
DOING BUSINESS ON THE INTERNET¹

VeriSign, Inc. helps millions of Internet users each day as the keeper of the database of dot-com and dot-net Internet addresses. VeriSign provides the infrastructure that translates Web sites and e-mail addresses into codes understood by the routers and switches that comprise the Internet. How does VeriSign make money? It offers a series of security, billing, and payment services to telecommunications and online retail customers. It is the ‘trusted third party’ for transactions of all types over the Internet. In this role, VeriSign provides security services to more than 3,000 businesses and 400,000 Web sites, according to *Information Week* (May 2, 2005).

VeriSign is an example of a completely new business made possible by the Internet. Not only is it the closest thing to the core of the Internet, since it is the trusted source of the dot-com and dot-net Internet addresses database, but the company figured out a business model to make money in a world where most expect services to be free. It has grown its reputation for trust into a business where customers are willing to pay a fee to ensure that the same level of trust covers their transactions.

In some ways, the Internet is a business domain that operates exactly like the physical business world. In other ways, it is an entirely different business domain from the physical world. The two worlds are similar in that both have customers and suppliers. Transactions occur between customers and suppliers. Customers pay suppliers, and suppliers deliver goods and services. But the similarities may end there. Doing business on the Internet, or e-business, has enabled an entirely different set of business models to emerge. With these new models comes a different vocabulary, a different set of assumptions, and a different set of opportunities.

Just to be perfectly clear, we use the terms e-business and e-commerce interchangeably. Earlier in the life of the Internet, these terms meant something different. E-business was more than e-commerce because it included any business activity conducted electronically between or within businesses, whereas **e-commerce** was defined to be just the electronic interactions that enable exchange of goods and services. However, as the medium has evolved, these two terms have come to mean the same thing.

¹ The authors wish to acknowledge and thank Matthew Spafford Sumsion, MBA 1999, for his help in researching and writing early drafts of this chapter.

The Internet is the backbone for e-business marketplaces in which transactions occur instantly over the network and involve virtually no paper. The world of e-business in general, and the Internet and World Wide Web in particular, changes so quickly that information in this textbook is surely out of date before the text reaches the student's hands. However, it is such an important topic that this chapter is provided as foundation for managers who will be managing companies in the Internet Age. Just about every business has some component of its operations on the Internet, therefore even a general manager must understand some of the basic background of this environment in order to be truly effective in the business. To that end, this chapter begins with an overview of the technology behind the Internet. It then describes a framework for thinking about the applications that might use e-commerce, with a focus on business and professional uses, not personal and individual uses, although the latter make up a very large percentage of the traffic over the Internet. The chapter concludes with two Food for Thought sections, one on e-learning and the other on blogs.

► OVERVIEW OF THE INTERNET

Because the Internet (Net) plays such a great part in e-business, it may be valuable at this point to define and give a short history of the “Internet” and the “World Wide Web.” These terms are often used interchangeably, but it is helpful to recognize the distinctions.

Internet

The **Internet** is a global, *interconnected network* (hence the name) of millions of individual computers (called hosts). The history of the Internet begins in 1969 with the U.S. Department of Defense's ARPANET, a network designed to support the communications between cities in the United States in the event of a major disaster. The idea was to build a network based on the concept of openness that would continue to work even if parts of it were destroyed. The network was designed for defense, not commerce. Handling large volumes of communications was not an initial design requirement. In 1985, the National Science Foundation built NSFNET using the ARPANET protocols. NSFNET was essentially the backbone network provided free to universities and research centers, requiring only that these organizations build a connection to it. NSF eventually withdrew as the manager of the network as commercial telecommunications companies and private and public institutions built their own links into the network and started using the Internet for commercial purposes. The often-proprietary demands of businesses and markets, however, are sometimes at odds with the principle of openness upon which the Internet is based. Today, no single “owner” controls the Internet. Instead, it is a collection of networks that all can link to each other, share the same protocols, and support the exchange of packets of information.

The breakthrough technology that allowed this critical interoperability was **TCP/IP**, which stands for *transmission control protocol and Internet protocol*. In the article “How the Internet Works,” Richard Wiggins explains that **protocols** “are the specifications for the interface between two computers, and they set stan-

dards to define how computers communicate with each other to accomplish specific tasks.” TCP/IP protocols define how to divide data into packets in order to transmit them over the Internet. Each TCP/IP packet of information contains three parts: header, data, and trailer. The TCP part of the protocol is connection oriented—it establishes a connection between processes on different host computers before data is transmitted. IP “defines a connectionless service through which data is delivered from computer to computer.”² Each node on the Internet has an IP address, or a 32-bit number assigned to it. When considering addressing, the TCP/IP packet delivers data in a way that can be compared to a standard letter, as diagrammed in Figure 7.1.

Statistics are difficult to acquire because no one well-defined way is available to measure usage. One thing is clear, however; the number of business and individual users continues to grow rapidly. Users from more than 400 countries can link to this computer network for exchanges of news, messages, data, and commerce. The Internet has no governing board or central control; all information available on the Net is simply provided by any individual or organization that chooses to make the information available to the Internet community. Available information can include anything from pictures of someone’s cat to Anheuser Busch’s current annual report to backwards recordings of Beatles records. This information is available to anyone with access to the Internet. This access is gained, usually by subscription, through an Internet service provider (ISP).

In the United States, it took seven years for at least 30 percent of the population to have access to the Internet. This figure contrasts with the seventeen years it took for television and the forty-six years that it took electricity to have similar penetration rates. In terms of the type of access, ever-increasing numbers of users are connecting to the Internet over broadband channels rather than slower telephone lines.³ **Broadband** refers to telecommunication such as cable systems and digital subscriber lines (DSLs) in which a wide band of frequencies is available to transmit information. Because a wide band of frequencies is available, more information may be transmitted in a given amount of time.⁴ Broadband

TCP/IP Packet				
Computer address of sender (HEADER)	Computer address of receiver (HEADER)	Packet length (HEADER)	Data	Checksum (TRAILER)
Regular Mail				
Return address	Address		Letter	

FIGURE 7.1 Comparison of regular mail and TCP/IP packet.

Source: This example was provided by Harold Miles.

² Richard Wiggins, “How the Internet Works,” *Internet World* (October 1996), pp. 59–60.

³ Available at www.cisco.com.

⁴ Definition of broadband from Searchnetworking.com, available at http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci211706,00.html (accessed January 26, 2003).

is much like having more lanes on a highway to allow more cars to travel on it at the same time.

World Wide Web

The **World Wide Web (WWW)**, also known simply as the Web, is an increasingly popular system for accessing much of the information on the Internet via the use of specially formatted documents. The documents can be formatted in a relatively simple computer language called hypertext markup language (HTML) or any one of a number of more sophisticated languages, such as JAVA or C++. HTML was created by a researcher, Tim Berners-Lee, and his colleagues at CERN in Switzerland in 1989. It is part of an Internet standard called the hypertext transport protocol (the “http” at the beginning of Internet addresses), which enables the access of information stored on other Internet computers, called servers. Hypertext is another name for the usually underlined links (or hyperlinks, hot links, or hot spots), which, by clicking on them, provide access to other documents, graphics, or files located anywhere in the world. In addition to HTML and HTTP, the Swiss researchers created two other WWW building blocks: a Web server and a basic text-based Web browser. **Web browsers** are software programs that enable a large number of users to easily navigate the World Wide Web.

In 1992, when Marc Andreessen, a University of Illinois graduate student, created MOSAIC, a browser with a graphical user interface, the WWW began to capture widespread interest. Soon MOSAIC was followed by many other browsers, including Netscape’s Navigator and Microsoft’s Internet Explorer.

More Nets: Intranets, Extranets, and Virtual Private Networks

Many derivatives were subsequently developed based on the Internet, including intranets, extranets, and virtual private networks.

An **intranet** looks and acts like the Internet, but it is comprised of information used exclusively within a company and unavailable to the Internet community as a whole. Employees of AT&T, for example, can use company computers to access an employee handbook (containing links to such things as employee data, benefit information, and procedures for dealing with irate callers) via the company’s intranet. Using Web browser technology and the TCP/IP protocol, companies build intranets to facilitate information sharing within their business. Because AT&T may not want its customers and competitors to have access to employee information, it may build a security “firewall” between the Internet and the AT&T intranet. Intranets serving as conduits for internal communications are one of the first, and still one of the most popular, Internet applications of many companies.

So what is an extranet? Some sources would argue that it is just another redundant term for the Internet, or that “there is no such thing.”⁵ It is not quite that simple, however, because a company can utilize an extranet that is distinctly different from its intranet or from the Internet as a whole. Just as a company’s intranet con-

⁵ Fairdene New Media, available at <http://www.fairdene.demon.co.uk/extranet.html> (accessed November 8, 1998).

tains Internet-style information for exclusive use within the company, the company could also have an **extranet** containing information for use outside the company. For example, extranet information could be intended for use by a company's subcontractors or suppliers, or for private use by a specific external subsidiary with a need to know. Dell Computers, for example, created for their key customers Web pages that contain company information and links that are specifically tailored to the interest of that customer. Wal-Mart's extranet provides links to major suppliers such as Proctor & Gamble. As with intranets, extranets are not accessible by the Internet at large and are usually protected by a security firewall.

