Audit and Control Measures Essential
to Success of Electronic Commerce

**Designing new applications that offer the same
reliability found in the voice network is key in Electronic commerce**

(Tag line doesn't link to message of article)

By Fern Halper, Ph.D.
Miklos Vasarheyi, Ph.D.

Service providers are actively assessing electronic commerce solutions in order to build customer relationships to help fight churn, to reduce costs, and to move out of the "providing pipe" mode and offer value added service they can sell to differentiate themselves in competitive market. Examples include: (1) using the Internet to support customer service activities such as account maintenance, ordering and provisioning, bill rendering, and trouble reporting; (2) using the Internet to procure both network and non-network gear from their suppliers; (3) supporting hosted trading communities as a value added service. (see side bar)

Electronic Commerce Solutions Need to be Robust

E-commerce is maturing to the point where it isn't a side "project' for companies anymore – it's becoming an extension of service providers' existing systems that are in use everyday. Therefore it needs to have the reliability – and security -- SPs expect from their existing systems, interface

---

Deleted: software

Deleted: [Fern: does limiting the above just to "sw apps" not demonstrate the sw+hw needed in e-comm apps?]¶

Deleted: help them streamline their own operations [reduce costs?],

Deleted: service their customers better [build customer relationships to help fight churn?],

Deleted: as a

Deleted: to grow their business [what about

Deleted: ?]

Deleted: What about idea that service providers want to do more than just "provide pipes" to customers…want to create value-added services that run on those connections.

Deleted: Doug: Do we need more description here, or will the side bar suffice? [if you flesh out the sidebar examples that should be enough…]¶

with those systems and provide the functionality that customers are demanding (more access to information, etc.).   Since service providers will be using these systems to run their business -- and make decisions -- based on the information coming out of the overall system, they need to trust these systems as much as they trust their existing ones.   [And, since these systems will be an extension of their existing systems the solutions need to be open and modular ?].

Simply put, these solutions need to be robust – especially in customer facing applications where business and residential users have come to expect nothing less than 100% . To the service provider, robust means the following:

> *Available, reliable, and scaleable*. The system is up and running when required, including when scaled up to include more processors, applications, and users.

> *Manageable and easy to maintain*.   The system includes provisioning, administration, and monitoring capabilities. Additionally, the system can be repaired without going off-line.

> *Secure and support transactional integrity*. The system protects sensitive information from unauthorized disclosure, ensures secure transmission and maintenance of data, and ensures accuracy and completeness of information

Transaction integrity and security are key factors when it comes to servicing customers and running a business. Solutions need to handle security issues such as authorization and confidentiality. Without this, the validity of the transaction may be questioned, fraud might occur, and payments for certain transactions might be lost or diverted. [Miklos- can you insert more about security?] In terms of transaction integrity, the proper controls need to be in place to make sure that, for example, if a customer places an order for service it gets sent to the

appropriate back office service order processing and service activation systems. Or, for a procurement system, that the data in a suppliers catalog is properly maintained and updated.

More specifically, controls need to be in place to ensure:

- completeness and accuracy of input and update (e.g. data doesn't get lost or corrupted)

- timeliness of data. (e.g. orders are received in a timely fashion)

- maintenance of data in the database. (e.g. data is accurate and complete)

- accuracy of computer programs processing data.

- reasonableness of the data. (i.e. a customer didn't place 1 million orders)

- retention/recovery of transaction. (e.g. if the system goes down mid-way in processing a transaction, it isn't lost)

Off-Setting the Risk

Until the advent of electronic commerce, business that was conducted electronically, was typically conducted over a private network between parties who were acknowledged business partners. With an overall contract specifying key protocols and transaction and dispute-resolution principles, there were few unknowns. Changes in standards and economics and that fact that the Internet is ubiquitous (reach) are driving businesses to use the public data infrastructure to conduct business .   However, in the current environment, where security concerns threaten to inhibit the widespread proliferation and acceptance of electronic commerce, companies engaging in electronic commerce most likely will need to prove to their customers that they employ sound business practices and controls.

The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) have taken the lead by creating the WebTrust(TM) (http://www.aicpa.org) seal and considering other forms of systems assurance [just curious, is Lucent involved with these groups at all?- no]. By assessing commerce web sites to assure they meet AICPA- and CICA-defined criteria for transaction integrity and information protection, WebTrust hopes to break down the barriers to mainstream consumer acceptance of electronic commerce [does this also apply to b-to-b ecom acceptance?- they were addressing consumer first, need to check with Miklos]. Those companies engaged in business over the Internet that demonstrate acceptable business practices and control can obtain WebTrust's seal to alleviate their customers' concerns.

The AICPA's new system assurance products (System Assurance, System Reliability, and others) are creating a consistent framework to set the bar on how web transactions should be done and a standard methodology for analyzing and evaluating the key factors in proper business practices and controls.

WebTrust places the risk of electronic commerce into two categories: transaction integrity risks (where transactions are altered or deleted) and security/information protection (where information is not protected and unauthorized disclosure results). In the scenario where businesses are entering into business with unknown entities, WebTrust also points to a third category of risk: business process risk. In this case, there is the risk that the entity does not follow sound business practice (e.g. fill the order, warranties, returns, etc.)

By deploying robust solutions that provide for security and transaction integrity, providers are well prepared to address the types of questions a WebTrust auditor would ask. For example,

Figure 2 shows a high level view of an electronic procurement system that connects a company with one of its suppliers over the Internet.

