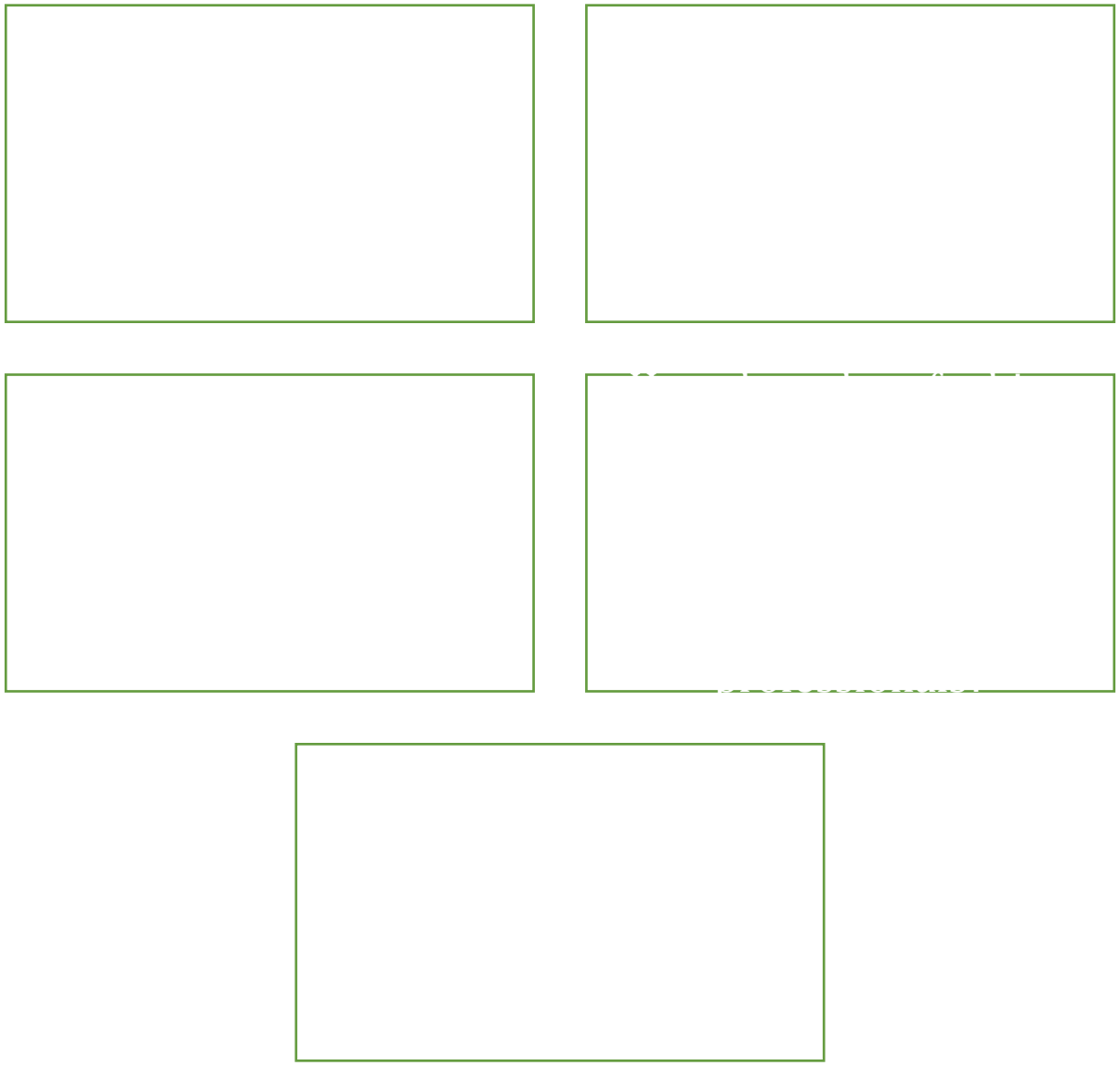
Module 2: Cyber-crimes and Cyber Laws

Objectives - Ethics for IT Workers and IT Users



Module 2

- Ethics for IT Workers and IT Users-IT Professionals-
- IT professional malpractice-IT,
- IT Act cyber laws -Information Technology Act, 2000 (“IT Act”) –
- Digital Signature – Confidentiality, Integrity and Authenticity
- (CIA)

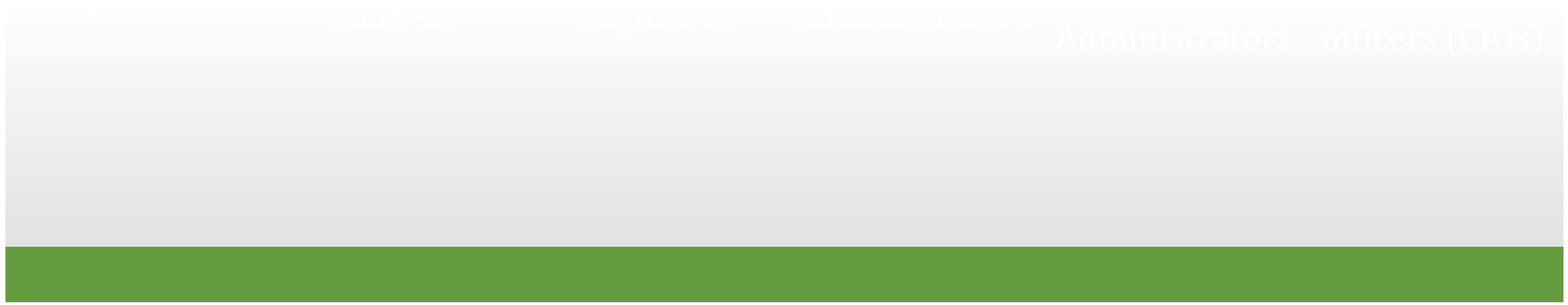
IT Professionals

- Specialized knowledge
- Long and intensive academic preparation

- Require advanced training and experience
- Must exercise discretion and judgment in their work
- Their work cannot be standardized
- Contribute to society, participate in lifelong training, assist other professionals
- Carry special rights and responsibilities

Are IT Workers Professionals?

