Attestation of EDI-Internet Transaction Systems

Marilyn Greenstein (E-mail: mmg0@leghigh.edu), Lehigh University

Abstract

This study examines the evolution of EDI systems into Internet-EDI systems and their related benefits and security issues. As business transactions on the Internet flourish, the role of the accountant is expanding. The evolving and expanding role of the accounting profession in providing assurance services is discussed, and the profession's newest certification service, the WebTrust seal, is explored.

Introduction

Internet based electronic commerce systems are presenting new challenges and opportunities for accounting professionals. As transaction data is exchanged over the Internet, the role of the accounting professional is expanding to include a new attestation service, the AICPA's WebTrust seal. This article reviews the evolution of EDI and electronic commerce and introduces the new web site attestation function.

Evolution of EDI Systems

EDI systems have been in existence in some form for over three decades. Most firms currently engaging in EDI, however, entered the electronic movement during the last decade. By the year 2000, forty percent of all businesses are projected by the Chicago Clearing House Association to engage in EDI. The methods of exchange of data between firms have evolved over time and standards have emerged.

In the traditional sense, EDI is the electronic exchange of business documents between

Readers with comments or questions are encouraged to contact the author via e-mail.

trading partners using a standardized format. EDI systems initially emerged as a mechanism to reduce the amount of paperwork in purchasing and sales order processing systems to reduce lead times. The start-up and maintenance of EDI systems precluded many smaller businesses from implementing EDI systems. The introduction of low-cost Internet-based systems is allowing smaller firms to implement EDI-compatible systems at a low cost.

Traditional EDI systems use either privately developed networks or VANs to exchange business documents and a financial network such as the Automated Clearing House (ACH) to transfer funds. These mechanisms have not provided nearly as much connectivity between businesses and consumers as can be provided by the Internet. The infrastructure of the Internet allows multitudes of additional parties, particularly medium and small-sized businesses and consumers, to utilize EDI technology at a lower cost.

Web browser EDI services that allow low cost connectivity and EDI translation software for Internet usage are currently available from many vendors. For low volume users of EDI, a low-cost mechanism is imperative, and

the packages available provide a new opportunity for small and medium size businesses to play on par with larger businesses in the EDI arena.

Figure 1 illustrates the transformation necessary from a forms-based web browser page to ANSI ASC X12 formatted data. The EDI web browser software packages easily allow firms to connect with EDI trading partners. The easiest way to do this is by using a VAN that provides the translation service seamlessly to the partners involved. The EDI translation from the web forms is performed by low cost packages such as IBM's Information Exchange and Harbinger's Harbinger Express. These companies offer a repository of forms that can be used by the trading partners in a web-based format, and they also provide the translation to and from the web-based form to ANSI ASC X12 format.

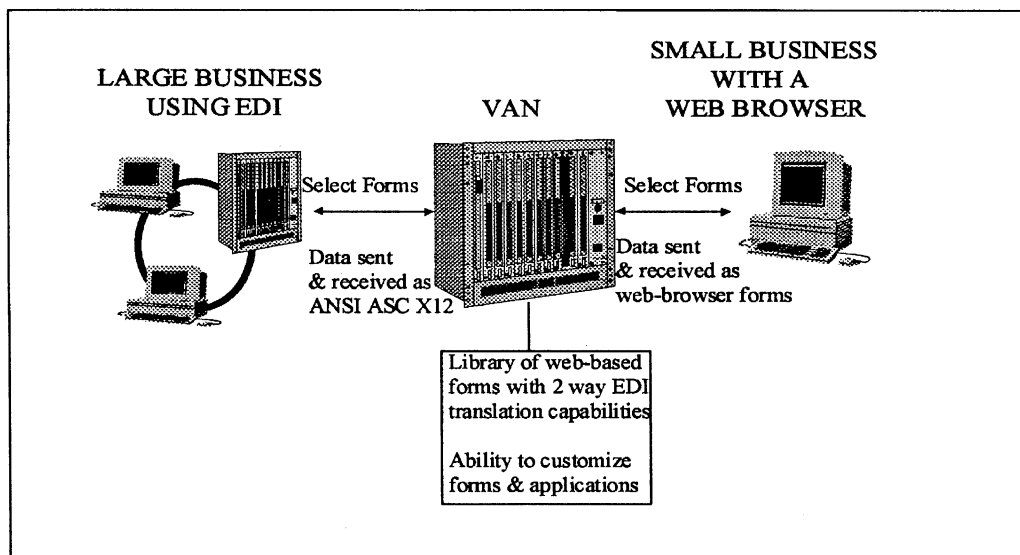**Benefits of Internet-Based EDI Systems**

EDI-Internet systems are capable of providing the following benefits: Greater connectivity, Lower entry cost, Greater sharing of information, and Greater tracking of market data. For consumers, the increased sharing of information and reduction in entry costs result in greater shopping power. Not surprisingly, consumers and business customers are beginning to demand greater access to product and pricing information. The Internet enables firms to deliver this requirement, and EDI-Internet systems allow firms to "close the sale" in addition to marketing product information. The reduction in entry costs is a direct result of the proliferation of Internet service providers during the mid-to-late 1990s and the accompanying competitive pricing strategies of these service providers.

