CHAPTER

12

Electronic Commerce Systems

Upon hearing the term *electronic commerce*, many people think of browsing an electronic catalog on the web or going Internet shopping at a virtual mall. This may be the predominant component of electronic commerce, but it is not the entire story.

Electronic commerce involves the electronic processing and transmission of data. This broad definition encompasses many diverse activities, including the electronic buying and selling of goods and services, online delivery of digital products, electronic funds transfer (EFT), electronic trading of stocks, and direct consumer marketing. Electronic commerce is not an entirely new phenomenon; many companies have engaged in electronic data interchange (EDI) over private networks for decades.

Driven by the Internet revolution, however, electronic commerce has dramatically expanded and undergone radical changes in recent years. This fast-moving environment has engendered an array of innovative markets and trading communities. While electronic commerce promises enormous opportunities for consumers and businesses, its effective implementation and control are urgent challenges facing organization management and accountants.

To properly evaluate the potential exposures and risks in this environment, the modern accountant must be familiar with the technologies and techniques that underlie electronic commerce. Hardware failures, software errors, and unauthorized access from remote locations can expose the organization's accounting system to specific threats. For example, transactions can be lost in transit and never processed, digitally altered to change their financial effect, corrupted by transient signals on transmission lines, and diverted to or initiated by the perpetrator of a fraud.

In this chapter and its appendix, we consider five aspects of electronic commerce: (1) Intra-organizational Networks and EDI, (2) Internet Commerce, (3) Risks Associated with

Learning Objectives

After studying this chapter, you should:

- Be acquainted with the topologies that are employed to achieve connectivity across the Internet.
- Possess a conceptual appreciation of protocols and understand the specific purposes that several Internet protocols serve.
- Understand the business benefits associated with Internet commerce and be aware of several Internet business models.
- Be familiar with the risks associated with intranet and Internet electronic commerce.
- Understand issues of security, assurance, and trust pertaining to electronic commerce.
- Be familiar with the electronic commerce implications for the accounting profession.

Electronic Commerce, (4) Security, Assurance, and Trust, and (5) Implications for the Accounting Profession. We examine the technologies, topologies, and applications of electronic commerce in each of these areas.

Intra-organizational Networks and EDI

Local area networks (LANs), wide area networks (WANs), and EDI are electronic commerce technologies that have been with us for decades. As such, these topics are frequently found among the subject matter of introductory information technology courses. Because many accounting and information systems students become familiar with these topics before taking an AIS course, this material is covered in the chapter's appendix. The body of the chapter focuses on the salient issues pertaining to Internet-based electronic commerce. Students who have not been exposed to network and EDI topologies and technologies, however, should review the appendix before proceeding, because the treatment in the chapter presumes this background.

Internet Commerce

Internet commerce has enabled thousands of business enterprises of all sizes, as well as millions of consumers, to congregate and interact in a worldwide virtual shopping mall. Along with enormous opportunities, however, the electronic marketplace has engendered unique risks. This section of the chapter examines the technologies, benefits, risks, and security issues associated with Internet commerce.

