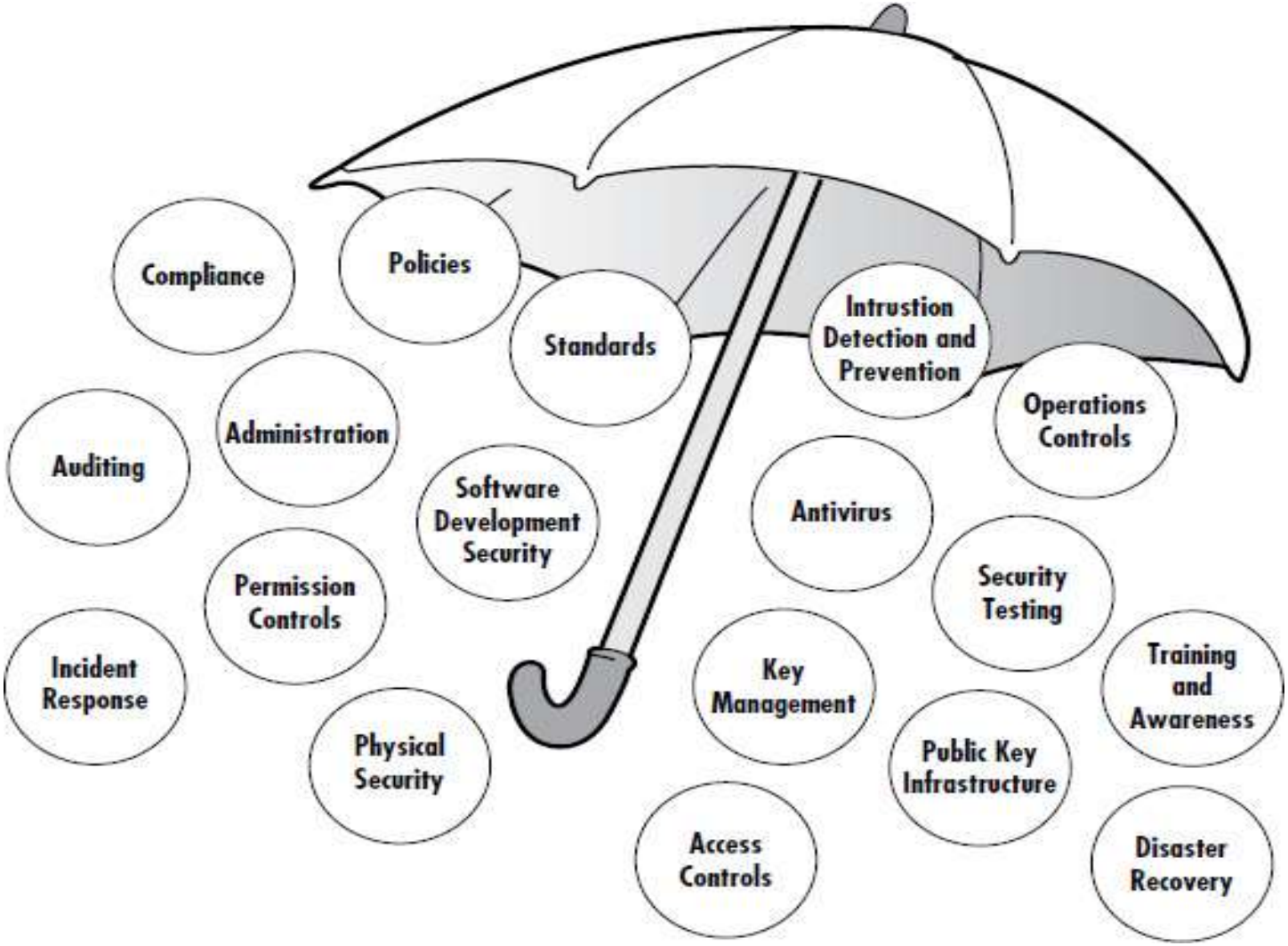
SEC-301 Information Security

What is information security?

- With the rapid advances in networked computer technology during the last few decades and the unprecedented growth of the Internet, the public has become increasingly aware of the threats to personal privacy and security through computer crime.
- Identity theft, pirated bank accounts, forgery—the list of electronic crimes is as unlimited as the imaginations of those who use technology in harmful and dangerous ways.
- To protect computers, networks, and the information they store, organizations are increasingly turning to information security specialists.

- information security is the process of protecting the confidentiality, integrity, and availability (CIA) of data from accidental or intentional misuse.
- Other attacks in recent years have included viruses, worm outbreaks, denial of service (DoS), and Trojan horse programs that prevent internal users from accessing the systems they need to perform their jobs.

CONTEXTUALIZING INFORMATION SECURITY



- Security administrators help to establish new user accounts, ensure that auditing mechanisms are present and operating as needed, ensure that communications between systems are securely implemented, and assist in troubleshooting problems and responding to incidents that could compromise confidentiality, integrity, or availability of the systems.
- Access coordinators are delegated the authority on behalf of a system owner to establish and maintain the user base that is permitted to access and use the system in the normal course of their job duties.
- Security architects and network engineers design and implement network infrastructures that are built with security in mind.
- Security consultants are usually internal personnel who are assigned to project-development teams and remain with the project from inception to implementation.
- Security testers are the white-hat hackers paid to test the security of newly acquired and newly developed or redeveloped systems.
- Policymakers and standards developers are the people who look to outside regulators and executive management to set the tone and establish the specific rules of the road when interacting with or managing information systems.