Figure 2 illustrates various system configurations and their degree of connectivity and data sharing with other businesses and consumers. Partially integrated EDI systems have more connectivity and sharing of data with business partners than do manual systems. Fully integrated EDI systems have substantially more sharing of data and somewhat more connectivity with business partners than do partially integrated EDI systems.

Partially integrated EDI-Internet sys-

Figure 1
Web Browser Forms and EDI Interface

Figure 2
Degree of Data Sharing and Connectivity
in EDI Systems
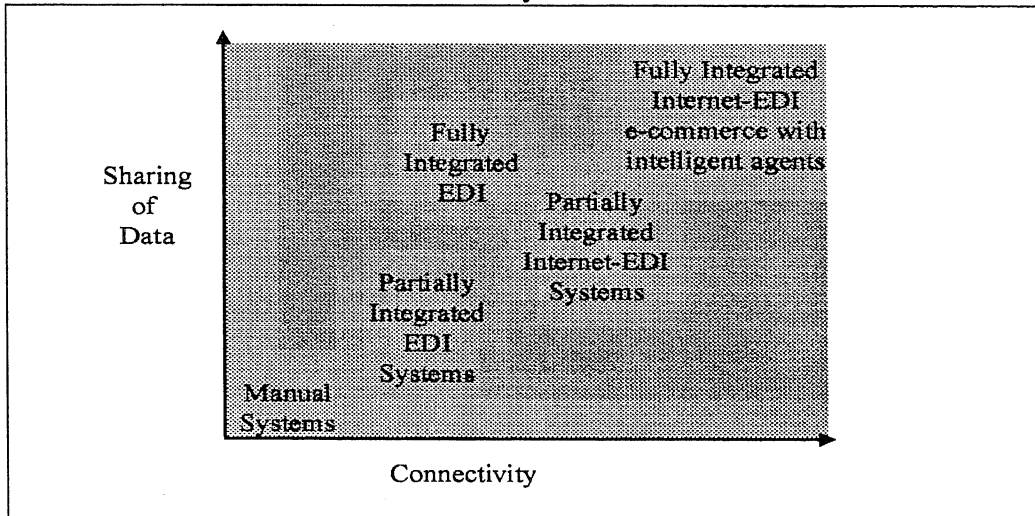
tems have more connectivity than fully integrated non Internet-based EDI systems because more suppliers and customers, and even the ultimate consumer, can be reached via the Internet connection. Partially integrated EDI-Internet systems, while they offer more connectivity, do not typically share greater amounts of information than fully integrated EDI systems. For example, a partially integrated EDI-Internet system may allow a greater number of customers to view product information and submit an order, but provide no other information to the consumer. However, while non-Internet, fully integrated EDI systems may connect to fewer customers, they may share more information, such as production schedules, with their trading partners.

Ultimately, fully integrated EDI-Internet systems provide the greatest amount of connectivity and sharing of data. Some companies are integrating or have plans to integrate their enterprise applications onto the Internet. Supply chain management and support can be greatly enhanced via Internet technology. For example, a manufacturer of high-speed fibre channel storage products, Vixel Corporation, is using an extranet-Internet model to allow it to electronically
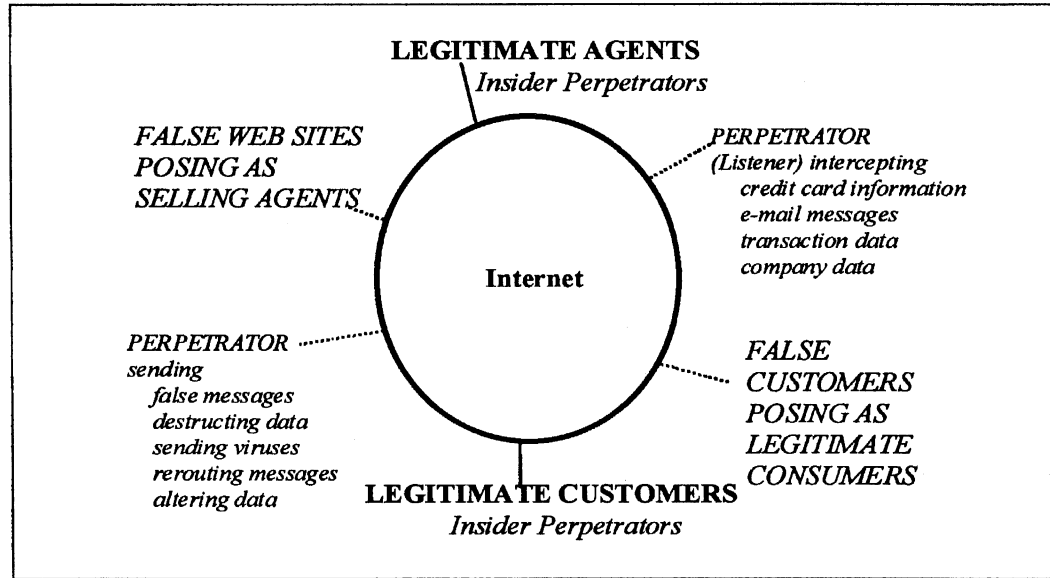
share revisions of manufacturing diagrams and engineering drawings with its subcontractors.