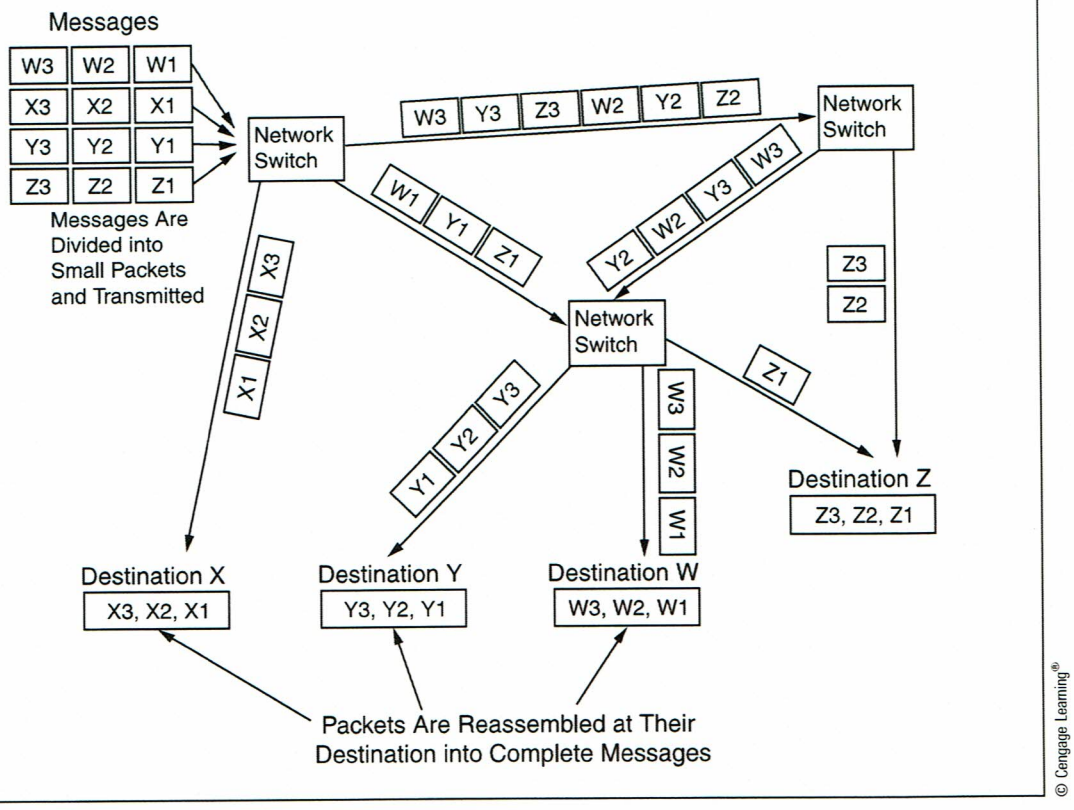
INTERNET TECHNOLOGIES

The Internet was originally developed for the U.S. military and later became used widely for academic and government research. Over recent years, it has evolved into a worldwide information highway. This growth is attributed to three factors. First, in 1995, national commercial telecommunications companies, such as MCI, Sprint, and UUNET, took control of the backbone elements of the Internet, and they have continued to enhance their infrastructures. Large Internet service providers (ISPs) can link into these backbones to connect their subscribers, and smaller ISPs can connect directly to the national backbones or into one of the larger ISPs. Second, online services like CompuServe and America Online connect to the Internet for e-mail, which enables users of different services to communicate with each other. Third, the development of graphics-based web browsers, such as Microsoft's Internet Explorer, has made accessing the Internet a simple task. The Internet thus became the domain of everyday people with personal computers rather than just scientists and computer hackers. As a result, the web has grown exponentially and continues to grow daily.

Packet Switching

The Internet employs communications technologies based on **packet switching.** Figure 12-1 illustrates this technique, whereby messages are divided into small packets for transmission. Individual packets of the same message may take different routes to their destinations. Each packet contains address and sequencing codes so they can be reassembled into the original complete message at the receiving end. The choice of transmission path is determined according to criteria that achieve optimum utilization of the long-distance lines, including the degree of traffic congestion on the line, the shortest path between the end points, and the line status of the path (that is, working, failed, or experiencing errors). Network switches provide a physical connection for the addressed packets only for the duration of the message; the line then becomes available to other users. The first international standard for wide area packet switching networks was X.25, which was defined when all circuits were analog and very susceptible to noise. Subsequent packet technologies, such as frame relay and SMDS (switched multimegabit data service), were designed for today's almost error-free digital lines.

FIGURE 12-1 MESSAGE PACKET SWITCHING



Virtual Private Networks

A **virtual private network (VPN)** is a private network within a public network. For years, common carriers have built VPNs, which are private from the client's perspective, but physically share backbone trunks with other users. VPNs have been built on X.25 and frame-relay technologies. Today, Internet-based VPNs are of great interest. Maintaining security and privacy in this setting, however, requires encryption and authentication controls discussed later in the chapter.

Extranets

Another variant on Internet technology is the **extranet.** This is a password-controlled network for private users rather than the general public. Extranets are used to provide access between trading partner internal databases. Internet sites containing information intended for private consumption frequently use an extranet configuration.