- Compliance officers check to see that employees remain in compliance with security policies and standards as they use information systems in their daily work. Compliance officers usually work with outside regulators when audits are conducted and are often charged with employee security training and awareness programs to help maintain compliance.
- Incident response team members are alerted when an intrusion or security incident occurs. They decide how to stop the attack or limit the damage as they collect and analyze forensics data while interacting with law enforcement personnel and executive management.
- Governance and vendor managers are needed to ensure that outsourced functions are operating within security policies and standards.

Information security Principles of success

PRINCIPLE 1: THERE IS NO SUCH THING AS ABSOLUTE SECURITY

Given enough time, tools, skills, and inclination, a malicious person can break through any security measure. This principle applies to the physical world as well and is best illustrated with an analogy of safes or vaults that businesses commonly use to protect their assets. Safes are rated according to their resistance to attacks using a scale that describes how long it could take a burglar to open them. Four common classes of safe ratings are B-Rate, C-Rate, UL TL-15, and UL TL-30:

- **B-Rate:** B-Rate is a catchall rating for any box with a lock on it. This rating describes the thickness of the steel used to make the lockbox. No actual testing is performed to gain this rating.
- • **C-Rate:** This is defined as a variably thick steel box with a 1-inch-thick door and a lock. No tests are conducted to provide this rating, either.
- The UL TL-15 label requires that the safe be constructed of 1-inch solid steel or equivalent. The label means that the safe has been tested for a net working time of 15 minutes using “common hand tools, drills, punches hammers, and pressure applying devices.”
- **UL TL-30:** UL TL-30 testing is essentially the same as the TL-15 testing, except for the net working time. Testers get 30 minutes and a few more tools to help them gain access.

PRINCIPLE 2: THE THREE SECURITY GOALS ARE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

All information security measures try to address at least one of three goals:

- Protect the confidentiality of data
- Preserve the integrity of data
- Promote the availability of data for authorized use

These goals form the confidentiality, integrity, availability (CIA) triad,

- ***Integrity Models***

  Integrity models keep data pure and trustworthy by protecting system data from intentional or accidental changes. Integrity models have three goals:

  • Prevent unauthorized users from making modifications to data or programs

  • Prevent authorized users from making improper or unauthorized modifications

  • Maintain internal and external consistency of data and programs

- ***Availability Models***

  Availability models keep data and resources available for authorized use, especially during emergencies or disasters. Information security professionals usually address three common challenges to availability:

  • Denial of service (DoS) due to intentional attacks or because of undiscovered flaws in implementation (for example, a program written by a programmer who is unaware of a flaw that could crash the program if a certain unexpected input is encountered)

  • Loss of information system capabilities because of natural disasters (fires, floods, storms, or earthquakes) or human actions (bombs or strikes)

  • Equipment failures during normal use

PRINCIPLE 3: DEFENSE IN DEPTH AS STRATEGY

- Layered security, as in the previous example, is known as defense in depth. This security is implemented in overlapping layers that provide the three elements needed to secure assets: prevention, detection, and response. Defense in depth also seeks to offset the weaknesses of one security layer by the strengths of two or more layers.

PRINCIPLE 4: WHEN LEFT ON THEIR OWN, PEOPLE TEND TO MAKE THE WORST SECURITY DECISIONS

- The primary reason identity theft, viruses, worms, and stolen passwords are so common is that people are easily duped into giving up the secrets technologies use to secure systems.

PRINCIPLE 5: COMPUTER SECURITY DEPENDS ON TWO TYPES OF REQUIREMENTS: FUNCTIONAL AND ASSURANCE

- Functional requirements describe what a system *should* do. Assurance requirements describe how functional requirements should be implemented and tested.
- Verification is the process of confirming that one or more predetermined requirements or specifications are met. Validation then determines the correctness or quality of the mechanisms used to meet the needs.

PRINCIPLE 6: SECURITY THROUGH OBSCURITY IS NOT AN ANSWER

- Security through obscurity means that hiding the details of the security mechanisms is sufficient to secure the system alone.

PRINCIPLE 7: SECURITY = RISK MANAGEMENT

- Security is concerned not with eliminating all threats within a system or facility, but with eliminating known threats and minimizing losses if an attacker succeeds in exploiting a vulnerability. Risk analysis and risk management are central themes to securing information systems. When risks are well understood, three outcomes are possible:
- **Extreme risk:** Immediate action is required.
- **High risk:** Senior management's attention is needed.
- **Moderate risk:** Management responsibility must be specified.
- **Low risk:** Management is handled by routine procedures.

- Determining the likelihood of a risk coming to life requires understanding a few more terms and concepts:
- Vulnerability
- Exploit
- Attacker
- Vulnerability refers to a known problem within a system or program.
- An exploit is a program or “cookbook” on how to take advantage of a specific vulnerability. It might be a program that a hacker can download over the Internet and then use to search for systems that contain the vulnerability it’s designed to exploit.
- The attacker has two characteristics: skill and will. Attackers either are skilled in the art of attacking systems or have access to tools that do the work for them.