Internet-EDI systems that employ intelligent agents have even greater ability to locate the best product at the best price. Intelligent agents allow customers' computers to conduct price and delivery comparisons. These agents are not yet widely used for these purposes, but their potential and growth is great.

Security and Reliability Concerns of Internet-Based Electronic Commerce

The primary deterrents to rapid growth of Internet-based electronic commerce are concerns regarding security risks and reliability. One of the Internet's greatest benefits, increased connectivity, is also at the root of businesses' greatest fear. Security risk concerns encompass the safety of mission-critical data and the unauthorized interception and/or alteration of transaction data that is displayed and transmitted over the Internet. Figure 3 illustrates the major players affecting electronic commerce on the Internet.

Figure 3
Threats Faced by Buyers and Sellers
on the Internet

```
LEGITIMATE AGENTS
    Insider Perpetrators

FALSE WEB SITES                              PERPETRATOR
POSING AS                                    (Listener) intercepting
SELLING AGENTS                                 credit card information
                                               e-mail messages
                                               transaction data
                   Internet                    company data

PERPETRATOR                                  FALSE
sending                                      CUSTOMERS
  false messages                            POSING AS
  destructing data                          LEGITIMATE
  sending viruses                           CONSUMERS
  rerouting messages
  altering data     LEGITIMATE CUSTOMERS
                   Insider Perpetrators
```

In terms of electronic commerce, risk is viewed as the possibility of loss of confidential data or the destruction, generation, or use of data or programs that physically, mentally, or financially harms another party, as well as the possibility of harm to hardware. Potential and actual threats to infrastructures critical to the operations of the U.S. government, and to the Internet in general, caused President Clinton to establish the President's Commission on Critical Infrastructure Protection (PCCIP) in July 1996. The Commission is charged with "recommending a national strategy for protecting and assuring critical infrastructures from physical and cyber threats". Interestingly, the Commission views national security over these critical infrastructures as a shared responsibility between public and private sectors.

Until relatively recently, most information security breaches were made by insiders, however, a 1997 study made the Computer Security Institute and the FBI (CSI/FBI study) indicates that this is rapidly changing. The findings indicate that the number of external attacks is growing because of the increased use of the Internet. Unfortunately, the threats from insiders have not decreased, so attacks on the whole are on the rise and designers of systems need to adequately ensure that controls are in place to prevent dangers from both internal and external threats.

External hackers enter their targets in a variety of ways and for a variety of purposes. A 1996 survey of Fortune 1000 firms by WarRoom Research LLC reported that the most common breaches involved probing the system, compromising internal documents and e-mail messages, introducing a virus, and compromising trade secrets. Each of the reported activities is troublesome, although some activities pose more of a threat than others. More than half (58%) of those firms responding to the survey indicated that their computer networks were attacked and penetrated by external perpetrators in the previous year. What is even more startling is that more than a quarter of the responding firms

(27%) do not have the controls in place to allow them to detect attempts by unauthorized users to access their computer systems.

The estimated cost of each successful intrusion is over $1 million for 15% of the cases for both insider and outsider perpetrators. For more than half of the successful outside intrusions the estimated cost is over $200,000. These costs are not trivial, and they are *per incident* costs. Firms currently connected to the Internet and those firms considering connecting to the Internet need to identify and manage the risks associated with these Internet connections. Management of identified risks is an important step in protecting a firm's assets and critical data, and risk management must be considered from a cost-benefit perspective. The accounting profession is affected because a part of any audit includes the assessment of internal controls.

Reliability concerns include the loss or delay of data that is transmitted, as well as web server response time and accuracy of data residing on the web site. The increased availability of alternative choices of suppliers on the Internet makes reliability a key factor in obtaining and maintaining customers. If a customer has to wait too long for the seller's web page to load or a confirmation of an order to be returned, they may become agitated and go to another seller's web site and purchase the product. The accounting profession is addressing some of the concerns of the customer mentioned in this section by providing a new service, web site attestation.