World Wide Web

The World Wide Web (web) is an Internet facility that links user sites locally and around the world. In 1989, Tim Berners-Lee of the European Center for Nuclear Research in Geneva developed the web as a means of sharing nuclear research information over the Internet. The fundamental format for the web is a text document called a **web page** that has embedded **Hyper Text Markup Language (HTML)** codes that provide the formatting for the page as well as hypertext links to other pages. The linked pages may be stored on the same server or anywhere in the world. HTML codes are simple alphanumeric characters that can be typed with a text editor or word processor. Most word processors support web publishing features that allow text documents to be converted to HTML format.

Web pages are maintained at **websites**, which are computer servers that support **Hyper Text Transfer Protocol (HTTP).** The pages are accessed and read via a web browser such as Internet Explorer. To access a website, the user enters the **Uniform Resource Locator (URL)** address of the target site in the web browser. When an Internet user visits a website, his or her point of entry is typically the site's **home page.** This HTML document serves as a directory to the site's contents and other pages. Through browsers, the web provides point-and-click access to the largest collection of online information in the world. The web has also become a multimedia delivery system that supports audio, video, videoconferencing, and three-dimensional animation. The ease of web page creation and navigation via browsers has driven the unprecedented growth of the web. In 1994, there were approximately 500 websites in the world; today there are millions.

Internet Addresses

The Internet uses three types of addresses for communications: (1) e-mail addresses, (2) website URL addresses, and (3) Internet protocol (IP) addresses of individual computers attached to a network.

E-MAIL ADDRESS. The format for an e-mail address is USER NAME@DOMAIN NAME. For example, the address of the author of this textbook isjahO@lehigh.edu. There are no spaces between any of the words. The user name (or in this case, the user identification [ID]) is jahO. A domain name is an organization's unique name combined with a top-level domain (TLD) name. In the previous example, the unique name is lehigh and the TLD is edu. Following are examples of TLD names:

.net	network provider
.org	nonprofit organization
.edu	education and research
.gov	government
.mil	military agency
.int	international/intergovernmental

Outside the United States, the TLD names consist of the country code, such as .uk for the United Kingdom and .es for Spain. The Internet Ad Hoc Committee has introduced a category called a generic top-level domain, which includes the following:

.firm	a business
.store	goods for sale
.web	WWW activities
.arts	culture/entertainment
.rec	recreation/entertainment
.info	information service
.nom	individual/personal

The Internet e-mail addressing system allows the user to send e-mail directly to the mailboxes of users of all major online services.

URL ADDRESS. The URL is the address that defines the path to a facility or file on the Web. URLs are typed into the browser to access website home pages and individual web pages, and they can be embedded in web pages to provide hypertext links to other pages. The general format for a URL is **protocol prefix, domain name, subdirectory name**, and **document name.** The entire URL is not always needed. For example, to access the South-Western Publishing home page, only the following protocol and domain name are required:

http://www.cengage.com/accounting/hall

The protocol prefix is http:// and the domain name is www.cengage.com/accounting/hall. From this home page, the user can activate hyperlinks to other pages as desired. The user can go directly to a linked page by providing the complete address and separating the address components with slashes. For example,

http://www.cengage.com/accounting/hall

Subdirectories can be several levels deep. To reference them, each must be separated with a slash. For example, the elements of the following URL for a hypothetical sporting goods company are described next.

http://www.flyfish.com/equipment/rods/brand_name.html

http://	protocol prefix (most browsers default to HTTP if a prefix is not typed)
www.flyfish.com/	domain name
equipment/	subdirectory name
rods/	subdirectory name
brand_name.html	document name (web page)

IP ADDRESS. Every computer node and host attached to the Internet must have a unique Internet Protocol (IP) address. For a message to be sent, the IP addresses of both the sending and the recipient nodes must be provided. Currently, IP addresses are represented by a 32-bit data packet. The general format is four sets of numbers separated by periods. The decomposition of the code into its component parts varies depending on the class to which it is assigned. Class A, class B, and class C coding schemes are used for large, medium, and small networks, respectively. To illustrate the coding technique, the IP address 128.180.94.109 translates into:

128.180	Lehigh University
94	Business Department faculty server
109	A faculty member's office computer (node)

PROTOCOLS

The word **protocol** has been used several times in this section. Let's now take a closer look at the meaning of this term. Protocols are the rules and standards governing the design of hardware and software that permit users of networks, which different vendors have manufactured, to communicate and share data. The general acceptance of protocols within the network community provides both standards and economic incentives for the manufacturers of hardware and software. Products that do not comply with prevailing protocols will have little value to prospective customers.

