

# STUDY UNIT FIFTEEN

## INFORMATION TECHNOLOGY V

15.1	<i>Electronic Commerce</i>	1
15.2	<i>Electronic Data Interchange (EDI)</i>	3
15.3	<i>Electronic Funds Transfer (EFT)</i>	5
15.4	<i>Point-of-Sale (POS) Transactions</i>	7
15.5	<i>Electronic Transaction Security</i>	7
15.6	<i>Malicious Software and Attacks</i>	8

This study unit is the last of five covering information technology (IT). E-commerce is the purchase and sale of goods and services by electronic means. E-business is a more comprehensive term defined as all methods of conducting business electronically. E-commerce may occur via online transactions over public networks (e.g., the Internet), electronic data interchange (EDI), electronic funds transfer (EFT), and email. Moreover, even traditional point-of-sale (POS) transactions have become part of e-commerce through the use of IT methods that allow instant capture of business information.

### 15.1 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.
    - 1) E-commerce comes in two basic varieties, business-to-business (B2B) and business-to-consumer (B2C). E-business and e-commerce are sometimes considered to be synonymous.
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.
  - a. B2B involves working with vendors, distributors, and other businesses over the Internet.
  - b. There are two types of B2B companies:
    - 1) **Vertical companies** work at all levels within an industry and mostly earn their revenues from advertising on a specialized sector or from transaction fees from the e-commerce they may host.
      - a) Websites of vertical companies are the most likely to contain such community features as industry news, articles, and discussion groups.
    - 2) **Horizontal companies** operate across numerous industries.
      - a) They provide products, goods, materials, or services that are not specific to a particular industry or company.

- c. **Benefits of B2B** include
  - 1) Reduced purchasing costs. Purchasing products online saves time, and electronically processing an order simplifies the ordering process.
  - 2) Increased market efficiency. By using the Internet, companies have easy access to price quotes from various suppliers. Buyers are more likely to get a better price, given the increased number of suppliers.
  - 3) Greater market intelligence. B2B provides producers with better insights into the demand levels in any given market.
  - 4) Decreased inventory levels. Companies can make better use of their inventory and raw materials. The Internet allows companies using JIT manufacturing techniques to achieve better control of their operations, for example, by more precise coordination of delivery of raw materials. It also allows companies to use less working capital to do the same amount of work, which allows those funds to be invested elsewhere.
- d. The overriding principle of online B2B is that it can make companies more efficient. Increased efficiency means lower costs, which is a goal that interests every company. Thus, the potential of B2B online commerce is enormous.
- 3. Because e-commerce transactions cross the boundaries of the enterprise, security is of primary concern.
  - a. **Security issues** include
    - 1) The correct identification of the transacting parties (authentication)
    - 2) Determination of who may rightfully make binding agreements (authorization)
    - 3) Protecting the confidentiality and integrity of information
    - 4) Assuring the trustworthiness of listed prices and discounts
    - 5) Providing evidence of the transmission and receipt of documents
    - 6) Guarding against repudiation by the sender or recipient
    - 7) The proper extent of verification of payment data
    - 8) The best method of payment to avoid wrongdoing or disagreements
    - 9) Lost or duplicated transactions
    - 10) Determining who bears the risk of fraud
  - b. **Responses to security issues** include
    - 1) Encryption and associated authentication methods, preferably by physically secure hardware rather than software
    - 2) Numerical sequencing to identify missing or false messages
    - 3) The capacity of the host computer to avoid downtime and repel attacks
    - 4) Nonrepudiation methods, such as digital certificates, which prove origination and delivery so that parties cannot disclaim responsibility for sending or receiving a message
      - a) Sellers and buyers routinely provide acknowledgments and confirmations, respectively, in a website dialogue to avoid later disputes.
      - b) In EDI (see Subunit 15.2), control over nonrepudiation is achieved by sequencing, encryption, and authentication.
    - 5) Adherence to legal requirements, such as privacy statutes
    - 6) Documenting trading agreements, especially the terms of trade and methods of authorization and authentication
    - 7) Agreements for end-to-end security and availability with providers of information services and value-added networks (see item 3.b. on page 4)
    - 8) Disclosure by public trading systems of their terms of business

