Information Security

Threats

The Art of War – Relevance to Information Security
Around 500 B.C., the Chinese military strategist **Sun Tzu** emphasized two core principles:

1. Know yourself
2. Know your enemy

In modern information security, these translate into:

- Know yourself → Understand your organization's:
    - Information assets (data, intellectual property, records)
    - Infrastructure (servers, networks, cloud systems)
    - Applications and services
    - People and access privileges
    - Business processes
- Know your enemy → Understand:
    - Threat actors
    - Attack techniques
    - System vulnerabilities
    - Industry-specific risks

A **threat** is any circumstance, actor, or event that has the potential to exploit a vulnerability and cause harm to an asset.
More formally:
Threat + Vulnerability = Risk
A threat does not cause damage by itself. It becomes dangerous when:

- A vulnerability exists
- An asset is exposed
- Safeguards are weak or absent

Types of Threats :

a. Human Threats (Hackers , Cyber Criminals , Insiders)
b. Technical Threats (Malware , Hardware failures , Software Bugs)
c. Environmental Threats (Fire , Flood)

Information Security

Assets at Risk and How Threats Affect Them

1. People

Threats:

- Social engineering
- Phishing
- Identity theft
- Harassment

Impact:

- Credential compromise
- Psychological harm
- Insider manipulation

2. Applications

Threats:

- Code injection
- Buffer overflow
- API abuse
- Zero-day exploits

Impact:

- Unauthorized access
- Data leakage
- Service disruption

3. Data

Threats:

- Data theft
- Ransomware
- Data corruption
- Unauthorized modification

Impact:

- Financial loss
- Legal liability
- Loss of confidentiality
- Regulatory penalties

4. Hardware

Threats:

- Physical theft
- Device tampering
- Equipment damage
- Sabotage

Impact:

- Downtime
- Loss of stored data
- Replacement costs

5. Network Infrastructure

Threats:

- Distributed Denial of Service (DDoS)
- Routing attacks
- Man-in-the-Middle (MITM)
- DNS poisoning

Impact:

- Connectivity loss
- Traffic interception
- Service outage

6. Organizational Reputation

Threats:

- Public data breaches
- Website defacement
- Regulatory violations
- Intellectual property theft

Impact:

- Loss of customer trust
- Stock value decline
- Legal consequences
- Competitive disadvantage

Information Security

Categories of Threats to Information Security

Category	Examples
Compromises to IP	Piracy, copyright infringement
Software Attacks	Viruses, worms, Denial of Service (DoS)
Quality of Service	ISP outages, power failures, WAN issues
Espionage/Trespass	Unauthorized access, data collection
Forces of Nature	Fire, flood, earthquake
Human Error	Employee mistakes, accidents
Information Extortion	Blackmail, data ransoming
Inadequate Planning	Disk drive failure without a backup/recovery plan
Inadequate Controls	Network compromise due to lack of a firewall
Sabotage/Vandalism	Destruction of systems or data
Theft	Illegal confiscation of equipment/info
Hardware Failure	Equipment breakdown
Software Failure	Bugs, code loopholes
Obsolescence	Using outdated, unsupported technology

Information Security

Deliberate Software Attacks (Malware)

A deliberate software attack occurs when an individual or group intentionally designs and deploys malicious programs to compromise, damage, or disrupt a target system.

Malware is typically engineered to exploit vulnerabilities in operating systems, applications, or user behavior.

These malicious programs are collectively called:

- Malicious code
- Malicious software
- Malware

Primary Objectives of Malware

- Destroy data
- Corrupt systems
- Deny service (DoS)
- Steal information
- Create unauthorized access
- Disrupt operations

Viruses

Viruses are self-replicating programs that attach themselves to other programs or files on host computers. They spread through infected media like songs, videos, or software downloads. Notable examples include file viruses, macro viruses, boot sector viruses, and stealth viruses.