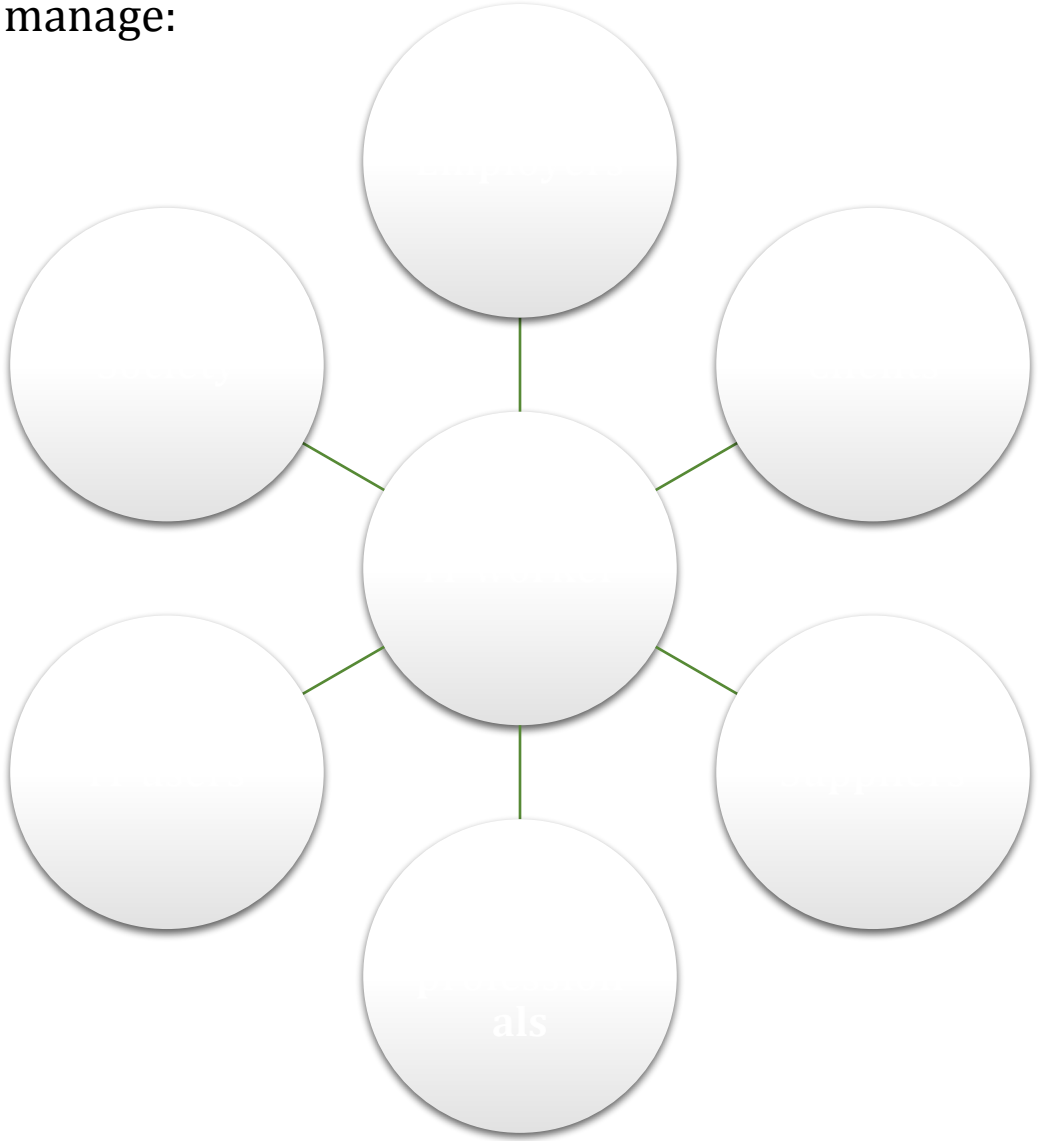
Partial list of IT specialists



- IT workers do not meet legal definition of professional
- Not licensed by state or federal government
- Not liable for malpractice

Professional Relationships That Must Be Managed

- In each relationship, an ethical IT worker acts honestly and appropriately.
- Professional relationships IT workers must manage:



Relationships Between IT Workers and Employers

Relationships Between IT Workers and Employers

Software piracy

violate laws and policies

to software to which they are not entitled

Relationships Between IT Workers and Employers

- The **Business Software Alliance (BSA)** is a **trade group** that represents the world's largest software and hardware manufacturers. Its mission is to stop the unauthorized copying of software produced by its members.
- **Trade secrecy** is another area that can present challenges for IT workers and their employers. A **trade secret** is information, generally unknown to the public, that a company has taken strong measures to keep confidential. It represents something of **economic value** that has required effort or cost to develop and that has some degree of uniqueness or novelty.
- **Trade secrets** can include the **design of new software code**, **hardware designs**, **business plans**, the **design** of a **user interface** to a **computer program**, and **manufacturing processes**.
- Examples include the Colonel's secret recipe of 11 herbs and spices used to make the original KFC chicken, the formula for Coke.
- Intel's manufacturing process for the i7 quad core processing chip.
- Employers worry that employees may reveal these secrets to competitors, especially if they leave the company.
- As a result, companies often require employees to sign confidentiality agreements and promise not to reveal the company's trade secrets.

Relationships Between IT Workers and Employers

- Another issue that can create friction between employers and IT workers is **whistleblowing**.
- **Whistle-blowing** is an effort by an employee to attract attention to a negligent, illegal, unethical, abusive, or dangerous act by a company that threatens the public interest.
- Whistle-blowers often have special information based on their expertise or position within the offending organization. For example, an employee of a chip manufacturing company may know that the chemical process used to make the chips is dangerous to employees and the general public.
- A **whistleblower** is a person, usually an employee, who exposes information or activity within a private, public, or government organization that is deemed illegal, illicit, unsafe, fraud, or abuse of taxpayer funds.

Relationships Between IT Workers and Clients

- Client trusts IT worker to act in client's best interests
- Client will provide relevant information, listen to and understand what the IT worker says, ask questions to understand impact of key decisions, and use the information to make wise choices
- Ethical problems arise if a company recommends its own products and services to remedy problems they have detected
- Creates a conflict of interest
- Problems arise during a project if IT workers are unable to provide full and accurate reporting of a project's status
- Finger pointing and heated discussions can ensue
- Client makes decisions about a project based on information, alternatives, and recommendations provided by the IT worker

Relationships Between IT Workers and Clients

- **Fraud** is the crime of obtaining goods, services, or property through deception or trickery.
- Fraudulent misrepresentation occurs when a person consciously decides to induce another person to rely and act on a misrepresentation.
- To prove fraud in a court of law, prosecutors must demonstrate the following elements:
  - The wrongdoer made a false representation of material fact.
  - The wrongdoer intended to deceive the innocent party.
  - The innocent party justifiably relied on the misrepresentation.
  - The innocent party was injured.
- **Misrepresentation statement** or incomplete statement of material fact.
- If misrepresentation causes a party to enter into a contract, that party may have the right to cancel contract or seek reimbursement for damages

Relationships Between IT Workers and Clients

Breach of contract

- One party fails to meet the terms of a contract.
- When there is material breach of contract:
    - The non-breaching party may revoke (cancel) the contract, seek restitution of any compensation paid to the breaching party, and be discharged from any further performance under the contract.

- When there are problems, it is difficult to assign who is at fault.

Relationships Between IT Workers and Suppliers

Develop good working relationships with suppliers:

- **To encourage flow of useful information and ideas to develop innovative and cost-effective ways** of using the supplier in ways that the IT worker may not have considered
- By **dealing fairly** with them
- By **not making unreasonable demands**

Bribery

- **Bribery** is the act of providing money, property, or favors to someone in business or government in order to obtain a business advantage.
- **U.S. Foreign Corrupt Practices Act (FCPA):** crime to bribe a foreign official, a foreign political party official, or a candidate for foreign political office
- At what **point does a gift become a bribe**?
- **No gift** should be hidden
- Perceptions of **donor and recipient can differ**
- United Nations Convention Against Corruption is a global treaty **to fight bribery and corruption**

Bribes & Gifts

TABLE 2-2 Distinguishing between bribes and gifts

Bribes	Gifts
Are made in secret, as they are neither legally nor morally acceptable	Are made openly and publicly, as a gesture of friendship or goodwill
Are often made indirectly through a third party	Are made directly from donor to recipient
Encourage an obligation for the recipient to act favorably toward the donor	Come with no expectation of a future favor for the donor

Source Line: Course Technology/Cengage Learning.

