

Using the CPA as a Consultant for Developing Security and Privacy Policies and Requirements for Electronic Commerce Software Systems

Robert J. Walsh
Marist College
School of Management
Poughkeepsie, NY 12601
Email: robert.walsh@marist.edu

Organizations continue to allocate large amounts of time and money to develop electronic commerce systems. These systems require input and expertise from a number of different individuals both inside and outside these organizations.

Requirements Engineering (RE) is concerned with identifying the purpose of a software system, and the contexts in which it will be used. Central to the success of an electronic commerce system is its ability to assure its users and consumers of the accuracy, security, confidentiality, privacy and viability of all transactions.

This paper posits that certified public accountants (CPAs) are uniquely qualified to act as consultants during the construction of the security and privacy policies for Internet and Web-based electronic commerce software systems:

- 1) CPAs possess domain knowledge that qualifies them as experts in the area of internal controls. The consideration of internal controls is of critical importance in requirements engineering and software design since the data received by and transmitted from a firm through an electronic commerce Web site affects multiple stakeholders throughout the entire firm; and
- 2) CPAs are keenly aware of the privacy aspects of Web sites through the *WebTrust* program and seal, which verifies the privacy aspects of customer data collected by a given Web site.

In the remainder of this paper, the educational and experiential background of CPAs will be highlighted. Connections will be made to demonstrate how the knowledge and experience of CPAs can be instrumental via a consulting role for developing security and privacy policies and the respective requirements for the electronic commerce software systems.

Assessing/Suggesting Security Requirements and Policies

A security policy establishes who the authorized user might be and how they will access either all of the database or some portion of the database [DEA00]. Such policies protect organizational assets and ensure the accuracy and integrity of documents and records.

CPAs, through their training in assessing the internal controls of an organization, are uniquely qualified to act as a consultant in the design and maintenance of security requirements and policies. Moreover, the national sponsoring organization for CPAs, the American Institute of Certified Public Accountants or AICPA, has issued guidelines for

maintaining strong internal controls and security on Web sites, since these sites represent a potential material impact on a firm's financial statements [CPA97]. Each of these security guidelines should be built into the software used for electronic commerce:

- 1) orders are checked for accuracy;
- 2) the customer acknowledges the order before it is processed;
- 3) the selling price along with all other costs are clearly displayed to the customer;
- 4) the customer is promptly notified about backorders and order exceptions; and
- 5) the billing of orders are processed as agreed.

Creating Privacy Policies

A privacy policy describes the information practices of a given organization and how certain individuals or organizations will or will not access portions of these web sites. Organizations are increasingly adopting and implementing effective online privacy policies to protect consumer's individual or personally identifiable information.

Privacy policies need to be monitored in order to ensure its goals are continually being met. Furthermore, the organization's compliance with these goals needs to be verified and that verification must be transmitted in the form of assurance to the public through some mechanism.

CPAs are uniquely qualified to act as consultants in attaining these goals of adoption/implementation and monitoring/public assurance. First, CPAs have long been called upon to implement information systems in organizations. In addition, the term assurance and accounting have long been linked due to the accounting profession's long standing reputation of performing traditional financial statement audits.

Furthermore, in 1997 the AICPA initiated the *WebTrust* program to address customer concerns about privacy issues. The result was the creation of the *WebTrust* seal, which can be obtained by a company who allows a CPA to perform an examination of the site's business practices, disclosure, transaction control and privacy practices. The initiative by the AICPA in 1997 also required the examination to be performed to the AICPA's Standards for Attestation Engagement No. 1. In addition, the CPA must attend a special AICPA training session and be approved to issue the *WebTrust* seal.

Some examples of information protection disclosure criteria as listed by the AICPA [CPA97] include:

- 1) controls to protect private customer information obtained during Internet transmission;
- 2) controls to protect private customer information from being obtained by outside parties;
- 3) the disclosure of private customer information is not intentionally disclosed to third parties without notifying the customer prior to collecting the data or receiving customer permission;

- 4) customer permission is received before storing, retrieving or altering information stored on the customer's computer (i.e., cookies); and
- 5) prevention techniques are used against transmission of viruses to customers.

References:

[CPA97] American Institute of Certified Public Accountants. The CPA WebTrust Seal Initiative. <http://www.cpawebtrust.org>.

[DEA00] T. Dean. Network+: Guide to Networks, *Course Technology*, 2000.