Key Characteristics:

- Self-replicating
- Requires user action (e.g., opening attachment)
- Modifies existing files

Information Security

Common Transmission Methods:

- Email attachments
- Infected USB drives
- Shared files
- Network transfers

Aspect	Virus	Malware
Definition	A type of malicious software	A broader category of harmful software
Behavior	Self-replicating	Can include viruses, worms, trojans, etc.
Spread	Often requires user interaction	Can spread through various methods, including email , downloads, and vulnerabilities
Damage	Can corrupt or delete files	Can cause a range of harm, including data theft, system damage, and spying
Detection	Can be detected by antivirus software	Requires comprehensive security measures and practices
Examples	Morris Worm	WannaCry ransomware , Zeus trojan

Type of Virus	Description
Boot Sector Virus	Attacks the part of the computer that starts up when you turn it on. Boot Sector Virus can also spread through devices like floppy disks. Often called a memory virus.
File Virus	Attaches to the end of a file and modifies how a program starts to run the virus's code first.
Email Virus	Hides in email messages and activates by clicking a link, opening an attachment, or interacting with the email.
Polymorphic Virus	Changes its form every time it installs to avoid detection by antivirus software.
Macro Virus	Activates by running a program capable of executing macros, often found in documents like spreadsheets.

Information Security

Type of Virus	Description
Multipartite Virus	Infects the computer’s boot sector, memory, and files, making it difficult to detect and remove.
Encrypted Virus	Uses encryption to hide from antivirus software, includes a decryption algorithm to run before executing.
Stealth Virus	Modifies detection code, making it very difficult to detect.
Resident Virus	Saves itself in the computer's memory and can infect other files even after the original program stops.
Direct Action Virus	Tied to an executable file, it activates when the file is opened but does not delete files or affect system speed; blocks file access.
Browser Hijacker Virus	Changes browser settings without permission, can redirect to malicious sites.

What is Antivirus?

Antivirus Software is a program that searches for, detects, prevents, and removes software infections that can harm your computer. Antivirus can also detect and remove other dangerous software such as worms, adware, and other dangers. This software is intended to be used as a preventative measure against cyber dangers, keeping them from entering your computer and causing problems. Antivirus is available for free as well. Anti-virus software that is available for free only provides limited virus protection, whereas premium anti-virus software offers more effective security. For example Avast, Kaspersky, etc.

Information Security

Worms

Worms share self-replicating capabilities with viruses but operate independently without attaching to host programs. Their key distinction is network awareness—they can travel between connected computers, typically consuming system resources and slowing performance rather than causing direct damage.

Examples:

- Code Red
- Sircam
- Nimda
- Klez
- MS-Blaster
- MyDoom
- Netsky

Trojan Horses

A Trojan horse is a type of malicious software (malware) that misleads users by disguisedly appearing as legitimate, safe software to gain unauthorized access to a computer system. Unlike viruses, Trojans do not self-replicate but spread via social engineering, enabling hackers to spy, steal data, or install backdoors.

Ransomware

Ransomware is a type of malicious software (malware) that encrypts a victim's data or locks their system, demanding payment (ransom) in exchange for restoring access , Often spread through phishing emails or malicious websites.

Cryptojacking

attackers deploy software on a victim’s device, and begin using their computing resources to generate cryptocurrency, without their knowledge. Affected systems can become slow and cryptojacking kits can affect system stability.

Information Security

Spyware

A malicious actor gains access to an unsuspecting user's data, including sensitive information such as passwords and payment details. Spyware can affect desktop browsers, mobile phones and desktop applications.

Adware

A user's browsing activity is tracked to determine behavior patterns and interests, allowing advertisers to send the user targeted advertising. Adware is related to spyware but does not involve installing software on the user's device and is not necessarily used for malicious purposes, but it can be used without the user's consent and compromise their privacy.

Fileless malware

no software is installed on the operating system. Native files like WMI and PowerShell are edited to enable malicious functions. This stealthy form of attack is difficult to detect (antivirus can't identify it), because the compromised files are recognized as legitimate.