PRINCIPLE 8: THE THREE TYPES OF SECURITY CONTROLS ARE PREVENTATIVE, DETECTIVE, AND RESPONSIVE

- Access to a bank's safe or vault requires passing through layers of protection that might include human guards and locked doors with special access controls (prevention).
- In the room where the safe resides, closed-circuit televisions, motion sensors, and alarm systems quickly detect any unusual activity (detection).
- The sound of an alarm could trigger the doors to automatically lock, the police to be notified, or the room to fill with tear gas (response).

PRINCIPLE 9: COMPLEXITY IS THE ENEMY OF SECURITY

- The more complex a system gets, the harder it is to secure.
- With too many “moving parts” or interfaces between programs and other systems, the system or interfaces become difficult to secure while still permitting them to operate as intended.

PRINCIPLE 10: FEAR, UNCERTAINTY, AND DOUBT DO NOT WORK IN SELLING SECURITY

- **PRINCIPLE 11: PEOPLE, PROCESS, AND TECHNOLOGY ARE ALL NEEDED TO ADEQUATELY SECURE A SYSTEM OR FACILITY**
- **PRINCIPLE 12: OPEN DISCLOSURE OF VULNERABILITIES IS GOOD FOR SECURITY!**

Information security: Common Body of knowledge

- The CBK is a compilation and distillation of all security information collected internationally that is relevant to information security professionals.
- The following describe the 10 domains of the CBK.

1. Information Security Governance and Risk Management

The Governance and Risk Management domain emphasizes the importance of a comprehensive security plan that includes security policies and procedures for protecting data and how it is administered. Topics include

- Understanding and aligning security functions with the goals, mission, and objectives of the organization
- Understanding and applying security governance
- Understanding and applying concepts of confidentiality, integrity, and availability
- Developing and implementing security policies
- Managing the information life-cycle (classification, categorization, and ownership)
- Managing third-party governance (on-site assessments, document exchange and review, process and policy reviews)
- Understanding and applying risk management concepts
- Managing personnel security
- Developing and managing security education, training, and awareness
- Managing the security function (budgets, metrics, and so on)

2. Security Architecture and Design

- The Security Architecture and Design domain one of the more technical areas of study within the CBK, discusses concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems, equipment, networks, applications, and other controls to enforce various levels of confidentiality, integrity, and availability.
  - Understanding the fundamental concepts of security models
  - Identifying the components of information systems security evaluation models
  - Recognizing software and system vulnerabilities and threats

3. Business Continuity and Disaster Recovery Planning

- Understanding business continuity requirements
- Conducting business impact analysis
- Developing a recovery strategy
- Understanding the disaster recovery process
- Exercising, assessing, and maintaining the plans

4. Legal Regulations, Investigations, and Compliance

- This domain covers the different targets of computer crimes, bodies of law, and the different types of laws and regulations as they apply to computer security.
- Understanding legal issues that pertain to information security internationally
- Adopting professional ethics
- Understanding and supporting investigations
- Understanding forensic procedures

5. Physical (Environmental) Security

- Topics covered in this domain include securing the physical site using policies and procedures coupled with the appropriate alarm and intrusion detection systems, monitoring systems, and so forth.
- Supporting the implementation and operation of perimeter security (physical access controls and monitoring, keys, locks, safes, and so on)
- Supporting the implementation and operation of facilities security (badges, smart cards, PINs, and so on)
- Supporting the protection and securing of equipment

6. Operations Security

- This domain covers the kind of operational procedures and tools that eliminate or reduce the capability to exploit critical information. It includes defining the controls over media, hardware, and operators with special systems privileges.
- Understanding security operations concepts (need-to-know, separation of duties, and so on)
- Employing resource protection
- Managing incident response
- Implementing preventable measures against attacks

7. Access Control

- Who may access the system, and what can they do after they are signed on? That is the focus of this CBK domain. Specific topics include
- Understanding identification, authentication, authorization, and logging and monitoring techniques and technologies
- Understanding access control attacks
- Assessing effectiveness of access controls

8. Cryptography

- It involves encrypting data so that authorized individuals may view the sensitive data and unauthorized individuals may not. Cryptography is a highly complex topic.
- Identifying the application and use of cryptography
- Comprehending the cryptographic life cycle
- Understanding encryption concepts
- Identifying key management processes

9. Telecommunications and Network Security

- This domain covers another technical segment of the CBK. Topics include not just network topologies, but also their weaknesses and defenses.
- Understanding secure network architecture and design
- Securing network components
- Establishing secure communications channels (VPN, SSL, and so on)
- Understanding network attacks (denial of service, spoofing, and so on)