Figure 2.
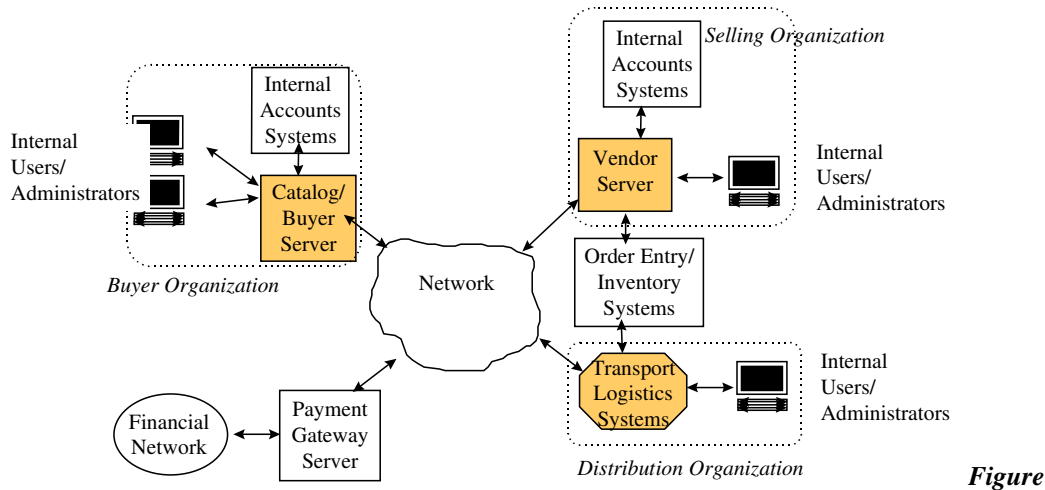
2 Caption: In this electronic procurement scenario, the catalog is hosted on the buyer side. The seller may have direct access to the catalog system in order to update information. After the selling organization receives an order from the buyer and fulfills it, payment validation may be required. This necessitates the need for payment gateways to credit card and other clearing houses. Additionally, links to transport and logistic systems are included in electronic procurements solutions to ensure delivery of product. Information about the transaction then needs to be sent to update both buyer and seller back-end systems as well as the general ledger.

An auditor might ask the following questions regarding input controls, processing controls, and output controls:

What controls are in place to ensure...[again, same concern on long lists…]

      - catalog information is current.

- catalog information and updates are complete and accurate.

- the existence and receipt of an order.

- all orders placed are accurate and complete.

- orders were fulfilled accurately and in a timely manner.

- transactions were posted to a database correctly.

- all transactions entered into the system can be accounted for.

- data was not altered in the any database (e.g., catalog).

- bills were calculated properly .

- all customers who were supposed to be billed, were billed.

- transactions can be recovered if system goes down.

Preparing for an Electronic Future

The use of the Internet in business is fast paced and aggressive -- with rapid innovation. And, nobody wants to be left behind. That's why companies from most business sectors want to do more than just make information available on-line to their potential customers; they want to make a sale. While electronic commerce is the obvious solution, there is far more to "setting up" shop on the Internet than just creating an electronic storefront.

Participants in electronic commerce will require assurance that their existing system is secure. In addition, appropriate controls must exist in supplier and customer organizations to limit access to authorized users as well as to protect an organization's confidential information. Also, transaction integrity must hold up to the audit process. Solutions that focus more on the catalog capabilities than the back-end issues may fall short of meeting these requirements.

Successful service providers have always demanded security and transaction integrity from the systems that support their sales and procurement activities. There's no reason to expect that they would settle for anything less in the new world of electronic commerce.

About the Authors:
Fern Halper, Ph.D., is the Electronic Commerce Offer Manager for Lucent Technologies Communications Software Group.

Miklos Vasarhelyi, Ph.D is the William Van Windom Professor of Accounting and Information Systems at Rutgers University. He also serves on the AICPA's systems reliability taskforce.

(need more bio?)

SIDEBAR:

Service Providers are implementing electronic commerce systems

Service providers are in various stages of implementing ecommerce systems. Two examples of applications are:

Customer self service: These solutions enable providers to service both their business and residential customers, on-line. Examples include: (1) order management – a customer can enter order information for a new service or change an existing service; (2) bill rendering or payment- a customer can obtain information on their current usage and pay their bill; (3) trouble management- a customer can enter information for a network trouble or obtain information about a previously reported trouble, online. Online self service solutions provide another channel to service customers, in addition to voice and IVR, and can provide significant cost savings as well as aid in customer retention. Ideally, these services should integrate into the service providers legacy environment for true automation. [insert picture from slide 1]

Deleted: Some

Deleted: that they are beginning to implement include the following

Deleted: :¶
¶

Deleted: enables employees to buy network and indirect supplies, etc…..¶
Better control over assets, etc. (PICTURE)

Procurement Solutions: Service providers would use this solution to streamline the purchase of both their network and non-network equipment. In the procurement scenario, the buying organization (the service provider) links to the catalogs of their sellers for network and non-network equipment. The service provider employee places an order and routes it internally through the organization to get authorized approval. Once the purchase is authorized, the order is sent to the supplier, and the item sent. Besides lowering costs associated with purchasing, this solution gives the buyer better control over their asset information. [insert picture from slide 2]

- *High availability*. System is ready for usage when required.

- *Reliable*. System includes fault tolerance software.

- *Confidential*. System protects sensitive information from unauthorized disclosure.

- *Transaction Integrity*. System ensures accuracy and completeness of information.

- *Ease of maintenance.* System has ability to undergo repairs without going off-line.

- *Scaleable*. System continues to function when scaled to serve a large number of   processors, users, applications, etc.

- *Manageable*. System includes provisioning, administration and monitoring   capabilities.