01.ford.001-010 10/31/00 5:02 PM Page 1

CHAPTER 1

Introduction

Electronic commerce (e-commerce) is rapidly and massively changing our business and personal lives—our jobs, our purchasing experiences, our fortunes, our business strategies, and our expectations for the times ahead. It is causing upheavals in the way that businesses, large and small, must strive to become or continue to be successful. It is changing the ways in which businesses and consumers interact with their product and service suppliers. It is creating opportunities for whole new breeds of business ventures. It is causing governments to rethink aspects of their traditional regulatory roles. It has an impact on virtually all businesses, professionals, consumers, entrepreneurs, investors, and governments. It is global in scope, with the ability to leap national boundaries in ways never seen before.

The term *electronic commerce* defies precise definition. Most fundamentally, e-commerce represents the realization of digital, as opposed to paper-based, commercial transactions between businesses, between a business and its consumers, or between a government and its citizens or constituent businesses. E-commerce is the practical result, in the business and government spheres, of the exploding availability, performance-curve advancement, and real-world adoption of technologies relating to the IC chip, personal computer, Internet-age communications, and advanced application software solutions. These technological advances reinforce and are reinforced by the emergence of a new, global, geopolitical-economic community.

01.ford.001-010 10/31/00 5:02 PM Page 2

1.1 The Upside

The opportunities that e-commerce presents to the business world include

- *Productivity advances:* E-commerce adoption represents one of the few remaining avenues for the productivity advances needed to satisfy shareholder value expectations, attract new investment capital, and overcome competitive onslaughts. In today's supercompetitive world, e-commerce frequently represents an essential avenue for corporate survival and success.
- *Expanded and better-focused markets:* E-commerce can expand market reach dramatically. For example, a small local firm can now easily market its wares on a national or even global scale. At the same time, new information-gathering and storage technologies allow market segments and individual leads to be more precisely targeted and more accurately qualified than in the past.
- *Cost reduction:* Costs of performing traditional business tasks—such as external and internal communications, inventory control, accounting, customer relations management, and procurement—can be slashed.
- *Quality gains:* Reductions in transaction times and error rates, resulting from the elimination of manual steps such as telephone operator and telesales representative transaction entry, can allow inventories to be trimmed, processes to be streamlined, and both customer and employee satisfaction to increase.
- *Improved customer appeal:* E-commerce empowers the customer by putting information and control of transactions in the customer's hands. Customers get better access to comparative shopping and new computer-based customization offerings such as the ability to specify a unique configuration of an otherwise mass-market product. Self-service customer support can be offered. These factors, coupled with an increasing range of services, faster response times, and fewer transaction errors, can improve customer satisfaction and increase customer retention levels.
- *Improved employee satisfaction:* As overall job satisfaction increases through the shift away from repetitive task execution and toward the knowledge-worker model, improved employee communication processes and hands-on access to benefits systems provide new opportunities to increase retention rates of most-valued employees.

01.ford.001-010 10/31/00 5:02 PM Page 3

- *New partnerships based on better information sharing:* Improved means for the controlled sharing of information with partners open up the opportunity for new forms of strategic business relationships.
- *New business opportunities:* The Internet world has spawned a set of entirely new business opportunities, such as online commodity marketplaces, online auction houses, online brokerages, and Internet trust institutions.

1.2 The Downside

While the potential benefits of e-commerce are multifaceted and vast, there is also a possible downside. The electronic systems and infrastructures that support e-commerce are susceptible to abuse, misuse, and diverse failures. Tremendous damage can occur to all e-commerce participants. The damage may result from human error, system failure, criminal intent, or mischief.

Risks to a business engaged in e-commerce include

- *Direct financial loss resulting from fraud:* An external attacker or a fraudulent insider might, for example, order goods but charge payment to someone else's or a nonexistent account, transfer funds between accounts without authorization, or destroy or hide financial records that might reveal illegal conduct.
- *Exposure of the "crown jewels":* Proprietary information, such as intellectual property or marketing or competitive pricing information, that is crucial to a business's success might be unwittingly exposed to competitors or others.
- *Damage to relations with customers or business partners:* Relationships might be severely damaged due to disclosure of confidential information, disputed transactions that are not easily resolved because of the absence of convincing records, or excessive unavailability or unreliability of information or services.
- *Unforeseen costs:* Legal, public relations, or business resumption costs might be incurred in recovering from a security compromise, whether caused by external intrusions, employee dishonesty, inadequate controls, human error, or electronic system failures. Also, final settlement of major business transactions might be delayed pending lengthy resolution of disputes, if convincing records are not at hand.