The data communications industry borrowed the term *protocol* from the diplomatic community. Diplomatic protocols define the rules by which the representatives of nations communicate and collaborate during social and official functions. These formal rules of conduct are intended to avoid international problems that could arise through the misinterpretation of ambiguous signals passed between diplomatic counterparts. The greatest potential for error naturally exists between nations with vastly dissimilar cultures and conventions for behavior. Establishing a standard of conduct through protocols, which all members of the diplomatic community understand and practice, minimizes the risk of miscommunications between nations of different cultures.

An analogy may be drawn to data communications. A communications network is a community of computer users who also must establish and maintain unambiguous lines of communication. If all network members had homogeneous needs and operated identical systems, this would not be much of a problem; however, networks are characterized by heterogeneous systems components. Typically, network users employ hardware devices (PC, printers, monitors, data storage devices, modems, and so on) and software (user applications, network control programs, and operating systems) that a variety of vendors produce. Passing messages effectively from device to device in such a multivendor environment requires ground rules or protocols.

What Functions Do Protocols Perform?

Protocols serve several network functions. First, they facilitate the physical connection between the network devices. Through protocols, devices are able to identify themselves to other devices as legitimate network entities and initiate (or terminate) a communications session.

Second, protocols synchronize the transfer of data between physical devices. This involves defining the rules for initiating a message, determining the data transfer rate between devices, and acknowledging message receipt.

Third, protocols provide a basis for error checking and measuring network performance. This is done by comparing measured results against expectations. For example, performance measures pertaining to storage device access times, data transmission rates, and modulation frequencies are critical to controlling the network's function. Thus, the identification and correction of errors depend on protocol standards that define acceptable performance.

Fourth, protocols promote compatibility among network devices. To transmit and receive data successfully, the various devices involved in a particular session must conform to a mutually acceptable mode of operation, such as synchronous, asynchronous and duplex, or half-duplex. Without protocols to provide such conformity, messages sent between devices would be distorted and garbled.

Finally, protocols promote network designs that are flexible, expandable, and cost effective. Users are free to change and enhance their systems by selecting from the best offerings of a variety of vendors. Manufacturers must, of course, construct these products in accordance with established protocols.

The Layered Approach to Network Protocol

The first networks used several different protocols that emerged in a rather haphazard manner. These protocols often provided poor interfaces between devices that actually resulted in incompatibilities. Also, early protocols were structured and inflexible, thus limiting network growth by making system changes difficult. A change in the architecture at a node on the network could have an unpredictable effect on an unrelated device at another node. Technical problems such as these can translate into unrecorded transactions, destroyed audit trails, and corrupted databases. Out of this situation emerged the contemporary model of layered protocols. The purpose of a layered-protocol model is to create a modular environment that reduces complexity and permits changes to one layer without adversely affecting another.

The data communication community, through the **International Standards Organization**,[1] has developed a layered set of protocols called the **Open System Interface (OSI).** The OSI model provides standards by which the products of different manufacturers can interface with one another in a seamless interconnection at the user level. This seven-layer protocol model is discussed in detail in the appendix.

INTERNET PROTOCOLS

Transfer Control Protocol/Internet Protocol (TCP/IP) is the basic protocol that permits communication between Internet sites. It was invented by Vinton Cerf and Bob Kah under contract from the U.S. Department of Defense to network dissimilar systems. This protocol controls how individual packets of data are formatted, transmitted, and received. This is known as a reliable protocol because delivery of all the packets to a destination is guaranteed. If delivery is interrupted by hardware or software failure, the packets are automatically retransmitted.