Often extranets are formed using a virtual private network. A **virtual private network (VPN)** is a private data network that leverages the public telecommunication infrastructure. It maintains privacy through the use of a tunneling protocol and security procedures. Using a client and server approach, a VPN's clients authenticate users, encrypt data, and otherwise manage sessions with VPN servers using a technique called tunneling. Companies realize cost savings by using a public infrastructure like the Internet instead of expensive private leased lines. VPNs are also used to support both remote access to an intranet and connections between multiple intranets within the same organization.

Evolution of E-business

Conducting business over electronic channels has been a reality for decades—well before the World Wide Web came into existence. One of the oldest forms of e-business is electronic data interchange. **Electronic data interchange (EDI)** is the direct computer-to-computer transfer of business information, using a standard format, between two businesses. It allows the transfer of business data (such as quote requests, order forms, and invoices) over leased lines with little or no human interaction. EDI uses standards (such as ANSI X12 or EDIFACT) to allow a software program on one company's computer system to relay information back and forth to a software program on another company's computer system, thus permitting organizations to exchange data pertinent to business transactions. Each transmission, or transaction set, comprises one or more data segments framed by header and trailer codes. One transaction set might contain information equivalent to that in a standard business document. Data segments, in turn, comprise strings of data elements, or facts such as prices or product specifications, separated by delimiters.⁶

EDI never lived up to its early growth projections. One reason for this may be that EDI requires substantial setup efforts on the part of the two trading partners. Although virtually all *Fortune* 500 firms were using EDI in the 1990s (and still do so today), smaller companies avoided the technology. Now that Internet EDI is available with the use of browsers and XML is simplifying the standardization process, more companies, especially smaller ones, are conducting their business transactions electronically—that is, they are using e-business.

⁶ Part of this description is based on information from Whatis.com, available at <http://whatis.com/edi.htm> (accessed November 8, 1998).

More typically the term **e-business** refers to business conducted over the Internet. Businesses on the Internet are usually described by a short acronym indicating the basic business model of the organization. Commerce between businesses (B2B) and between businesses and their customers (B2C), are the basic models of e-business. The difference is in who is targeted as the customer. B2B companies primarily focus on selling and interacting with other businesses, usually as part of the overall value chain (see Chapter 2 for a discussion of the value chain model). Their customers are other businesses who, in turn, either sell goods and services to other businesses or to eventual end-customers. B2C businesses are those that sell directly to consumers. For example, Amazon.com is considered a B2C e-business, selling primarily to consumers. A derivative of the B2C model directly links customers to customers—the C2C model. One of the most successful e-businesses, eBay, pioneered the C2C model. Figure 7.2 summarizes some of the many derivatives of the B2B model.

Despite its short history, business on the Internet has evolved through a number of stages. Commercial Web sites have moved from being content providers to transaction forums, integrated business platforms, and catalysts for industry transformation.

Content Provider: Stage I

The earliest commercial Web sites were viewed as an effective way of providing information to customers, suppliers, and even employees. Reports and printed advertisements were transported to the Web, with attempts to make the Internet version as similar as possible to the printed copy. Businesspeople could see the advantage of the Web in reaching millions of people, but had not yet grown to appreciate what the Web could allow them to do. They took little advantage of the Web’s interactive and multimedia capabilities.

Transaction Forum: Stage II

After a few years, many businesses started capitalizing upon the Web’s ability to interact with their customers. Though some fears arose about the security of electronic payments, businesses timidly started offering online sales. Their focus was on business-to-consumer (B2C) transactions. The sales were seen to supplement the

B2B	Business-to-business targets sales and services primarily to other businesses.
B2C	Business-to-consumer targets sales and services primarily to consumers.
B2E	Business-to-employee provides services other companies can use to interface with employees (like retirement funds management, health care management, and other benefits management).
B2G	Business-to-government involves companies who sell the bulk of their goods and services to state, local, and national governments.
C2C	Consumer-to-consumer sites primarily offer goods and services to assist consumers to interact (e.g., auctions).
Hybrid	Combines B2B and B2C models.

FIGURE 7.2 Basic business models for the Internet.

bread and butter of bricks-and-mortar companies. This “bricks-and-clicks” business model combines an e-business with a physical business. Its Web site is coupled with a traditional, physical business to leverage the best of both the Internet world and the bricks-and-mortar business. The Web business traditionally brings new thinking, new distribution possibilities, and new sales outlets to the table, while the physical business brings some sense of stability and possibly even customers, concepts, brand recognition, and other resources to the Web business. The resulting hybrid is a business model intended to be the best of both worlds. However, unlike the fledgling dot-coms that started surfacing in the mid-to-late 1990s, the Web site transaction processing of bricks-and-clicks initially was not integrated with the more traditional operations.

Integrator: Stage III

Eventually Web-based business operations were linked smoothly to legacy systems as businesses realized that e-business was in fact part of their business. B2B sites gained favor as businesses started integrating their online transaction systems with fulfillment, payment, service and support, and personnel systems. Eventually Web sites began integrating the entire chain of sales transactions, order processing, and other such activities with legacy, ERP, and CRM systems. Integrated supply chains (Chapter 5) are common and in many cases are a necessary way to do business today.

Catalyst for Industry Restructuring: Stage IV

By the new millennium it became clear that business over the Internet was transforming a number of industries. Some industries were reshaped by compressions and expansions in electronic channels. Other industries were transformed by new information-intensive offerings. For example, E-stamp, stamps.com is attempting to transform postage stamp distribution channels by allowing customers to download computer-generated postage from the Internet. Customers may buy postage online by credit card, electronic funds transfer (EFT), or check. When it is time to place the postage on the envelope, the customer draws the amount from secure hardware called a vault to which stamps.com has already downloaded the purchased postage. A barcode approved by the U.S. Postal Service is printed by a laser printer onto the envelope. The barcode indicates the amount of postage, the ID of the customer and the vault, the address where the mail is going, the date the postage was printed, the postal rate category, and a digital pattern to inhibit counterfeiting. As the number of e-stamp customers grows and as other players enter the field, the face of the postage stamp distribution industry may change dramatically.

E-channel Patterns

An **e-channel** is the chain of electronic “relationships between companies and customers and between companies and their partners/resellers.”⁷ E-channels can lead to industry restructuring when massive changes are brought about by e-channel compression and channel expansion.

⁷ R. Kalakota and M. Robinson, *e-Business 2.0* (Boston: Addison-Wesley, 2001), p. 76.

E-channel Compression

E-channel compression means eliminating redundant components in the channel. Often e-channel compression is undertaken to cut costs, improve the efficiency of channel operations, and eliminate unnecessary middlemen, or intermediaries. Shortening a channel results in the disintermediation, or the removal of one or more businesses from the e-channel. Targets of disintermediation include travel agents who no longer take part in the sale of Southwest Airlines' tickets over the Internet, and resellers or retailers whom manufacturers remove from the sales process so that they can establish direct links with their customers over the Internet.

An example of an industry transformed through e-channel compression is the music industry. In the old distribution industry, numerous intermediaries were involved in the production, marketing, and distribution of albums. Each intermediary added its margin to the cost of the album. However, a new digital music industry dramatically compresses the length of the channel and, consequently, the price to the customer. Now the 93 percent of artists who were not represented by major labels can provide their music online through companies like MP3.com. One source of revenue for MP3.com is through the sales of CDs by specific artists and the sales of compilation CDs. Consumers now can purchase specific songs on an album (as opposed to the whole album) directly through companies like MP3.com. As noted in Figure 7.3, this option resulted in the disintermediation of record companies, distributors, and retailers.

Not surprisingly, the record companies are fighting back. They argue that many of their traditional activities such as finding and promoting new talent, producing and recording music, and securing airplay are still needed in the industry. They brought lawsuits against Napster.com, an intermediary that made possible the free downloading of digital music. Even though the lawsuits forced Napster to redesign its business model, other companies soon sprang up to fill in the gap. For example, iTunes, run by Apple Computer, charges a small fee for each song downloaded, rather than facilitate free exchange of music files. The record companies are also responding by offering value-added extras for musicians' fans—preference in buying concert tickets, the possibility of climbing on stage, and e-mail exclusives.⁸ They are hoping to entice fans to develop an ongoing relationship with the artists whose music they purchase. Each time they buy an album, fans will be given a unique serial number that the record companies will use to maintain and personalize the relationship. The record companies, like other companies faced with massive industry restructuring, cannot afford to stand still.

E-channel Expansion

E-channel expansion results in lengthening the legacy channel by adding brokering functionality.⁹ In e-channel expansion, intermediaries are added to the channel

⁸ J. Ordonez and C. Goldsmith, "Music Industry Hopes Exclusives Can Blow Pirates Out of Water," *The Wall Street Journal* (September 16, 2002), p. B8.

⁹ R. Kalakota and M. Robinson, *e-Business 2.0* (Boston: Addison-Wesley, 2001), p. 76.

