Chapter 2

Electronic Commerce and the Internet

INTRODUCTION

THE INTERNET AND WORLD WIDE WEB
Internet Addresses and Software
Intranets and Extranets
The World Wide Web
E-mail, Groupware, and Electronic Conferencing
XBRL—Financial Reporting on the Internet

ELECTRONIC COMMERCE
Retail Sales
E-Payments and E-Wallets
Business to Business E-Commerce
Electronic Data Interchange

PRIVACY AND SECURITY ON THE INTERNET
Privacy
Security
Firewalls and Proxy Servers
Data Encryption
Digital Signatures
Digital Time Stamping

AIS AT WORK—THE SEC HOSTS FAKE COMPANY WEB SITES

SUMMARY

KEY TERMS YOU SHOULD KNOW

DISCUSSION QUESTIONS

PROBLEMS

INTERNET EXERCISES

CASE ANALYSIS
DeGraaf Office Supplies
Small Business Computers, Inc.

REFERENCES, RECOMMENDED READINGS, AND WEB SITES

After reading this chapter, you will:

1. Understand IP, URL, and web page addresses on the Internet.
2. Appreciate why electronic communication is useful to accountants.
3. Know why XBRL is important to the future of financial reporting.
4. Understand electronic data interchange (EDI), and why it is important to AISs.
5. Know the differences between business-to-consumer and business-to-business electronic commerce.
6. Appreciate the privacy and security issues associated with electronic commerce.
7. Know why businesses use firewalls, proxy servers, and encryption techniques.
The days when the Internet was primarily a research tool are long gone. Today, it is positioned as the engine that will drive the future of business.


**INTRODUCTION**

It is difficult to discuss accounting information systems without also discussing the Internet and electronic commerce. Reasons for this are abundant. For many accountants, for example, electronic communication has become as natural a form of communication as speaking over a telephone system. Similarly, most accountants now use the World Wide Web—the graphic component of the Internet—as a valued research and learning tool. Then, too, auditors now regularly recommend and evaluate those Internet controls and procedures that ensure complete, accurate, and authentic transmissions over Internet transmission channels. The Internet is both a disruptive technology (because it changes so much) and an enabling technology (because it makes the economy more efficient). The Internet may be even more influential than previous technologies because of the speed of adoption and impact. Consider that in 1993 only 90,000 Americans were online versus in 143 million in September 2001.1 It took twenty years for the television to reach 50 million people and only four years for the Internet to do the same.

This chapter describes the Internet and some of its accounting uses in detail. The first section describes Internet components such as Internet addresses and software. This section also discusses some Internet concepts of special importance to accountants (i.e., intranets, extranets, the World Wide Web, and e-mail). We next discuss XBRL, a financial reporting language that will improve access to and analysis of corporate financial data.

One of the most important uses of the Internet is for electronic commerce (e-commerce)—the topic of the second section of this chapter. While the terms e-commerce and e-business are often used interchangeably; there is actually a difference. E-commerce involves buying and selling electronically, whereas e-business entails automating business processes in general via the Internet. Here, we discuss such vital concepts as retail sales, E-cash, business-to-business e-commerce, and electronic data interchange.

As more organizations conduct at least some business on the Internet, it is only natural that managers increasingly recognize the importance of Internet privacy and security. This includes protecting consumers’ personal privacy, protecting data from external hackers, and safeguarding information that businesses send to one another over the Internet. The final section of this chapter discusses these topics in detail.

---

THE INTERNET AND WORLD WIDE WEB

The Internet is a collection of hundreds of thousands of local and wide area networks that are now connected together via the Internet backbone (i.e., the main electronic connections of the system). Describing the Internet as an “information superhighway” makes sense because it now connects almost 200 million people in more than 200 countries electronically just as a set of state, interstate, and international highways connect people physically. Experts estimate that the Internet is growing at the rate of 40 percent per year. Almost all universities are connected to the Internet, as are most commercial information services, businesses, government agencies, and not-for-profit organizations.

If you are taking classes at a college or university, there is a good chance that your school has a direct (“hard-wired”) link to the Internet. This link is usually a high-capacity, dedicated phone line that connects your school’s computer(s) to at least one other Internet computer. Alternatively, you may have an account with an Internet service provider (ISP) such as America Online, Bellsouth, Ameritech, Netcom, AT&T, or Sprint, each of which maintains its own Internet computers.

Internet Addresses and Software

To transmit data over the Internet, a computer uses an Internet address and a forwarding system that works much the same way as the post office system. On the Internet, the initial computer transmits a message to other computers along the Internet’s backbone, which then relay the message from site to site until it reaches its final destination. If the message is long, the original data packet may be divided into pieces and even routed along separate routes. The receiving computer then reassembles the packets into a complete message at the final destination.

Message-routing is important to accountants because the security of a data transmission rests on the safety of all the intermediate computers along a given communications pathway. Thus, the further the distance between the sending station and the destination computer, the more intermediary routing computers are involved in the transmission and the more vulnerable a message becomes to interception and abuse. This is why businesses often use their own (proprietary) networks or encrypted (coded) messages when transmitting data electronically. We shall return to this point shortly.

An Internet address begins as a domain address, which is also called a universal resource locator (URL). This is text—for example, AccountName@computerX.siteY.com. As suggested by this generic example, the lead item is an account name, the first element following the @ symbol is a particular computer, and the second element following the @ symbol is a site locator. The last entry (com or commercial user) is the organization code. Other organization codes are edu (education), gov (government), mil (military), net (network service organization), org (miscellaneous organization), and int (international treaty organization).

For transmission purposes, Internet computers translate text-based domain addresses into a pure numeric Internet protocol (IP) address such as “198.105.232.4.” The elements in this address contain a geographic region (“198”), an organization number (“105”), a computer group (“232”), and a specific computer (“4”). The IP address enables Internet computers to deliver a specific file to a specific computer at a specific computer site—for example, an e-mail message to a
friend at another university—using the standard Transmission Control Protocol (TCP)/IP Internet protocol. (TCP/IP lets computers communicate with each other across networks.) IP addresses are important to auditors because they help identify the sender, an important control in electronic commerce applications.

**Intranets and Extranets**

Because Internet software is so convenient to use, many companies also create their own **intranets** for internal communications purposes. These are networks that use the same software as the Internet (discussed later), but are internal to the organization that created them. Thus, outsiders cannot access the information on intranet networks (unless special provision is made for this)—a convenient and often-desirable security feature.

Companies are finding many uses for their intranets. These systems allow more users to access and interact with a range of internal and external databases. Advanced search engine technology coupled with an intranet can deliver user-defined information when needed. For example, a manager can request notification from the intranet when departmental expenses exceed a prespecified dollar amount. Employee information sharing is another value-added use of an intranet. Employees can collaborate with each other by posting messages and data on the internal network. Another valuable use of the intranet concerns the human resource process. Employees can update records, check out job postings, fill out forms to request goods and services, and enter expenses (e.g., travel expenses) through their organization’s intranet. Case-in-Point 2.1 describes how James River Corporation uses an intranet for employee services.