## 15.2 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. EDI was the first step in the evolution of e-business.
    - 1) Successful EDI implementation begins with mapping the work processes and flows that support achievement of the organization's objectives.
    - 2) EDI was developed to enhance just-in-time (JIT) inventory management.
  - c. **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.
  - d. **Disadvantages** of EDI include the following:
    - 1) Information may be insecure.
      - a) Thus, end-to-end data encryption should be used to protect data during EDI.
    - 2) Data may be lost.
    - 3) Transmissions to trading partners may fail.
    - 4) EDI is less standardized and more costly than Internet-based commerce, which ordinarily uses XML.
      - a) EDI requires programming expertise and leased telephone lines or the use of a value-added or third-party network, whereas XML is simple and easy to understand.
  - e. An extension of EDI is computer-stored records, which can be less expensive than traditional physical file storage.
2. **Terms and components** of EDI include the following:
  - a. Standards concern procedures to convert written documents into a standard electronic document-messaging format to facilitate EDI.
  - b. Conventions are the procedures for arranging data elements in specified formats for various accounting transactions, e.g., invoices, materials releases, and advance shipment notices.
  - c. A data dictionary prescribes the meaning of data elements, including specification of each transaction structure.
  - d. Transmission protocols are rules used to determine how each electronic envelope is structured and processed by the communications devices.
    - 1) Normally, a group of accounting transactions is combined in an electronic envelope and transmitted into a communications network.
    - 2) Rules are required for the separation and transmission of envelopes.
3. **Methods of communication** between computers include the following:
  - a. A point-to-point system requires the use of dedicated computers by all parties.
    - 1) Each computer must be designed to be compatible with the other(s). This system is very similar to a network within one company. Dedicated lines or modems are used.

- b. Value-added networks (VANs) are private, third-party providers of common interfaces between organizations.
    - 1) Subscribing to a VAN eliminates the need for one organization to establish direct computer communication with a trading partner.
    - 2) VANs provide translation of the sender's protocol (data configuration) to the receiver's protocol. Thus, the sender and receiver do not have to conform to the same standards, conventions, and protocols.
    - 3) Moreover, VANs eliminate the need for dedicated computers waiting for incoming messages.
    - 4) In addition, VANs store messages so companies can batch outgoing and incoming messages.
  - c. An **extranet** is another means of carrying on e-commerce.
    - 1) Extranets rely on the established communications protocols of the Internet. Thus, the expensive, specialized equipment needed for EDI is unnecessary.
    - 2) **Firewalls**, special combinations of hardware and software [see item 3.a.6)c) in Subunit 13.2], provide security.
    - 3) The extranet approach is based on less formal agreements between the trading partners than in EDI and requires the sending firm to format the documents into the format of the receiving firm.
4. The use of EDI has certain **implications for control**.
- a. EDI eliminates the paper documents, both internal and external, that are the traditional basis for many controls, including internal and external auditing.
  - b. Moreover, an organization that has reengineered its processes to take full advantage of EDI may have eliminated even the electronic equivalents of paper documents.
    - 1) For example, the buyer's **point-of-sale (POS)** system may directly transmit information to the seller, which delivers on a JIT basis. Purchase orders, invoices, and receiving reports are eliminated and replaced with
      - a) Evaluated receipts settlements (authorizations for automatic periodic payment);
      - b) A long-term contract establishing quantities, prices, and delivery schedules;
      - c) Production schedules;
      - d) Advance ship notices; and
      - e) Payments by EFT.
  - c. Accordingly, auditors must seek new forms of evidence to support assertions about EDI transactions, whether it exists at the client organization, the trading partner, or a third party, such as a VAN.
    - 1) Examples of such evidence are
      - a) The authorized paper purchase contract,
      - b) An electronic completed production schedule image, and
      - c) Internal and external evidence of evaluated receipts settlements sent to the trading partner.
    - 2) Auditors must evaluate digital signatures and reviews when testing controls.
    - 3) Auditors may need to consider other subsystems when testing a particular subsystem. Thus, production cycle evidence may be needed to test the expenditure cycle.