Relationships Between IT Workers and Other Professionals

- Ethical problems among the IT profession.
    - Inappropriate sharing of corporate information
    - Information might be sold intentionally or shared informally with those who have no need to know.
- Professionals owe each other adherence to their profession's code of conduct.
- Professionals feel a degree of loyalty to other members of their profession.

Relationships Between IT Workers and Society

- Society expects members of a profession:
  - To provide significant benefits
  - To not cause harm through their actions
- Professional organizations provide **codes of ethics to guide** IT workers' actions.
- Actions of **an IT worker can affect society.**

Relationships Between IT Workers and IT Users

- **IT user**: person using a hardware or software product

IT workers' duties:

- Understand users' needs and capabilities
- Deliver products and services that meet those needs
- Establish an environment that supports ethical behavior:
    - To discourages software piracy
    - To minimize inappropriate use of corporate computing resources
    - To avoid inappropriate sharing of information

IT Users – supporting ethical issues

- Establishing Guidelines for Use of Company Software
- Company IT managers must provide clear rules that govern the use of home computers and associated software.

Professional Codes of Ethics

- **Professional code of ethics** states the principles and core values that are essential to the work of a particular occupational group**.**
- **Most codes of ethics include**:
  - What the **organization aspires to become**
  - **Rules and principles** by which members of the organization are expected to abide
  - Many codes also include **commitment** to continuing education for those who practice the profession

Professional Codes of Ethics

- Following a professional code of ethics can produce benefits for the individual, the profession, and society as a whole:

  - **Ethical decision making:**
    practitioners use a common set of core values and beliefs as a guideline for ethical decision making.
  - **High standards of practice & ethical behavior:**

    Adherence to a code of ethics reminds **professionals of the responsibilities and duties** that they may be tempted to compromise to meet the pressures of day-to-day business.

    The code also defines **acceptable and unacceptable behaviors** to guide professionals in their interactions with others.

    Strong codes of ethics have procedures for censuring professionals for serious violations, with penalties that can include the loss of the right to practice

  - **Trust and respect from general public:**

  Adherence to a code of ethics enhances trust and respect for professionals and their profession
  - **Evaluation benchmark for self-assessment:**

    A professional can use as a means of self-assessment. Peers of the professional can also use the code for recognition or censure.

Professional Organizations

Four of the most prominent organizations include:

- Association for Computing Machinery (ACM)
- Institute of Electrical and Electronics Engineers Computer Society (IEEE-CS)
- Association of IT Professionals (AITP)
- SysAdmin, Audit, Network, Security (SANS) Institute

Certification: indicates that a professional possesses a particular set of skills, knowledge, or abilities in the opinion of the certifying organization.

- Can also apply to products
- Generally voluntary
- May or may not require **adherence** to a code of ethics
- Employers view as **benchmark of knowledge**
- Opinions are divided on the **value of certification**

Vendor Certifications

Vendor Certifications

workers

salaries and career prospects

or certain

aspects of broader roles

hands-on lab to demonstrate skills and knowledge

necessary experience

expensive

Industry association certifications

Industry association certifications

perspective than vendor certifications

written exam

that new technologies

business, and behavioral competencies

Industry Association Certifications

Certificate	Subject matter
Microsoft Certified Technology Specialist	Designing and optimizing solutions based on Microsoft products and technologies
Cisco Certified Internetwork Expert	Managing and troubleshooting large networks
Cisco Certified Network Professional Security	Configuring and designing firewalls and the security settings on routers and switches
CompTIA A+	Performing computer and network maintenance, troubleshooting, and installation—including addressing security issues
Project Management Institute's Project Management Professional (PMP)	Leading and directing projects

Government Licensing

- **License** is a government-issued permission to engage in an activity or operate a business
- Generally administered at the state level in the United States often requires that recipient pass a test.
- Some professionals must be licensed – doctors, lawyers, CPAs, medical and day care providers, engineers

  One goal: protect public safety
- Without licensing, there are no requirements for heightened care and no concept of professional malpractice
- fishing; hunting; marrying; driving a motor vehicle; providing health care services; practicing law; manufacturing; engaging in retail and wholesale commerce; operating a private business, trade, or technical school;

Issues associated with government licensing of IT workers:

- There are few licensing programs for IT professionals:
- There is no universally accepted core body of knowledge
- It is unclear who should manage content and administration of licensing exams
- There is no administrative body to accredit professional education programs.
- There is no administrative body to assess and ensure competence of individual workers

.

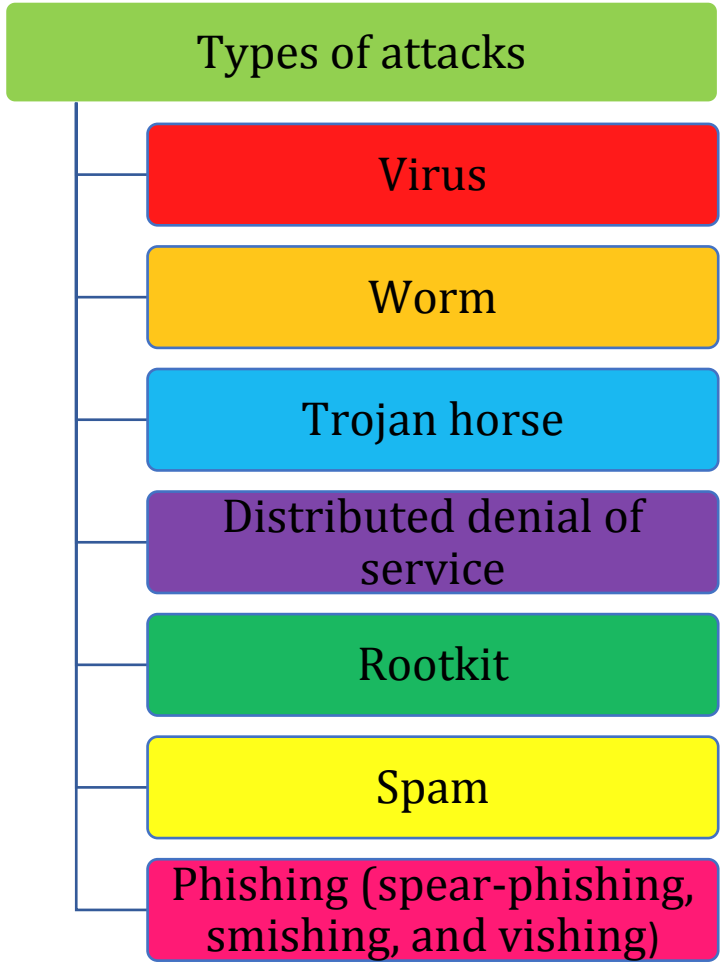
.