**Case-in-Point 2.1** James River Corporation, a leading maker of consumer products, used Lawson Insight’s human resources system to develop an intranet for employees to retrieve and update their personal information. The Lawson system lets employees go to the intranet to change W-4 forms, check on their vacation time, and make changes to personal information such as address and phone number. For many personnel functions, employees can now serve themselves.2

Some businesses are creating **extranets** that enable selected outside users to access their intranets. Connections are either through the Internet itself or through a separate data communications channel. An example is a large manufacturer that wants to communicate electronically with its vendors. Thus, extranets are networks that organizations establish between themselves and their trading partners. An example is the extranet created by General Electric (Case-in-Point 2.2).

**Case-in-Point 2.2** GE, which spends about $30 billion on supplies, now uses its proprietary “Trading Process Network” (TPN) to communicate with more than 1,400 suppliers online. TPN enables GE to distribute requests for bids to both large and small vendors, provide information about how to bid, and obtain bids electronically in a fraction of the time it takes to exchange manual documents. In 1997, GE purchased nearly $1 billion worth of supplies in this manner. It expects to save $500 million over the next three years using this extranet.

---

The World Wide Web

The software that we use to send and receive messages on the Internet includes general types of e-mail software, and also specialized search software such as Gopher and Veronica. All these items are text-based software that limits viewable outputs to words and phrases—not figures, graphics, or animated outputs.

The graphics portion of the Internet is commonly called the World Wide Web, or just "the web." As you probably already know, you view the graphics files available through this portion of the Internet using a software package called a web browser. The two most popular web browsers today are Microsoft's Internet Explorer and Netscape's Navigator, but there are many other, less-popular software packages as well.

A typical output on the web is called a web page (Figure 2-1) (i.e., a collection of text, graphics, and links to other web pages that are stored in one or more files on Internet-connected computers). Many web pages, in fact, are collections of files drawn from both local and distant sources. This is one reason why some web pages take so long to appear onscreen after the initial host is contacted; you may be waiting for your system to assemble text and graphics images from distant sources.

Developers create web pages in an editing language such as hypertext markup language (html) or a programming language such as Java. Figure 2-2 shows a portion of the html code for the web page of Figure 2-1. The Internet transfers these web pages from one computer to another using a communications proto-
Your web browser then deciphers the editing language and displays the text, graphics, and other items of the web page on your display screen.

The first web page that a user sees when he or she supplies a web browser with a domain address is called the web site’s home page. Typically, this home page acts as a table of contents with hyperlinks to other web pages that contain more specific information. These links are the icons, colored text, or graphic images on which you click, for example, when your mouse pointer turns into a hand icon onscreen. Typically, these other web pages are stored on distant computers, making access speeds slow during times of peak Internet usage.

**E-mail, Groupware, and Electronic Conferencing**

E-mail is short for electronic mail. In a typical e-mail application, you create a message on your microcomputer, and then send it to someone else using the recipient’s e-mail address. On local area networks, a person’s e-mail address is usually the same as the person’s account number or name, for example, “AnnBorland.” If you send e-mail over the Internet, you must also include the full domain address, for example, AnnBorland@computerX.siteY.edu.
When a computer system receives an e-mail message, it stores it in the user's mail box (on disk) as a text file. The recipient then uses e-mail software to read the message and respond as necessary. This person can also forward the message to others, print a hard copy, or delete it. E-mail attachments allow users to append separate files to e-mail messages, for example, graphics files or text files in non-ASCII formats. Figure 2-3 lists some additional advantages of e-mail.

E-mail enables individuals or companies to communicate with other Internet users around the corner or around the world. This allows accountants, for example, to gather information from remote or distant sources, consult with experts outside their organization on complex technical issues, and forward accounting documents such as a set of financial statements for review by corporate headquarters. A problem with e-mail is that hackers can use it to spread computer viruses, as described in the following case.

**Case-in-Point 2.3** In May, 2000, companies and individuals were hit with the worst computer virus to date, the LoveLetter worm. A hacker sent a message worldwide with the subject line “I Love You.” Opening the attachment caused the virus to replace or hide numerous picture, music, and video files. It also quickly replicated itself and spread. The “I Love You” virus may have attacked more than 40 million people’s computers and damages were in the billions of dollars. This type of virus illustrates the vulnerability of information systems to widespread attacks.

Newer work group software called groupware allows users to send and receive e-mail, plus perform a wide range of other tasks. Examples include Exchange (Microsoft), Groupwise (Novell), Lotus Notes (Lotus Development Corporation) and Outlook (Microsoft). In addition to e-mail support, these network packages allow users to collaborate on work tasks, make revisions to the same document, schedule appointments on each other’s calendars, share files and databases, conduct electronic meetings, and develop custom applications.

At the high end of groupware communications packages are electronic conferencing tools that enable users to teleconference with one another. These packages, for example, enable accountants to use computers and phone lines to interview re-

---

**FIGURE 2–3** Some advantages of e-mail.

1. **Eliminates “telephone tag.”** Your message goes directly to your recipient.
2. **Eliminates inaccurate or misleading messages.** Your message will be delivered in exactly the same way as you send it. Some e-mail software includes spell checkers to eliminate spelling errors.
3. **No interruptions.** E-mail is delivered silently and users do not have to be physically present to receive messages.
4. **Time shifting.** Messages can be sent to people in different time zones.
5. **Message distribution.** You can send the same message to many different individuals without composing a separate message to each one.
6. **Facilitates replies.** You can enclose a copy of the message you receive as part of the message you send. This makes it easy to ask specific questions, or to reply to specific parts of an earlier message.
7. **Maintaining information.** E-mail software enables you to maintain messages in an orderly, paperless fashion. Some e-mail software enables you to archive your messages, sort them by date of receipt or sender, or search them for key words.
8. **Attaching files.** You can attach files in different formats to your e-mail message, including text and graphics files.
mote clients, consult with one another about tax or audit problems, or plan corpo-
rate budgets.

Groupware has been the technology behind the knowledge sharing that many professional service firms (such as accounting and consulting firms) use as a competitive advantage. Knowledge sharing allows an organization to distribute expertise within the organization. Large consulting and accounting firms, for example, have access to a wealth of information within their organizations. This information includes descriptions of clients' best practices, research, links to business web sites, and customized news. An employee with a client issue can access the knowledge database to find out how other clients handle that issue. For example, what is the best practice for processing accounts payable transactions? Case-in-Point 2.4 describes one such system.

Case-in-Point 2.4 In 1997, Arthur Andersen, a large professional service firm, launched KnowledgeSpace, a web-based repository of knowledge for employees and business subscribers. The knowledge database included global best practices, links to over 400 business resources, stock quotes and portfolios, book recommendations, and online conferences on hot issues. A basic subscription to the service cost less than $400 per year and allowed employees and subscribers to receive custom information that fit their user profile.