RootKits

Software is injected into applications, firmware, operating system kernels or hypervisors, providing remote administrative access to a computer. The attacker can start the operating system within a compromised environment, gain complete control of the computer and deliver additional malware.

Virus and Worm Hoaxes

Not all virus alerts are real.

A **virus hoax** is:

- A false warning message about a non-existent virus.

Problems caused:

- Panic
- Email flooding
- Productivity loss
- Unnecessary system changes

Users often:

- Forward warning emails widely.
- Overload networks.
- Ignore official reporting procedures.

Deviations in Quality of Service (Availability Threats)

An organization's information system does not operate in isolation. It depends on multiple interdependent support systems, including:

- Power grids
- Telecommunications networks
- Internet Service Providers (ISPs)
- Hardware suppliers
- Cloud vendors
- Service contractors
- Physical facility services (water, waste, custodial staff)

If any of these supporting systems fail or degrade, the organization's availability is affected.

Technical Hardware Failures or Errors

Failures due to manufacturing defects or hardware flaws.

Types of Failures

- Terminal failures (irrecoverable)
- Intermittent failures (sporadic, hard to diagnose)

Technical Software Failures or Errors

Software defects (bugs) that cause:

- Unexpected behavior
- Security vulnerabilities
- System crashes

Causes

- Incomplete testing
- Hardware–software incompatibility
- Programmer shortcuts

Trap Doors (Backdoors)

Hidden access mechanisms that:

- Bypass security checks
- May be intentionally or unintentionally left in code

Security Impact

- Unauthorized access
- Privilege escalation
- Data breach

Technological Obsolescence

Outdated technology increases security risk due to:

- Lack of vendor support
- Unpatched vulnerabilities
- Incompatibility with modern systems

Risks

- Data integrity loss
- Increased attack surface
- Compliance failure

Prevention

- Technology lifecycle management
- Budget allocation for upgrades
- Continuous infrastructure evaluation

Attack and Vulnerability

An **attack** is a deliberate act that exploits a vulnerability in a controlled system to:

- Compromise confidentiality
- Disrupt availability
- Violate integrity
- Steal or damage assets

An attack is carried out by a **threat agent**.

Information Security

Vulnerability

A vulnerability is a weakness in a system where:

- Controls are missing,
- Controls are misconfigured, or
- Controls are ineffective.

Key Difference

- **Threat** → Always present (e.g., possibility of storm).
- **Attack** → Occurs only when the threat is actively exploiting a vulnerability.
- **Vulnerability** → Weakness that enables the attack.

Vector	Description
IP Scan & Attack	Scans IP ranges and exploits known vulnerabilities
Web Browsing	Infects web content; spreads when users visit pages
Virus	Infects executable/script files
Unprotected Shares	Copies itself through open file-sharing systems
Mass Mail	Sends infected emails via address books
SNMP Exploitation	Uses default passwords in network management protocol

Back Doors and Trap Doors

Back Door

A hidden access mechanism allowing attackers to bypass authentication.

Trap Door

Inserted intentionally by programmers and:

- Often excluded from audit logs
- Difficult to detect

Impact:

- Persistent unauthorized access
- Privilege escalation

Information Security

1. Password Attacks

1.1 Password Cracking

- Involves reverse-calculating passwords from stored hashed values.
- Attackers obtain hashed password files (e.g., SAM file).
- They hash guessed passwords using the same algorithm.
- If the generated hash matches the stored hash → password is cracked.
- Common in offline attacks after system compromise.

1.2 Brute Force Attack

- Attempts every possible password combination.
- Uses high computational power.
- Guaranteed success if time and resources are sufficient.
- Highly effective against short or weak passwords.