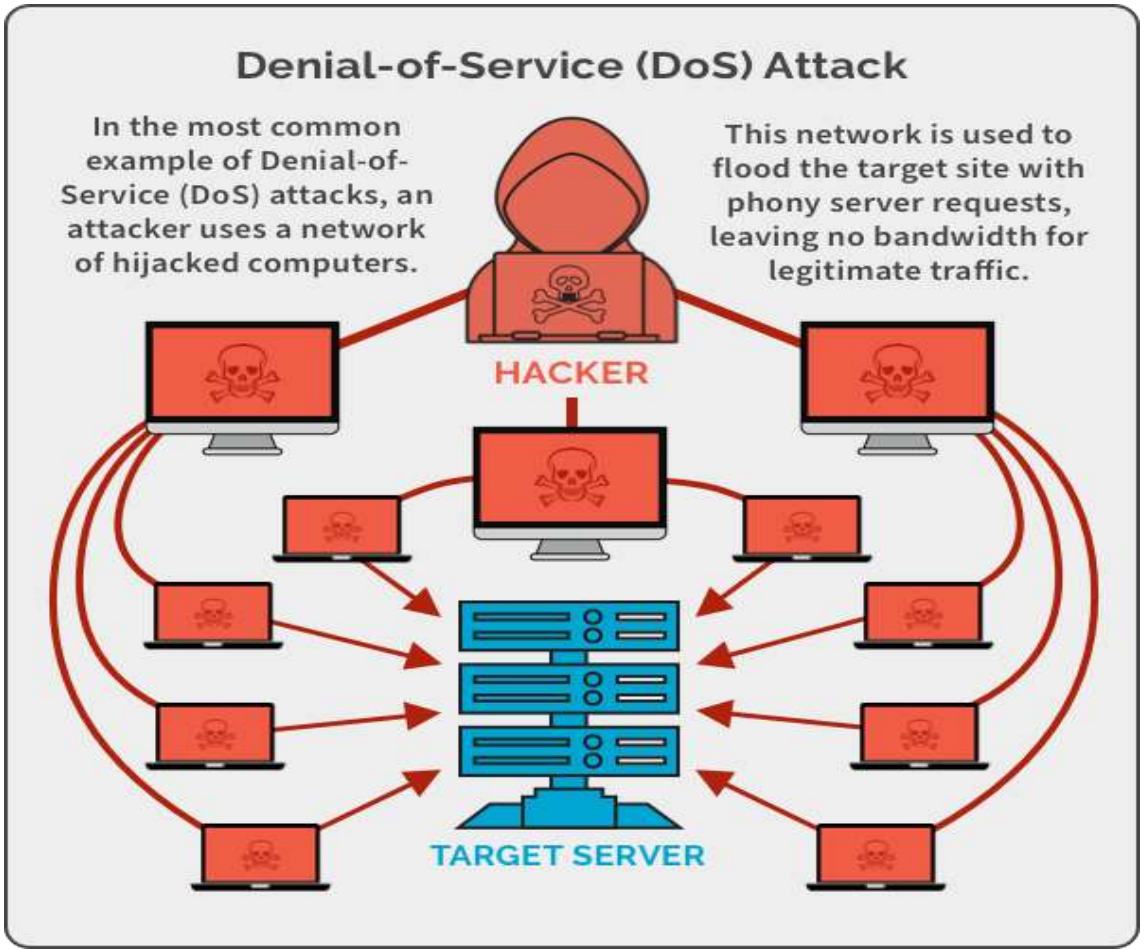
Law, Investigations, and Ethics

TYPES OF COMPUTER CRIME

- **Military and intelligence attacks:** Criminals and intelligence agents illegally obtain classified and sensitive military information and police files.
- **Business attacks:** Increasing competition between companies frequently leads to illegal access of proprietary information.
- **Financial attacks:** Banks and other financial institutions provide attractive targets for computer criminals, for obvious reasons.
- **Terrorist attacks:** The U.S. Department of Homeland Security monitors the level of "chatter" on the Internet, looking for evidence of planned terrorist attacks against computer systems and geographic locations.
- **Grudge attacks:** Companies are increasingly wary of disgruntled employees who feel mistreated and exact their revenge using computer systems.
- **Thrill attacks:** Unlike grudge attackers who want some kind of revenge, thrill attackers hack computer systems for the fun of it, for bragging rights, or simply for a challenge.

HOW CYBERCRIMINALS COMMIT CRIMES

- **Denial of service (DoS) attacks:** This tactic overloads a computer's resources (particularly the temporary storage area in computers, called the buffers) from any number of sources (referred to as a distributed denial of service, or DDoS, attack) until the system is so bogged down that it cannot honor requests.