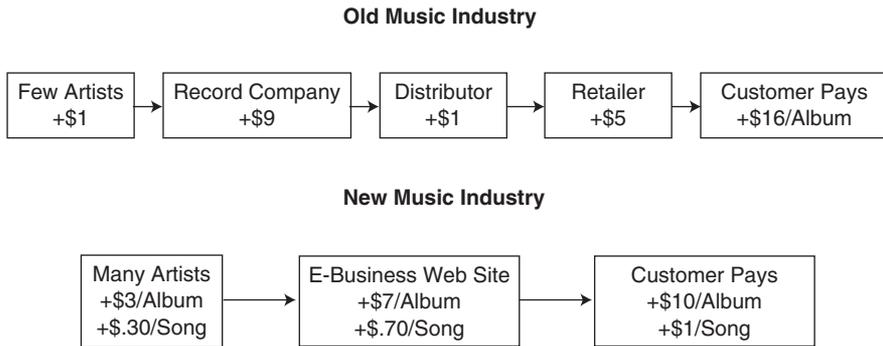


FIGURE 7.3 Example of channel compression.

Source: Adapted from Kalakota and Robinson, *E-Business 2.0* (Boston: Addison-Wesley, 2001).

because they offer services or products to improve operations. Some new intermediaries provide additional information, such as CarPoint (www.autos.msn.com) that offers information to people researching a car purchase. Others provide services needed to complete the transaction online. Some major new intermediaries include companies expediting electronic payment or the delivery of goods purchased online.

E-channel expansion is demonstrated in e-marketplaces. E-marketplaces are a special kind of B2B network that bring together different companies. Sometimes called net-markets or exchanges, these networks are typically built by a consortium of key businesses in the marketplace or by a third-party e-business interested in providing the marketplace. Much like the New York Stock Exchange creates a physical marketplace for trading stocks, e-marketplaces create a virtual marketplace for buying, selling, or trading goods and services. E-marketplaces are especially viable in fragmented markets populated by numerous buyers and sellers. Vertical e-marketplaces operate in specific industries, like DirectAg.com, a virtual marketplace for agriculture goods, and Covisint (www.covisint.com), a virtual marketplace for the automobile industry. Horizontal e-marketplaces operate across industries, typically targeting a specific business function or need that occurs in many types of businesses. TradeOut.com is an example of a horizontal e-marketplace site that provides a trading place for surplus equipment.

E-marketplaces may be most appropriate for ordering noncritical products whose delayed receipt would not hold up production, or for simple commodity products that are easy to describe. However, companies may be less willing to turn away from trusted suppliers and succumb to the lure of lower prices on an e-marketplace. This is especially true for production materials that require prequalification and specialized training and tools. Not surprisingly, many SCM executives sing the familiar refrain, “Why switch over to a new technology when the existing one is working well?” They continue to use EDI with long-term trading partners, though they may periodically use e-marketplaces to test prices every two or three years.

E-channels affect the relationship of businesses with consumers over time. In the content provider stage, the Internet promoted a one-to-many broadcast mode. The transaction forum and integrator stages made the one-to-many relationship

more efficient. Initially little personalization occurred in the message. Over time, the relationship may remain one-to-many, but the technology, especially CRM, creates the impression in the customer's eye that the relationship is one-to-one.

► FRAMEWORK OF ELECTRONIC COMMERCE

Kalakota and Whinston offer a generic framework for e-commerce, shown in Figure 7.4. The framework assumes that new applications will continue to be built on existing technology infrastructure—the computers, communications networks, and communication software that comprise the Internet. It uses four key building blocks:

1. Common business services, for facilitating the buying and selling process
2. Messaging and information distribution, as a means of sending and retrieving information
3. Multimedia content and network publishing, for creating a product and a means to communicate about it
4. The Internet, for providing the highway system along which all e-commerce travels

Two pillars supporting all e-commerce are integral to the framework:¹⁰

- Public policy, to govern such issues as universal access, privacy, and information pricing
- Technical standards, to dictate the nature of information publishing, user interfaces, and transport in the interest of compatibility across the entire network

Common Business Services Infrastructure

The first of the four building blocks is the common business services infrastructure. This building block consists of five main elements: security, electronic payments, search engines, web services, and personalization.

Security

Security is a major concern for doing business on the Internet. Businesses feel vulnerable to attack. Customers wonder how safe their credit card numbers are if they type them into a Web-based order form. Technologies have come a long way to provide security. Innovative businesspeople use tools that encrypt or otherwise disguise personal information, financial information, and business information. Web sites, called security validators, validate the security level of other sites, and provide a seal of approval when a particular Web site is protected. American Express,

¹⁰ R. Kalakota and A. Whinston, *Frontiers of Electronic Commerce* (Reading, MA: Addison-Wesley, 1996), p. 4.

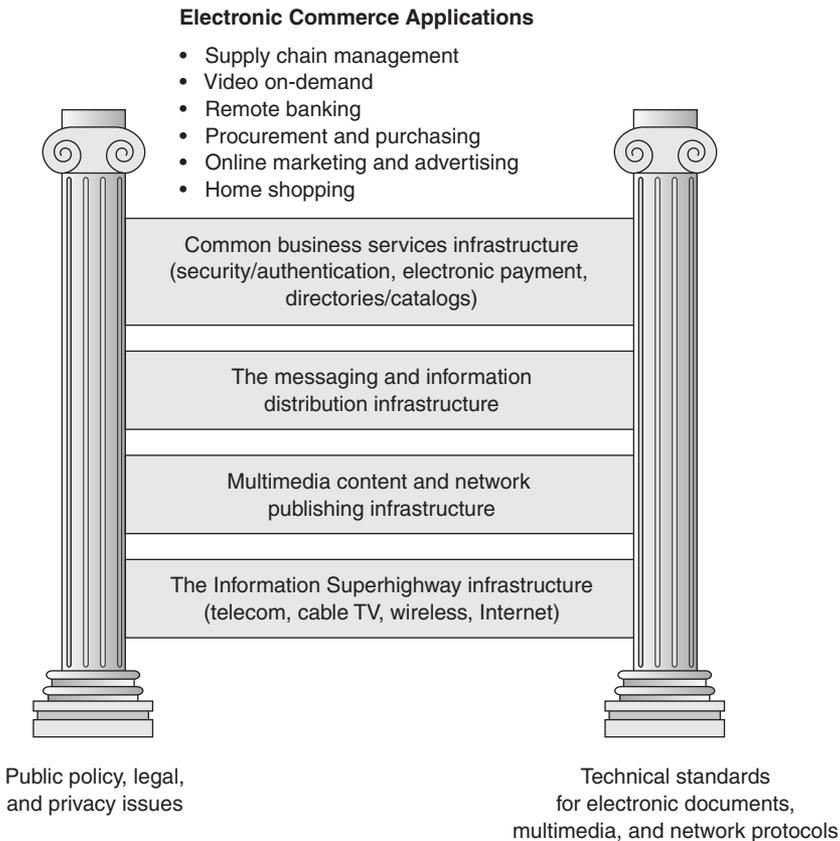


FIGURE 7.4 Generic framework for electronic commerce.

Source: R. Kalakota and A. Whinston, *Frontiers of Electronic Commerce* (Reading, MA: Addison Wesley, 1996), p. 4.

MasterCard, and Visa are promoting one-time credit card numbers that only exist for the duration of a single transaction. Businesses themselves make security measures more visible through explicit statements, icons, pop-up windows, and other means of communication.

Concerns remain about the safety of e-commerce transactions—what if, for example, someone were to steal all those credit card numbers as they are relayed over the Internet? The risk of the interception of e-commerce data may be no greater than the risks of paper transactions: credit card receipts (and credit cards themselves) are stolen and the numbers used fraudulently. Checkbooks are stolen and signatures are fraudulently forged. Transactions with a paper trail are hardly foolproof and may indeed be riskier than e-commerce transactions. Copy machines can make multiple copies of secure documents just as easily as e-mails can be sent with multiple copies. The difference is in the speed of the communication. A file with secure information can be sent anywhere in the world in a matter of seconds

over the Net, whereas the paper-based file takes longer to reach a destination. The security of e-commerce continues to improve. Innovations such as authentication, passwords, digital signatures, encryption, secure servers, and firewalls are already in place, and transactions need no longer be relayed via public forums like e-mail.

Authentication is a security process whereby proof is obtained that the users are truly who they say they are (i.e., their identity is verified as authentic). Authentication can be as simple as verifying the name and password of a user prior to allowing him or her access to an account. Additionally, it can include the use of a digital signature. Authentication can also be used to ensure that data transmissions are delivered to the appropriate receiver; to verify the source (or sender) of the data, and to ensure that the data have not been tampered with en route to their destination.

One simple way to provide authentication is through the use of a password. A **password** is a string of arbitrary characters known only to a select person or group. A computer or software program can be programmed to respond to commands or open messages only after the correct password has been entered; in this way, the system authenticates the identity of the user and prevents unauthorized access. Passwords are most effective when users select characters that would be difficult for others to guess; in practice, however, most people select simple passwords such as birthdates and nicknames, weakening the efficacy of the authentication process. To deal with this security problem, managers must be vigilant in assigning, rotating, and enforcing passwords.

Much like a handwritten signature is used to guarantee that the signer of a paper document is truly the person who composed it, a **digital signature** can be used to prove that the sender of a message (e.g., a file or e-mail message) is truly who he or she claims to be. A digital code is applied to an electronically transmitted message. The recipient of the message can compare this code upon receipt of the message with the sender's digital signature. If the two do not match, either the message originated somewhere other than with the stated sender, or the message has been intercepted and altered. Different forms of encryption can be used to ensure that digital signatures cannot be forged.