Characteristics:

- Computationally intensive
- Time-consuming
- Automated using scripts/tools

Defense:

- Account lockout policies
- Limit login attempts
- Strong password requirements
- Change default credentials
- Multi-factor authentication (MFA)

1.3 Dictionary Attack

- Uses a predefined list of common passwords.
- Faster than brute force.
- Exploits predictable human password choices.

Defense:

- Enforce complex password policies
- Require special characters and numbers
- Prevent use of common passwords

- Implement MFA

2. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)

2.1 Denial-of-Service (DoS)

- Attacker floods target system with excessive requests.
- System becomes overloaded.
- Legitimate users cannot access services.
- May cause system crash or severe slowdown.

2.2 Distributed Denial-of-Service (DDoS)

- Large-scale attack from multiple compromised systems.
- Attacker creates a botnet (zombie machines).
- Coordinated traffic flood launched simultaneously.
- Harder to detect and block than DoS.

Process:

1. Attacker compromises many systems.
2. Converts them into bots/zombies.
3. Launches coordinated attack.

Example:

- MyDoom
- Targeted SCO Group website
- Massive DDoS campaign

Impact:

- Service disruption
- Revenue loss
- Brand damage
- Loss of customer trust

⚠ Often called a “weapon of mass disruption” on the Internet.

3. Spoofing (IP Spoofing)

Definition:

- Forging source IP address to appear as a trusted host.

Purpose:

- Bypass authentication filters
- Evade detection
- Impersonate legitimate systems

Method:

- Modify packet headers
- Insert forged IP addresses

Defense:

- Router filtering rules
- Firewalls
- Packet inspection systems
- Strong authentication mechanisms

4. Man-in-the-Middle (MITM) / TCP Hijacking

Definition:

- Attacker intercepts communication between two parties.
- Modifies and forwards altered packets.

Capabilities:

- Eavesdropping
- Message alteration
- Data deletion
- Session hijacking
- Traffic redirection

Advanced MITM:

- Intercepts encryption key exchange.
- Decrypts supposedly secure communication.
- Enables invisible surveillance.

Impact:

- Confidentiality breach
- Data manipulation
- Identity theft
- Financial fraud

Information Security

5. Spam

Definition:

- Unsolicited commercial email sent in bulk.

Effects:

- Wastes bandwidth
- Consumes storage
- Reduces productivity
- Used to deliver malware
- Enables phishing attacks

Example:

- Malware embedded in spam attachments (e.g., MP3 files).

6. Mail Bombing

Definition:

- Flooding a mailbox with massive volumes of email.
- Specialized form of DoS attack.

Methods:

- Exploiting SMTP weaknesses
- Forged email headers
- Using multiple compromised systems

Impact:

- Email server crash
- Storage exhaustion
- Communication disruption
- Service unavailability

7. Sniffers

Definition:

- Programs/devices that monitor network traffic.

Types:

- Legitimate network analyzers
- Unauthorized packet sniffers

What Sniffers Capture:

- Passwords (if sent in plain text)

- Emails
- Documents
- Sensitive application data

Why Dangerous:

- Hard to detect
- Passive operation
- Can be installed silently

Defense:

- Encryption (TLS, HTTPS)
- Secure protocols
- Network segmentation
- Avoid transmitting clear-text data

Social Engineering

Social engineering is the practice of manipulating human psychology rather than technical vulnerabilities to gain unauthorized access to data or systems. As Kevin Mitnick famously noted, **people are the "weakest link"** in security; even the most advanced firewalls cannot stop an employee from voluntarily giving away a password.

Common Tactics & Patterns

- **Authority & Hierarchy:** Attackers often pose as someone higher in the organizational chart (e.g., an executive or the CIO) to intimidate or compel victims into compliance.
- **Information Gathering:** Attackers use "unrelated" data (names of managers, company lingo, or software names) gathered from websites or switchboards to make their false personas more credible.
- **Emotional Manipulation:** Techniques include threatening (fear of firing), cajoling (persuasion), or begging for assistance.

