higher security level**. For example, if Bob is given the security clearance of secret, this rule states that he cannot read data classified as top secret. If the organization wanted Bob to be able to read top-secret data, it would have given him that clearance in the first place.

The ***-property rule** (star property rule) states that a subject in a given security level cannot write information to a lower security level.
The simple security rule is referred to as the “no read up” rule, and the *-property rule is referred to the as the “no write down” rule.
The third rule, the **strong star property rule**, states that a subject that has read and write capabilities can only perform those functions at the same security level, nothing higher and nothing lower. So, for a subject to be able to read and write to an object, the clearance and classification must be equal.

Biba Model

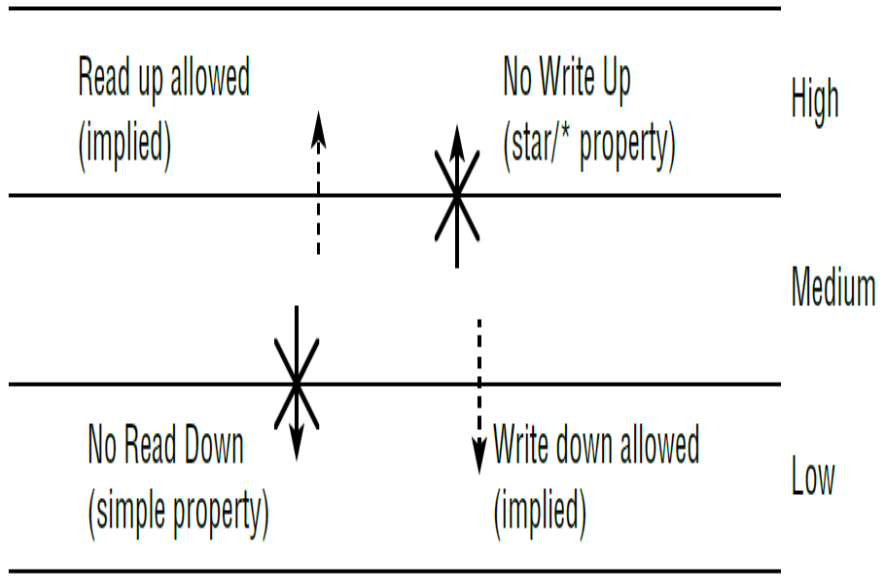
Biba is often known as a reversed version of Bell-LaPadula, as it focuses on integrity labels, rather than sensitivity and data classification. Biba covers integrity levels, which are analogous to sensitivity levels in Bell-LaPadula, and integrity levels cover inappropriate/unauthorized modification of data. Biba requires that all subjects and objects have a classification label.

Biba was designed to address three integrity issues:

- Prevent unauthorized modification of objects by authorized subjects
- Prevent modification of objects by unauthorized subjects
- Protect internal and external object consistency

Biba has two main rules to provide protection:

- **Simple integrity axiom:** A subject cannot read data from an object at a lower integrity level ("no read down").
- ***(star) integrity axiom:** A subject cannot write data to an object at a higher integrity level ("no write up").



Biba Model - Drawbacks

■■ It addresses only integrity, not confidentiality or availability.

■■ It focuses on protecting objects from external threats; it assumes that internal threats are handled programmatically.

■■ It does not address access control management, and it doesn’t provide a way to assign or change an object’s or subject’s classification level.

■■ It does not prevent covert channels.

Bell-LaPadula & Biba Model – Comparisons

- The Bell-LaPadula and Biba models are informational flow models because they are most concerned about data flowing from one level to another.
- Both are built on the state machine and multilevel model and both are very similar.
- Both are written for and derived by US govt./military.

Contras:

- The Bell-LaPadula model is used to provide confidentiality, whereas the Biba model is used to provide integrity.
- Bell-LaPadula was designed to keep secrets, not to protect data integrity. On the other hand, Biba was designed to protect system integrity not to keep secrets.
- The Biba model was developed after the Bell-LaPadula model.
- In both the Biba and Bell–LaPadula models, there are two properties that are inverses of each other: simple and * (star).

Clark-Wilson

Clark-Wilson model addresses data integrity. Clark-Wilson attempts to define a security model based on accepted business practices for transaction processing. Much more real-world-oriented than the other models described, it articulates the concept of well-formed transactions that

- ❑ Perform steps in order
- ❑ Perform exactly the steps listed
- ❑ Authenticate the individuals who perform the steps

The Clark-Wilson model is trying to separate a subject completely from an object in a CDI through the use of an intermediary. This separates duties so the subject cannot access the object directly, as it is not part of the subject's duty.

The principles are the well-formed transaction and separation of duty from beginning to end, but the task should be divided among two or more people to prevent fraud by one person acting alone.

The Clark-Wilson Model deals with two types of objects:

- ✓Constrained data items (CDIs) and
- ✓Unconstrained data items (UDIs)

Clark-Wilson

- Created in 1987
- Differed from previous models as it was developed to be used for commercial activities
- Introduces the concept of triples:
  - Subject
  - Program
  - Object
- Subjects can only manipulate data objects through the use of a defined program
- Set of rules designed to ensure data integrity for all operations
- All changes must be Logged
- Dictates that
  - Separation of duties must be enforced
  - Subjects must access data through an application
  - Auditing is required
- Differs from the Biba model in that subjects are restricted
  - A subject at one level of access can read one set of data while a subject at another level of access has access to a different set of data