Encryption is the translation of data into a format that can only be read by the intended receiver. Here's how it works (Figure 7.5 includes a diagram of the process): the sender composes a message for the recipient in plain text, then uses an encryption key to encode it. The recipient has a **decryption** key and uses it to decode and read the sender's message, once again, as plain text. If an intruder were to observe the sender's message to the recipient, it would be incomprehensible, or **cipher text**.

If both the sender and recipient use the same special "key" to encrypt and decrypt the data, it is called **symmetric encryption**. Another common type of encryption, **asymmetric encryption**, uses differentiated keys, called **public keys** and **private keys**. The sender, for example, has access to the recipient's public key, but so do others. Any of them can compose a message to the recipient and encrypt it with his public key. The message, however, must be decrypted with a private key, and only the recipient has access to it. Two of the most widely used symmetrical encryption types are DES (data encryption standard) and PGP (pretty good privacy). RSA is a popular asymmetric encryption type.

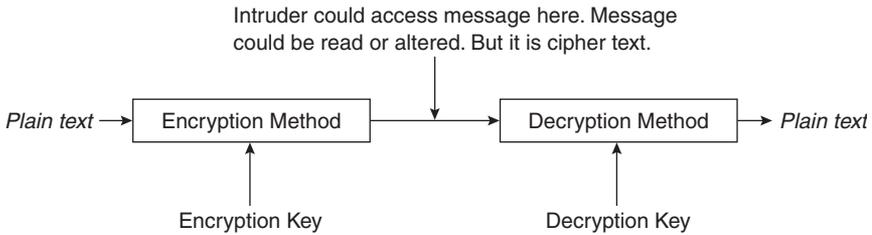


FIGURE 7.5 Encryption.

Many companies doing business on the Web use what are called secure servers in order to protect the privacy of the data they send and receive. Normally, text transferred from a browser to a Web server is sent as plain text; if anyone were to intercept the transmission, it would be legible. To prevent the interception of plain text, **secure servers** employ encryption technology to convert plain text into encrypted text before it is transmitted. Internet merchants that do not have their own secure servers can partner with an e-commerce provider that will allow the merchant's sensitive transactions to occur on the provider's secure site.

Firewalls are a different type of security measure. **Firewalls** consist of hardware and software that block out undesirable requests for entrance into a Web site, and keep those on the outside from reaching inside. For example, a hacker trying to reach a corporate Web site in order to plant a bug or virus could encounter a firewall, making it much more difficult to get access to the servers. Firewalls and other technological controls must be constantly improved to accommodate new technologies. For example, Web services allow transaction data to go through corporate firewalls and enable outsiders to invoke internal applications, potentially giving outsiders access to sensitive information.¹¹ In fact, it is possible to use a rogue Web service as a Trojan horse.¹²

Of course, even with these innovations, security remains an important concern of any business. All managers should be aware of potential hackers and, more importantly, disgruntled employees. They should be actively involved in the company's technology and maintain audit trails for computer use that will signal possible data corruption. They should regularly back up their data and ensure that any backup capabilities have been put into place by the IT department are actually followed in their departments.

As important as authentication, encryption, and firewalls are to security, companies cannot forget about making all aspects of their systems secure. In addition to the network, the database, operating system, and buildings in which the systems are housed, and the personnel who have any opportunity to access the system must be considered when making a system secure. Managers must develop a compre-

¹¹ J. Clabby, *Web Services Explained* (Upper Saddle River, NJ: Prentice Hall, 2003); H. M. Deitel, P. J. Deitel, B. DuWaldt, and L. K. Trees, *Web Services: A Technical Introduction* (Upper Saddle River, NJ: Prentice Hall, 2003).

¹² A. Gurugé, *Corporate Portals Empowered with XML and Web Services* (Boston, MA: Digital Press, 2003).

hensive set of policies and procedures to prevent internal and external threats to the entire system.

Electronic Payments

A number of payment vehicles are used by businesses to make and receive payments on the Internet, including credit cards, electronic checks, EFT, smart cards, e-cash, and intermediaries such as PayPal and iTransact. Perceptually, these methods are simply the electronic equivalents of everyday, off-line payment methods (e.g. credit cards, checks, and cash). But because transactions on the Internet happen virtually instantaneously, these payment vehicles are designed a bit differently than their physical cousins. A few of the more popular variations are described below.

- **Virtual Terminals**—This is the Internet equivalent to a credit-card swipe machine, since Internet businesses do not typically have the actual credit card to swipe through their physical machines. Virtual terminal providers generally assess a per-transaction fee and offer the service of accepting credit card payments.
- **Transaction Processors**—These intermediaries offer the convenience of virtual terminals but go a step further. They enable the merchant to stay out of the financial transaction completely. This service is ideal for merchants who wish to sell products but do not want to handle credit card information themselves. Companies like iTransact and PayPal handle these transactions, and deposit collected funds directly in the account of the business. PayPal is also popular among individuals as a method of payment for transactions (such as a purchase on eBay or a donation to a local charity).
- **Internet Checking**—This is a similar service to a virtual terminal, except it is for checks. It allows businesses to accept checks over the Internet. Typically the customer sends the vendor check information such as bank routing number, account number, and amount, and the vendor is able to electronically create a check with an indication that the customer has authorized this transaction. The check is routed in the same manner as any other paper check. Many banks offer this service and charge a fee per check issued.
- **Electronic Funds Transfer (EFT)**—This service simply transfers funds from the customer's bank account to the merchant's bank account, without any paper checks. EFT providers may charge a fee for each transaction; however, the transaction occurs virtually instantly.

In deciding on a payment acceptance scheme, managers must take into account factors such as efficiency, security, price, availability, and ease of use. Protecting against identity theft is a major concern.

Search Engines

Additional components of the common business services infrastructure include services used to index the contents of the Internet, such as search engines. Managers should pay attention to these services for two reasons: first, they provide useful and extensive information about the Internet, and second, they can provide the visibility that becoming listed with them provides in giving potential customers a route of access.

A **search engine** is a program that searches the Internet (or an intranet or individual site) for specified keywords. A search engine typically contains an interface, allowing a user to enter these keywords. The search engine then sends out a “crawler” or “spider” to collect documents that contain the keywords. It then indexes the collected documents for easy review. Popular search engines on the Internet include Yahoo!, Excite, Google, AskJeeves, and Alta Vista. Founded in 1998 by two Stanford Ph.D. students, Google quickly became the most popular search engine.

Search engines are important because they help potential customers find their way to a company’s Web site when hundreds, if not thousands, of competing sites are available. To be listed first on a search list can be crucial for the success, or even survival, of an e-business site. To improve the chances of its Web site being prominently displayed, a company may pay a subscription fee to the search engine, or may program the metatags in the HTML document so that search engines looking at metatags would retrieve the site’s address.

Web Services

A **Web service** is “a standardized way of integrating Web-based applications. It allows organizations to share data without needing to know the details of other organizations’ computer systems.”¹³ Based on standardized technologies such as XML, Web services enable applications built with different programming languages and on different platforms to communicate with each other. That means that developers using Web services can focus on the description of the business problems, without having to worry about the execution details.

Web services are the basic building blocks of service-oriented architecture (SOA), an emerging enterprise architecture (discussed in Chapter 6) that creates highly agile and flexible applications. Because interoperability and modularity are key design features, Web services are excellent for integrating systems across organizational boundaries. That is why they are becoming increasingly popular in ERP, CRM, and SCM systems that were originally implemented as large client-server systems with proprietary software and proprietary data integration tools. A company using Web services can start off slowly by integrating a few applications, say with its key supplier, and then easily integrate more applications “on the fly” without having to invest in expensive middleware.

¹³ Source: http://www.hwcs.com/news_events/glossary.asp (accessed May 15, 2005).

Personalization

According to PricewaterhouseCoopers' technology forecast, **personalization** is "the selective delivery of content and services (such as specific product and service offerings, advertising, coupons, and other promotions) to customers and prospective customers."¹⁴ Personalization software allows e-businesses to offer customized services to meet the past and current interests of customers based upon data about them that is captured in an electronic format. The data needed for personalization are gathered from many sources: clickstream data, registration data that the customer supplies, past purchases, demographics supplied by third-party vendors, and customer ratings. These data are then processed by a variety of techniques including rule-based systems, neural networks, and artificial intelligence to generate and update customer profiles. In turn, these profiles are used by the firm in many ways, including as a basis for selecting the Web site content that is presented to the customer as a part of marketing, sales, and customer service efforts. For example, by analyzing a customer's current navigation through a site and comparing it to customer profiles, the personalization software can recommend specific products or services to the visitor. Personalization works hand-in-hand with CRMs in catering to customers.

Messaging and Information Distribution Infrastructure

The second building block in the generic framework for electronic commerce is the messaging and information distribution infrastructure. Messaging software facilitates the movement of information through the channels of the Internet. It takes such forms as e-mail, instant messaging, voice over IP, point-to-point file transfers, and groupware.

