E-commerce Disadvantages

Although the list of e-commerce advantages is long, the e-commerce environment is far from perfect. In fact, some of the e-commerce disadvantages cause both consumers and businesses to suffer considerable anxiety. Although cost savings are usually mentioned, there are hidden costs that can quickly turn a credit into a debit. In addition, the technology is not perfect: network unreliability is a continuing concern. And the thin – and getting thinner -- e-commerce margins mean that staying in business can become an ever-growing struggle. Perhaps the greatest concerns involve security, the loss of privacy, low and remote service levels, and complex legal issues. We will examine each of these issues next.

Hidden costs

Although buying on-line is convenient, the cost of this convenience is not always clear at the front end. For example, on-line purchases are often accompanied by high shipping and re-stocking fees, a lack of warranty coverage, and unacceptable delivery times. The online purchases must be shipped and the shipping charges may be considerable. In fact, too many e-commerce companies have developed a reputation of overcharging for shipping and handling. Some e-commerce managers argue that the extra charges are actually a way for them to recover revenue they lost due to the extra thin profit margins with which they normally operate. That argument provides scant solace to the customer. (See “From Shipping Free to Big Fee$”, Reuters, June 13, 2001, obtained from http://www.wirednews.com/). According to NPD Group Inc., excessive shipping fees constitute one of the major obstacles for online customers when deciding whether to buy online or at a traditional store. (See Pastore, Michael, “Shoppers Say E-Commerce Was Good For Them”, http://cyberatlas.internet.com/, January 8, 2001.)

Network Unreliability

With a user population of well over 100 million users in North America alone, the Internet is a very busy information highway. Although the Internet is designed to overcome the single point of failure problem, there have been several well-publicized incidents of network failures during the past few years. (See “Network Failures”). When an e-commerce website cannot service any customers because its Internet connection is down, there is more than just a momentary interruption. An e-commerce web site that cannot serve its customers loses sales, credibility, and even customers. In effect, a network failure can be compared to having a location at an exclusive mall that is in middle of nowhere and has no access roads that lead to it.
Network Failures

In an increasingly connected world, network breakdowns impact end-users and business alike, producing lost of productivity and sales.

- In June 2001, thousands of web hosts accounts were unable to browse even their own web sites due to an electricity blackout in California. The interruption, that lasted a few hours, was significant enough to affect thousands of businesses and end-users connected to two major Internet service providers. Source: Borland, John, “ISP squabble sparks Net traffic jam”, June 6, 2001, www.zdnet.com.

- Network problems can also affect free market trademarks, such as the Nasdaq. On June 29, 2001, stock trading came to a halt due to network problems. This outage caused all major electronic trading systems to stop for several hours. The impact of the breakdown was later compounded when businesses realized that their closing sales prices were incorrectly reported. Sources: “Outage hits online Nasdaq”, ZDNN, June 2, 2001, www.zdnet.com; and “Persistence Software Comments on Impact of Nasdaq System Failure”, PR Newswire, July 2, 2001, www.zdnet.com.

Network reliability problems may be generated by such factors as:

- Equipment failure in the network connection provider or ISP.
- Long response time due to increased network traffic or inadequate bandwidth.
- Accidental problems caused by nature – such as lightning, floods, earthquakes that affect communication lines – or by human error – such as a road construction worker severing a network line by accident.

The cost of staying in business

We included operational cost savings and lower barriers of entry in the list of e-commerce advantages. That is, getting into business is relatively easier in an e-commerce environment. Unfortunately, the flip side of the coin is that staying in business may be more difficult. Remember that the easy access means increased competition, thus causing businesses to operate with very thin profit margins. To be profitable, e-businesses must maintain high sales volumes – which in turn means developing and maintaining a big and loyal customer base. Attracting customers and transforming them into repeat buyers is the key to profitability. For example, since its creation in 1997, CheapTickets.com has built a customer base of over seven million registered users that have allowed the company to remain profitable (see Schwalb, Stephanie, “Staying a Steady Course”, Internet World, January 15, 2001).

To survive and remain competitive, businesses must invest heavily in often-costly technology. (One of our clients wound up investing more than $1.5 million per machine to maintain the expected high-quality custom item production and delivery requirements triggered by increased competition.) The introduction of computer technology within a business not only automates the business process but it also changes the way the company does business internally and externally. (The extent of the change is a function of the company’s willingness to adopt and integrate technology). Such synergy between technology and business operations makes the company more dependent on technology, therefore making it more vulnerable to the pace and
speed with which technology changes and varies. Therefore, companies tend to get on a technology investment treadmill in order to remain competitive. For example, Delta Airlines invested nearly one billion dollars on the development of its Delta Nervous System (DNS) technology in order to improve its operations, see (Schwartz, Jeffrey and Tillett Scott, “Delta Syncs Data, Ops”, InternetWeek, June 25, 2001, p.1 and 50). Clearly, technology is a mixed blessing for any business in the e-commerce business environment; its proper use can position companies to reap huge benefits and its improper use can lead to the company’s rapid demise. The only thing technology managers can be sure of is the presence of continuous technological change and all the costs associated with such change. Worse, because e-commerce is relatively new and changes constantly, there is no set of accepted rules to follow. Most e-commerce business models are based on a series of very complicated arrangements and most of them are untested and unproved.