XBRL—Financial Reporting on the Internet

More and more companies are reporting financial information on the Internet. While it’s easy enough to view one company’s financial reports and other disclosures, it is not so easy to access financial information about multiple enterprises for comparison purposes. If you were to try to compare several companies within one industry in terms of a specific financial statement element, such as current assets, you could not do so. The primary repository of financial information on the Internet is the Security and Exchange Commission’s Electronic Data Gathering and Retrieval (EDGAR) database. This database contains the financial report filings of U.S. publicly held companies. The reports, however, are in a plain text format. You can search for information for one company, for example, Company ABC’s 10-Q filing for the third quarter of 2001. However, you cannot access account information from one company and compare it to that of another. To overcome the search limitations in the EDGAR database, PricewaterhouseCoopers developed EdgarScan™. EdgarScan takes the information in the database and changes it to a common format, which allows users to extract data from multiple companies and compare it. EdgarScan even includes graphical capabilities that allow you to show bar charts comparing, for example, the sales revenues of two or more companies for the same period. Figure 2-4 shows a bar chart in Microsoft Excel format produced by EdgarScan’s Benchmarking Assistant feature.

While the EDGAR database and EdgarScan are valuable resources for obtaining financial information about publicly traded companies, they are limited to formal financial report filings for a limited set of enterprises. The information they include is historical and concerns past performance. Many financial managers, investors, and other information users are interested in obtaining financial information that is reported on a more timely basis. While the Internet allows for this type of reporting, retrieving the information requires a common specification for reporting and analyzing financial data. eXtensible Business Reporting Language (XBRL) is a specialized software language for the financial reporting industry.
XBRL is a subset of **eXtensible Markup Language (XML)**. Most Internet users are somewhat familiar with Hypertext Markup Language (HTML). HTML is the source code for web pages. If you wanted to format your own web page, you would do so using the tags defined in HTML. These tags are specifications in brackets surrounding the text that describe how to display the data. For example, `<TITLE>XYZ Corporation Financial Statements<TITLE>` indicates that “XYZ Corporation Financial Statements” should appear in a web browser’s title bar or at the top of the web page. HTML has a limited set of predefined tags; users cannot create new ones.

XML is similar to HTML in that it also uses tags to describe data. There are two important differences, however. XML’s tags are “extensible,” which means users can create new tags. Another difference is that the tags in XML actually describe the data rather than indicating how to display it. Suppose a business wants to report Sales Revenue of $1,000,000. HTML tags may specify how to display the dollar amount (e.g., in the title or in a table), but they will not convey meaning about what it represents. You could use XML tags to mark the data as: `<Sales Revenue>$1,000,000<Sales Revenue>`. Now the data has meaning. One problem remains, however. Perhaps you mark your financial statements with a tag for sales revenue but another company chooses to use a different marker for sales revenue, for instance, Revenues. Without a predefined standard set of markers, users still are not able to extract data for comparison purposes, nor can they exchange financial information. To enable information preparation, publication, exchange and analysis, industries are creating their own dialects of the XML language. XBRL is the XML-based language specification for the accounting industry. Figure 2-5 shows XML-tagged data describing income statement information.

XBRL is a global effort of groups with a stake in financial reporting, such as the American Institute of Certified Public Accountants. Software vendors are involved too and they’re building XBRL into their software applications. XBRL-compliant software will insert the appropriate tags automatically. The XBRL Steering Committee (see www.xbrl.org) is working to spread the development and usage of XBRL standards. Developing XBRL is not easy. The language requires classification systems for different reporting segments and standards such as US generally accepted accounting standards (GAAP). The various classification systems define the tags and describe the relationships among the data items. To understand the need for multiple...
sets of tags, think about the charts of accounts in different industries. The oil and gas industry has accounts regarding reserves, for instance. Sets of tags need to be created for each industry’s financial reports, each set of accounting standards, and also for information that doesn’t appear on formal financial statements. For instance, for businesses to exchange financial information, they need to agree on the markers in source documents, such as purchase orders.

XBRL has many potential benefits. A company that needs to file its financial information can do so in just one format, avoiding the errors that may come from re-entering data multiple times. They can save financial data in their software in the XBRL format. The Securities and Exchange Commission (SEC) will accept this format for electronic filing of financial statement reports. Creditors can accept the filing and convert it to complete forms for loans. The company can directly upload their business information in this format onto their web site. Anyone interested in comparing the cash and cash equivalents of several companies can search for the data and export it to a spreadsheet for analysis purposes. The hope is that XBRL will make financial information available on the Internet more accessible and of greater use. It should do this, too, for less cost since the business had to key-in the data only once.

Despite the benefits, XBRL may take a while to catch on. While the SEC supports the idea of a financial reporting standard, it does not yet endorse XBRL. Few companies to date have chosen to file their SEC reports in XBRL format either. Finally, XBRL does not resolve the issues of standardized financial reporting. The primary motivator for using XBRL is likely to be a reduction in cost that comes from single data entry. Until the standard becomes more widely accepted, however, users will not be able to easily access the wealth of financial information that’s available on the web.

**ELECTRONIC COMMERCE**

The term **electronic commerce (EC)** refers to conducting business with computers and data communications. Often, EC is done over the Internet, but businesses also conduct a great deal of electronic commerce over proprietary transmission lines, for example, over extranets set up between suppliers and their manufacturers. The FBI estimates that the banking industry transfers over $1 trillion each week by electronic means. The impact of business-to-business e-commerce is likely to have a major impact on accountants. As a result, the American Institute of Public Accountants (AICPA) ranked business-to-business e-commerce as the most important technology application.
and technology issue for the year 2000. Some general categories of electronic commerce and usage are retail sales, e-payments and e-wallets, and electronic data interchange, each of which we examine briefly in the paragraphs that follow.

**Retail Sales**

The World Wide Web has enabled businesses to open virtual stores that sell merchandise directly to customers. Some obvious advantages of such virtual stores are (1) creating web pages is usually much cheaper than creating and mailing catalogs; (2) distribution is worldwide; (3) selling takes place around the clock with no additional staffing requirements; (4) product descriptions, sales prices, and information on merchandise availability can be updated immediately as they become known or change; (5) customers create their own sales orders online; and (6) the sales personnel required for these virtual stores is minimal, thus reducing labor costs per dollar of sales.

Testimony to the success of retail electronic commerce abounds. The number of online shoppers has increased steadily during the past few years. More than half the US population is online, and about 39 percent of Internet users have bought something. Online retail sales increased so much during the 1999 holiday season that some Internet companies couldn’t keep up with sales.