IT Professional Malpractice

- **Negligence:** not doing something that a reasonable person would do, or doing something that a reasonable person would not do.
- **Duty of care**: refers to the obligation to protect people against any unreasonable harm or risk.
- **Reasonable person standard** – to evaluate how an objective, careful and conscientious person would have acted in the same circumstances.
- **Reasonable professional standard** – defendants who have particular expertise or competence are measured.
- A **breach of the duty of care** is the failure to act as a reasonable person would act. A breach of duty might consist of an action, such as throwing a lit cigarette into a fireworks factory and causing an explosion, or a failure to act when there is a duty to do so—for example, a police officer not protecting a citizen from an attacker.
- Professionals who breach the duty of care are liable for injuries that their negligence causes. This liability is commonly referred to as **professional malpractice**.
- For example, a CPA who fails to use reasonable care, knowledge, skill, and judgment when auditing a client's books is liable for accounting malpractice.
- Professionals who breach this duty are liable to their patients or clients, and possibly to some third parties.

Types of Exploits

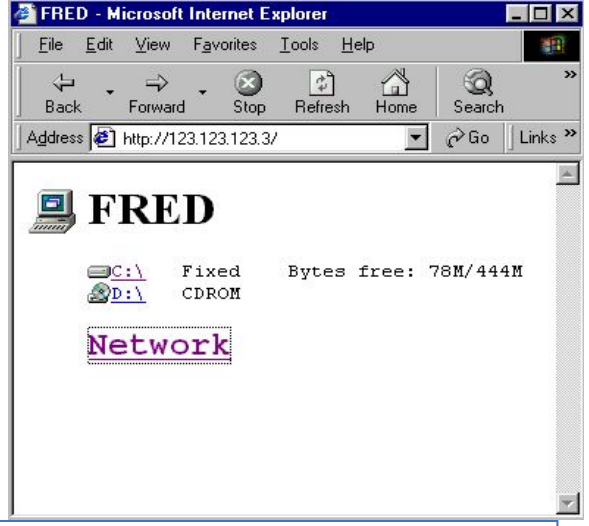
Computers as well as smartphones can be target



Worms

A **worm** is a harmful program that resides in the active memory of the computer and duplicates itself.

Worms differ from viruses in that they can propagate without human intervention, often sending copies of themselves to other computers by email.



A **worm** is a program that makes copies of itself and causes major damage to the files, software, and data

- **Method of replication:**
  - Email
  - File sharing

W32/Bugbear-A

- is a network worm that spreads by emailing attachments of itself
- It creates a thread which attempts to terminate anti-virus and security programs
- The worm will log keystrokes and send this information when the user is connected online
- The worm will open port 80 on the infected computer

Trojan Horses- when the user downloads and installs a file onto their system

- A **Trojan horse** is a program in which malicious code is hidden inside a seemingly harmless program.
- The program's harmful payload might be designed to enable the hacker to destroy **hard drives, corrupt files, control the computer remotely, launch attacks against other computers, steal passwords or Social Security numbers, or spy on users by recording keystrokes and transmitting them to a server operated by a third party.**
- This opens a port without the knowledge of the user. The open port gives the remote user access to one's computer.
- Delivered via email attachment, downloaded from a Web site, or contracted via a removable media device
- **Logic bomb**
  - Another type of Trojan horse
  - Executes when triggered by certain event
  - For example, logic bombs can be triggered by a change in a particular file, by typing a specific series of keystrokes, or by a specific time or date.

Distributed Denial-of-Service (DDoS) Attacks

- A **distributed denial-of-service (DDoS) attack** is one in which a malicious hacker takes over computers via the Internet and causes them to flood a target site with demands for data and other small tasks.
- A distributed denial-of-service attack does not involve infiltration of the targeted system.
- The computers that are taken over are called **zombies**.
- **Botnet** is a very large of such computers.
- Botnets are installed by virus or worm, allow remote unreserved access to the system.
- Does not involve a break-in at the target computer
- Target machine is busy responding to a stream of automated requests
- Legitimate users cannot access target machine