The TCP portion of the protocol ensures that the total number of data bytes transmitted was received. The IP component provides the routing mechanism. Every server and computer in a TCP/IP network requires an IP address, which is either permanently assigned or dynamically assigned at start-up. The IP part of the TCP/IP protocol contains a network address that is used to route messages to different networks.

Although TCP/IP is the fundamental communications protocol for the Internet, the following are some of the more common protocols that are used for specific tasks.

File Transfer Protocols

File Transfer Protocol (FTP) is used to transfer text files, programs, spreadsheets, and databases across the Internet. **TELNET** is a terminal emulation protocol used on TCP/IP-based networks.

1 The International Standards Organization (ISO) is a voluntary group comprising representatives from the national standards organizations of its member countries. The ISO works toward the establishment of international standards for data encryption, data communication, and protocols.

It allows users to run programs and review data from a remote terminal or computer. TELNET is an inherent part of the TCP/IP communications protocol. While both protocols deal with data transfer, FTP is useful for downloading entire files from the Internet; TELNET is useful for perusing a file of data as if the user were actually at the remote site.

Mail Protocols

Simple Network Mail Protocol (SNMP) is the most popular protocol for transmitting e-mail messages. Other e-mail protocols are **Post Office Protocol** and **Internet Message Access Protocol.**

Security Protocols

Secure Sockets Layer (SSL) is a low-level encryption scheme used to secure transmissions in higher-level HTTP format. **Private Communications Technology (PCT)** is a security protocol that provides secure transactions over the web. PCT encrypts and decrypts a message for transmission. Most web browsers and servers support PCT and other popular security protocols, such as SSL. **Secure Electronic Transmission** is an encryption scheme developed by a consortium of technology firms and banks (Netscape, Microsoft, IBM, Visa, MasterCard, and so on) to secure credit card transactions. Customers making credit card purchases over the Internet transmit their encrypted credit card number to the merchant, who then transmits the number to the bank. The bank returns an encrypted acknowledgment to the merchant. The customer need not worry about an unscrupulous merchant decrypting the customer's credit card number and misusing the information. **Privacy Enhanced Mail (PEM)** is a standard for secure e-mail on the Internet. It supports encryption, digital signatures, and digital certificates as well as both private and public key methods (which will be discussed later).

Network News Transfer Protocol

Network News Transfer Protocol (NNTP) is used to connect to Usenet groups on the Internet. Usenet newsreader software supports the NNTP protocol.

HTTP and HTTP-NG

HTTP controls web browsers that access the web. When the user clicks on a link to a web page, a connection is established and the web page is displayed, and then the connection is broken. **HyperText Transport Protocol-Next Generation (HTTP-NG)** is an enhanced version of the HTTP protocol that maintains the simplicity of HTTP while adding important features such as security and authentication.

HTML

HyperText Markup Language (HTML) is the document format used to produce web pages. HTML defines the page layout, fonts, and graphic elements as well as hypertext links to other documents on the web. HTML is used to lay out information for display in an appealing manner, such as one sees in magazines and newspapers. The ability to lay out text and graphics (including pictures) is important in terms of appeal to users in general. Even more pertinent is HTML's support for hypertext links in text and graphics that enable the reader to virtually jump to another document located anywhere on the World Wide Web.

Advances in Internet technology and connectivity have moved corporations toward disclosure of corporate financial information in a form compatible with standard web-browsing tools. In this way, investors and analysts may have access to current corporate information. Dissemination of HTML-based financial reports, however, is limited to presentation only. If the receiving organization wishes to perform computer analysis on this information, such as comparing performance of several corporations within an industry, it must manually enter the financial data into its system for processing. Unlike XML and XBRL (discussed in Chapter 8), HTML does not support the exchange of information in a relational form that can be automatically imported into the receiving organization's internal database and analyzed.

INTERNET BUSINESS MODELS

Virtually all businesses engage in some form of Internet commerce to achieve one or more of the following benefits:

- Access to a worldwide customer and/or supplier base.
- Reductions in inventory investment and carrying costs.
- The rapid creation of business partnerships to fill market niches as they emerge.
- Reductions in retail prices through lower marketing costs.
- Reductions in procurement costs.
- Better customer service.