**Case-in-Point 2.5**

Wal-Mart Stores, Inc. posted a note on its web site in early December 1999 that it couldn’t guarantee on-time Christmas deliveries. When toysrus.com let customers know they might not be able to make deliveries, customers were particularly upset. Telling kids the toys weren’t under the tree because of online shopping problems wasn’t a pleasant task. One of the authors of this book ordered a book for her son for Christmas. When the book hadn’t arrived by December 20, she checked her order at Amazon.com online to find that the book was back-ordered but would be shipped soon. Two days after Christmas the book arrived—or at least the packing slip for the correct book came, accompanied by a different book. A call to Amazon (getting through took about two minutes) resulted in instruction to return the book. The author had to go to the post office to mail the book back in order to receive a refund. To their credit, Amazon tried to make up for their error with a gift certificate. Since the book originally ordered appeared to be on back-order for weeks, the author finally cancelled the order for it.

Many traditional brick-and-mortar companies were at first slow to get online. This phenomenon allowed some previously unknown businesses to grab market share of online sales first. It appears though that brand names are important to customers, whether they are in line or on line. Media Metrix, a company that tracks web site traffic, reported that almost half of the 50 most visited web sites during the 1999 holiday season were associated with older, established businesses. These companies included Toys “R” Us, J.C. Penney Co., Sears, Roebuck & Co., and Wal-Mart Stores Inc. As the dot com “bubble” burst at the onset of the new millennium, it became increasingly clear that many of the new Internet retailers would lose out to the “click and mortars.” Features that make online retailers successful include the web site’s appearance, the ease with which customers can search the site for desired products, customer service, product availability, pricing, and ability to deliver as promised.

While many of these features are common to brick and mortar stores too, the Internet introduces special issues. Customers have to rely on e-mail to handle customer service complaints, and do not have the satisfaction of speaking with someone in per-
son. Online stores frequently rely on suppliers rather than their own shelves for merchandise to satisfy orders and this can create stock out and backorder problems.

There are also security and privacy issues. The online communication in an electronic purchase transaction provides retailers with a wealth of data about customers. They can use this data to better serve customers, but there are also privacy and security concerns. For example, suppose you buy mysteries from an online bookseller. The bookseller’s information system, tracking your purchase history, could offer to e-mail you as books you might be interested in reading become available. This is a benefit to you as a consumer, but you might be concerned about the retailer maintaining rich data about your purchase patterns. A later section of this chapter addresses privacy and security issues in depth.

E-Payments and E-Wallets

How do customers pay for the merchandise they order over the Internet? You are probably already familiar with the most common method—supplying a credit card number. But this method presents a problem to vendors because acceptable credit card numbers only indicate that a card is valid. They do not indicate that an online customer is authorized to use it. This is also a problem for the customer because identity fraud, in which individuals discover that their identities have been stolen and their good credit used by others to buy merchandise, is on the rise. A related problem with online payments is that, while an online customer might not mind sending their credit card number to a trusted merchant, they do not wish to share the number with lesser known businesses or individuals. Finally, another issue is that not everyone has a credit card, or one with available credit.

Some merchants and auction sites solve these problems with electronic payment (e-payments), which proponents claim is a faster, easier, and safer way for both customers and sellers to handle online transactions. The following Case-in-Point describes how one such system works.

Case-In-Point 2.6 Users who have bought and sold on Ebay or other online auction sites may be familiar with PayPal (www.paypal.com), an online payment system that operates via e-mail. Customers who successfully bid for an item in an online auction, but who don’t wish to share their credit card number with sellers, may open an account with PayPal. Account-holders can put cash in their PayPal account through their credit or debit card, or via their checking account. PayPal sends an e-mail to the sellers, notifying them that the payment has been put in their PayPal account. Upon request, PayPal will transfer the money to the sellers’ bank accounts or send them checks.

Another payment option is the e-wallet. Despite the fact that many potential customers lack available credit, it’s still likely that most online consumers will use credit cards directly to make their purchases for some time to come. E-wallets are software applications that store consumers’ personal information, including credit card numbers and shipping addresses. To use an e-wallet, a shopper can reference it when completing an online retailer’s checkout payment form and charge a purchase easily, as described in Case-in-Point 2.7.

Case-In-Point 2.7 Quick Checkout is America Online’s e-wallet application. AOL partners with a number of online retail merchants such as Macy’s and Eddie Bauer, and shoppers can
use Quick Checkout at all of them. When you visit an affiliated retailer, the Quick Checkout software enters your name, address, phone, credit card number, and other relevant information automatically in the payment form.

The advantages of an e-wallet are that you have access to passwords and credit card numbers as you visit various retail web sites and you do not have to enter all your information each time you make an online purchase. Also, because the information is usually stored on the hard drive of a shopper’s own computer, it is controlled by the user. E-wallets may be as important for retailers as they are for consumers because many consumers cancel e-commerce transactions before they are complete, for example, due to frustrations in filling out online forms. Case-in-Point 2.8 describes another e-wallet application.

Case-In-Point 2.8  
An online vendor may maintain an e-wallet for its customers. Amazon.com’s 1-Click technology is an example of this approach. Amazon lets shoppers choose its 1-Click option where the retailer automatically inserts all the personal shipping and billing information from the last purchase. The downside of the 1-Click approach is that it only works at one online store. To counter this problem, Amazon and others are seeking ways for shoppers to use similar technology at multiple vendors.

Business-to-Business E-Commerce

In 1999, online retail sales were approximately $16 billion. While there has been tremendous growth in retail e-commerce during the past few years, it is dwarfed by the actual and potential growth in the business-to-business (or b2b) e-commerce segment (i.e., one business firm selling goods or services to another business firm). According to Forrester Research, e-commerce revenues should grow to $2.7 trillion by 2004. Businesses are increasingly buying and selling from each other over the Internet.

A big part of b2b e-commerce concerns purchases of supplies and equipment electronically or electronic procurement. Buying goods online shortens the time from purchase to delivery, and also allows purchasing departments to choose from vendors all over the world. Employees in an organization can select their items for purchase themselves, from online catalogues. A company’s e-commerce software sends the employee order to the appropriate sites for approvals. Electronic procurement systems benefit an organization by reducing prices paid for goods and services and also by reducing the cost of processing purchase requisitions, as described in Case-in-Point 2.9.

Case-In-Point 2.9  
Owens Corning, a global glass maker, was able to use e-procurement to cut costs of several of its products, including water jugs, stretch wrap, and rock salt. In total, the firm was able to cut its annual purchases spending of more than $3 billion, by 10 percent! Some businesses use e-procurement for just some of their purchases. Lucent Technologies, for example, uses e-procurement to buy about 15 percent of their indirect materials and Hewlett-Packard Co. saved money by buying electrical power online.3

Another feature of b2b e-commerce is real-time business views that allow you to access up-to-date information at any time. By having real-time information about

---

operations (such as various expense items) available, managers can act instantly to adjust spending. There are many other uses of this “instant” information availability. For example, customers of delivery services such as Federal Express or UPS can track their packages online, truckers can check cargo status online to make carry loads more efficient, and workers in a manufacturing plant can have up-to-the-minute information about product and parts status on the assembly line.