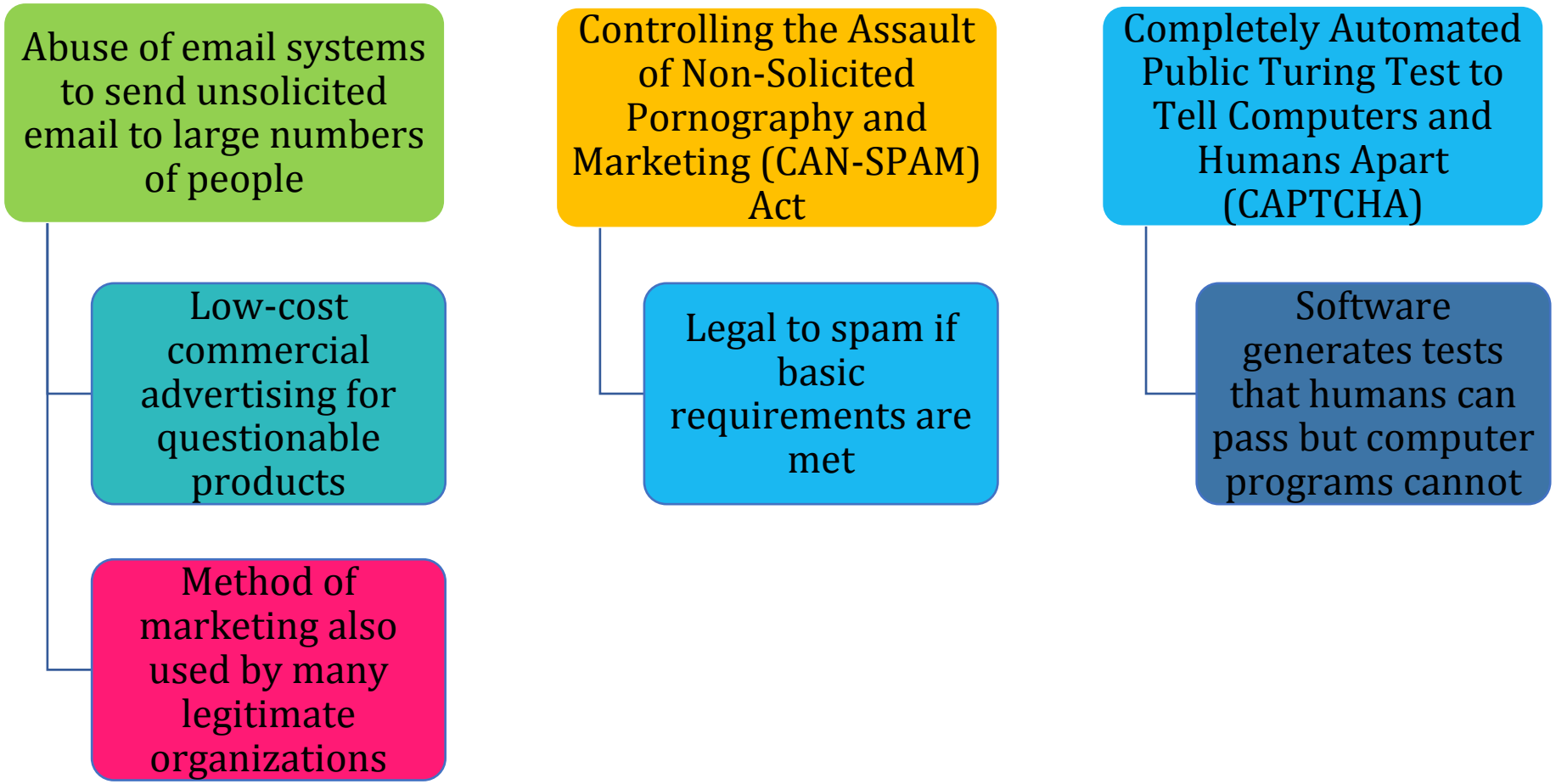
Rootkits

- A **rootkit** is a set of programs that enables its user to gain administrator-level access to a computer without the end user's consent or knowledge.
- Once installed, the attacker can gain full control of the system and even obscure the presence of the rootkit from legitimate system administrators.
- Attackers can use the rootkit to **execute files, access logs, monitor user activity, and change the computer's configuration.**
- **Rootkits** are one part of a blended threat, consisting of the **dropper, loader, and rootkit.**
- The **dropper code** gets the rootkit **installation started** and can be **activated by clicking on a li**nk to a malicious Website in an email or opening an infected PDF file.
- The **dropper launches the loader program** and then **deletes itself**.
- The **loader loads the rootkit** into memory; at that point, the computer has been compromised.
- Rootkits are designed so cleverly that it is difficult even to discover if they are installed on a computer.

Symptoms of rootkit infections:

- The computer locks up or fails to respond to input from the keyboard or mouse.
- The screen saver changes without any action on the part of the user.
- The taskbar disappears.
- Network activities function extremely slowly.

Spam


Abuse of email systems to send unsolicited email to large numbers of people
Low-cost commercial advertising for questionable products
Method of marketing also used by many legitimate organizations
Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act
Legal to spam if basic requirements are met
Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA)
Software generates tests that humans can pass but computer programs cannot

Phishing

- **Phishing** is the act of fraudulently using email to try to get the recipient to reveal personal data.
- In a phishing scam, con artists send legitimate-looking emails urging the recipient to take action to avoid a negative consequence or to receive a reward.
- The requested action may involve clicking on a link to a Web site or opening an email attachment.
- **Spear-phishing** is a variation of phishing in which the phisher sends fraudulent emails to a certain organization's employees.
- It is known as spear-phishing because the attack is much more precise and narrow, like the tip of a spear.

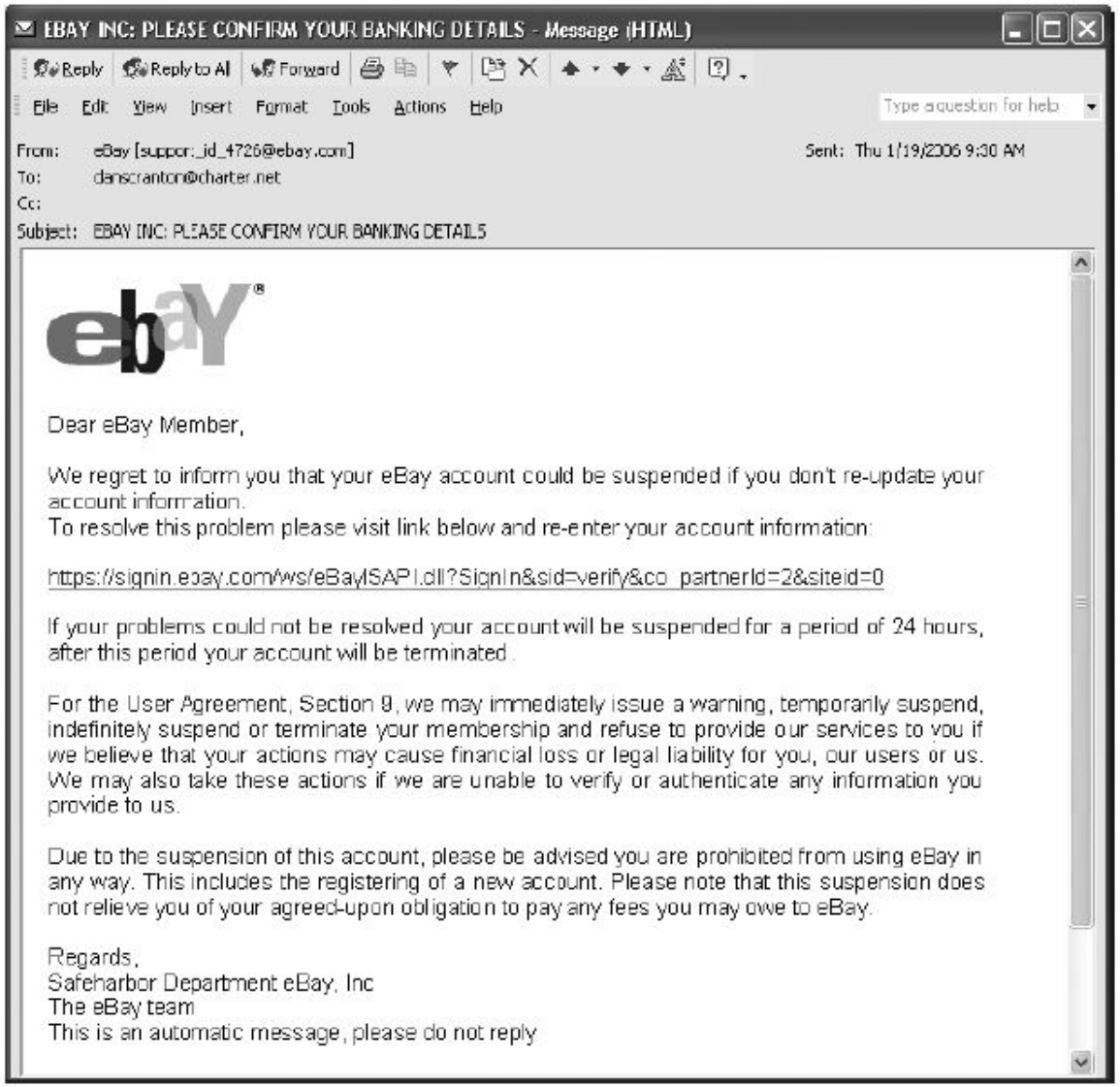


FIGURE 3-3 Example of phishing

Source Line: Course Technology/Cengage Learning.

Smishing & Vishing

- **Smishing** is another variation of phishing that involves the use of Short Message Service (SMS) texting.
- In a smishing scam, people receive a legitimate-looking text message on their phone telling them to call a specific phone number or to log on to a Web site. This is often done under the guise that there is a problem with their bank account or credit card that requires immediate attention.
- **Vishing** is similar to smishing except that the victims receive a voice mail telling them to call a phone number or access a Web site.

The C I A Security Triad

- **Confidentiality** ensures that only those individuals with the proper authority can access sensitive data such as employee personal data, customer and product sales data, and new product and advertising plans.
- **Integrity** ensures that data can only be changed by authorized individuals so that the accuracy, consistency, and trustworthiness of data are guaranteed.
- **Availability** ensures that the data can be accessed when and where needed, including during times of both normal and disaster recovery operations.
- **Confidentiality, integrity, and availability** are referred to as the **CIA security triad**.