The actual benefits attained depend upon the degree of organizational commitment to an Internet business strategy. The following section describes three levels of Internet activity.

INFORMATION LEVEL. At the **information level** of activity, an organization uses the Internet to display information about the company, its products, services, and business policies. This level involves little more than creating a website, and it is the first step taken by most firms entering the Internet marketplace. When customers access the website, they generally first visit the home page. This is an index to the site's contents through other web pages. Large organizations often create and manage their websites internally. Smaller companies have their sites hosted on servers maintained by an ISP.

TRANSACTION LEVEL. Organizations involved at the **transaction level** use the Internet to accept orders from customers and/or to place them with their suppliers. This involves engaging in business activities with total strangers from remote parts of the world. These may be customers, suppliers, or potential trading partners. Many of the risks that are discussed later in the chapter relate to this (and to the next) level of electronic commerce. Success in this domain involves creating an environment of trust by resolving the key concerns listed below:

- Ensure that data used in the transaction are protected from misuse.
- Verify the accuracy and integrity of business processes used by the potential customer, partner, or supplier.
- Verify the identity and physical existence of the potential customer, partner, or supplier.
- Ascertain the reputation of the potential customer, partner, or supplier.

DISTRIBUTION LEVEL. Organizations operating on the **distribution level** use the Internet to sell and deliver digital products to customers. These include subscriptions to online news services, software products and upgrades, and music and video products. In addition to these traditional consumer products, recent years have seen rapid growth in the sale and distribution of an array of computing services to business entities that are collectively referred to as **cloud computing.** Key elements of this concept are presented in the next section.

CLOUD COMPUTING

A number of definitions exist for cloud computing. This section is based on the following one:

> *Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*[2]

2 The NIST Definition of Cloud Computing, Peter Mell and Tim Grance, 10-7-09, http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

The key features of cloud computing implied by this definition are:

- Client firms can acquire IT resources from vendors on demand and as needed. This is in contrast to the traditional IT outsourcing model (see Chapter 15) in which resources are provided to client firms in strict accordance with long-term contracts that stipulate services and time frames.
- Resources are provided over a network (private or Internet) and accessed through network terminals at the client location.
- Acquisition of resources is rapid and infinitely scalable. A client can expand and contract the service demanded almost instantly and often automatically.
- Computing resources are pooled to meet the needs of multiple client firms. A consequence of this, however, is that an individual client has no control over, or knowledge of, the physical location of the service being provided.

Cloud computing offers three primary classes of computing services. These are: *Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS)*, and *Platform-as-a-Service (PaaS)*.

Software-as-a-Service (SaaS) is a software distribution model in which service providers host applications for client organizations over a private network or the Internet. The 1990s saw the emergence of business software hosting organizations called Application Service Providers (ASP). SaaS is an extension of this concept. A key difference is the nature of the software product being hosted. ASPs typically host the software of third-party software vendors, which is configured to the unique needs of the client organization and requires installation of software on the client's in-house computers. SaaS vendors typically develop and manage their own web-based software, which is general purpose, designed to serve multiple businesses and users, and requires only an Internet connection to access.

Another difference between ASP and SaaS is the licensing and payment model used. ASP contracts are typically fixed-period or one-time licensing agreements. SaaS vendors often employ a subscription model in which clients pay as they go based on usage. SaaS applications may be acquired directly from the vendors or from third-party consolidators who bundle various SaaS products and offer them as a suite of resources.

Infrastructure-as-a-Service (IaaS) is the provision of computing power and disk space to client firms who access it from desktop PCs. The client firm can configure the infrastructure for storage, networks, and other computing needs, including running operating systems and data processing applications. The advantage to the client is that the IaaS provider owns, houses, and maintains the equipment, and the client pays for it on a per-use basis. Another advantage is scalability, which is the ability to rapidly respond to usage changes. IaaS providers, such as Amazon Web Services (AWS), offer infrastructure capacity that can grow and contract almost instantly with an organization's shifts in demand.