One of the first uses of the Internet, e-mail, still constitutes a good portion of Internet traffic. Most e-mail messages consist strictly of text, but e-mail can also be used to transfer images, video clips, sound clips, and other types of computer files.

Many e-mail services (e.g., Eudora, Outlook Express) require the user to have an account with a domain or an ISP. An **Internet service provider (ISP)** is a company that sells access to the Internet. Incoming and outgoing e-mail is routed through the domain's or ISP's mail server, and all e-mail a user receives is stored on his or her own computer. However, a growing number of Web-based search engines and e-mail providers allow a user to send and receive e-mail from any computer by accessing the provider's Web site and entering a user name and password. Web-based search engines and e-mail allows a user to keep the same e-mail address long term (i.e., as long as the provider stays in business), whereas e-mail routed through an ISP usually contains the name of the ISP as part of the e-mail address, and a user must therefore change e-mail addresses each time he or she changes ISPs. Disadvantages of Web-based services include limits on the number of messages that can be stored and on the size of files that can be sent and received. Web-based e-mail is typically offered

¹⁴ PricewaterhouseCoopers, *Technology Forecast: 2002-2004, Volume 1: Navigating the Future of Software* (Menlo Park, CA, 2002), p. 385.

free; service providers display advertisements on users' pages and collect demographics and other marketing data from users upon enrollment.

Another permutation of e-mail is the mailing list server. Users subscribe to a mailing list; when any user sends a message to the server, a copy of the message is sent to everyone on the list. This service allows for restricted-access discussion groups; only subscribed members can participate in or view the discussions that are transmitted via e-mail. Popular mailing list providers include ListServ and Majordomo.

Instant messaging (IM) is an Internet protocol (IP)-based application that provides convenient communication between people using a variety of different device types, including computer-to-computer and mobile devices, such as digital cellular phones.¹⁵ It can identify which “buddies” have a “presence” and are able to receive messages at the moment. If a “buddy” is available, the sender's typed message pops up on the receiver's computer screen. Failing to respond quickly to the message typically is perceived to be rude. Although initially a communication tool used exclusively by teenagers, IM now serves as an internal communication systems in large companies, and even allows managers to verify whether their telecommuting employees are logged on to their computer at their homes. With most systems, people need to agree to be on a potential sender's buddy list, and they can set their status to “busy” or “away” if they do not want to be disturbed. Even then, IM is sometimes criticized for being distracting and reducing privacy, especially by people who are not good at doing a number of things at the same time.

Voice over Internet Protocol (VoIP), is “a method for taking analog audio signals, like the kind you hear when you talk on the phone, and turning them into digital data that can be transmitted over the Internet.”¹⁶ It is rapidly gaining in popularity because the free VoIP software that is available with proprietary systems such as Skype allows people to make free Internet phone calls without using the phone company. While there are no complaints about its costs, there are some about VoIP's reliability and inability to function in power outages.

File transfer consists simply of transferring a copy of a file from one computer to another on the Internet. The most common procedure, file transfer protocol (FTP), allows entire files—even large ones—to be transferred within an office or across the globe more quickly and securely than with e-mail.

Groupware¹⁷ is software that enables group members to work together on a project, even from remote locations, by allowing them to simultaneously access the same files. Calendars, documents, e-mail messages, databases, and meetings are popular applications. Groupware is often broken down into categories describing whether the members work together in real time or at different times. For example, products such as Lotus Notes, Lotus Domino, and Microsoft Exchange enable groups to share information asynchronously, while products such as Microsoft

¹⁵ Available at http://www.iec.org/online/tutorials/instant_msg/ IEC definition of IM (accessed September 9, 2002).

¹⁶ Adapted from <http://computer.howstuffworks.com/ip-telephony.htm> (accessed August 3, 2005).

¹⁷ Adapted from <http://whatis.techtarget.com> (accessed August 3, 2005).

NetMeeting and Webex enable groups to share information, such as an electronic presentation, synchronously.

Multimedia Content

Multimedia content comprises the third building block in the generic framework for electronic commerce. Commerce involving the transmission of movies or electronic books, for example, requires routing them according to the technical specifications of their individual components. If movies comprise video and audio components, and electronic books include text, graphics, and photographs, then each may be transmitted quite differently on the Internet.¹⁸

After such multimedia content is created, it is stored as electronic documents on servers, which in turn are linked to each other via networks. Customers access them via software and hardware clients. Because multimedia files tend to be substantially larger than text files, accessing them is best done with high-speed broadband connections.

Internet Infrastructure

The fourth and final building block in the generic framework for electronic commerce is the infrastructure of the Internet. How does the Internet actually work? Of what does it consist? To answer these questions, a manager must first understand that information transmitted via the Web is first broken into data “packets.” These packets travel independently of each other across the Web, sometimes following entirely different routes. Once the packets arrive at their destination, they are reassembled into a complete message. Rus Shuler of the Revere Group maps the journey of these packets in Figure 7.6 (note that CSU/DSU is channel service unit/data service unit).

An Internet service provider maintains a pool of modems for customers who dial in. A computer manages this pool and controls the flow of data from each modem to a backbone or dedicated line router. The computer usually collects billing and usage information as well. Packets from a customer’s computer traverse the public network and the ISP’s local equipment and are routed onto the ISP’s backbone. From there the packets may pass through several other routers and backbones, dedicated lines, and other networks until they find their destination, a single computer with a specified address.¹⁹

Public Policy

This chapter discussed the four building blocks in the generic framework. Just as important are two pillars supporting that framework: public policy and technical standards.

In the rapidly developing world of e-commerce, basic policy and legal questions are emerging. Because of the tremendous potential impact of the Internet

¹⁸ R. Kalakota and A. Whinston, *Frontiers of Electronic Commerce* (Reading, MA: Addison Wesley, 1996), pp. 5–6.

¹⁹ Available at http://rus1.home.mindspring.com/whitepapers/internet_whitepaper.html (accessed December 13, 1998). Copyright © 1998 Rus Shuler/The Revere Group.

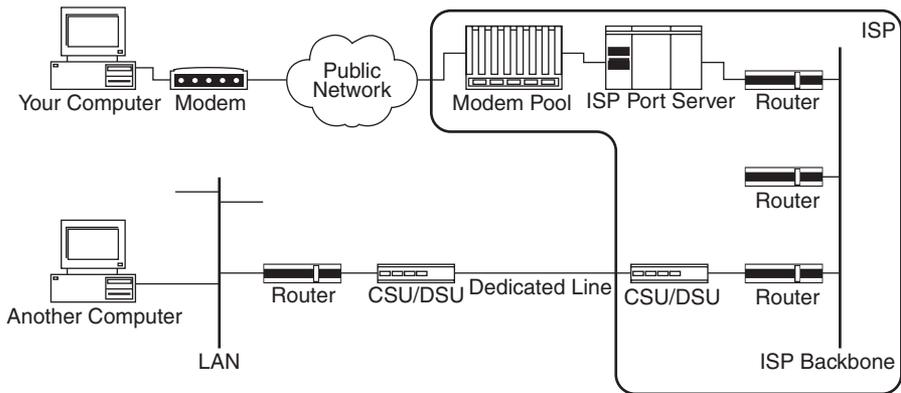


FIGURE 7.6 A sample journey of information from one Internet computer to another.

Source: Rus Shuler, Ballantyne Consulting Group. Used with permission.

on their economies, governments around the world have started to politicize the Web. The United States is contemplating policies, regulations, and laws over a broad range of issues including the cost of accessing information, taxation of online sales, regulation to protect consumers from fraud and to protect their right to privacy, and the policing of information traffic to detect terrorism, pirating, or pornography.²⁰ For example, the Justice Department's Anti-Terrorism Act of 2001 expanded the federal government's authority to conduct electronic surveillance and otherwise collect information about U.S. citizens. Many claim that this act weakens privacy protection without increasing security.

The U.S. Department of Commerce released "The Emerging Digital Economy," a detailed report about the evolution of e-commerce. Privacy issues figured prominently. The report cited three common e-commerce practices as causing privacy concerns: requesting personal information from new visitors to a site, creating customer profiles based on personal information gathered in order to deliver purchased goods, and leaving electronic "footprints" of visits to different Web sites and of purchases made, without the knowledge of the customer. The report argued that consumers should be given the opportunity to block the gathering of information or, when they freely give it, to indicate how they would like it to be used.²¹

When it comes to regulation, two approaches are possible: self-regulation and imposed regulation. For the time being, at least, the U.S. government relies on industry self-regulation to address these privacy issues. For example, the private sector is encouraged to establish rules of conduct, which would be disclosed to consumers, as well as mechanisms for tracking compliance and offering recourse to

²⁰ R. Kalakota and A. Whinston, *Frontiers of Electronic Commerce* (Reading, MA: Addison Wesley, 1996), p. 6.

²¹ Available at <http://www.ecommerce.gov/emerging.htm>, Chapter 5 (accessed November 8, 1998).

consumers in situations of noncompliance. Consumers should know the identity of any collector of personal information and the intended uses of the information. In addition, they should have the right to access information about themselves that a company holds and to correct or amend it as necessary.²² In contrast the governments of China and the United Arab Emirates are adopting a policy of imposed regulation when they use firewall systems that control the access of their citizens to certain types of Internet sites—those that contain nudity, sexual content, or religious information. China even restricts its citizens' access to parts of the popular Google search engine.²³

Because of its global reach, it is impossible for any one nation to regulate the Internet. Consider the attempts of the U.S. government to ban pornography when it only has jurisdiction over sites in the United States. Sites of companies based in Denmark are not subject to this legislation. When the U.S. government attempted to ban online gambling, companies with gambling sites merely moved to locations outside of the United States.