Web Site Attestation

The AICPA initiated the WebTrust program to address the concerns of customers regarding security and privacy issues. Griffin et al. [1998] surveyed Internet users and found that 63% felt unsecure about transmitting credit card or other financial information over the Internet. The presence of the WebTrust seal is to ensure a feeling of customer confidence when transacting with a Web site. In order to provide this serv-

ice, CPA's must attend special AICPA administered training sessions and receive certification. A potential customer shopping on the Internet can verify the seal by visiting a trusted third-party service organization, currently Verisign, to verify the authenticity of the WebTrust seal.

The WebTrust seal itself indicates that a specially licensed WebTrust CPA has examined the web site's compliance within the last 90 days and issued an unqualified opinion that the site is in compliance with three categories of risk: business practices, transaction integrity, and information protection. The seal must be refreshed at least every 90 days. The individual CPA may use judgment as to how much and what type of testing must be conducted for seal refreshment.

Business Practices

The customer is informed about the business policies of the organization represented by the web site, such as delivery policies, return of merchandise, and warranties. The customer can feel assured that the web site does not change its business policies at random and that the business has an established history of maintaining such business practices.

Transaction Integrity

The customer gains assurance that he/she will be billed the appropriate agreed-upon amount and can gain confidence in using a credit-card payment mechanism. Trading partners that have credit agreements can be assured that billing disputes will be minimized.

Information Protection

Consumers can gain assurance that the business uses appropriate data encryption and firewall mechanisms to protect sensitive information, such as credit card data, both during transmission of such data over the Internet and during storage of the data by the site's Internet-connected server.

The issuance of the WebTrust seal promises to be a new service offered by professional accounting firms of all sizes. As of June, 1998, approximately 60 U.S. firms had at least one WebTrust licensed CPA on staff as reported by the AICPA's web site, yet only two sites other than the AICPA's web site, bore the seal. The first two web sites to bear the seal, other than the AICPA's web site, were issued by non-Big 5 accounting firms. Many businesses that transact on the Internet are small in nature and not the typical type of client sought by the big accounting firms. This leaves a wide-open market for small accounting firms. The Big 5 firms are aggressively pursuing this line of business and have web seals for large corporate sites that are scheduled to be issued in mid-1998.

Limitations of the WebTrust Seal

The WebTrust seal is not a costless endeavor for businesses. The client is expected to incur 35-40 hours of attestation work performed by the CPA at standard hourly rates, plus incur a seal registration fee with Verisign. Further, as illustrated in Figure 3, many threats exist to businesses transacting on the Internet. The WebTrust program only addresses the concerns faced by consumers. The concerns faced by businesses due to threats to their systems are not addressed by this program. While the WebTrust program will probably build upon the confidence consumers place in professional accounting certification, it does not solve all Internet-security issues. Other certification agencies are offering web site certification procedures to attest to the integrity of the systems. The International Computer Security Association (ICSA) offers web site certification on an annual basis that is broader in scope than the web site attestation services offered by the AICPA. Some large sites have engaged ICSA to certify their sites and bear the ICSA's certificate on their web sites.

Conclusion

Transaction processing systems have evolved over time and the services provided by accounting professionals have also evolved to meet the needs of their clients. Large accounting firms are developing new divisions to offer this new attestation service, and smaller firms are sending their employees to the necessary training seminars in order to be eligible to offer this new product to small businesses that may not have required traditional assurance services. The question remains whether the accounting profession has responded quickly or adequately enough. The first two web sites, other than the AICPA, exhibiting the AICPA's WebTrust seal appeared in April 1998. The ICSA seal has appeared over the past two years on numerous sites and is more comprehensive in nature.

Implications for Future Research

As the WebTrust seal begins to appear on more sites, research needs to be conducted to determine if customers are more confident in the site as reflected by an increase in sales. If sales do not increase, the site will most probably drop the seal, as it is an additional cost. Further, researchers can examine whether sites with alternative certifications, such as the ICSA, also engage CPA firms in order to bear the WebTrust Seal. If both certifications are seen as redundant, then research can illuminate the relative worth of each certification.📖

References

1. Computer Security Institute, *Computer Security Issues and Trends – 1997 CSI/FBI Computer Crime and Security Survey.* Spring 1997.
2. Griffin, K., P. Ladd, and R. Whitehead, "Internet Commerce: Security Is Still a Concern," *The Review of Accounting Information Systems*, Vol. 2, No. 1, pp. 67-71, 1997-1998.
3. Stein, T., "Enterprise Risk - Extending Enterprise Applications to the Internet has Benefits and Dangers, Users Say," *InformationWeek,* October 27, 1997.
4. WarRoom Research LLC, *1996 Information Systems Security Survey.* 1996.