### 15.3 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.
  - a. The result has been to reduce the significance of paper checks because EFT provides means to make payments and deposit funds without manual transfer of negotiable instruments. Thus, wholesale EFTs among financial institutions and businesses (commercial transfers) are measured in the trillions of dollars.
    - 1) The two major systems for these "wire" or nonconsumer transfers are Fedwire (Federal Reserve wire transfer network) and CHIPS (New York Clearing House Interbank Payment System). Private systems also are operated by large banks.
3. The emergence of EFT systems offered by financial institutions created a need to refine consumer protection legislation. Hence, Congress enacted the **Electronic Fund Transfer Act of 1978 (EFTA)** to regulate electronic banking services.
  - a. The primary purpose of the EFTA is to provide disclosure to consumers who use these services. EFT services include
    - 1) Automatic teller machines (ATMs),
    - 2) Point-of-sale systems (POS),
    - 3) Direct deposit and payment, and
    - 4) Payment by telephone (PBT).
  - b. The EFTA applies to banks, savings and loan institutions, and credit unions. It does not cover commercial transfers.
  - c. The act is implemented by the Federal Reserve through its Regulation E.
  - d. The EFTA requires that the financial institution provide an easily understandable written contract explaining the system and the consumer's rights and duties. For each EFT, the financial institution must furnish a receipt for the transaction unless it is initiated by telephone. When a receipt is required, it must set forth the following:
    - 1) Amount involved,
    - 2) Date of the transaction,
    - 3) Type of transfer,
    - 4) Identity of the account,
    - 5) Identity of any third party from whom or to whom funds are transferred, and
    - 6) Location or identification of the electronic terminal involved.
  - e. The EFTA also requires that the financial institution provide a statement, typically monthly, for each account accessible by EFT. The statement must set forth a record of transactions and must include
    - 1) The amount of fees or charges assessed for maintenance of the account,
    - 2) The balances of the account at the beginning and end of the period, and
    - 3) The address and telephone to be used in case of error.

- f. Customers have 60 days after receiving a statement to report errors. The financial institution then has 10 days after it receives a report of an error to investigate.
  - 1) If an error is found, the bank has 1 day to correct it.
    - a) As an alternative, a financial institution may credit a customer's account and then have 45 days to investigate (in contrast with the 10-day limit).
- g. To protect consumers, the EFTA sets limits on liability. Consumers are liable for a maximum of \$50 for unauthorized transfers.
  - 1) A consumer may be liable for up to \$500 if (s)he does not notify the bank within 2 business days after (s)he discovers the loss of an EFT card or personal identification number (PIN).
  - 2) If the customer does not give notice within 60 days after receiving a statement showing the transfers, (s)he has unlimited liability.
- 4. EFT differs from the use of **electronic money**, which may someday supplant traditional currency and coins.
  - a. For example, stored-value cards (such as phone cards) are already in wide use.
  - b. Smart cards contain computer chips rather than magnetized stripes. A smart card therefore can store data and security programs. It not only stores value but also authenticates transactions, such as by means of its digital signature.
    - 1) A potentially important use of smart cards is to transmit funds over the Internet as part of online banking transactions. Currently, online (virtual) banks must receive most deposits in traditional ways.
  - c. A disadvantage of electronic money is that most types are not covered by the insurance offered by the Federal Deposit Insurance Corporation (FDIC). Federal Reserve rules concerning EFT (Regulation E) also do not extend to electronic money.
    - 1) Users of electronic money are protected by the Federal Trade Commission Act of 1914 (as amended). It empowers the FTC to protect consumers from "unfair or deceptive acts or practices in or affecting commerce."
    - 2) Furthermore, common law principles, such as those pertaining to contracts and federal privacy laws, should apply.
  - d. Methods other than providing a credit card number or using electronic money may be used to make electronic payments.
    - 1) One such method is an online payment system (OPS), such as PayPal. A buyer makes a payment by a customary method to the OPS. The OPS then notifies the seller that payment has been made. The final step is to transfer the money to the seller's account.
    - 2) Another method is the electronic wallet, which is a software application that stores credit card numbers and other personal information and is usually kept on the buyer's computer. As the buyer visits different websites, (s)he can refer to the wallet instead of providing all the information for each transaction.