Information Technology Act, 2000

Information Technology Act, 2000

- The **Information Technology Act, 2000** (also known as **ITA-2000**, or the **IT Act**) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000.
- It is the primary law in India dealing with cybercrime and electronic commerce.
- It is based on the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model) recommended by the general assembly of United Nations by a resolution dated 30th January 1997.

- The laws apply to the whole of India.
- Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India.

Information Technology Act 2000, has 13 chapters, 94 sections and 4 schedules.

- First 14 sections deals with some legal aspects concerning digital signature.
- Further other sections deal with certifying authorities who are licensed to issue digital signature certificate.
- Sections 43 to 47 provide for penalties and compensation.
- Sections 48 to 64 deals with Tribunals a appeal to high court.
- Section 65 to 79 of the act deals with offences.
- Section 80 to 94 deals with miscellaneous of the Act.

Definitions (section 2)

- "computer" means electronic, magnetic, optical or other high-speed date processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or relates to the computer in a computer system or computer network;
- "computer network" means the inter-connection of one or more computers through-
- (i) the use of satellite, microwave, terrestrial lime or other communication media; and
- (ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

Definitions (section 2)

- "computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable being used in conjunction with external files which contain computer programmes, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions;
- "data" means a representation of information, knowledge, facts, concepts or instruction which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

Definitions (section 2)

- "electronic record" means date, record or date generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;
- “secure system” means computer hardware, software, and procedure that-

  (a) are reasonably secure from unauthorized access and misuse;

  (b) provide a reasonable level of reliability and correct operation;

  (c) are reasonably suited to performing the intended function; and

  (d adhere to generally accepted security procedures
- “security procedure” means the security procedure prescribed by the Central Government under the IT Act, 2000.
- “secure electronic record” – where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification

Commission of cyber crime

Three basic groups:

- Individual
- Organisation
- Society at Large

Against Individual

- Harassment via Emails
- Cyber Stalking
- Dissemination of obscene material
- Defamation
- Hacking/Cracking
- Indecent Exposure

Individual Property

- Computer Vandalism
- Transmitting Virus
- Network Trespassing
- Unauthorized Control over Computer System
- Hacking/Cracking

Against Organisation

- Hacking & Cracking
- Possession of unauthorised Information
- Cyber- Terrorism against Government Organisation
- Distribution of Pirated Software Etc

Against Society at Large

- Pornography
- Polluting the youth through indecent exposure
- Trafficking

Section	Offence	Description	Penalty
65	Tampering with computer source documents	If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	Imprisonment up to three years, or/and with fine up to ₹200,000
66	Hacking with computer system	If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.	Imprisonment up to three years, or/and with fine up to ₹500,000

66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.	Imprisonment up to three years, or/and with fine up to ₹100,000
66C	Using password of another person	A person fraudulently uses the password, digital signature or other unique identification of another person.	Imprisonment up to three years, or/and with fine up to ₹100,000
66D	Cheating using computer resource	If a person cheats someone using a computer resource or communication.	Imprisonment up to three years, or/and with fine up to ₹100,000
66E	Publishing private images of others	If a person capture, transmits or publishes images of a person's private parts without his/her consent or knowledge.	Imprisonment up to three years, or/and with fine up to ₹200,000

66F	Acts of cyberterrorism	If a person denies access to an authorised personnel to a computer resource, accesses a protected system or introduces contaminant into a system, which the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyberterrorism.	Imprisonment up to life.
67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	Imprisonment up to five years, or/and with fine up to ₹1,000,000
67A	Publishing images containing sexual acts	If a person publishes or transmits images containing a sexual explicit act or conduct.	Imprisonment up to seven years, or/and with fine up to ₹1,000,000

67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18.	Imprisonment up to five years, or/and with fine up to ₹1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to ₹1,000,000 on second conviction.
67C	Failure to maintain records	Persons deemed as intermediatary (such as an ISP) must maintain required records for stipulated time. Failure is an offence.	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder. Any person who fails to comply with any such order shall be guilty of an offence.	Imprisonment up to three years, or/and with fine up to ₹200,000

69	Failure/refusal to decrypt data	If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person incharge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.	Imprisonment up to seven years and possible fine.

70	Securing access or attempting to secure access to a protected system	The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment up to three years, or/and with fine up to ₹100,000

Electronic World

- Electronic document produced by a computer. Stored in digital form, and cannot be perceived without using a computer
  - It can be deleted, modified and rewritten without leaving a mark
  - Integrity of an electronic document is “genetically” impossible to verify
  - A copy is indistinguishable from the original
  - It can’t be sealed in the traditional way, where the author affixes his signature
- The functions of identification, declaration, proof of electronic documents carried out using a digital signature based on cryptography.

Electronic World

- A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It's the **digital equivalent of a handwritten signature or stamped seal**, but it offers far more inherent security. A digital signature is intended to solve the problem of **tampering and impersonation** in digital communications.
- Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages.
- Digital signatures created and verified using cryptography.
- Public key System based on Asymmetric keys
  - An algorithm generates two different and related keys
    - Public key $(P_{U,} P_{R})$
    - Private Key
  - Private key used to digitally sign.
  - Public key used to verify.

Role of the Government

- Government has to provide the definition of
  - the structure of PKI
  - the number of levels of authority and their juridical form (public or private certification)
  - which authorities are allowed to issue key pairs
  - the extent to which the use of cryptography should be authorised for confidentiality purposes
  - whether the Central Authority should have access to the encrypted information; when and how
  - the key length, its security standard and its time validity

Section 3 Defines Digital Signatures

- The authentication to be affected by use of asymmetric crypto system and hash function
- The private key and the public key are unique to the subscriber and constitute functioning key pair
- Verification of electronic record possible

THE CIA SECURITY TRIAD

- **Confidentiality** ensures that only those individuals with the **proper authority** can access **sensitive data** such as employee personal data, customer and product sales data, and new product and advertising plans.
- **Integrity** ensures that data can only be **changed by authorized individuals** so that **the accuracy, consistency, and trustworthiness of data** are guaranteed.
- **Availability** ensures that the **data can be accessed** when and where needed, including during times of both normal and disaster recovery operations

Confidentiality

Confidentiality: It refers to preventing the disclosure of information to unauthorized individuals or systems. Privacy or the ability to control or restrict access so that only authorized individuals can view sensitive information. One of the underlying principles of confidentiality is "need-to-know" or "least privilege". In effect, access to vital information should be limited only to those individuals who have a specific need to see or use that information.Confidentiality is necessary for maintaining the privacy of the people whose personal information a system holds.

For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Integrity

Integrity: Information is accurate and reliable and has not been subtly changed or tampered with by an unauthorized party. Integrityincludes:

- Authenticity: The ability to verify content has not changed in an unauthorized manner.
- Non-repudiation & Accountability: The origin of any action on the system can be verified and associated with a user.

The term Integrity is used frequently when considering Information Security as it is represents one of the primary indicators of security (or lack of it). The integrity of data is not only whether the data is 'correct', but whether it can be trusted and relied upon.Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people.