Platform-as-a-Service (PaaS) enables client firms to develop and deploy onto the cloud infrastructure consumer-generated applications using facilities provided by the PaaS vendor. PaaS tools include facilities for application development, program testing, program implementation, system documentation, and security. The advantage to the client organization is that it can, with limited internal expertise, rapidly build and deploy web applications.

Virtualization

The technology that has unleashed cloud computing is **virtualization.** In the traditional (nonvirtual) computing environment, a single computer runs a single operating system and a single real-time application. This results in considerable unused physical hardware capacity. Virtualization multiplies the effectiveness of the physical system by creating virtual (software) versions of the computer with separate operating systems that reside in the same physical equipment. In other words, virtualization is the concept of running more than one "virtual computer" on a single physical computer. Since each virtual system runs its own application, total computing power is multiplied with no additional hardware investment.

In addition to virtual computers, virtualization has exploded into two other areas of IT that have enabled the concept of cloud computing to gain traction in recent years: *network virtualization* and *storage virtualization*.

Network virtualization increases effective network bandwidth by dividing it into independent channels, which are then assigned to separate virtual computers. Network virtualization optimizes network speed, flexibility, and reliability; most importantly, it improves network scalability. Network virtualization is especially effective in networks that experience sudden, large, and unforeseen surges in usage.

Storage virtualization is the pooling of physical storage from multiple network storage devices into what appears to be a single virtual storage device. This pool is then managed from a central server. Storage virtualization increases storage capacity utilization by allowing multiple servers to consolidate their private data onto an array of disks. Storage virtualization accelerates data access and dynamically expands storage capacity as demand increases.

Cloud Computing Implementation Issues

In spite of its convenience and potential for cost savings, cloud computing is not a realistic option for all companies. For smaller businesses, startup companies, and some new applications, the cloud concept is a promising alternative to in-house computing. The information needs of large companies, however, are often in conflict with the cloud solution for the following three reasons.

- First, large firms have typically already incurred massive investments in equipment, proprietary software, and human resources. These organizations are not inclined to walk away from their investments and turn over their entire IT operations to a cloud vendor.
- Second, many large enterprises have mission-critical functions running on legacy systems that are many decades old. These systems continue to exist because they continue to add value. The task of migrating legacy systems to the cloud would require new architectures and considerable reprogramming. Given their typically high utilization, performance, and throughput, the cost/benefit of the cloud alternative is debatable.
- Third, a central tenant of cloud computing is the philosophy that IT is a one-size-fits-all commodity asset. Indeed, the economies of scale that cloud vendors achieve depend upon standardization of solutions across all clients. Cloud vendors treat all workloads and all clients as commodities and do not provide the special treatment required by some organizations. Larger companies are more likely to have esoteric information needs and pursue strategic advantage through IT systems. A commodity provision approach is incompatible with the need for unique strategic information.

Finally, internal control and security issues are concerns for companies of all sizes that outsource their IT to the cloud. When an organization's critical data reside outside its corporate walls, it is at risk. The client firm has little option but to trust to the ethics, competence, and internal controls of the vendor. The relevant risk issues include an extensive set of topics, such as technology failures in the cloud, distributed denial of service attacks, hacking, vendor exploitation, vendor failure to perform, and the loss of strategic advantage. Internet risks are examined later in this chapter, and the security and controls that mitigate such risks are presented in Chapter 16. Outsourcing (both traditional and cloud) risks and controls are covered in Chapter 15.

Dynamic Virtual Organizations

Perhaps the greatest potential benefit to be derived from electronic commerce is the firm's ability to forge dynamic business alliances with other organizations to fill unique market niches as opportunities arise. These may be long-lasting partnerships or one-time ventures. Electronic partnering of business enterprises forms a **dynamic virtual organization** that benefits all parties involved.

For example, consider a company that markets millions of different products, including books, music, software, and toys, over the Internet. If this were a traditional organization created to serve walk-in customers, it would need a massive warehouse to store the extensive range of physical products that it sells. It must also make significant financial investments in inventory and personnel to maintain stock, fill customer orders, and control the environment. A virtual organization does not need this physical infrastructure. Figure 12-2 illustrates the partnering relationship possible in a virtual organization.