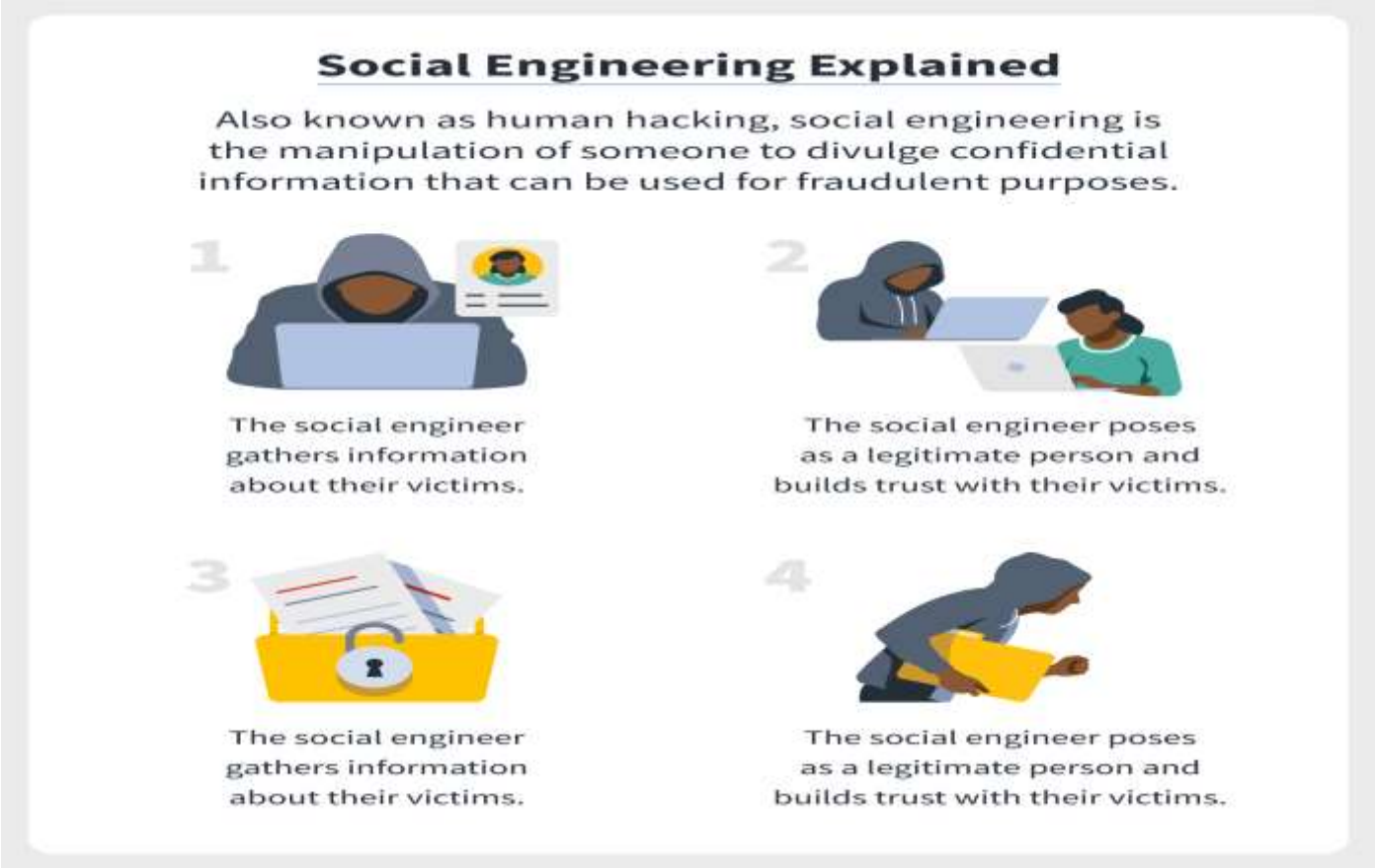
- **Rogue code:** The user inadvertently launches software that can log a user's keystrokes and either send them to a remote server or perform other undesirable activities, such as deleting files or destroying the operating system, rendering the computer useless.
- **Software piracy:** The attacker copies or downloads software and using it without permission.

Software piracy is the act of

stealing software that is legally protected.

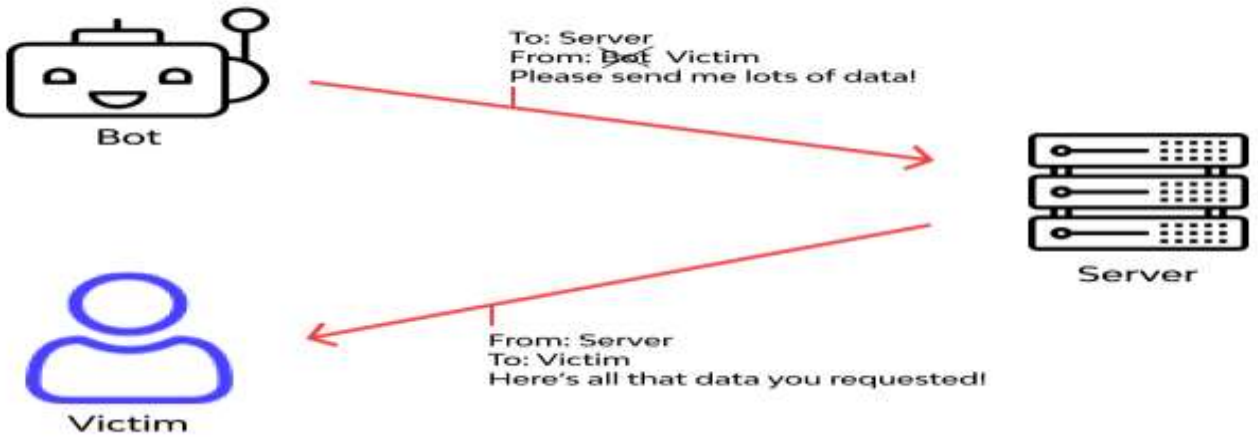
This stealing includes selling, distributing, modifying or copying the software.

- **Social engineering:** Using deception, the attacker solicits information such as passwords or personal identification numbers (PIN) from unwitting victims.