Availability

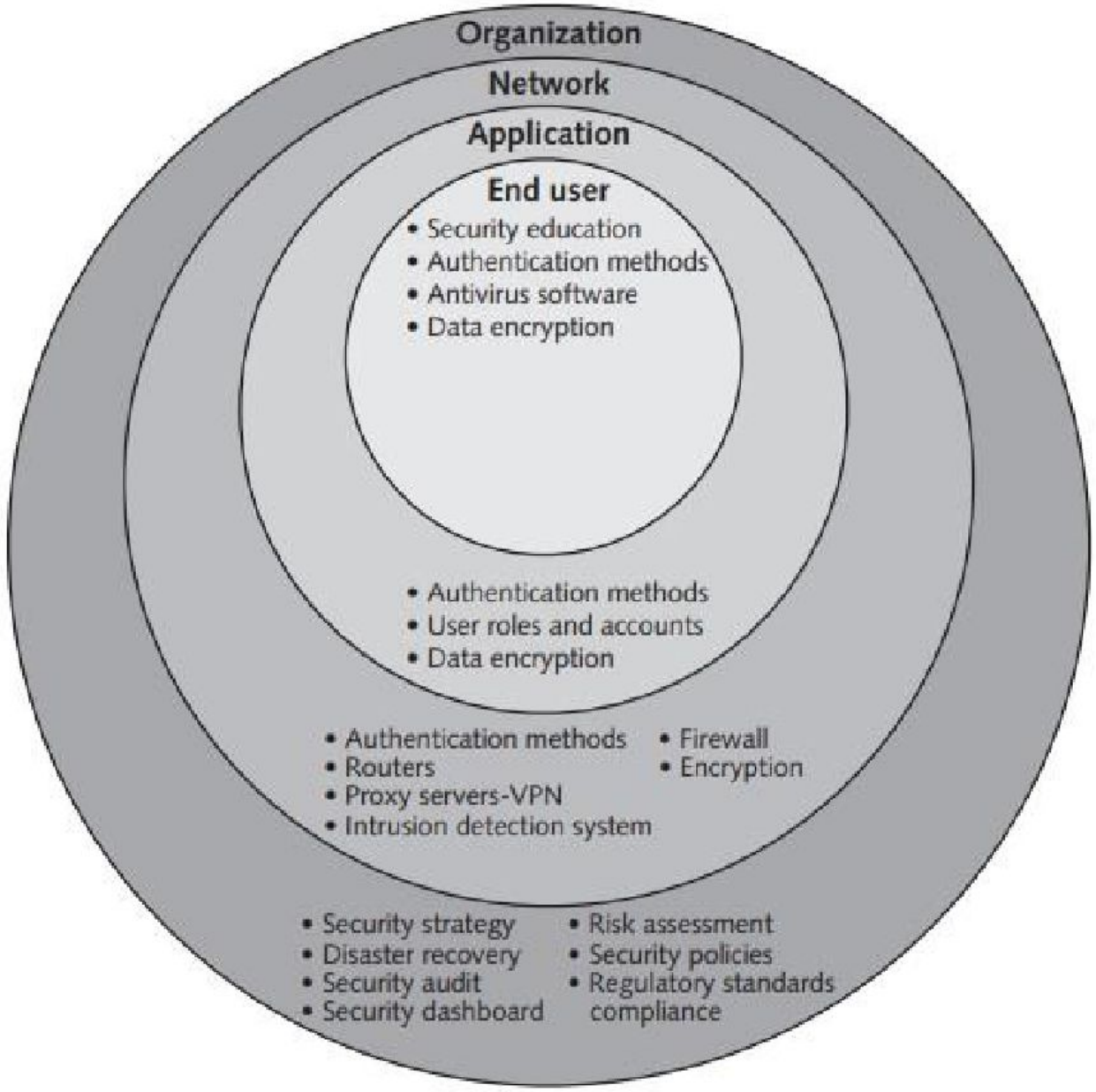
Availability: For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks. Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

It is important to note that confidentiality, integrity and availability are not the exclusive concern of information security. Business continuity planning places a significant emphasis on protecting the availability of information as part of the overall objective of business recovery. Common back office procedures, such as maker/checker, quality assurance, change control, etc. along with such regulatory areas as SOX 404(SOX or Sarbanes-Oxley Act is nothing but the USA version of Clause 49) focus on ensuring the integrity of information.

CIA

CIA	Risks	Controls/Remedy	Primary Focus
Confidentiality	Loss of privacy. Unauthorized access to information. Identity Theft	Encryption, Authentication, Access controls	Information Security
Integrity	Information is no longer reliable or confidence, Loss of revenue	Maker/Checker, Quality Assurance, storage, Sufficient capacity	Operational Planning
Availability	Business disruption, Loss of customer	BCP Plans and Tests, Back-up	Business Continuity

CIA Security Triad



Implementing CIA at the Organization Level

- Security Strategy
- Risk Assessment
- Disaster Recovery
- Security Policies
- Security Audits
- Regulatory Standards Compliance
- Security Dashboard

Implementing CIA at the Network Level

- Authentication Methods
- Firewall - next-generation firewall (NGFW)
- Routers
- Encryption
- Proxy Servers and Virtual Private Networks
- Intrusion Detection System

Implementing CIA at the Network Level

- A **firewall** is a system of software, hardware, or a combination of both that stands guard between an organization's internal network and the Internet and limits network access based on the organization's access policy.
- A **next-generation firewall (NGFW)** is a hardware- or software-based network security system that is able to detect and block sophisticated attacks by filtering network traffic dependent on the packet contents.
- A **router** is a networking device that connects multiple networks together and forwards data packets from one network to another.
- A **proxy server** serves as an intermediary between a web browser and another server on the Internet that makes requests to websites, servers, and services on the Internet for you.
- A **VPN** enables remote users to securely access an organization's collection of computing and storage devices and share data remotely.