Specific Social Engineering Attacks

Information Security

1. Phishing & Its Variants

Phishing is an attempt to acquire sensitive information by masquerading as a trustworthy entity in electronic communication.

Type	Description
Standard Phishing	Mass-distributed emails (often mimicking banks like Regions or AOL) designed to trick users into clicking links or running malicious "test" programs.
Spear Phishing	A highly targeted attack aimed at a specific individual or small group, often using personal details to appear as a known colleague or employer.
Phone Phishing	Also known as **Pretexting**; the attacker calls the victim directly to extract records (health, financial, employment) by pretending to be a person of authority.

Pharming

Unlike phishing, which relies on a user clicking a bad link, **pharming** redirects legitimate web traffic to a fraudulent site automatically.

- **Methods:** Uses Trojans or worms to alter the browser's address bar or exploits the **Domain Name System (DNS)** via "DNS cache poisoning" to resolve a correct URL to an incorrect IP address.

Timing Attacks

These attacks focus on the browser's local environment:

- **Browser Cache:** Exploring the cache to plant malicious cookies that gather data on how to access protected sites.
- **Cryptography:** Intercepting cryptographic elements to reverse-engineer encryption keys or algorithms.

Information Security

Role of Policy in Information Security

- Information security is primarily a management issue, not just a technical issue.
- Policies form the foundation of all security planning, design, and deployment.
- Policies:
    - Direct how technologies should be used.
    - Define acceptable and unacceptable behavior.
    - Do not describe technical configuration details (these belong in standards and procedures).
- Policies must:
    - Never conflict with laws.
    - Be legally defensible.
    - Be properly administered and enforced.

Definition of Policy

A policy is:

A formal statement from senior management that establishes expectations, rules, and responsibilities.

Policies:

- Support the organization's mission (purpose of the organization).
- Align with the vision (future goals).
- Support strategic planning (roadmap to reach vision).

An Information Security Policy:

Information Security

- Protects confidentiality, integrity, and availability (CIA) of information assets.
- Acts as an organizational law.

Types of Security Policies (According to National Institute of Standards and Technology – SP 800-14)

Management must define three types of security policies:

1. Enterprise Information Security Policy (EISP)

2. Issue-Specific Security Policy (ISSP)

3. Systems-Specific Security Policy (SysSP)

Criteria for Policy Effectiveness (Legal Enforceability)

For a policy to be enforceable, it must include:

✓ Dissemination

- Policy must be distributed to all employees.
- Can be hard copy or electronic.

✓ Review

- Must be readable and understandable.
- Available in multiple languages if needed.

✓ Comprehension

- Organization must prove employees understood the policy.
- Methods: quizzes, assessments.

✓ Compliance

- Employees must formally agree.
- Methods:

- Signed documents
- Logon banners

✓ Uniform Enforcement

- Must apply equally to all employees.
- No discrimination in enforcement.

Enterprise Information Security Policy (EISP)

Definition:

A high-level executive document that sets the strategic direction for security.

Characteristics:

- Usually 2–10 pages.
- Created by senior management (often CIO/CISO).
- Modified only when strategic direction changes.

Key Elements of EISP:

1. Statement of purpose
2. Definition of information security
3. Need for information security
4. Security responsibilities and roles
5. References to other standards and laws
6. Compliance and disciplinary measures

Purpose:

- Establishes overall security philosophy.
- Defines security structure.
- Assigns responsibilities.

Information Security

Issue-Specific Security Policy (ISSP)

Definition:

Policy addressing specific technologies or issues.

Examples:

- E-mail usage
- Internet usage
- Personal device use (BYOD)
- Anti-virus configuration
- Telecommunications usage
- Prohibition of hacking

Characteristics:

- Requires frequent updates.
- Focuses on specific technology or issue.

Approaches to ISSP Creation

1. Independent Documents
    - Separate policy for each issue.
    - May cause inconsistency.
2. Single Comprehensive Policy
    - One large document.
    - Easier management but may overgeneralize.
3. Modular ISSP (Best Approach)
    - Central management.
    - Individual modules for each issue.
    - Balanced and scalable.