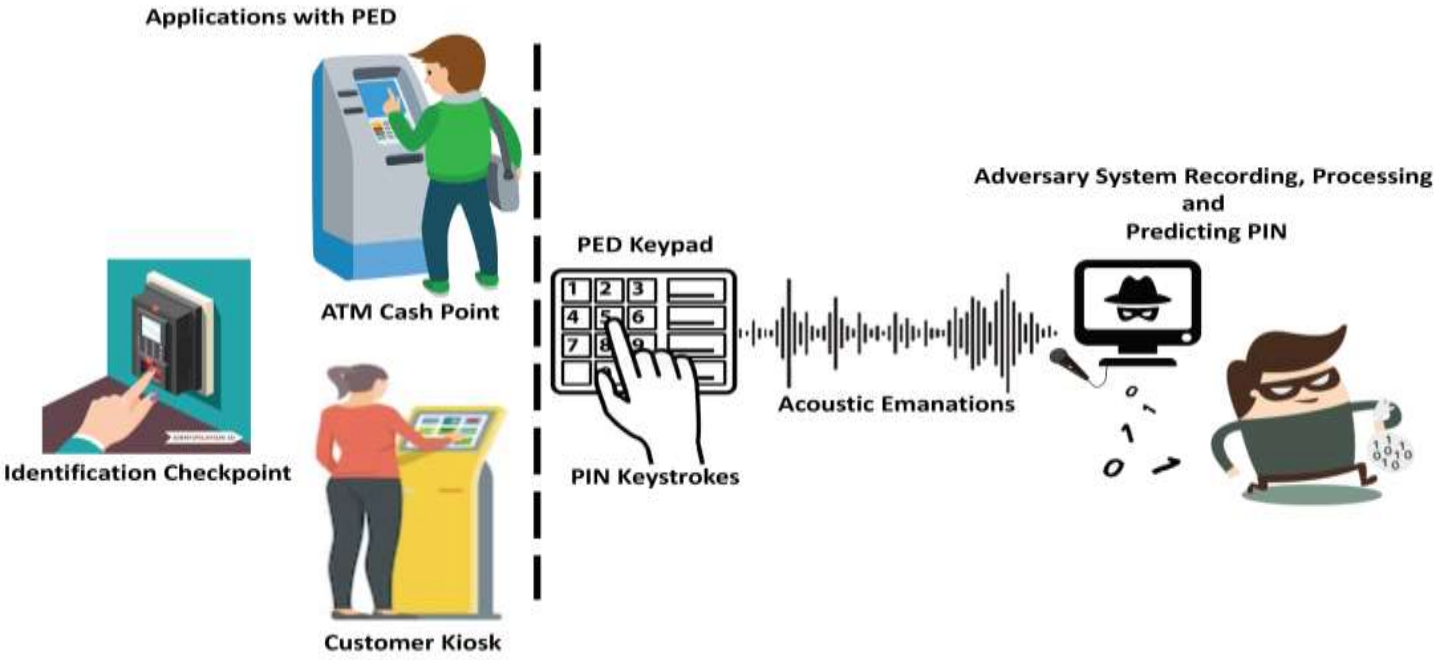


- **Dumpster diving:** This no-tech criminal technique is the primary cause of ID theft. A criminal simply digs through trash and recycling bins looking for receipts, checks, and other personal and sensitive information.

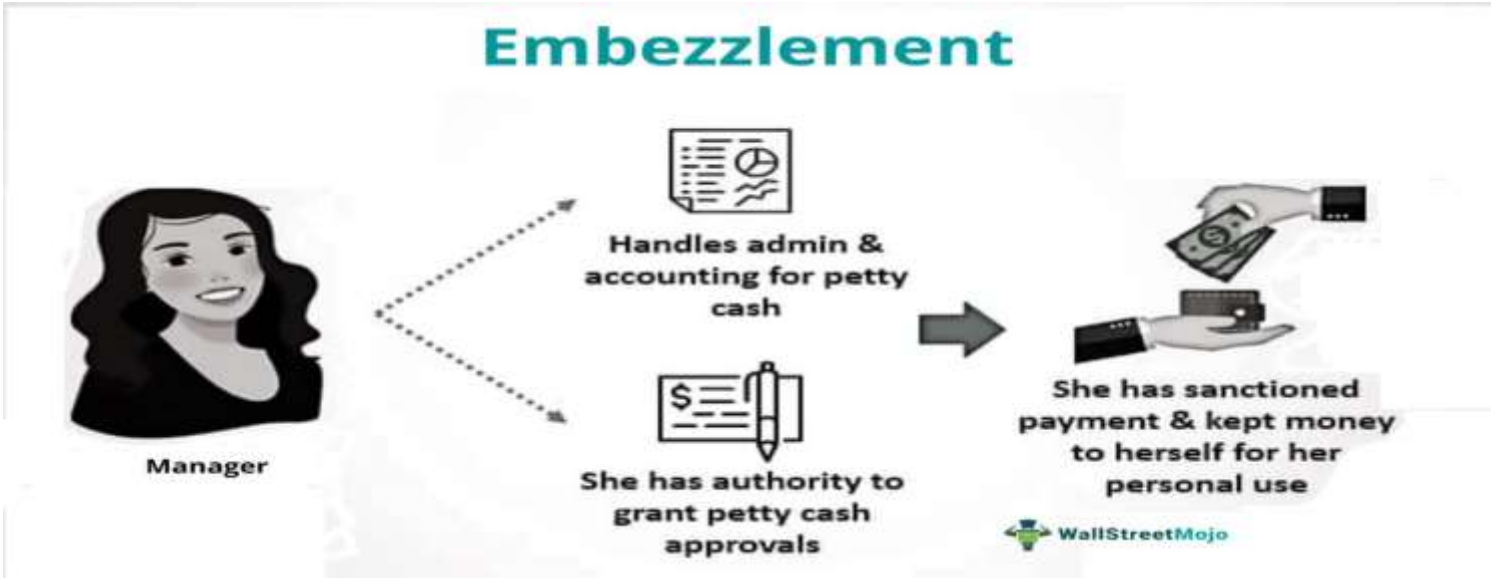
- **Spoofing of Internet Protocol (IP) addresses:** The attacker sends a message with a false originating IP address to convince the recipient that the sender is someone else. Every computer on the Internet is assigned a unique IP address.