As far as AISs are concerned, the Internet has had a large impact on the accounting and enterprise software world. Even vendors of very inexpensive software now include an e-commerce interface with their products. (A good example is Peachtree software’s Peachblink feature that provides users with tools to create and use a web site and accept Internet orders.) Enterprise resource planning (ERP) vendors (see Chapter 6) were not as quick as the marketplace would have liked in developing their e-commerce products. In the recent past, businesses made big investments in ERP systems both to avoid the y2k problem and to integrate their internal business processes. Once they realized the benefits from improving their internal functions, their interest shifted to external relations, notably the supply chain between a company and its customers and suppliers. E-commerce links to internal ERP systems provide advantages to companies in terms of better supplier and customer relationships. Suppliers and customers have better access to company information through a web site. For example, customers can check on the progress of their orders. Suppliers can look ahead to see when their product might be needed. ERP vendors can offer web site add-ons to their software that provide these capabilities.

While the Internet is speeding up the supply chain in terms of procurement and inventory tracking, it has been slow to impact the accounts payable and accounts receivable aspects of an AIS. In part, this is because companies like to hold onto their money as long as possible, making use of the float that comes from paying bills in less than real time. Prompt bill payment, however, works two ways. While a business may enjoy float on the accounts payable side, a lack of speed in collecting accounts receivable works to the company’s disadvantage. Software such as that produced by Time Capital allows vendors and customers to view purchase and shipping documents so that they can resolve discrepancies quickly and cut checks or make electronic payments faster. Companies engaged in electronic commerce are likely to realize more benefits as new software and services become available to speed up the payment process along with the shipping process.

Electronic Data Interchange

Electronic Data Interchange (EDI) allows organizations to transmit standard business documents over high-speed data communications channels. Examples of EDI business documents include requests for quotes (RFQs), purchase orders, bills of lading, freight bills, sales invoices, customs documents, payment remittance forms, and credit memos, all of which are relayed electronically—and therefore almost instantaneously—to their recipients. Thus, EDI automates the exchange of business information and permits organizations to conduct many forms of commerce electronically, as shown in Case-in-Point 2.9.

Case-in-Point 2.9 Pratt and Whitney is a large-engine manufacturer that buys over 26,000 parts from more than 700 suppliers. This company now transmits over 50,000 EDI documents per month, including purchase orders, procurement schedules, and sales invoices.
The company estimates savings between $10 and $20 on every purchase order—over $6 million per year.

For many firms, EDI is a superior way of doing business. Perhaps the most important advantage is that EDI users no longer are required to manually transcribe the data from a trading partner’s hard-copy forms (such as purchase order information) into their own systems—the data are already in computer-readable formats. This saves businesses time and labor, and significantly reduces the number of errors typically introduced into job streams when manual data transcription is required. EDI also streamlines processing tasks because (1) business partners exchange documents quickly and easily, (2) there are no postal delays, and (3) EDI eliminates most of the paperwork.

Although most EDI applications are found in private businesses, EDI can also be used effectively by government agencies. One example is the U.S. Customs Service:

**Case-in-Point 2.10** Before EDI, imported goods could wait on docks for weeks while officials processed the paperwork. But information about some imports can be sent weeks before the merchandise itself arrives. The U.S. Customs Service now uses EDI to process almost 95 percent of all customs declarations. This usage has lowered error rates from 17 percent before EDI, to about 1.7 percent now. This improvement translates into annual savings of $500 million in processing costs, and also into productivity gains of about 10 percent.

Some firms find the advantages of EDI so compelling that they refuse to do business with those companies that do not use EDI. This helps explain why EDI has been the fastest-growing segment of electronic commerce, with an annual growth rate of greater than 20 percent. But EDI also places a greater burden on auditors because electronic transactions are more difficult to verify, authenticate, and therefore audit. We shall return to this point shortly.

To implement EDI applications, most businesses currently use private, point-to-point communication channels called **value-added networks (VANs)**. These VANs are proprietary networks that large IT organizations design and maintain for their customers. When it first implements an EDI system, the user, for example, a large retailer, assigns each vendor a unique account code that simultaneously identifies the supplier and authenticates the supplier’s subsequent electronic transactions. Figure 2-6 depicts a VAN-based EDI system.

![Figure 2-6: A VAN-based EDI system.](image-url)
An alternative to VAN-based EDI is to use the Internet, which is also growing rapidly. One advantage of Internet-based EDI over VAN-based EDI is the ability to use well-understood Internet technology and a preexisting, costless network to transmit business data. This allows a company to avoid acquiring or building a private VAN. Another advantage is convenience. For example, several familiar accounting packages now support Internet modules that enable users to transmit basic accounting data electronically. (Again, as with PeachLink in Peachtree Accounting.)

PRIVACY AND SECURITY ON THE INTERNET

The most important advantage of the Internet and World Wide Web—accessibility—is also its greatest weakness—vulnerability. This means that someone who poses as an authorized user may be able to access any e-mail, web page, or computer file that an authorized user can access through the Internet. This section of the chapter discusses privacy and security on the Internet in detail. Chapter 10 discusses internal control and third-party assurance associated with the Internet.

Privacy

An Internet presence for companies introduces unique privacy and security concerns. Customers who shop on the web want to know that their privacy is protected. But companies doing business on the web are sometimes hard pressed not to use the wealth of data that online shoppers provide them, as illustrated by Case-in-Point 2.11.

Case-in-Point 2.11 Amazon.com’s use of “purchase circles” upset privacy advocates. The “circles” are lists of best selling products based on the most frequent purchases of specific customer sectors such as corporations and universities. The targeted best-seller lists are sales tools for potential customers as they tell them what others in their sector are buying. After privacy advocates protested the practice, Amazon gave customers the option of declining to participate.

Most web sites accessed by online users collect personal information. What they collect and how they use it are dictated by their privacy policy. An example is the one issued by www.jcrew.com (February 13, 2001). J Crew’s privacy policy states that the company may make their customer list available to a limited number of parties, but they will not share e-mail addresses with anyone who would use the addresses to send unsolicited e-mail. Shoppers are given the option of choosing or declining to receive promotional e-mails from J Crew. Finally, the policy promises that the company will not use your phone number for promotional purposes. Because businesses vary widely in the amount of privacy protection for customers, it is important to read a company’s privacy policy carefully. State governments, prompted by concerns over consumer privacy rights, particularly in the financial and health care industries, are introducing a variety of privacy legislation. Groups such as The Electronic Frontier Foundation and the Online Privacy Alliance are also working to protect the privacy of data transmitted over the Internet.
Security

Security includes the policies and procedures that ensure authorized access to data and information transmitted electronically. When ordering from J Crew, shoppers interact with the company’s computers in a secure mode as evidenced by the use of “https” as the web address versus “http.” Sometimes security and privacy issues are at odds with one another as demonstrated by the “too” smart card in Case-in-Point 2.12.