01.ford.001-010 10/31/00 5:02 PM Page 4

- *Public relations damage:* Damage to corporate image or credibility might result from outsiders' masquerading as corporate spokespersons, manipulation of corporate Web site content, spreading of malicious rumors (such as in the investment community), or bad press resulting from newsworthy security penetrations.
- *Uptake failure due to lack of confidence:* Security concerns, whether founded or unfounded, can easily diminish the uptake of e-commerce generally, resulting in loss of business opportunity and lack of realization of the benefits identified in section 1.1.

Consumers also face risks, despite consumer protection regulation. The consumer who entrusts his or her money to electronic systems that are attacked or fail can unquestionably suffer loss. Ultimately, all of the business risks noted earlier can hurt consumers, in the form of direct costs, hidden costs passed on by businesses, or inconvenience factors.[1]

There have been many well-documented reports of attacks on, or failures of, computer networks and e-commerce services, including alteration of content on commercial or government Web sites, falsification of news bulletins, penetration of a major bank's cash management system, and systematic "sniffing" of passwords on a scale of millions.

It is not easy to assemble reliable statistics on the likelihood that such attacks will affect a given business, nor on the real costs of such attacks. An organization that suffers a security-related attack or failure must consider carefully whether or not to publicize it. The publicity may be so damaging, in terms of loss of customer confidence or competitive advantage, that it is easier, and possibly more profitable, to absorb quietly the resulting damages.

Notwithstanding the reluctance to disclose details of security compromises or related losses, it is clear to anyone following the popular press that security risks for e-commerce are real and can have a massive impact on businesses. Prudent users of e-commerce systems cannot ignore security concerns on the grounds that a successful attack is statistically unlikely to occur. Rather, all users must take protective steps, including appropriate countermeasures and recovery strategies, to avert or marginalize the damage caused by such attacks.

The perception of the role of security in e-commerce has changed in recent years. Whereas security was once widely considered as an optional, discretionary add-on feature, it is now painfully evident that security is an essential ingredient of any e-commerce solution. Therefore, security is now recognized as not just a safeguard of e-commerce but

01.ford.001-010 10/31/00 5:02 PM Page 5

more an *enabler* of it. Furthermore, artful businesses can leverage their risk management strengths into positive success factors, driving competitive advantage and creating strategic barriers to entry.

1.3 E-Commerce Compared with Paper-Based Commerce

The need for commerce to be secure is not new. Traditional commercial transaction systems have always shared the needs for predictability, confidentiality, and resistance to fraud. So why is e-commerce different?

Much has been learned about the nature of computer-based information since it became a subject of renewed concern in the mid- to late 1980s. For example, great intellectual energy has been spent in trying to define a precise legal and business equivalency between paper-based and computer-based data. Most of these efforts have failed.[2]

It is now apparent that there are fundamental, practical, and legal differences between traditional paper-based commerce and computer-based commerce. Signed paper documents have inherent security attributes that are absent in computer-based records. These attributes include the semipermanence of ink embedded in paper fibers, the uniqueness of any particular printing process (such as for letterhead), watermarks, the biometrics of signatures (where characteristics such as pressure, shape, and pen direction are unique to the signer), the availability of time stamps (such as a postmark), and the obviousness of modifications, interlineations, and deletions.

Computer-based messages and records do not inherently enjoy such security attributes, if any at all. Computer-based messages are simply strings of binary digits or *bits*—zeros and ones—that represent information, such as words and numbers, in a coded form. The difference between a zero and a one depends on where the message happens to currently reside. For example, when residing in a computer memory, the difference amounts to a fraction of a volt variation at some point within an electronic circuit. Without the application of specialized external security mechanisms, computer-based records can be modified freely and without detection. That is, certain supplemental control mechanisms, including both physical and electronic protections, must be applied to achieve a level of trustworthiness comparable to that which inherently exists on paper.