Technical Standards

The second pillar upon which the e-commerce framework rests is technical standards for electronic documents, multimedia, and network protocols. Such standards are essential to e-commerce because they ensure seamless integration across the data transportation network, as well as access for consumers on any device they choose—laser disc, PC, handheld devices—and on all operating systems.²⁴

All Internet-connected computers, regardless of manufacturer or operating system, must speak the TCP/IP language in order to communicate with each other. Therefore, before investing in computers and networking systems, managers should ascertain that the systems conform to these standards.

A considerable number of application protocols are also basically transparent to the Internet user, but are used in conducting business on the Internet. They include file transfer protocol (FTP), hypertext transfer protocol (HTTP), simple network management protocol (SNMP), post office protocol (POP), and multimedia Internet mail extensions (MIME). Further, institutions such as ISO, IEEE, and ANSI define standards for hardware configurations and software. Standards for emerging technologies such as Web services and RFID are still being defined.

Because the Internet is relatively new, at least from a commercial perspective, it is often hard to predict future standards. Managers who bet on the wrong standard often put their companies at a distinct competitive disadvantage. A classic case is when managers chose to use what they considered to be the better Beta standard instead of VHS, which ultimately dominated the market. In today's multimedia environment,

²² Ibid.

²³ Y. Dreazen, "Computer Whiz Tois to Save Internet's Soul," *The Wall Street Journal* (September 16, 2002), p. B1.

²⁴ R. Kalakota and A. Whinston, *Frontiers of Electronic Commerce* (Reading, MA: Addison Wesley, 1996), p. 7.

Real, Windows Media, and QuickTime are all competing for users and distributors. Microsoft and Sun are both jockeying to create a Java standard that best suits their own company. Unfortunately, picking the wrong standard can make a company uncompetitive down the road. Managers must stay informed of technical standards for their information systems as well as industry technical standards that may impact their supply chain.

► THREATS ON THE INTERNET

With the increased proliferation of the Internet comes a number of threats that must be managed. The three significant threats discussed here are: Spam, Phishing, and Identity Theft.

Spam

Spam is the name given to unsolicited e-mails sent over the Internet. These e-mails are often sent out in bulk, similar to they way bulk advertisements are sent through the physical postal system. Some even contain viruses or other programs specifically designed to harm or infiltrate the recipient's computer. The sender's computer typically uses existing e-mail name lists to create a distribution list of millions of e-mails, expecting that only a few recipients will respond to their offer. However, while bulk mail is paid for by the sender in the form of postage, paper, and printing costs, spam is relatively free to send. The cost burden falls on the recipient, whose e-mail system is clogged with hundreds of unwanted e-mails, and businesses, that have to keep their e-mail systems running despite the large volume of unwanted e-mails, have to fight against the potential invasion of viruses and other damaging bugs, and whose employees often face reduced productivity managing the e-mails they do receive. One source²⁵ estimates that spam costs businesses over \$850 per employee per year, and each employee spends 6.5 minutes per day managing spam, resulting in a loss of about 1.4 percent of each employee's productivity each year.

The problem is so large in the United States that the government passed the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" to control spam. Commonly known as the "Can Spam Act of 2003," it took effect on January 1, 2004. This law requires that those sending unsolicited e-mails clearly label the e-mail as advertising, use a truthful and relevant subject line and a legitimate return e-mail address, and provide a valid physical address and a working and speedy option to "opt-out" if the recipient so chooses. Violations of this law can result in damages of up to \$2 million or more, and jail time for the individuals responsible.

Phishing

When an e-mail arrives in an inbox from a reputable source, it is more likely to be read by the recipient. Phishing is the act of sending an e-mail that looks like it is

²⁵ Source: Darwin Magazine, www.darwinmag.com (accessed August 5, 2005).

from a reputable source, but it's not. These e-mails typically tell the recipient that some information is needed by the reputable company and provide a Web link to the site. When the recipient clicks on the Web link, they are not taken to the reputable company's site, but to a fake site that asks for personal information such as social security number, account numbers, name, and address. If the recipient enters this information, it is often used for identity theft (see section below).

The damages due to this threat are costly and dangerous. Since the e-mails are sent suggesting that a reputable company needs information, the reputation of that company can be severely damaged. Unsuspecting customers have a difficult time distinguishing between a valid and an invalid e-mail from these organizations.

Identity Theft²⁶

An important issue for managers doing business on the Internet is identity theft. Identity theft is a crime in which the thief uses personal information of the victim to impersonate the victim. On the Internet, the information often consists of private account numbers such as a credit card number, bank account number, Social Security number, or driver's license number. Typically, the thief uses the stolen numbers to obtain an additional credit card account or to steal funds from a bank account. The problem is compounded when the victim does not discover the theft until the crime is long past. Victims often learn about the crime when applying for additional credit, home mortgages, or other financial services and learn that their credit limits are overdrawn. In extreme cases, the thief has caused a criminal record to be created in the name of the victim and law enforcement personnel are forced to sort out the truth.

According to subject matter experts, identity theft is categorized in two ways: true name and account takeover. True name identity theft means that the thief uses personal information to open new accounts. The thief might open a new credit card account, establish cellular phone service, or open a new checking account in order to obtain blank checks. Account takeover identity theft means the imposter uses personal information to gain access to the person's existing accounts. Typically, the thief will change the mailing address on an account and run up a huge bill before the person whose identity has been stolen realizes there is a problem.

While identity theft can occur without the Internet, the Internet has made it easier for identity thief. Thieves can obtain information more easily by either hacking into a business, school, or other depository of personal information and stealing files of information or by sending out emails formatted to appear to be from legitimate sources but send unsuspecting victims to the thief's Web site and ask for personal information. In addition it is easier to use the information they've stolen because transactions can be made without any personal interaction when done over the Internet. The transactions are often falsely made on behalf of a well-known business such as a bank or credit card company. As with phishing above, customers have a difficult time distinguishing between valid and an invalid e-mail from these organizations.

²⁶ Some information in this section is adapted from information found at <http://searchsecurity.techtarget.com> (accessed August 4, 2005).

Identity theft is a problem for both individuals and businesses. The U.S. government keeps statistics on reported cases of identity theft.²⁷ In 2004, identity theft losses cost over \$500 million dollars. There were over 388,000 cases of identity theft reported, and over 10 percent of those cases involved theft of more than \$1 million each.

Individuals suffer from loss of credit worthiness and from problems associated with inaccurate criminal and financial records. Often it takes years to clear up these problems. To combat theft, individuals are encouraged to take precautions. A majority of the 389 chief security officers (CSOs) and senior security executives recently surveyed by *CSO Magazine* believe that taking the precautions listed in Figure 7.7 can help protect the average consumer from becoming a victim of identity theft.

Businesses are also subject to significant losses due to identity theft. Illegitimate e-mail messages that solicit personal information for the thief can ruin a business's hard won reputation. Purchases made by the thief must be paid for, and often that loss is covered by the business. The U.S. Federal Trade Commission (FTC) maintains a Web site to help both individuals and businesses manage identity theft (<http://www.consumer.gov/idtheft/>).

► FOOD FOR THOUGHT I: E-LEARNING

E-learning is using the Internet to enable learning. The Internet provides a basis for radically changing the way learning is done. Traditional learning takes place in a classroom, typically with an instructor and a room full of students. Regardless of whether the students are graduates, undergraduates, executives, or even those attending a corporate training session, the traditional model is

- Do not share passwords or PIN numbers with anyone
- Do not reply to, or click on links within, e-mail or pop-up messages that ask for personal or financial information
- Update virus protection software regularly
- Update security patches for Web browsers and operating systems regularly
- Protect your Social Security number at all costs (i.e., do not give it out unless it is mandatory)
- Shred, or otherwise destroy, all documents with personal information prior to disposal
- Monitor personal credit reports and statements from financial accounts regularly
- Install firewall software
- Before transmitting personal information online, verify that the connection is secure (i.e., check for an “s” after “http” in the URL, as well as a lock symbol in the lower right-hand corner of the screen, which indicates the transmission is encrypted)
- Do not e-mail personal or financial information

FIGURE 7.7 Precautions to take to reduce identity theft.

Excerpted from *CSO.online*, News Bureau, “Chief Security Officers Remind Citizens of the Danger of Cyberattacks and Recommend Tips,” July 21, 2005, available at <http://www2.csoonline.com/info/release.html?CID=9065>.

²⁷ Source: <http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf> (accessed August 4, 2005).

the default model for most learning situations. The Internet is beginning to change that.

Today, businesses do not want their employees to ever stop learning. In the fast-paced environment of today's business world, having current knowledge is a strategic advantage. Further, relatively little within an organization is static. That was not the case a short while ago. In the past, someone wanting to go to work received training by apprenticing with an expert whom the student modeled, studied, and imitated in order to learn a trade. When the apprenticeship ended, the worker was considered fully trained and ready to earn a living practicing the trade. But that is not the case any longer. A business that does not encourage employees to continually learn and adapt, and that does not build in the ability to learn and adapt, is setting itself up for failure.