Case-In-Point 2.12 Five years from now each US citizen may have a taxpayer’s digital certificate (discussed later in the chapter) within a smart card. Citizens could use the smart card for all their transactions with the federal government. The government program responsible for developing this card is called Access Certificates for Electronics Services project, or ACES. While ACES is meant to ensure secure communications, privacy advocates are afraid that maybe the cards are too smart, since they contain all your personal information in one place. ACES does include safeguards to ensure that the data on the cards can’t be used in the private sector and is available only to a federal or authorized agency but those concerned with privacy worry that the existence of the card will prove tempting for unintended uses.

Privacy and security concerns associated with the Internet and electronic commerce call for specialized controls that limit data and information access to authorized users. Firewalls, proxy servers, and data encryption (discussed in the next sections) are effective controls over access. They use filtering and authentication techniques to limit access to authorized users. Authentication involves verifying that users are, indeed, who they say they are.

There are three levels of authentication: (1) what you have, (2) what you know, and (3) who you are. What you have may be a plastic card that provides you physical access. Examples of these cards are your ATM debit card or a key card that provides you access to certain premises. What you know refers to unique information you possess, such as a password. You can authenticate who you are with a unique physical characteristic such as your fingerprint or the pattern of the retina in your eye. As you might guess, using security that forces a user to display a unique physical characteristic (i.e., who they are) is the highest level of authentication. Some security systems require users to make use of a combination of authentication techniques. For example, you use both your debit card and your password to withdraw cash from an ATM.

Firewalls and Proxy Servers

To gain access to a company’s files, a computer hacker (an unauthorized user) must obtain access to that company’s computers. Firewalls and proxy servers are designed to protect against unwarranted intrusions from external parties.

Firewalls One way to guard against unauthorized access to sensitive file information from external Internet users is to create a firewall (Figure 2-7). This is security software that a company installs on Internet computers and that limits file accesses to authorized users.

Firewall software examines packets of incoming messages and ensures that they are from authorized users. To do this, the software maintains an access control list of bonafide IP addresses that company network administrators create for this purpose. If the software does not recognize the IP address of an external user, it refuses
that user access to the files he or she requested. Although firewalls are an obvious control for commercial applications, universities commonly use the same technique to limit access to their library and research resources to authorized parties.

A firewall is a useful Internet security control but (like most security features) is not foolproof. One obvious problem is spoofing (i.e., masquerading as an authorized user with a recognizable IP address). A less obvious, but potentially more serious, problem is the ability of a determined hacker to copy the contents of the access control list itself. If a hacker obtains the information in this file, he or she has the ability to pose as one of many authorized users—a security breach that is especially difficult to overcome.

**Proxy Servers** Given the large amount of information now available on the web, some organizations seek to limit the number of sites that employees can access, for example, to ensure that employees do not use web-access privileges for frivolous or counterproductive purposes. A proxy server is a computer and related software that creates a transparent gateway to and from the Internet, and that can be used to control web accesses. In a typical application, the user logs onto his or her familiar file server as before. But when this user attempts to access a page on the World Wide Web, the initial network server contacts the proxy server to perform the requested Internet access.

One advantage of using a proxy server is the ability to funnel all incoming and outgoing Internet requests through a single server. This can make web access more efficient because the proxy server is specifically designed to handle requests for Internet information. A second advantage is the proxy server’s ability to examine all incoming requests for information and test them for authenticity (i.e., the ability to act as a firewall). Yet a third advantage is the proxy server’s ability to limit employee Internet access to approved web sites (i.e., to only those IP addresses contained in an access control list). This enables an organization to deny employees access to pornographic or game-playing web sites that are unlikely to have any productive benefits.
A fourth advantage is the ability to limit the information that is stored on the proxy server to Internet-related materials—information that the company can afford to lose. If this server fails or is compromised by hackers, the organization is only marginally inconvenienced because its main servers remain functional. To recover, the company can simply restart the system and reinitialize the server with backup data.

A final advantage of proxy servers is the ability to store frequently accessed web pages on the server's own hard disk. This enables the server to respond quickly to user requests for information because the data are already available locally. The savings in time can be considerable, for example, Netscape Communications estimates that between 30 and 60 percent of Internet requests are redundant. This feature also enables managers to obtain some idea of what information employees most need and perhaps to take steps to provide it internally (rather than through web sources).

Firewalls and proxy servers give online companies some protection from hackers, but they cannot protect against denial of service attacks. These attacks occur when hackers “flood” a web site with bogus traffic. Case-in-Point 2.13 describes a denial of service attack on popular web sites.

Case-in-Point 2.13  In February, 2000, hackers launched a series of denial of service attacks against several popular online companies, including Amazon, eBay, ETrade, Buy.com, and ZDNet. In some cases, the attacks blocked access to the web sites for several hours. The attacks differed from previous denial of service attacks because they used many layers of computers to “launder” their location and they harnessed hundreds of computers in the attack. The problem with this type of security violation is that it is difficult to prevent. This particular coordinated attack highlighted the vulnerability of companies doing business online.

Data Encryption

Because so much of the information transmitted over the Internet is private or sensitive, businesses often use data encryption techniques to transform plaintext messages into unintelligible cyphertext ones. The transformed messages are then decoded at the receiving station back into plaintext for use. The advantage of this system is that the encrypted message cannot be understood during data transmission, even if unauthorized users intercept it.

There are many encryption techniques and standards. The simple method shown in Figure 2-8 uses a cyclic substitution of the alphabet with a displacement value of “5” to transform the letters of a plaintext message into alternate letters of the alphabet. To decode the message, the recipient’s computer performs the encryption process in reverse, decrypting the coded message back into readable text. To make things more secure, the sender can use a different displacement value for each coded message.

The method that computers use to transform plaintext into cyphertext is called the encryption key. This is typically a mathematical function that depends on a large prime number. The data encryption standard (DES) system used by the U.S. government to encode documents employs such a system. DES uses a number with 56 binary digits to encode information, a value equal to approximately 72 quadrillion. Thus, to crack the code, a hacker must guess which of 72 quadrillion values was used to encrypt the message.
The data encryption method illustrated in Figure 2-8 uses a single cryptographic key that is shared by the two communicating parties and is called secret key cryptography. This system derives its name from the fact that the key must be kept secret and controlled only by the parties with access to it. The most common encryption methods today use public key encryption, a technique that requires each party to use a pair of public/private encryption keys. Two examples are SSL (Secure Socket Layer) and S-HTTP (Secure Hypertext Transport Protocol).

To employ public key encryption, the party sending information uses his or her private key to encode the message and the receiving party uses a second private key to decode it. A major advantage of public key encryption is that the same private key cannot be used to both encode and decode a message. The sending party retains one key as a private key and uses the receiving party’s public key to encode the message. The recipient uses the public key as well as a second private key to decode the message and translate it into plaintext. Data transmissions using public key encryption are likely to be secure because the transmitted message itself is scrambled and because neither of the parties knows the other’s private key. This is the main reason why most web applications use the public key encryption system.

