Chapter 19

"**Computer crime**, or **cybercrime**, is a term used broadly to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity."

Types of Computer Crime

- Computer as targets- targets a computer system, to acquire information stored on that computer system, to control the target system without authorization or payment (theft of service), or to alter the integrity of data or interfere with the availability of the computer or server
- Computer as storage devices- unlawful activity by using a computer or a computer device as a passive storage medium. For example, the computer can be used to store stolen password lists, credit card or calling card numbers
- Computer as communication tools - traditional crimes that are committed online. Examples include the illegal sale of prescription drugs, controlled substances, alcohol, and guns; fraud; gambling; and child pornography

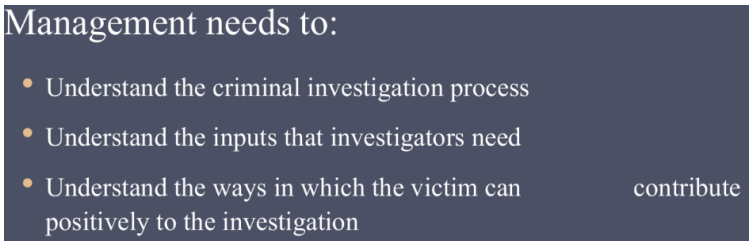
Cybercrime involves law enforcement agencies, cybercriminals & cybervictims.

For law enforcement agencies, cybercrime presents some unique difficulties.

- Proper investigation requires a good grasp of the technology
- Resources like computer processing power, communications capacity, and storage capacity may be beyond the budget of individual jurisdictions.
- Crimes will involve perpetrators who are remote from the target system (anywhere in the world)
- lack of collaboration and cooperation with remote law enforcement agencies

Lack of success in bringing **cybercriminals** to justice has led to an increase in their numbers, boldness, and the global scale of their operations. Reporting rates by **cybervictims** tend to be low because of a lack of confidence in law enforcement,

Executive management and security administrators need to look upon law enforcement as another resource and tool, alongside technical, physical, and human-factor resources.



The law dealing with cyber crimes in Pakistan is Prevention of Electronic Crimes Act, 2016 ("Act") which is applicable to every citizen of Pakistan wherever he may be and to every other person who is stationed in Pakistan for the time being.

Intellectual property: Any intangible asset that consists of human knowledge and ideas. Examples include software, data, novels, sound recordings, the design of a new type of mousetrap, or a cure for a disease.

There are three main types of intellectual property for which legal protection is available: copyrights, trademarks, and patents.

COPYRIGHTS Copyright law protects the tangible or fixed expression of an idea, not the idea itself. A creator can claim copyright, and file for the copyright at a national government copyright office, if the following conditions are fulfilled:[4]

- The proposed work is original.
- The creator has put this original idea into a concrete form, such as hard copy (paper), software, or multimedia form.

PATENTS A patent for an invention is the grant of a property right to the inventor. The right conferred by the patent grant is, in the language of the U.S. statute and of the grant itself, "the right to exclude others from making, using, offering for sale, or selling" the invention in the United States or "importing" the invention into the United States. Similar wording appears in the statutes of other nations. There are three types of patents:

- **Utility patents**: May be granted to anyone who invents or discovers any new and useful process, machine, article of manufacture, or composition of matter, or any new and useful improvement thereof;
- **Design patents**: May be granted to anyone who invents a new, original, and ornamental design for an article of manufacture; and
- **Plant patents**: May be granted to anyone who invents or discovers and asexually reproduces any distinct and new variety of plant.

TRADEMARKS A trademark is a word, name, symbol, or device that is used in trade with goods to indicate the source of the goods and to distinguish them from the goods of others. A servicemark is the same as a trademark except that it identifies and distinguishes the source of a service rather than a product. The terms **trademark** and *mark* are commonly used to refer to both trademarks and servicemarks. Trademark rights may be used to prevent others from using a confusingly similar mark, but not to prevent others from making the same goods or from selling the same goods or services under a clearly different mark.

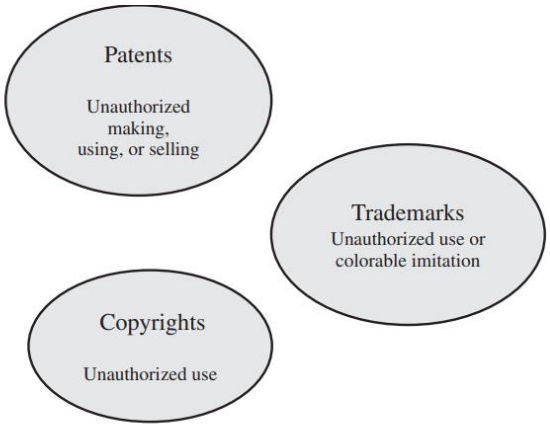


Figure 19.1 **Intellectual Property Infringement**

shows a breakdown of privacy into four major areas, each of which has one or more specific functions:

- **Anonymity**: Ensures that a user may use a resource or service without disclosing the user's identity. Specifically, this means that other users or subjects are unable to determine the identity of a user bound to a subject (e.g., process or user group) or operation. It further means that the system will not solicit the real name of a user. Anonymity need not conflict with authorization and access control functions, which are bound to computer-based user IDs, not to personal user information.
- **Pseudonymity**: Ensures that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use. The system shall provide an alias to prevent other users from determining a user's identity, but the system shall be able to determine the user's identity from an assigned alias.
- **Unlinkability**: Ensures that a user may make multiple uses of resources or services without others being able to link these uses together.
- **Unobservability**: Ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used. *Unobservability* requires users and/or subjects cannot determine whether an operation is being performed. *Allocation of information impacting*

- Both policy and technical approaches are needed to protect privacy
- In terms of technical approaches, the requirements for privacy protection for data stored on information systems can be addresses in part using the technical mechanisms developed for database security
- With regard to social media sites, technical controls include:
  - The provision of suitable privacy settings to manage who can view data on individuals
  - Notification when one individual is referenced or tagged in another's content
  - Although social media sites include some form of these controls, they are constantly changing, causing frustration for users who are trying to keep up with these mechanisms
- Another approach for managing privacy concerns in big data analysis is to anonymize the data, removing any personally identifying information before release to researchers or other organizations for analysis

Data Privacy

In terms of policy, guidelines are needed to manage the use and reuse of big data, ensuring suitable constraints are imposed in order to preserve privacy

- Consent
  - Ensuring participants can make informed decisions about their participation in the research
- Privacy and confidentiality
  - Privacy is the control that individuals have over who can access their personal information
  - Confidentiality is the principle that only authorized persons should have access to information
- Ownership and authorship
  - Addresses who has responsibility for the data, and at what point does an individual give up their right to control their personal data
- Data sharing – assessing the social benefits of research
  - The social benefits that result from data matching and reuse of data from one source or research project in another
- Governance and custodianship
  - Oversight and implementation of the management, organization, access, and

Ethics refers to a system of moral principles that relates to the benefits and harms of particular actions, and to the right ness and wrongness of motives and ends of those actions.

A classic paper on computers and ethics [PARK88] points out that ethical issues arise as the result of the roles of computers, such as the following:

- **Repositories and processors of information**: Unauthorized use of otherwise unused computer services or of information stored in computers raises questions of appropriateness or fairness.
- **Producers of new forms and types of assets**: For example, computer programs are entirely new types of assets, possibly not subject to the same concepts of ownership as other assets.
- **Instruments of acts**: To what degree must computer services and users of computers, data, and programs be responsible for the integrity and appropriateness of computer output?
- **Symbols of intimidation and deception**: The images of computers as thinking machines, absolute truth producers, infallible, subject to blame, and as anthropomorphic replacements of humans who err should be carefully considered.

- Concern with balancing professional responsibilities with ethical or moral responsibilities
- Types of ethical areas a computing or IT professional may face:
  - Ethical duty as a professional may come into conflict with loyalty to employer
  - "Blowing the whistle"
  - Expose a situation that can harm the public or a company's customers
  - Potential conflict of interest
- Organizations have a duty to provide alternative, less extreme opportunities for the employee
  - In-house ombudsperson coupled with a commitment not to penalize employees for exposing problems
- Professional societies should provide a mechanism whereby society members can get advice on how to proceed

Codes of conduct by ACM, IEEE, AITP

- All three codes place their emphasis on the responsibility of professionals to other people
- Do not fully reflect the unique ethical problems related to the development and use of computer and IT technology
- Common themes:
  - Dignity and worth of other people
  - Personal integrity and honesty
  - Responsibility for work
  - Confidentiality of information
  - Public safety, health, and welfare
  - Participation in professional societies to improve standards of the profession
  - The notion that public knowledge and access to technology is equivalent to social power

The Rules

- Collaborative effort to develop a short list of guidelines on the ethics of computer systems
- Ad Hoc Committee on Responsible Computing
  - Anyone can join this committee and suggest changes to the guidelines
  - Moral Responsibility for Computing Artifacts
    - Generally referred to as The Rules
    - The Rules apply to software that is commercial, free, open source, recreational, an academic exercise or a research tool
  - Computing artifact
    - Any artifact that includes an executing computer program

As of this writing, the rules are as follows:

1) The people who design, develop, or deploy a computing artifact are morally responsible for that artifact, and for the foreseeable effects of that artifact. This responsibility is shared with other people who design, develop, deploy or knowingly use the artifact as part of a sociotechnical system.

2) The shared responsibility of computing artifacts is not a zero-sum game. The responsibility of an individual is not reduced simply because more people become involved in designing, developing, deploying, or using the artifact. Instead, a person's responsibility includes being answerable for the behaviors of the artifact and for the artifact's effects after deployment, to the degree to which these effects are reasonably foreseeable by that person.

3) People who knowingly use a particular computing artifact are morally responsible for that use.

4) People who knowingly design, develop, deploy, or use a computing artifact can do so responsibly only when they make a reasonable effort to take into account the sociotechnical systems in which the artifact is embedded.

5) People who design, develop, deploy, promote, or evaluate a computing artifact should not explicitly or implicitly deceive users about the artifact or its foreseeable effects, or about the sociotechnical systems in which the artifact is embedded.