- **Emanation eavesdropping:** The attacker intercepts radio frequency (RF) signals emanated by wireless computers to extract sensitive or classified information.



- **Embezzlement:** In the movie *Office Space*, three disgruntled employees modify computer software to collect round-off amounts (fractions of a penny) from a company's accounting program.



- **Information warfare** includes attacks upon a country's computer network to gain economic or military advantage.

- Researchers have reported to the Indian government a cyber attack campaign routed by Pakistani hackers, suspected to be aided by China, with the aim of stealing critical data by targeting key personnel in India's Defence force.

THE COMPUTER AND THE LAW

- 1. **Legislative Branch of the Legal System**
- The legislative branches (Congress and Senate) are responsible for passing statutory laws. A statutory law is a law written through the act of a legislature declaring, commanding, or prohibiting something.
- 2. **Administrative Branch of the Legal System**
- Administrative law is also referred to as natural justice. We owe this legal concept to the Romans, who believed certain legal principles were “natural” or self-evident and did not need to be codified by statute.

- 3. **Judicial Branch of the Legal System**

  The following are three primary categories of laws within the common law system:

- **Civil law:** Civil laws are written to compensate individuals who were harmed through wrongful acts known as torts. A tort can be either intentional or unintentional (as in the case of negligence). Common law is generally associated with civil disputes in which compensation is financial but does not involve imprisonment.

- **Criminal law:** Criminal law punishes those who violate government laws and harm an individual or group. Unlike civil law, criminal law includes imprisonment in addition to financial penalties.

- **Regulatory law:** Regulatory law is administrative laws that regulate the behavior of administrative agencies of government. Considered part of public law, regulatory law addresses issues that arise between the individual and a public entity. Regulatory laws can also exact financial penalties and imprisonment.


ADMINISTRATIVE
LAW


§
RULES
STATUTES


BRANCHES OF CIVIL LAW
POW!
CONTRACT
TORT
CONTRACTS
PROPERTY
FAMILY
legaldictionary.net

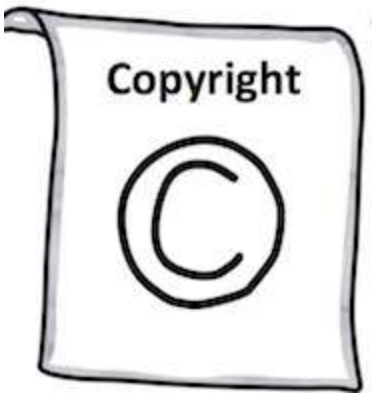

TRANSPARENCY
REQUIREMENTS
LAW
COMPLIANCE
RULES
POLICIES
REGULATIONS
STANDARDS
Download from
Dreamstime.com

INTELLECTUAL PROPERTY LAW

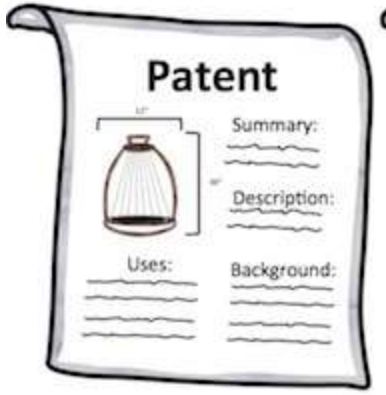
- Copyright
- Patent
- Trademark
- Tradesecret

Copyright

- Copyright (or author's right) is a legal term used to describe the rights that creators have over their literary and artistic works.
- Exhaustive lists of works covered by copyright are usually not to be found in legislation. Nonetheless, broadly speaking, works commonly protected by copyright throughout the world include:
- literary works such as novels, poems, plays, reference works, newspaper articles;
- computer programs, databases;
- films, musical compositions, and choreography;
- artistic works such as paintings, drawings, photographs, and sculpture;
- architecture; and
- advertisements, maps, and technical drawings.
- Copyright protection extends only to expressions, and not to ideas, procedures, methods of operation or mathematical concepts as such. Copyright may or may not be available for a number of objects such as titles, slogans, or logos, depending on whether they contain sufficient authorship.
- Copyright can be granted for the period of 50 years and last up to 70 years.



Patent



- A patent is an exclusive right granted for an invention, which is a product or a process that provides, in general, a new way of doing something, or offers a new technical solution to a problem.
- To get a patent, technical information about the invention must be disclosed to the public in a patent application.
- Patent can be granted on man-made products , machines, chemical and mathematical expressions.
- To grant a patent, the user has to show his/her inventions to the authority.
- The authority checks for the uniqueness of the product and grant patent for the 20 years.
- Example: light bulb, telephone.

Trademark

- The term trademark refers to a recognizable insignia, phrase, word, or symbol that denotes a specific product and legally differentiates it from all other products of its kind.
- A trademark is a sign capable of distinguishing the goods or services of one enterprise from those of other enterprises.
- Trademarks can be granted for 10 years and can be renewed also.
- Example: Trademark for Puma is PUMA

Trade secret

- A trade secret is **any practice or process of a company that is generally not known outside of the company**.
- Information considered a trade secret gives the company a competitive advantage over its competitors and is often a product of internal research and development.
- Example:
- KFC’s secret blend of 11 herbs and spices.
- Coca-Cola’s recipe for their signature drink.
- Google’s search algorithm.
- McDonald’s Big Mac “special sauce.”
- Secret client lists at any company.