### Digital Signatures

Many businesses require proof that the accounting documents they transmit or receive over the Internet are authentic. Examples include purchase orders, bids for contracts, and acceptance letters. To authenticate such documents, a company can transmit a complete document in plaintext, and then also include a portion of that same message or some other standard text in an encrypted format, that is, can include a digital signature.

In 1994, the National Institute of Standards and Technology adopted Federal Information Processing Standard 186—the digital signature standard (DSS). The presence of the digital signature authenticates a document. The reasoning is straightforward: if a company’s public key decodes a message, then that company must also have created the message. Thus, some experts consider digital signatures even more secure than written signatures (which can be forged). Further, if the sender includes a complete message in both plaintext and cyphertext, the encrypted message provides assurance that no one has altered the readable copy. (If someone has altered the plaintext, the two copies will not match.)

Another authentication technique is the digital certificate. Digital certificates are verification of identity provided by an independent third party called a certificate...
authority. Certificate authorities, such as Thawte and VeriSign, issue certificates to individuals and organizations. These certificates are signed documents with sender names and public key information. Certificates are generally encoded, possibly in a certificate standard such as the X.509 certificate format. Digital certificates can also be used to assure customers that a web site is real.

Digital Time Stamping

Many important business documents are time sensitive. Examples include bidding documents that must be submitted by preestablished deadlines, deposit slips that must be presented to banks before the close of business, buy orders for stock purchases that depend on the date and time of issue, and legal documents that must be filed in a timely fashion. Then, too, most businesses also want to know when particular purchases were ordered, when funds were disbursed for required expenditures, or when specific data items were entered or modified in important databases. What these items have in common is the need for a time stamp that unambiguously indicates the time of transmission, filing, or data entry.

The PGP Digital Time Stamping Service is one of several digital time-stamping services (DTSSs) that attaches digital time stamps to documents either for a small fee or for free. In a typical application, the user sends the document to the service’s e-mail address along with the Internet address of the final recipient. When the service receives the document, it performs its time-stamping task and then forwards the document as required.

Digital time stamping performs the same task electronically that official seals and other time stamps perform manually. It authenticates the time and perhaps the place of a business transaction. This can be important over the Internet. Although most documents are transmitted almost instantaneously, time delays can occur, for example, when file servers temporarily falter or power failures disrupt wide area networks. Time stamps enable businesses to overcome these problems.

AIS AT WORK

The SEC Hosts Fake Company Web Sites

The Securities and Exchange Commission (SEC) has become concerned about investors being “scammed” by investing in companies that aren’t real. The ability for anyone to develop and host a web site means that some unscrupulous parties have developed sites with fictitious information. These sites masquerade as legitimate corporate sites and include information about a fictitious company that is designed to lure site visitors to investing in the business.

To show how easy it is to fall prey to such a hoax, the SEC developed several “fake” company sites of its own. An example is the McWhortle Enterprises site at www.mcwhortle.com. McWhortle’s home page describes the company as a manufacturer of biological defense mechanisms that it sells to Fortune 500 companies. As you read the page, it becomes clear that the Bio-Hazard Alert Detector is a pretty exciting
and timely product. McWhortle’s homepage includes links to more information, including testimonials, press releases, and an opportunity to invest. When you click on the “About Us” link, you will see a very nice picture of McWhortle’s headquarters offices and you’ll also learn about the company’s founder, James McWhortle, III. Clicking on the “Invest Now” link takes users to a web page that explains that the Pre-IPO investment has been oversubscribed, but there are still investment opportunities remaining. A link on that page states that you should click on it when you’re ready to invest in the company. Click on that link, and you pull up a web page that begins with the phrase, “If you responded to an investment idea like this … You could get scammed!” It is only there that an unsuspecting Internet investor-wannabe will learn that the entire McWhortle site is a fraud!

The SEC hopes that its fake company examples will help to educate Internet users about the potential for fraud on the Internet. The McWhortle site contains many helpful links where users can learn more about investment scams and ways to protect themselves (e.g., a link to the SEC’s brochure, “Internet Fraud: How to Avoid Investment Scams”). The site further reminds users that they should do their own research before making investments and identifies some of the giveaways that should have alerted a user that the McWhortle site promises were unlikely to be real. The use of sites, such as McWhortle by the SEC, is an interesting approach to combating some of the new risks introduced in an E-business environment.

**SUMMARY**

The Internet is a collection of local, wide-area, and international networks that accountants can use for communication, research, and business purposes. Most accountants also use the World Wide Web—the graphics portion of the Internet—for similar purposes. Intranets are private networks that enable employees to use web browser software and that businesses create for such internal purposes as distributing e-mail. Extranets are similar to intranets, except that they allow external parties to access internal network files and databases.

One use of the Internet is for electronic communication (i.e., transmitting text messages and perhaps graphics attachments over the Internet). Groupware is software that supports e-mail on business networks, plus allows users to share computer files, schedule appointments, and develop custom applications. Knowledge sharing enables accountants to share research and information about the best practices of their clients throughout their businesses.

To make all the financial information available on the Internet accessible, users will need a new reporting language such as XBRL. XBRL is a form of XML and provides a common format for financial data that allows searches of the data and extraction for comparison purposes.

Another important application of the Internet is electronic commerce (EC). Retail sales are booming on the Internet, as are applications of electronic data interchange (EDI). For a variety of reasons, most businesses prefer to use private value-added networks (VANS) rather than the Internet to support EDI applications. This may change, however. Business-to-business electronic commerce will be the biggest Internet application yet.

Privacy and security concerns associated with the Internet prompt many businesses to construct firewalls, use proxy servers, and employ data encryption techniques, digital signatures, and digital time stamping to achieve control objectives. One issue that is of concern over the Internet is authentication—the ability for users to prove they are who they say they are. Privacy is also an important issue. This concerns users’ ability to protect data about themselves and the transactions in which they engage while buying and selling online.
KEY TERMS YOU SHOULD KNOW

access control list  
authentication  
certificate authority  
data encryption  
data encryption standard (DES)  
denial of service attacks  
digital certificate  
digital signature  
digital signature standard (DSS)  
digital time stamping service  
domain address  
EdgarScan™  
electronic commerce (EC)  
electronic conferencing  
Electronic Data Gathering and Retrieval (EDGAR)  
Electronic Data Interchange (EDI)  
electronic mail  
electronic payments (E-payments)  
electronic procurement  
encryption key  
e-wallet  
Extensible Business Reporting Language (XBRL)  
Extensible Markup Language (XML)  
extranets  
firewall  
groupware  
home page  
hyperlinks  
hypertext markup language (HTML)  
hypertext transfer protocol (HTTP)  
identify fraud  
Internet  
Internet protocol (IP)  
Internet service provider (ISP)  
intranets  
knowledge sharing  
proxy server  
pubic key encryption  
secret key cryptography  
spoofing  
supply chain  
tags  
universal resource locator (URL)  
value-added networks (VSNs)  
web browser  
World Wide Web