Furthermore, paper-based and computer-based documents may not perform equal or exactly analogous functions in business and law. Negotiable documents of title exemplify

01.ford.001-010 10/31/00 5:02 PM Page 6

differences between these media because of their need for originality and uniqueness. The negotiation of a paper document of title serves legally to transfer the goods or property that the document represents. The recipient of that document can have confidence that the transfer will be legally recognized, in part because proof of transfer is evidenced by a unique, original, paper document.

In contrast, computer-based records are not inherently unique. Indeed, one benefit of digital data is that one can make any number of identical copies with a simple keystroke, with each copy being indistinguishable from the original. Unfortunately, this characteristic counters the use of such records for providing robust legal proof in the same way as traditional paper-based documents. Thus, the inherent differences between paper documents and computer-based records demand different methods and procedures for achieving negotiability and other similar legal functions. Whereas a single paper document is adequate to negotiate a transfer of title, it may take a series of cryptographically secured computer-based messages, in conjunction with logical and physical controls, to accomplish the same task with a computerized title registry.

In reality, there are few straightforward, one-to-one, legal analogs for paper-based transactions in the e-commerce world. Rather, it is necessary to find relative *functional* analogs while taking into account the unique qualities of digital media.

1.4 Making E-Commerce Secure

The risks inherent in e-commerce can be mitigated by the use of appropriate security countermeasures in conjunction with the establishment of necessary business and legal frameworks. Some of the security safeguards required are comparatively obvious—for example, restricting access to systems that store sensitive information or performing background checks on personnel trusted to perform critical tasks—and we shall not spend time on them in this book. Rather, we focus on special security countermeasures and the supporting technical and legal infrastructure needed because of the unique characteristics of the e-commerce environment. Apart from the fundamental issues identified in section 1.3, environmental factors include

- *Open communications infrastructure:* E-commerce is largely conducted on open, interconnected, unregulated, and largely unpoliced or unpoliceable networks

01.ford.001-010 10/31/00 5:02 PM Page 7

(such as the Internet), as compared with the closed, point-to-point channels (such as leased circuits between major trading partners) typically used in earlier business communications systems.

- *Global reach:* Businesses now demand to trade globally, with at least a comparable degree of confidence as in the insular, controlled digital communities of the past. Because trading partners can reside halfway around the world, there is a great incentive to avoid legal disputes that might end up in a foreign court. This is particularly important when one considers that cyberspace may have no clear jurisdictional boundaries and that messages can pass through a potentially uncontrollable number of jurisdictions. E-commerce may become the most regulated activity in history, with every jurisdiction through which a message passes claiming at least some authority.[3] By utilizing good security methods, parties can provide and secure the best possible probative evidence of their transactions and avoid such a legal quagmire.
- *Real-time trading:* In comparison to the batched, EDI-style,[4] delayed transactions of the past, real-time trading has both negative and positive implications. On the negative side, real-time trading diminishes the opportunity for parties to meaningfully investigate one another and erodes other safety factors inherent in delayed transactions. On the positive side, an opportunity is introduced for real-time authentication of the transacting parties and the excuse that "the check is in the mail" can less easily be used to gain an unintended free trial period before making final payment.
- *Political influences:* Information security has become a major political issue, involving industrial/economic, national security, and law enforcement communities. The interests of the latter two communities often diverge from those of the business community. Information security issues also raise questions about fundamental constitutional rights.

Secure e-commerce means the reliable execution of business transactions over untrustworthy underlying communications and storage systems, in which transactions may be exposed to unknown parties. Furthermore, business information needs to be secured between users who may never meet each other personally. Satisfaction of these requirements depends heavily on widespread deployment of information security solutions, including authentication, confidentiality, access control, and integrity.

01.ford.001-010 10/31/00 5:02 PM Page 8

Most significantly, secure e-commerce depends upon the use of cryptographic-based technologies, such as digital signatures and encryption, especially when valuable or private information is involved or when the potential for repudiation of transactions is considered a material risk.

Cryptographic-based technologies are not new. However, until the emergence of e-commerce, their use was essentially limited to the national security arena and a limited set of banking applications. E-commerce has raised many new questions and issues regarding the deployment of cryptographic and related information security technologies on a large—ideally global—scale. In particular, scalability and non-repudiation requirements have led to the widespread application of *public-key cryptography,* which satisfies these needs well. This, in turn, has created demand for *certification authorities* and other *public-key infrastructure* (PKI) functions.