Consider Cisco, the maker of routers and other devices used to create networks that become roadways for the Internet. John Chambers, CEO, believes e-learning is a critical success factor for Cisco. "There are two fundamental equalizers in life—the Internet and education. E-learning eliminates the barriers of time and distance creating universal, learning-on-demand opportunities for people, companies, and countries."²⁸ Cisco managers believe that e-learning helps them increase productivity as well as build loyalty. How do they and others investing in e-learning participate?

Many different types of e-learning exist. Figure 7.8 summarizes some of them, including computer-based training, distance learning, online learning, and on-demand learning. In today's environment, the terms are often used interchangeably, but several distinct concepts are embedded within the alternatives. Distance learning, for example, is when students are geographically spread out, but use technology to engage in a collective learning session such as a class. This learning experience is different from online learning, where the learner uses a computer as the primary teaching vehicle. It is somewhat different from on-demand learning, where information is broken up into small chunks, or nuggets, and pushed out to learners within the context of their work processes.

If learning can be embedded within the business processes executed by workers, then organizations can make major changes in their business strategy and their organization strategy. Embedding learning within a business process means that when the individual executing the process requires assistance, the process is smart enough to detect it and push information out to the learner to assist him or her in completing the task. It might operate somewhat like an electronic "on-the-job training" opportunity. The advantage is that if it is done right, the skills needed to complete the job change. It may mean hiring different types of individuals for the job. Further, if the information pushed out to the learner must be updated, the computer system can do it instantly. It provides a distinct advantage over traditional courses, where materials must be prepared weeks in advance in order to be ready for the classroom.

E-learning is a relatively new concept. The features of the Internet are enabling innovative organizations to rethink how they disseminate knowledge, information,

²⁸ John Chambers as quoted on the Cisco Web site (May 25, 2000), available at www.cisco.com.

Type of E-learning	Definition
Computer-based training	Any course or lesson presented on a computer, typically not connected to a network.
Distance learning	Any type of educational situation in which the instructor and students are separated by location.
Online learning	Courses presented on a computer that is hooked up to a network
Technology-based instruction	Training through media other than the classroom. That includes computers, but also refers to television, audio-tape, videotape, and print.
Web-based instruction	Courses available on the Internet which typically have embedded links to other Web-based resources.
On-demand learning	Learning broken up into knowledge chunks and delivered as demanded within a business process.

FIGURE 7.8 Types of e-learning.

Source: Adapted from S. Carliner, "An Overview of Online Learning," a White paper published by Lakewood conferences (May 25, 2000), available at <http://www.lakewoodconferences.com/wp>.

and training to their employees. And the effects this technology will have on universities and traditional schools is one of the most debated topics of e-business.

► FOOD FOR THOUGHT II: WEB LOGS (BLOGS)

Web logs (Blogs) are online journals that link together into a very large network of information sharing. Blogs started out as a hobby for individuals who like to chronicle everything in their lives and have taken on a key role in information sharing on the Internet. The topics are as varied as the number of people who write them. But what exactly is a blog and why are they so powerful?

Blogs discuss topics ranging from poetry to vacation journals to constitutional law to political opinions. In 2005, there were 9 million blogs with an estimated 40,000 new ones generated each day, according to *BusinessWeek* (May 2, 2005). Blogs can take the form of a simple diary in which the owner enters his or her thoughts whenever the mood strikes. Or they can take any one of a number of other forms, such as:

- **Moblogging**—posting to a blog on the go from a camera phone or hand-held device. Most of the content of these blogs is news, posted the very minute it happens, such as photos of the iPod Shuffle when it was launched at Apple's Computerworld.
- **Vlogging**—video blogs, in which video diaries are posted online. Applications for this trend are to sell ads or products or to keep in touch with a critical customer base, as was evident when Microsoft set up its Channel 9 vlog to help the company communicate directly with its developer community.

- Podcasting—a form of blog with an audio file attached that can be downloaded into an iPod (hence the name) or other audio system. This technology allows individuals to create their own radio shows and deliver them via files on the Internet, but corporations are using this media to propagate news about their latest products and services.

It was the presidential election of 2004 that put blogs in the spotlight. During that race, politicians began to use blogs to share their ideas on the issues in their races. Critics and opponents used blogs to voice the counter opinion. When Dan Rather reported on President Bush's National Guard duty, it was a blog that dug into the authenticity of memos the reporter used.

Why are blogs so important? They make every individual a virtual publisher, and that can cause significant changes in the business environment. First, it adds a medium in which new insights can be added to events that go way beyond what the traditional media cover. For example, when the tsunami hit Thailand, early reports were from blogs. Blogs provide news and information in the moment to potentially thousands of individuals connected with an event or situation. *Business Week* calls it "Micro-news" when a blog is devoted to a niche topic. Second, it changes the method of communication for many companies. Marketing specialists spend significant resources crafting just the right message and the right medium for communicating with clients and their other constituencies. How will companies ensure that the message remains intact when they cannot control what is written in the blogs? Third, it opens up an entirely new world for information exchange, once again plunging the world into a lawless environment. Laws governing this new world must be written. For example, is a negative blog entry an opinion of free speech or a libelous statement? In January 2005, a new Google employee began a blog about his first few days on the job. Google traditionally was a company few knew about from the inside, so this blog was of great interest. When the blog carried the employee's dissatisfaction with benefits and the work environment, he was fired, sending a clear message to the blogging community: If your opinion is something that could cause harm to you or others, then don't put it in a blog. There are consequences for your actions.

But Blogs are a new media that corporations must learn to use and possibly harness. Companies such as Plaxo, an Internet-contact management company, use blogs as a key part of their marketing and promotion strategy. General Motors uses them to connect with the press. The vice chairman has launched his own blog site and receives numerous suggestions and criticisms from customers. Further, when a conflict arose between an outside company and GM, journalists were sent to a blog run by GM for details. GM is taking a lead in experimenting with this technology to manage the media. But the biggest application for blogs is advertising. Some companies have even begun to create fake blogs, using made-up names, to jump-start the buzz around products or services. For example, in March 2005, Captain Morgan, the rum distributor, was said to have created a fake blog for its rum drinks.

► SUMMARY

- The Internet is a global marketplace. Internet-based e-commerce is becoming less mysterious and more commonplace; soon it will be second nature to consumers. Quite simply, the Internet provides a popular method for conducting business, whether it is B2B transactions or B2C transactions. Its rules, however, are still in the formative stages, so innovative and forward-thinking business people have the potential to shape them in lucrative and otherwise rewarding ways.
- Derivatives of the Internet include intranets (networks used within a business to communicate between individuals and departments) and extranets (networks that connect a business with individuals, customers, suppliers, and other stakeholders outside the organization's boundaries). Virtual private networks (VPNs) are a form of extranets that make use of public telecommunication infrastructures, maintaining privacy through the use of a tunneling protocol and security procedures.
- Web sites continue to go through a number of stages ranging from content provider to transaction forum, integrator and catalyst for industry restructuring.
- If managers are to use e-commerce for maximum effectiveness and efficiency, they must understand the elements that comprise it. Kalakota and Whinston place the key elements in a generic framework for electronic commerce, which consists of four building blocks and two pillars. (The framework is depicted in Figure 7.5.)
- The first building block is the common business services infrastructure, and it includes security and authentication (various methods a manager can use to protect electronic information), electronic payment (ways in which a business can accept payments via the Internet), search engines (services a manager can use both to locate important business information and to increase market awareness of his or her business offering), Web services (a standardized way of integrating Web-based applications), and personalization (the selective delivery of content and services).
- The second building block is the messaging and information distribution infrastructure, which includes electronic methods whereby a business can increase the efficiency of its internal and external communications.
- The third building block is multimedia content to disseminate business offerings.
- The final building block is the Internet infrastructure, which is the technology behind how information gets from point A to point B on the Internet.
- The first pillar is composed of public policy and legal and privacy issues. Managers must stay abreast of these issues because they are still being formulated and fundamentally affect how business is conducted on the Internet. The second pillar consists of technical standards and protocols. TCP/IP is a protocol critical for Internet operations. Managers must ascertain that their systems, as well as their electronic products and services, speak the Internet's language.
- Business managers can expect a future in which the Internet becomes larger, faster, more powerful, and more commonplace. Therefore, consideration of the Internet and its role in the exploding world of e-commerce should figure into all important business decisions. Managers must ask themselves these questions: Which elements of our business can be made available online? If elements of our business can be electronically automated but are not yet, how long can we afford to perform them manually? If we offer a product or service that

potentially can be delivered online, even in part, are we prepared to offer it online? If we are not yet prepared to do so, will we be prepared before our competitors are or before an online substitute becomes available? In addressing these questions, managers can gain efficiencies, improve products, and open markets.