## 15.4 POINT-OF-SALE (POS) TRANSACTIONS

1. Electronic POS systems permit **instant capture** (for example, by bar code scanning) and transmission of retail transactional information. For example, retail and grocery stores are equipped with POS terminals that allow the instant capture of sales data, resulting in realtime updating of inventory data and reporting of sales and cash collections. A POS system may
  - a. Update and analyze the perpetual inventory records for each outlet
  - b. Perform other accounting tasks, such as crediting revenue accounts and debiting cash, accounts receivable, and cost of goods sold
  - c. Provide marketing information to
    - 1) Identify and respond to trends,
    - 2) Make sales forecasts,
    - 3) Determine which products are or are not in demand,
    - 4) Improve customer service,
    - 5) Target products and promotions to customers with different demographic traits,
    - 6) Evaluate the effects of promotions, including coupons
  - d. Help control liquid assets
  - e. Facilitate purchasing decisions
  - f. Minimize costs
  - g. Record personal and transactional information about specific customers, including tracking of warranties, deposits, rentals, progressive discounts, and special pricing
  - h. Process all forms of payment, including credit cards
  - i. Combine order processing and POS activities
  - j. Use bar coding in association with the stocking and warehousing functions to reduce the costs of data entry, including the effects of human error
  - k. Permit instant price changes
  - l. Permit integration with Internet sales applications

## 15.5 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.
    - 1) The machine instructions necessary to code and decode data can constitute a 20%-to-30% increase in system overhead.
  - 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.

- b) Since the public and private keys must form a mathematically related pair, a trusted third party is needed to issue the keys. Such a third party is called a certificate authority (CA). VeriSign is the best-known such issuer.
  - c) The most widely used public-key encryption method is RSA, named for its developers Rivest, Shamir, and Adelman.
- 2. A **digital certificate** is another means of authentication used in e-commerce. The CA issues a coded electronic certificate that contains the holder's name, a copy of its public key, a serial number, and an expiration date. The certificate verifies the holder's identity.
  - a. The recipient of a coded message uses the CA's public key (available on the Internet) to decode the certificate included in the message. The recipient then determines that the certificate was issued by the CA. Moreover, the recipient can use the sender's public key and identification data to send a coded response.
  - b. Such methods might be used for transactions between sellers and buyers using credit cards. A certificate also may be used to provide assurance to customers that a website is genuine.

## 15.6 MALICIOUS SOFTWARE AND ATTACKS

- 1. The problem of malicious software and attacks is not limited to e-commerce applications. However, it is especially important in this context because much e-commerce is conducted using publicly available systems.
  - a. Perfect security is not possible because system access cannot be eliminated without shutting down e-commerce.
  - b. Furthermore, the threats to e-commerce from malicious software and attacks are continually evolving as technology advances.
- 2. **Malicious software (malware)** may exploit a known hole or weakness in an application or operating system program to evade security measures. This kind of vulnerability may have been caused by a programming error. It may also have been intentionally (but not maliciously) created to permit a programmer simple access (a back door) to the code.
  - a. Having bypassed security controls, the intruder can do immediate damage to the system or install malware.
    - 1) A Trojan horse is an apparently innocent program (e.g., a spreadsheet) that includes a hidden function that may do damage when activated.
    - 2) A virus is a program that copies itself from file to file. The virus may destroy data or programs. A common way of spreading a virus is by email attachments and downloads.
    - 3) A worm copies itself not from file to file but from computer to computer, often very rapidly. Repeated replication overloads a system by depleting memory or overwhelming network traffic capacity.
    - 4) A logic bomb is much like a Trojan horse except it activates only upon some occurrence, e.g., on a certain date.
    - 5) A maliciously created back door can be used for subsequent high level access to data, computers, and networks.
    - 6) Malware may create a denial of service by overwhelming a system or website with more traffic than it can handle.
      - a) In other cases, a malware infection may have little or no effects noticeable by users.