DISCUSSION QUESTIONS

2-1. What is the Internet? What is an Internet domain address? What is an IP address?
2-2. What are intranets? What are extranets? Why are intranets and extranets important to accountants?
2-3. What is hypertext markup language? How does it differ from XML and XBRL?
2-4. How does e-mail work? What are some advantages of e-mail? How might the employees of a public accounting firm use e-mail?
2-5. Describe some important uses of electronic commerce. Why is EC important to accountants?
2-6. What are electronic payments? How are they different from credit card payments?
2-7. What is electronic data interchange? Why do companies use EDI?
2-8. Most retail-sales web sites require customers to use their credit cards to make purchases online. How comfortable are you in providing your credit card number in such applications? Why do you feel this way?
2-9. What are Internet firewalls and proxy servers? How are they created? How do businesses use them for Internet security?
2-10. What is data encryption? What techniques are used for data encryption?
2-11. Describe and contrast the three levels of authentication. Can you think of a business situation where someone would need to use a combination of all three levels to gain access to information?
2-12. What are digital signatures? Why do businesses use them? How can businesses use a digital certificate for Internet security?

2-13. Analysts claim that businesses can increase sales on the Internet, but not profits. What evidence does this chapter provide to support or refute this claim? Discuss.

PROBLEMS

2-14. The Internet uses many acronyms. Within the context of the present chapter, what words were used to form each of the following?
   a. ISP  
   b. URL  
   c. IP address  
   d. WWW  
   e. http  
   f. e-mail  
   g. EC  
   h. VANs  
   i. IETF  
   j. EDI  
   k. XML  

2-15. Examine the data encryption technique illustrated in Figure 2-8. Use a displacement value of “8” to encrypt the following message:

   “Those who ignore history are forced to repeat it.”

2-16. The message below was encrypted using the technique illustrated in Figure 2-8 (using a displacement key other than 5). Using trial and error, decode it:

   OZ OY TUZ CNGZ CK JUTZ QTUC ZNGZ NAXZY AY
   OZ OY CNGZ CK JUTZ QTUC ZNGZ PAYZ GOTZ YU

INTERNET EXERCISES

2-17. Visit the e-Bay (www.ebay.com) web site. How can buyers and sellers in an auction exchange their goods and money?

2-18. A number of accounting journals now publish portions of their journals or even complete issues online. Access the Journal of Accountancy web site at www.aicpa.org (or another web site selected by your instructor). Select an article of interest and write a one-page report on it. What are some of the advantages of publishing journal articles online?

2-19. Using your Internet browser and a search engine such as Yahoo, find a separate web site that sells each of the following products: (a) books, (b) CDs, (c) cars, (d) stocks, (e) clothing, (f) tools, and (g) airline tickets. Which product(s) would you be willing to purchase on the Internet? Which products would you prefer to purchase in a store? Provide reasons for your answers.

CASE ANALYSES

2-20. DeGraaf Office Supplies (Business Web Sites and Security)

DeGraaf Office Supplies is a national retailer of office supplies, equipment, and furnishings. The company opened its first store in 1932, in Columbus, Ohio. Currently, DeGraaf has 300 stores nationwide. Owner-managers purchase and run franchised stores. Kim DeGraaf, the founder’s daughter, currently is President and CEO of the corporation.
Sales revenues grew steadily during the past decade, but 2002 sales were quite disappointing, down 8 percent from 1998. The company’s stock price has also taken a big hit during the past few months. Kim resisted developing an Internet presence for the company, and it appears now that this was a mistake. Online sales of office supplies are growing rapidly, particularly in the business-to-business sector as business organizations are finding it faster and more efficient to enter their office supply orders electronically. The following is a conversation between Kim and Peter Brewer, Vice President of Marketing.

Peter: “Kim, I warned you that we were going to see sales decline if we didn’t hurry up and get on the Internet. The established brick-and-mortar businesses in many industries are suffering.”

Kim: “You were right, Peter. I think I’ve been overly concerned about security and privacy issues. I also didn’t really believe that online sales in our industry would take off the way they have. I hope we’re not too late, because I want to move ahead immediately in developing a web site. I know other companies have a jump start but hopefully our brand name recognition and reputation for quality will help us. I have contracted with a consulting firm to start the web site development and am going to give a press release this afternoon about our plans. Fortunately, our current enterprise software has electronic commerce features and the consultants tell me that our Internet site should be ready for business in about six months. I need you to have your staff prepare an analysis of our competitor web sites. I would also like as much information as possible related to providing retail and business customers with security and privacy over online transactions with us.”

Peter: “This is great news! I will get my staff busy at once providing you and the consulting team with the information they need. There will be a lot of decisions to make. I’ve studied all the office supply web sites and they are organized in a variety of ways. For instance, some sites provide customers with the option to select a type of product such as ballpoint pens and then show the vendor options in that category, while other sites are organized around the vendors. This type of site allows customers to select a vendor name, such as PaperMate, and then lists all the product offerings from that vendor. Hopefully, the consultants have a lot of experience with business web sites and they can help us with many of these issues.”

Requirements

1. Visit the web sites of two office supply stores on the Internet. Develop a set of four to five criteria for evaluating their web site.
2. Evaluate DeGraaf’s chances for catching up to competitors in the online marketplace.
3. Discuss the privacy and security concerns for companies doing business electronically. Make recommendations to DeGraaf Office Supplies for addressing these concerns.

2-21. Small Computers, Inc. (Security on the Internet)

The following stated policies pertain to the e-commerce web site for Small Computers, Inc., a personal and handheld computer manufacturer and seller.
Privacy Statement

• We will only use information collected on this web for legitimate business purposes. We do not give away or rent any information to third parties.

• We will only contact you for legitimate business purposes, possibly from time to time, as needed. Please be 100 percent assured that we hold all transactions between you and our company in the strictest confidence.

Disclosure of Business Practices, Shipping, and Billing

• We will ship all items at the earliest possible date.

• We will not require you to accept items that you did not order.

• We will accept any returns from you of damaged or defective merchandise.

• In the event that we should accidentally bill you more than once for the same item, we will immediately issue you a refund.

Requirement

Evaluate these stated policies in terms of how well they promote customer trust and confidence in Small Computers, Inc.’s electronic business operations.

REFERENCES, RECOMMENDED READINGS, AND WEB SITES

References and Recommended Readings


Web Sites
To access EdgarScan, visit http://edgarscan.pwcglobal.com.
You can access the EDGAR database through the website of the Securities and Exchange Commission at www.sec.gov.
Two sites with resources, references, and examples for XBRL are: www.xbrl.org and www.xbrlsolutions.com
There are several web sites associated with online payment systems. Check out www.paypal.com., www.billpoint.com., and www.checkfree.com.
There are several research firms that collect and distribute data about e-commerce. Two of these are Forrester Research at www.forrester.com and Gartner Group, www.gartner.com. These companies charge for some of their research but they also publish many reports for free.