Structure of an ISSP

1. Statement of policy (scope, responsibilities)
2. Authorized access and usage
3. Prohibited usage
4. Systems management
5. Violations and penalties
6. Policy review
7. Limitations of liability

Systems-Specific Security Policy (SysSP)

Definition:

Policies related to configuration and operation of systems.

SysSPs function as:

- Standards
- Technical procedures
- Configuration guides

Types of SysSP

1️⃣ Managerial Guidance SysSP

- Management direction for implementing security controls.
- Example:
    - Restricting employee internet access via firewall.

2️⃣ Technical Specification SysSP

Information Security

Created by system administrators to implement managerial intent.

Two main implementation methods:

A. Access Control Lists (ACLs)

ACLs define:

- Who can access
- What they can access
- When they can access
- Where they can access from

ACLs regulate:

- Files
- Applications
- Network devices
- Communication systems

Common permissions:

- Read
- Write
- Modify
- Delete
- Execute

B. Configuration Rule Policies

These define how systems react to data.

Used in:

- Firewalls

- Intrusion Detection and Prevention Systems (IDPS)
- Proxy servers

They translate policy into technical rules.

Combination SysSP

- Combines managerial guidance and technical specifications.
- Practical for small organizations.
- Provides clarity for implementers.

Key Differences Summary

Policy Type	Level	Focus	Audience
EISP	Strategic	Overall security direction	Executives
ISSP	Tactical	Specific issues (email, internet)	Employees
SysSP	Operational	System configuration	Administrators

The Importance of Policy Management

Writing a policy is only the first step. For a security policy to be effective, it must be **disseminated**—meaning it is distributed, read, understood, agreed to, and uniformly applied. Without active management, policies become "shelved" and lose their utility.

Policies During Organizational Change

Policies face maximum stress during **mergers, acquisitions, and divestitures**.

- **Mergers:** Vulnerabilities arise if two companies maintain incongruent or separate security policies.

- **Divestitures:** A company splitting in two may find that a previously unified policy no longer fits the needs of the separate entities.
- **Human Factor:** During these times, employees are distracted and uncertain; clear policy management helps maintain a resilient organization.

The Four Pillars of Policy Viability

To remain valid and enforceable, every security policy must include the following four elements:

1. The Policy Administrator (Responsible Individual)

Every policy needs a "champion" to oversee its lifecycle.

- **Role:** Responsible for the creation, revision, distribution, and storage of the document.
- **Expertise:** They do not need to be a technical expert, but they must have a moderate technical background and be able to solicit input from both security pros and business managers.
- **Visibility:** They must be clearly identified on the document as the primary point of contact for feedback or questions.

2. Schedule of Reviews

Policies are not static; they must change with the environment to avoid becoming liabilities.

- **Frequency:** Policies should generally be reviewed **at least annually**.
- **Due Diligence:** Regular reviews demonstrate that the organization is actively meeting market and legal requirements.

3. Review Procedures and Practices

There must be a clear "mechanism" for employees to suggest improvements.

- **Feedback Loops:** Recommendations can be gathered via email, office mail, or **anonymous drop boxes**.

- **Anonymity:** Essential for controversial policies, as employees may be intimidated by management and hesitate to offer honest critiques otherwise.

4. Policy and Revision Dates

Dating is a critical, yet often overlooked, administrative task.

- **Date of Origin & Revision:** Prevents confusion and "legal headaches" caused by employees following outdated versions.
- **Sunset Clauses:** Some policies (especially for short-term business associations) include an expiration date. This prevents temporary rules from mistakenly becoming permanent.

Modern Policy Tools

Automated Policy Management

A new category of software has emerged to handle the "busywork" of policy administration. This software automates the management of technical controls and ensures the administrative lifecycle (distribution, tracking, and versioning) is handled efficiently.