► KEY TERMS

asymmetric encryption (p. 172)	extranet (p. 165)	secure servers (p. 173)
authentication (p. 172)	file transfer (p. 177)	symmetric encryption (p. 172)
broadband (p. 163)	firewalls (p. 173)	TCP/IP (p. 162)
cipher text (p. 172)	groupware (p. 177)	transaction processors (p. 174)
decryption (p. 172)	instant messaging (IM) (p. 177)	virtual private network (VPN) (p. 165)
digital signature (p. 172)	Internet (p. 162)	virtual terminals (p. 174)
electronic data interchange (EDI) (p. 165)	Internet checking (p. 174)	Voice over Internet Protocol (VoIP) (p. 177)
electronic funds transfer (EFT) (p. 174)	Internet service provider (ISP) (p. 176)	Web browsers (p. 164)
e-business (p. 166)	intranet (p. 164)	Web logs (p. 185)
e-channel (p. 167)	password (p. 172)	Web service (p. 175)
e-commerce (p. 161)	personalization (p. 176)	World Wide Web (WWW) (p. 164)
e-learning (p. 183)	private keys (p. 172)	
encryption (p. 172)	protocols (p. 162)	
	public keys (p. 172)	
	search engine (p. 175)	

► DISCUSSION QUESTIONS

1. What is the difference in B2B and B2C applications on the Internet? What features of the Internet are more relevant to B2B transactions? To B2C transactions? Give examples of each type of transaction. What might be the next business model?
2. What are current uses of the Internet for organizations with which you have worked? How might they use the Internet to improve their organizational strategy? Their business strategy?
3. When an organization implements a Web site, what changes in its organizational strategy should it anticipate? Why?
4. What is your prediction of the next big breakthrough for the Internet? Support your forecast with points drawn from this chapter and from your experience with the Internet.
5. How will e-learning change the business strategy of an organization? The organizational strategy? Support your claims with examples, either hypothetical or from real companies.
6. Melinda Mason is contemplating entering cyberspace. Her flower shop in Manhattan's Upper West Side has been in the family for three generations. Over the years the business carefully cultivated a large number of regular customers. Lately many of these customers asked her when Mason's Flower Shop will have a Web site. They told her they would like the ease of ordering online along with the option of ordering and paying for flowers online.

Many of her customers order elaborate arrangements on a periodic basis. One, like Mr. Schliermann, likes to buy a single red rose for his wife each Tuesday.

In addition to these customers, Melinda also realizes that a Web site for ordering and paying for flowers would be appealing to the increasingly large number of customers who winter in South Florida, but who send flowers to their friends and family in New York City. Plus she read that being a brick-and-click can open your business to customers around the globe. Naturally this prospect is appealing to her.

Melinda hired you to explore the options for online payment. In particular, she heard about Mondex from her friends and wonders whether she should make it a payment option. She is not sure how Mondex compares to such electronic payment options as PayPal. Finally, she heard about iTransact from the shopkeeper next door and wonders whether this payment option might be best for her.

Melinda would like you to evaluate these options and make a recommendation to her about the online payment option(s) that she should adopt. She wants an approach that is easy for her and her customers to use, but that is a good value in terms of cost. Her steady customers in Florida must be able to pay online, and it would be nice if the payment approach also could appeal to customers around the globe. Most of the online orders will be over \$25, though she would also like to have an option that purchasers of a single rose could use.

CASE STUDY 7-1

AMAZON.COM

No company exemplifies the new business era of the Internet more than Amazon.com. What started out as a book company emerged as a serious competitor to dozens of industries. If founder and CEO Jeff Bezos achieves his vision, “Amazon.com will be a place where you can find anything.” Given the activities, expansions, and successes to date, Amazon is making significant headway on its ambitious plans to take over the entire e-commerce e-tailing world.

Amazon.com started in 1996 selling books over the Internet. Since that time, the company pioneered many of the innovations that define electronic shopping, such as one-click shopping, customer reviews, affiliation programs, and online gift-wrapping. It was the first site for customers to actually buy anything over the Internet. It is the largest seller of online books, music, and videos. It went public in 1997, and the stock price eventually rose from \$1.50 a share into the heady triple digits.

To increase the number of customers to its site, Amazon.com established an affiliation program that awards other sites a percentage of the sale when customers are linked from their site to Amazon.com to make a recommended purchase. A customer visiting the Amazon.com site is greeted with a busy Web page showing key specials that day, and giving opportunity to navigate to the type of product the customer wants to buy. If books are the purchase to be made that day, the customer can click on the books link, and search for a book by title, author, or subject. So far, the scenario is not much to get excited about, but the power behind the Amazon.com business model is not yet shown. If a customer searches for a particular book, not only does Amazon.com’s site give the details of the book, but potential buyers can read the table of contents, look at comments written by other readers of the book, and link to other books of a related topic or by the same author. Comments give a sense of community to the Amazon.com site where customers can contribute or read com-

ments easily. Further, the Amazon.com systems track purchases of the book at hand, and can tell the new customer of other books purchased by those who purchased the current book. Their “suggestions” are based on real data culled from an extensive database of transactions, making the suggestions that much more relevant to the current customer.

The purchasing transaction is innovative, too. The standard process lets customers add a selection to their shopping cart and either continue shopping or finish out the transaction. Shipping options are presented and purchases are paid for with credit cards. If the customer is a repeat customer, the system already has payment and shipping information, and the purchase can be quickly made with a single “click” of the mouse. E-mail is sent to the purchaser at several points along the process, including a confirmation that the order was received and a notice of the shipping of the order. E-mail is also automatically generated to alert customers of specials related to purchases they made, such as a new book by a favorite author. By combining a transaction system with real time information, customer connections and dissemination systems make retailing on the Web, or e-tailing, a different experience from traditional buying at the local bookstore or mall.

Bezo’s vision is for Amazon.com to be the center of the e-commerce world. That goal means selling or at least locating books, videos, CDs, electronics, pet food, housewares, garden supplies, games, or whatever a shopper on the Internet wants to buy. The company also offers an online auction. In mid-1999, Amazon.com announced two more e-tailing options. All Product Search is a product browser that helps customers locate items at Amazon.com, its partners, or anywhere on the net. Amazon.com hosts Z-shops, an online mall, where anyone or any company can set up a store, by paying a small monthly fee and commission. In return, these stores gain potential access to the 25 million customers of Amazon.com. It now also hosts online operations and fulfillment for more established retail rivals like Toys “R” Us, Target, and Circuit City in return for a percentage of sales, per-unit payments, or periodic fixed payments. For example, in their partnership with Toy “R” Us, the toy company provides the product while Amazon.com sells and delivers it. This partnership suggests that Amazon realizes it can’t compete outside its core markets without significant help and Toys “R” Us acknowledges that it needs to build upon its core competency.

What is next for Amazon.com? Bezos is quoted as saying, “The idea is to let people find anything they might want to buy online. Amazon is a ‘Kathryn Store’ or a ‘Jeff Store.’ The notion is that you take the customers and put them at the center of their own universe.”

Discussion Questions

1. How has Amazon.com and their use of the Internet changed the retailing industry? Give some specific examples.
2. Comparisons have been made between giant bookstore retailer Barnes & Noble and Amazon.com. Barnes & Noble operates dozens of bookstores in many local communities. Yet Amazon.com’s reach goes anywhere and everywhere with the Web. What, in your opinion, should Barnes & Noble do to compete with Amazon.com?
3. In order to more quickly realize and sustain its profitability should Amazon.com have remained a solely clicks-based e-business (without warehouses) selling only books? Why or why not?
4. How can Amazon.com complete Bezos’s vision? What do they need to do to individualize their services to 25 million customers?

Source: Adapted from Katrina Brooke, “Amazon vs. Everybody,” *Fortune* (November 8, 1999), pp. 120–128; and Chip Bayers, “The Last Laugh,” *Business 2.0* (September 2002), pp. 86–93.

CASE STUDY 7-2**APPLE WORMS ITS WAY INTO THE MUSIC INDUSTRY**

Digital music is revolutionizing the music industry. It is now possible to send digital music files over the Internet in much the same way that voice is sent over the Internet in VoIP phone calls. One advantage of digital music for online digital music stores such as Apple's iTunes is that they do not need to build a large physical inventory of CDs. Rather, the music is stored on servers and distributed over the Internet upon request. The stores are open 24/7, and once a song is stored it is likely to be available for purchase forever. Further, instead of bundling 12 or so songs onto a CD and charging \$15, songs can be purchased individually at a relatively minimal price.

Apple has emerged a clear leader in the new music revolution, and it soon hopes to displace Wal-Mart as the world's largest music distributor. To reach and keep that lead Apple is already setting up barriers to entry: its digital music platform is proprietary. That means that it is incompatible with other systems, and the songs purchased from iTunes can only be played on Apple's iPods.

Apple's ostensible argument for the proprietary system is that a closed system is the only way that Apple can assure music labels and artists that their songs won't be pirated. Apple is hopeful that it can quickly reach critical mass in sales of digital music, and that it can become the de facto digital music standard before its competitors can do anything about it.

Discussion Questions

1. What is the disadvantage of an open standard for Apple? How could a proprietary standard become a problem for Apple?
2. In what ways, if any, would Figure 7.3 (Example of Channel Compression) need to be changed to reflect iTunes's business model?
3. What is critical mass, and why is it important for Apple to gain critical mass in the sales of digital music?

Source: Adapted from C. Willard, "Apple Worms Its Way into the Music Industry," *Financial Times* (October 26, 2005), p. 17.