Proxy Servers and Virtual Private Networks

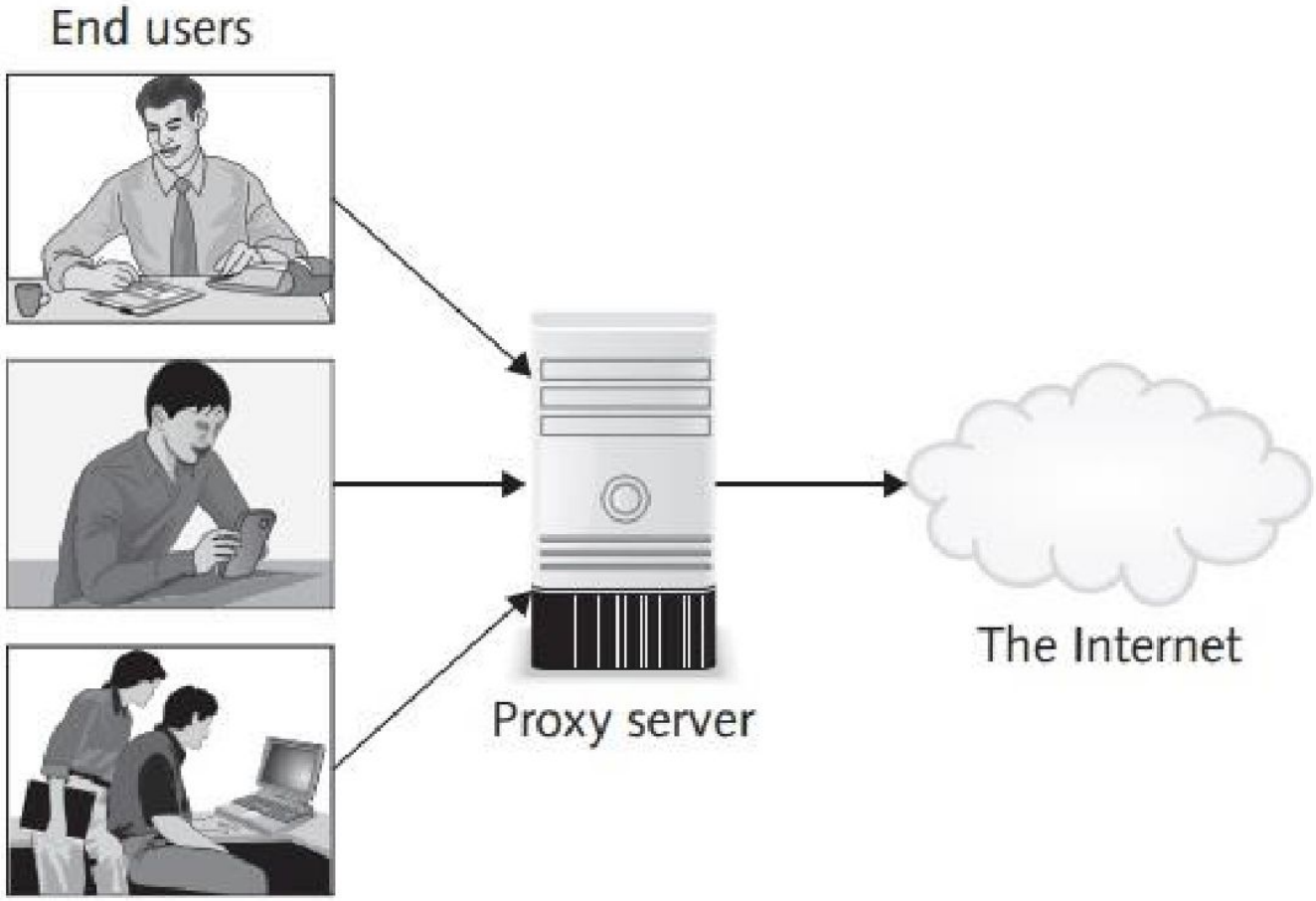


FIGURE 3-6 Proxy server

Intrusion detection system (IDS)

- An intrusion detection system (IDS) is software and/or hardware that monitors system and network resources and activities and notifies network security personnel when it detects network traffic that attempts to circumvent the security measures of a networked computer environment.

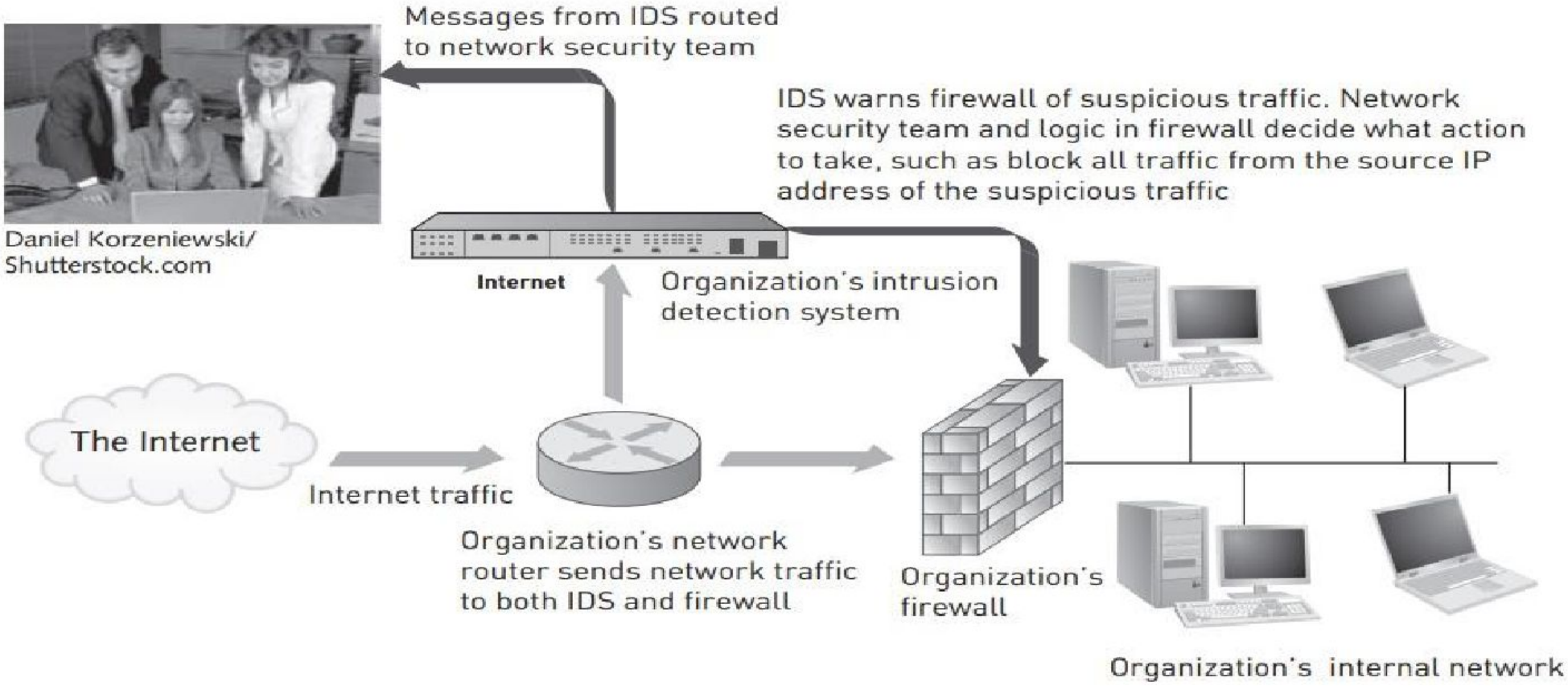


FIGURE 3-7 Intrusion detection system

Implementing CIA at the Application Level

- Authentication Methods
- Two-factor authentication requires the user to provide two types of credential before being able to access an account; the two credentials can be any of the following:
    - PIN or password
    - Some form of security card or token
    - Such as a biometric (for example, a fingerprint or retina scan)
    - User Roles and Accounts
    - Data Encryption
    - enterprise resource planning (ERP), customer relationship management (CRM), and product lifecycle management (PLM)

Implementing CIA at the End-User Level

- Security Education
- Authentication Methods
- Antivirus Software
- Data Encryption
- Security Education
    - Guarding their passwords to protect against unauthorized access to their accounts
    - Prohibiting others from using their passwords
    - Applying strict access controls (file and directory permissions) to protect data from disclosure or destruction
    - Reporting all unusual activity to the organization’s IT security group
    - Taking care to ensure that portable computing and data storage devices are protected (hundreds of thousands of laptops are lost or stolen per year)