CPA BEC - STUDY UNIT 15
Information Technology V: Core Concepts

A. Electronic Commerce

1. **E-business** is an umbrella term referring to all methods of conducting business electronically. This can include strictly internal communications as well as nonfinancial dealings with outside parties (e.g., contract negotiations).
   a. **E-commerce** is a narrower term referring to financial transactions with outside parties, e.g., the purchase and sale of goods and services.
2. **Business-to-business commerce (B2B)** is not limited to EDI and other direct links between businesses but also involves activities within the broader electronic market. B2B involves working with vendors, distributors, and other businesses over the Internet.
   a. **Benefits of B2B** include reduced purchasing costs, increased market efficiency, greater market intelligence, and decreased inventory levels.
3. Because e-commerce transactions cross the boundaries of the enterprise, security is of primary concern.
   a. **Responses to security issues** include such measures as encryption and numerical sequencing.

B. Electronic Data Interchange (EDI)

1. **Electronic data interchange (EDI)** is the leading method of carrying on e-commerce.
   a. EDI involves the communication of data in format agreed to by the parties directly from a computer in one entity to a computer in another entity, for example, to order goods from a supplier or to transfer funds.
   b. **Advantages** of EDI include reduction of clerical errors, speed of transactions, and the elimination of repetitive clerical tasks, such as document preparation, processing, and mailing.
   c. **Disadvantages** of EDI include the following: information may be insecure, data may be lost, transmissions to trading partners may fail, and EDI is less standardized and more costly than Internet-based commerce, which ordinarily uses XML.
2. **Value-added networks (VANs)** are private, third-party providers of common interfaces between organizations.
   a. An **extranet** is another means of carrying on e-commerce.

C. Electronic Funds Transfer (EFT)

1. EFT is a service provided by financial institutions worldwide that is based on electronic data interchange (EDI) technology.
   a. An EFT is a **transfer of funds** via an access device, i.e., an electronic terminal (e.g., ATM or POS terminal), telephone, computer, or magnetic tape (e.g., credit, debit, and check cards).
   b. EFT transaction costs are lower than for manual systems because documents and human intervention are eliminated from the transaction process. Moreover, transfer customarily requires less than a day.
   c. A typical consumer application of EFT is the **direct deposit** of payroll checks in employees' accounts or the automatic withdrawal of payments for cable and telephone bills, mortgages, etc.

2. The most important application of EFT is **check collection**. Because of the enormous volume of paper, the check-collection process has been computerized.
3. EFT differs from the use of **electronic money**, which may someday supplant traditional currency and coins. For example, stored-value cards (such as phone cards) are already in wide use.

D. Point-of-Sale (POS) Transactions

1. Electronic POS systems permit **instant capture** (for example, by bar code scanning) and transmission of retail transactional information. A POS system allows the retailer to update and analyze the perpetual inventory records for each outlet and provide marketing information.

E. Electronic Transaction Security

1. **Encryption** technology is vital for the security and therefore the success of electronic commerce, especially with regard to transactions carried out over public networks.
    - a. The sender's encryption program encodes the data prior to transmission. The recipient's program decodes it at the other end. Unauthorized users may be able to intercept the data but, without the encryption key, they will be unable to decode it.
    - b. Two major types of encryption routine are in general use.
        - 1) **Private-key**, or symmetric, encryption is the less secure of the two because there is only one key. The single key must be revealed to both the sender and recipient.
        - 2) **Public-key**, or asymmetric, encryption is the more secure of the two. The public key used by the sender for encoding is widely known, but the related private key used by the recipient for decoding is known only to the recipient.
            - a) The analogy is a post office box. The box number is known to all and anyone can send a letter to it, but only the box owner can retrieve the letters.

F. Malicious Software and Attacks

1. Malicious software (malware) may exploit a known hole or weakness in an application or operating system program to evade security measures. Types of malware include **Trojan horse, virus, worm, logic bomb, and back door**. Malware may create a denial of service by overwhelming a system or website with more traffic than it can handle.
2. **Controls** to prevent or detect infection by malware are particularly significant for file servers in large networks.
3. All organizations involved in electronic commerce must have an intrusion detection system (IDS). The goal of an IDS is to detect breaches of an organization's information security regime before they can do damage.