CHAPTER 12

ELECTRONIC COMMERCE SYSTEMS

This chapter discusses one of the most visible segments of the business world today—e-commerce. In general terms, the issues involve the electronic processing and transmission of data for many reasons: electronic buying and selling, on-line delivery, electronic funds transfer (EFT), stock trading, and of course, marketing. One form of e-commerce has been around for several decades—electronic data interchange (EDI). However, the “Internet revolution” has led to expansion and many changes and challenges. Today’s accountant must be knowledgeable with regard to technology and all of the control issues related to e-commerce.

This chapter looks at three areas: use of networks inside organizations, traditional business-to-business (B2B) use of EDI, and the implications of the Internet for B2B and consumer-to-consumer commerce. Of particular interest for accountants are issues related to security and assurance services.

The objectives of this chapter are:

• to be acquainted with the topologies that are employed to achieve connectivity across the Internet;

• to possess a conceptual appreciation of protocols and understand the specific purposes served by several Internet protocols;

• to understand the business benefits associated with Internet commerce and be aware of several Internet business modes;

• to be familiar with the risks associated with intranet and Internet electronic commerce;

• to understand issues of security, assurance, and trust pertaining to electronic commerce; and

• to be familiar with the electronic commerce implications for the accounting profession.
I. Intra-Organizational Networks and EDI

The Appendix to the chapter covers local area networks (LANs), wide area networks (WANs) and electronic data interchange (EDI). Students who have not learned of these technologies should study the appendix carefully.

II. Internet Commerce

Most students today are familiar with the Internet and with browsing the World Wide Web. Much of the popularity of the Internet is a reflection of the fact that the individual does not need to know too much about technical details behind browsers, Internet providers, online services, e-mail, etc. However, the importance of the Internet to businesses and the impact that it is having on doing business indicate that accountants need to know more than the average layman. This part of the chapter provides an excellent overview.

A. Internet Technologies

It appears to be very easy to log on to the Internet and browse. This section discusses some issues that deserve some attention. Yes, the material is technical. No, you should not ignore it “because some computer guy will worry about it.” The key issues are:

1. packet switching
2. virtual private networks
3. extranets
4. the world wide web
5. Internet addresses
6. e-mail addresses
7. URL addresses, and
8. IP addresses.

B. Protocols

The term protocol refers to rules of behavior. It is not a new term. The international community has long recognized that different cultures act differently, and successful communication requires the following of protocol.

The same can be said about communication between networks. This section examines protocols and the way in which they make a physical connection possible, synchronize the transfer of data, permit error checking, make compatibility easier, and standardize network designs. These ideas are very technical.
C. Internet Protocols

When you read about the Internet, the material seems to be filled with jargon—in particular acronyms. This section will describe some of the key Internet-related acronyms and explain their purposes. Read carefully about: **TCP/IP, FTP, SNMP, SSL, NNTP, HTTP** and **HTTP-NG, HTML, XML, and XBRL**. The last of these, XBRL, is receiving a great deal of attention as a means of financial reporting, so read this carefully.

D. Benefits from Internet Commerce

Much is written about e-commerce today. Often in the business press there are estimates of the expansion of **business-to-business (B2B)** e-commerce. Although the estimates vary, no one watching the issue suggests that the Internet will not have a profound and permanent change on how businesses do business. Read carefully the discussion of:

1. Internet business models,
2. information levels,
3. transaction levels,
4. distribution levels, and
5. dynamic virtual organizations.

III. Risks Associated with Electronic Commerce

A great deal of attention has been paid lately to the **risks** associated with e-commerce. The risks are real, and accountants need to know what they are and what the alternatives are.

A. What is Risk

**Business risk** is the possibility of a loss or injury that can reduce or eliminate an organization’s ability to achieve its objectives. Any loss, theft, or destruction of data or misuse of data or programs meets the definition.

B. Intranet Risks

Intranets are networks **within** an organization that handle transaction processes and e-mail within the organization and are linked to the outside. The threats that are usually tied to intranets are
unauthorized and illegal employee activities – whether to steal or harm the organization. A number of possibilities exist.

1. interception of network messages,
2. access to corporate databases,
3. privileged employees, and
4. company reluctance to prosecute.

C. Internet Risks

This section will consider risks to consumers, risks to businesses, and some general concerns.

1. Risks to consumers include theft of credit card numbers, theft of passwords, privacy questions, and cookies. Read this material carefully – both as accountants and as consumers.