The widespread deployment of digital signatures and other cryptographic technologies also raises many issues relating to legal and business practices and controls. The roles and responsibilities of the parties involved, the legal effect of the information transferred, and the efficacy of computer-based commercial practices in general all present issues pertinent to secure e-commerce.

This book covers the breadth of these issues, within the context of the following definition of secure e-commerce: *Secure e-commerce is e-commerce that uses security procedures and techniques, including cryptography and digital signatures, commensurate with anticipated risks.*

1.5 Book Road Map

This book is structured with the following chapters:

- *Chapter 2—The Internet:* For the uninitiated, this chapter introduces various fundamental concepts and terminology relating to computer networking and, in particular, the Internet. The primary Internet applications and main roles in the Internet community are introduced. E-commerce transactions and their use of the Internet are discussed, together with some examples.
- *Chapter 3—Business and Legal Principles:* This chapter explains the general business and legal concepts that relate to this field and proposes business-legal models that may be considered to underlie e-commerce. Particular attention is

01.ford.001-010 10/31/00 5:02 PM Page 9

given to the enforceability and provability of digital commerce transactions. Efforts to address uncertainties in the current legal context of e-commerce are discussed.

- *Chapter 4—Information Security Technologies:* Primarily for the benefit of the reader without a background in information security, this chapter presents an overview of information security principles and explains the main technological concepts and terms used later in the book. Topics covered include cryptography, digital signatures, cryptographic key management, and authentication techniques.
- *Chapter 5—Internet Security:* This chapter addresses how to take advantage of the Internet's capabilities without exposing oneself to unacceptable risks. Coverage includes technology such as firewalls, virtual private networks, Internet mail security, and World Wide Web security.
- *Chapter 6—Certificates:* This chapter describes the role of public-key certificates and the entities that issue such certificates. Standard certificate formats are described, and general procedures for key and certificate management, including certificate revocation, are outlined.
- *Chapter 7—Public-Key Infrastructure:* This chapter discusses several issues associated with building public-key infrastructures (PKIs) capable of supporting very large user populations. Topics addressed include ways to structure relationships between multiple certification authorities, ways to associate different certification policies and practices with different certification paths, and certificate management protocols used in interfacing application products to a supporting PKI.
- *Chapter 8—Legislation, Regulation, and Guidelines:* This chapter discusses recent efforts to reduce legal uncertainties—including U.S. and other national laws, international conventions, guidelines, and model agreements and provisions—that affect computer-based commerce generally or digital signatures and PKI in particular.
- *Chapter 9—Non-repudiation:* This chapter discusses the concept of non-repudiation, including several of the finer points of the non-repudiation problem. It describes procedures and protocols for supporting non-repudiation characteristics. The role of trusted third-party services, including time-stamping and notary services, is also described.
- *Chapter 10—Certification Policy and Practices:* This chapter provides guidance on the development of certificate policies and certification practice statements to support secure e-commerce infrastructures. Topics addressed include responsibili-

01.ford.001-010 10/31/00 5:02 PM Page 10

ties of the parties concerned, legal safeguards, operational procedures, personnel controls, audits, and general security measures.

- *Chapter 11—Public-Key Infrastructure Assessment and Accreditation:* This chapter describes requirements and processes for ensuring that certification authorities meet requisite criteria for trustworthiness and interoperation.

Ancillary information is provided in the appendixes.

Notes

1. Traditionally, "consumers" are often defined as those who purchase goods or services for personal, family, or household purposes, and thus many consumer protection rules are intended to protect the consumer as the *buyer.* Paradoxically, e-commerce may render such rules ineffective for many related transactions. For example, eBay <http://www.ebay.com> and other e-auction sites service a disproportionate number of individual "consumers" as sellers rather than buyers. And yet, each eBay Web page states that the "seller assumes all responsibility for listing this item."
2. Nevertheless, some people continue to postulate such equivalents in the hope of one day discovering the elusive link.
3. This point was noted by Christopher Millard, a U.K. computer law expert.
4. Electronic data interchange—this term is generally associated with the pre-Internet form of business-to-business e-commerce.