COPYRIGHT

Protection is automatically granted to the author for their original, creative or intellectual work.

Works: Books, lectures, dramatic and musical works, cinematography, drawings, paintings, architecture, sculpture, photographs, illustrations, maps, plans sketches etc.

Rights: To distribute copies or phonorecords of the work to the public by sale or other transfer of ownership, or by rental, lease, or lending; To perform the work publicly in person or through audio transmission.

Validity: Registration not mandatory but recommended. Valid through the lifetime of the author and 60 years after his/her death. Owner has protection in most countries.

TRADEMARK

This is a brand element which distinguishes your goods and services from those of your competitors and other traders.

Marks: Word mark, a logo mark or a slogan, shapes, and unconventional marks like colours, sounds, gestures, animation, holograms etc are also registrable as a trademark.

Rights: Exclusive right to use the mark and prevent anyone from using it without permission. It also gives the owner the right to license, assign and sell the mark in return of some compensation.

Validity: 10 years which can be made perpetual, as along as renewed every 10 years. Should be applied separately in every country in which protection is required and has a market in.

PATENT

This concerns obtaining protection for new inventions that are new, original and useful.

Invention will be patented if: Novel or Original, has an Inventive step (non-obvious) and has some Industrial application.

Rights: Exclusive authority over the patented invention, right to exclude others and exploit the patent and earn from it.

Validity: Patent protection is territorial right and therefore it is effective only within the territory of India. Separate patents required to be filed for each country where protection is required. Patent is valid for period of 20 years after which it goes in public domain.

PRIVACY AND THE LAW

- **Notice/awareness:** In general, websites should tell the user how they collect and handle user information. The notice should be conspicuous, and the privacy policy should clearly state how the site collects and uses information.
- **Choice/consent:** Websites must give consumers control over how their personally identifying information is used. Abuse of this practice is gathering information for a stated purpose but using it in another way, one to which the consumer might object.
- **Access/participation:** Perhaps the most controversial of the fair practices, users would be able to review, correct, and, in some cases, delete personally identifying information on a particular website. Most companies that currently collect personal information have no means of allowing people to review what the company collected, nor do they provide any way for a person to correct incorrect information.
- **Security/integrity:** Websites must do more than reassure users that their information is secure with a “feel-good” policy statement. The site must implement policies, procedures, and tools that will prevent unauthorized access and hostile attacks against the site.

International Privacy Issues

- **Notice:** Companies must notify individuals about what personally identifying information they are collecting, why they are collecting it, and how to contact the collectors.
- **Choice:** Individuals must be able to choose whether and how their personal information is used by, or disclosed to, third parties.
- **Onward transfer:** Third parties receiving personal information must provide the same level of privacy protection as the company from which the information is obtained.
- **Security:** Companies housing personal information and sensitive data must secure the data and prevent its loss, misuse, disclosure, alteration, and unauthorized access.
- **Data integrity:** Companies must be able to reassure individuals that their data is complete, accurate, current, and used for the stated purposes only.
- **Access:** Individuals must have the right and ability to access their information and correct, modify, or delete any portion of it.
- **Enforcement:** Each company must adopt policies and practices that enforce the aforementioned privacy principles.

COMPUTER FORENSICS

- Investigating crimes committed with computers is known as computer forensics.
- The intangibility of computer evidence makes the job of prosecuting cybercrime more difficult than with traditional crime.
- The following are among the many arguments for such services:
- Successful litigation frequently depends on obtaining irrefutable computer evidence. Without solid computer evidence, you might not have a case.
- Your evidence might not be as good as the opposition's if you are using less sophisticated data detection techniques.
- Your adversaries do not want you to obtain the data you need.
- The technology used to create the data you need might have already disappeared. Time is of the essence.


AUTHORIZED
PERSONNEL

- Cyber forensics is a process of extracting data as proof for a crime (that involves electronic devices) while following proper investigation rules to nab the culprit by presenting the evidence to the court. Cyber forensics is also known as computer forensics.
- Computer forensics can do the following:
  - It can recover deleted files, chat logs, emails, etc
  - It can also get deleted SMS, Phone calls.
  - It can get recorded audio of phone conversations.
  - It can determine which user used which system and for how much time.
  - It can identify which user ran which program.

- Importance of Computer forensics:
  - Cyber forensics helps in collecting important digital evidence to trace the criminal.
  - Electronic equipment stores massive amounts of data that a normal person fails to see. For example: in a smart house, for every word we speak, actions performed by smart devices, collect huge data which is crucial in cyber forensics.
  - It is also helpful for innocent people to prove their innocence via the evidence collected online.
  - It is not only used to solve digital crimes but also used to solve real-world crimes like theft cases, murder, etc.
  - Businesses are equally benefitted from cyber forensics in tracking system breaches and finding the attackers.

Questions

1. Explain information security principles of success.
2. What are the types of crimes? How cyber criminals commit crime?
3. Write a short note on computer forensics.
4. Explain privacy and law.
5. Explain international privacy issues.
6. Write a short note on patent / trademark / tradesecret. Or Intellectual property law.
7. Explain judicial branch of a legal system.
8. Explain ten domains of CBK.