2. Risks to businesses are different. The two primary issues discussed are IP spoofing and denial of service attacks. A number of news stories in the last few months relate to these “techniques.”

Other issues discussed for business include the problems related to technology failures and especially malicious programs. You have, no doubt, heard of the Melissa virus and the LoveBug!

IV. Security, Assurance, and Trust

Awareness of problems is a start. Taking the necessary precautions is the necessary follow-up. Three areas of precaution are discussed: data encryption, digital authentication, and firewalls.

A. Encryption

Encryption is the process of coding data before it is transmitted and decoding it after. The key issues relate to the key(s) used for the process and who knows them. Two basic methods are presented: data encryption standard (DES) and public key encryption. Read to understand the techniques and their differences.
B. Digital Authentication

Authentication relates the techniques to support the authenticity of transmitted data. In other words, techniques used to prove the transaction is authentic. Two techniques are discussed: digital signatures and digital certificates.

C. Firewalls

A firewall is a combination of hardware and software used to keep out intruders. This section discusses both network-level firewalls and application-level firewalls.

[Note also that firewall software is available to consumers and is recommended for individuals who have opted for full-time Internet access through cable connection. Since the connection is continuous, with a fixed IP address, protection from the outside is recommended.]

D. Seals of Assurance

It is only natural that the risks associated with the Internet have spawned organizations offering protection. Many seals of assurance – the Good Housekeeping seal for Internet sites – have appeared. This sections discusses six. Note, however, that others will appear, and all are not created equal. Read the characteristics carefully. They are designed for different purposes. This area also invites scams!

The seals discussed in this section include: BBBOnline, TRUSTe, VeriSign, Inc., International Computer Security Association (ICSA), AICPA/CICA WebTrust, and AICPA/CICA SysTrust.

V. Implications for the Accounting Profession

So, what does all of this mean for the accounting profession? In just a few words – Things are going to change! And the changes will affect how accountants are trained and how they do their job – new ways to do old tasks and many new responsibilities. [If you have not yet had your auditing course, be patient and store this information for future reference.]

With business activity being increasingly automated, auditors must use new techniques in evaluating control adequacy and in verifying that economic events did, in fact, occur and were properly recorded.
A. Privacy Violation

Companies must protect customer and trading partner data. Both as accountants and as consumers we have good reason to be concerned about the use companies make of the data they collect on their customers and trading partners. Five key questions are raised:

- Does the organization have a stated privacy policy?
- What mechanisms are in place to assure the consistent application of stated privacy policies?
- What information on customers, trading partners, and visitors does the company capture?
- Does the organization share or sell its customer, trading partner, or visitor information?
- Can individuals and business entities verify and update the information captured about them?

Privacy violation is a serious worry. The book discussed a KPMG white paper and the Safe Harbor Agreement between the U.S. and the European Union that was implemented in 1995.

B. Safe Harbor Agreement

Key condition for compliance relates to:

- notice to individuals of the information collected and shared;
- choice must be given to customers on sharing;
- limits must exist on onward transfer;
- assurance of security and data integrity must exist;
- individuals must be given access to information about themselves with the ability to correct, amend or delete; and
- enforcement of rules must be assured.

C. Audit Implications of XBRL

XBRL has been well studied but weaknesses exist from the audit standpoint. These relate to:

- the taxonomy—if improperly structured could lead to misrepresentation of financial data;
- the need to verify reports—instant documents; and
• questions related to audit scope and timeframe. Auditors are now responsible for printed statements and support materials. What about electronically distributed reports?

D. Continuous Auditing

Given the uses of technology in accounting, questions exist about the adequacy of an “annual” audit.

E. Electronic Audit Trails

If transactions can occur automatically between trading partners via EDI using an independent value added network, must all players be examined as part of the audit?

F. Confidentiality of Data

As more organizations exchange information electronically, issues of confidentiality of data require greater attention.

G. Authentication

Accountants need to be familiar with methods used to determine that transactions are authentic.

H. Nonrepudiation

Can trading partners change their minds and not pay?

I. Certification Authority Licensing

Methods are needed to authenticate organizations that present themselves as certification authorities.

J. Data Integrity

Can electronically transmitted data be intercepted and changed?

K. Access Controls

Accountants must be able to evaluated controls in place to keep intruders out.

L. A Changing Legal Environment

Legal issues with regard to taxes, privacy, security, intellectual property rights, and libel will continue to
evolve and inspire discussion and disagreement. Stay tuned!

Review Questions for Chapter 12: 1-31

Discussion Questions for Chapter 12: 1-28