3. **Controls** to prevent or detect infection by malware are particularly significant for file servers in large networks. The following are broad control objectives:
  - a. A policy should require use only of authorized software.
  - b. A policy should require adherence to licensing agreements.
  - c. A policy should create accountability for the persons authorized to maintain software.
  - d. A policy should require safeguards when data or programs are obtained by means of external media.
  - e. Antivirus software should continuously monitor the system for viruses (or worms) and eradicate them. It should also be immediately upgraded as soon as information about new threats becomes available.
  - f. Software and data for critical systems should be regularly reviewed.
  - g. Investigation of unauthorized files or amendments should be routine.
  - h. Email attachments and downloads (and files on unauthorized media or from networks that are not secure) should be checked.
  - i. Procedures should be established and responsibility assigned for coping with malware.
    - 1) Procedures should reflect an understanding that another organization that has transmitted malware-infected material may have done so unwittingly and may need assistance. If such events occur repeatedly, however, termination of agreements or contacts may be indicated.
    - 2) Procedures and policies should be documented, and employees must understand the reasons for them.
  - j. Business continuity (disaster recovery) plans should be drafted, e.g., data and software backup.
  - k. Information about malware should be verified and appropriate alerts given.
  - l. Responsible personnel should be aware of the possibility of hoaxes, false messages intending to create fear of a malware attack. For example, a spurious email message may be received instructing users to delete supposedly compromised files.
  - m. Qualified personnel should be relied upon to distinguish hoaxes from malware.
4. **Password attacks** attempt access to a system by stealing the passwords of legitimate users and then masquerading as those users.
  - a. Two principal methods are used.
    - 1) A brute-force attack uses password-cracking software to try large numbers of letter and number combinations to access a network.
      - a) A simple variation is the use of software that tries all the words in a dictionary.
    - 2) Passwords (and user accounts) also may be discovered by Trojan horses, IP spoofing, and packet sniffers.
      - a) Spoofing is identity misrepresentation in cyberspace, for example, by using a false website to obtain information about visitors.
      - b) Sniffing is use of software to eavesdrop on information sent by a user to the host computer of a website.

- b. Once an attacker has access, (s)he may do anything the rightful user could have done.
    - 1) If the rightful user has privileged access, the attacker may create a back door to facilitate future entry despite password and status changes.
    - 2) The attacker also may be able to leverage the initial access to obtain greater privileges than the rightful user.
    - 3) If a user has the same password for multiple hosts, cracking the password for one host compromises the rest of them.
  - c. Effective methods of thwarting password attacks are one-time passwords and cryptographic authentication.
    - 1) The best standard passwords are randomly-generated 8-character or longer combinations of numbers, uppercase and lowercase letters, and special symbols.
    - 2) A disadvantage is that users often write down passwords that are hard to remember. However, software has been developed that encrypts passwords to be kept on a handheld computer. Thus, the user needs to know only one password.
5. A **man-in-the-middle attack** takes advantage of network packet sniffing and routing and transport protocols to access packets flowing through a network.
- a. These attacks may be used to
    - 1) Steal data
    - 2) Obtain access to the network during a rightful user's active session
    - 3) Analyze the traffic on the network to learn about its operations and users
    - 4) Insert new data or modify the data being transmitted
    - 5) Deny service
  - b. Cryptography is the effective response to man-in-the-middle attacks. The encrypted data will be useless to the attacker unless it can be decrypted.
6. A **denial-of-service (DOS) attack** is an attempt to overload a system (e.g., a network or Web server) with messages so that it cannot function (a system crash).
- a. A distributed DOS attack comes from multiple sources, for example, the machines of innocent parties infected by Trojan horses. When activated, these programs send messages to the target and leave the connection open.
  - b. A DOS may establish as many network connections as possible to exclude other users, overload primary memory, or corrupt file systems.
7. 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.
- a. An IDS examines user log files and patterns of traffic over the organization's network to catch suspicious activity. The IDS alerts IT personnel who can then take the appropriate action.