**Lack of security**

One of the main roadblocks to the wide acceptance of e-commerce by businesses and consumers alike is the perceived lack of adequate security for on-line transactions. For example, consumers are growing increasingly weary about providing credit card information over the Internet. During the past few years, the press has been filled with reports about hackers breaking into e-business web sites and stealing credit card information. In many cases, the break-ins passed inadvertently for several months before either the seller or the buyer discovered the problem. (See “Thousands of Customers Credit Cards Stolen from E-Commerce Site”).

---

**Thousands of Customer Credit Cards Stolen from E-Commerce Site**

In the first quarter of 2001, Amazon.com announced that customer credit card information was stolen from one of its subsidiaries. The theft has gone unnoticed for over five months and was discovered only after a security audit was triggered due to one of its web pages being changed by a hacker. The company had to inform 98,000 customers about the break-in and the possibility that their credit cards being used illegally. The Amazon subsidiary was still looking into the source of the attack and it’s not ruling out the possibility of being an insider job.

This incident, and many others like this, highlights the need for better security and privacy standards for e-commerce merchants. Several credit card companies are currently working on a set of standards to make credit card transactions on the web more secure.


---

Securing on-line transaction data during its generation and then safeguarding it after it has been stored in the database are critical issues to be faced. For example in June of 2001, a small computer retailer exposed credit card information through its web site. The problem, caused by a coding error in a web page, allowed unauthorized access to stored order and credit card information for thousand of customers, dating as far back as one year. (See Delio, Michelle, “HQ for Exposed Credit Numbers”, June 18, 2001, [http://www.wirednews.com/](http://www.wirednews.com/)).
Lack of privacy

Ensuring the security of the data is of paramount importance to customers and to the credibility of the business. Customers also worry about the privacy implications of data gathered by organizations of all types and sizes. The incredible data collection process is a mixed blessing to customers. Even at the simplest data level, sales information is stored in databases connected to web servers, thus exposing the information to cyber criminals. Because data gathering on the web is so easy, databases routinely contain information about customer purchasing habits, demographic data, credit information, and so on.

In many cases, companies sell customer database information to marketing companies. In turn, the marketing companies engage in massive email campaigns to attract new customers. It doesn’t take long for the customer’s email box to be filled with unwanted and unsolicited email (also know as “spam”). The growing sales of personal firewalls and the large number of “hits” on websites that deal with privacy issues are testimony to the fact that customers are growing increasingly worried about their on-line privacy, and that they are seeking ways to protect themselves from cyber attackers. Bob Sullivan, from MSNBC.com (http://www.msnbc.com/news/491587.asp), has a very informative web page that informs users what they can do to protect their privacy online. (See Figure 14.4).

Fig14.4 Protecting your Privacy
Low service levels

Another common complaint about doing business on-line is the low level of customer service that on-line companies tend to provide. Although technology has automated business transactions to a large extent, there remains a real need for the human touch. Therefore, customer service has become a major differentiating factor. Because the web buying experience is much more impersonal than the traditional one, providing good customer service is critical to the survival of any e-business. Therefore, e-commerce web sites must provide

- a pleasant and problem-free pre-ordering and ordering experience. The website design is an important interface.
- readily available easily used feedback options. Major customer complaints include the lack of contact information on websites and the difficulty of contacting a customer service representative.
- quick and courteous complaint resolution
- timely — and low-cost -- shipping and prompt delivery of merchandise to customers.

Legal issues

Legal problems encountered in the e-commerce environment include

- software and copyright infringements. The amount of illegal content flowing freely on the Internet is illustrated by the so-called Napster case. Napster, a popular music web site, was sued by the Recording Industry Association because it hosted millions of illegal digital copies of copyrighted songs that were freely downloaded by millions of users worldwide. After court action, Napster was forced to change its business model and to eliminate all illegal material from its web site.
- credit card fraud and stolen identities. The lack of security we mentioned earlier has put credit card fraud on the proverbial front burner. In addition, lack of security makes it relatively easy to assume another person’s identity in order to make fraudulent transactions. Loss of confidence in the security of on-line transactions is a brake on the e-business train.
- business fraud. Online fraud also takes the form of companies that fail to deliver products and/or services to the customers who paid for them. The Federal Bureau of Investigation’s Internet Fraud Complaint Center receives numerous complaints on a daily basis. (See Glasner, Joanna, “FBI: Net Fraud Reports Rising”, www.wirednews.com, June 13, 2001). As a consumer, you could contact the National Fraud Information Center (www.fraud.org) to get current information about Internet fraud. (See Figure 14.5).
Figure 14.5 Fraud.org: An Internet Fraud Watchdog Organization

Obviously, fraud raises the issue of e-commerce credibility. That is why consumer unions are working to develop standards to measure web credibility. (See Miles, Stephanie, “Consumers Union: Let’s measure Web Credibility”, The Wall Street Journal Online, June 21, 2001).