Global Information Assurance Certification Paper

CPA WEB TRUST- Assurance on Security for Business to Consumer
By,
Daryn Smith

Overview:

"The AICPA rolled out an initiative in 1998 that makes cyberspace a safer place to shop. A CPA WebTrust is uniquely designed to provide consumer protection on the Internet through private sector controls" (www.mocpa.org/leg_federal.html). CPA WebTrust was developed as a response by consumer and business demand for safe and reliable web sites. The original program focused on three main areas, including Business and Information Privacy Practices, Transaction Integrity, and Information Protection. Basically, CPA WebTrust is a service that CPA firms provide to ensure that a companies web site is safe for business. The firm reviews the web site according to the procedures as outlined by the AICPA-American Institute for Certified Public Accountants and places a seal of trust after completion. The original three areas as mentioned above have been expanded over time to meet business and consumer needs. The purpose of this paper is to describe the new defined area of Security Principle's and Criteria that the AICPA is going to implement in the near future.

Before analyzing this new service and what it will accomplish, one must understand the three basic foundations on which the WebTrust Program was developed.
The first principle, "Business and Information Privacy Practices" focuses on the entities disclosures for e-commerce transactions. The firm reviews all the disclosures that the web site states and verifies that the information is correct and applied correctly. The second main area is Transaction Integrity. The CPA reviews and verifies aspects of the web site to ensure that customers transactions are properly completed and billed. Finally, the third main area of assurance that WebTrust provides is that the entity maintains information protection for all transactions involving e-commerce (www.verisign.com/webtrust/faq.html). After reviewing and testing the business web site in all these area's a WebTrust seal is placed on the web site ensuring that it is secure for consumer use (www.cpawebtrust.org/).

All of these areas have overtones that involve web security and thus the AICPA has proposed new criteria and principles for security by itself. CPA firms will hopefully implement this program for web security in the near future. The purpose of this paper is to discuss the security principles and criteria in hope to assess the overall value of the proposed service.

Security for WebTrust:

The key principle for security is as follows: "The entity discloses key security policies, complies with such security policies, and maintains effective controls to provide reasonable assurance that access to the electronic commerce system and data is restricted only to

authorized individuals in conformity with its disclosed security policy" (www.aicpa.org/webtrust/transsec.htm).

The criteria that the AICPA has established to comply with this principle is divided into four different areas: disclosures; policies, goals, and objectives; procedures and technology tools; and finally, monitoring/performance measures. Each is discussed in more detail below.

Security disclosures are very important for the consumer to feel safe when using a web site. The criteria, states that the CPA firm makes sure that the entity discloses its security practices such as; registration and authorization of new users, maintaining and terminating authorized user access, procedures in the event of a breach, steps it will take for consumer recourse if information is misappropriated, and procedures for resolving disputes. The web sites can comply with these criteria by stating on their web site such information as; please chose a strong password, the information provided is encrypted using SSL technology, transaction disputes will always be refunded in the case information is lost and so forth. Proper disclosure is reviewed and tested for truthfulness (www.aicpa.org/webtrust/transsec.htm).

The second major criterion relates to polices, goals, and objectives. In this area, the firm reviews and tests that the client has a firm security policy, that the employee's know of and follow the policy, accountability is assigned for the policy, the client secures its data and programs, the client's policies comply with law and regulations and so on. The CPA firm can look at the policy itself, review documentation of problems, interview employees to make sure they know what they are talking about and have a good understanding of the policy, inspect backup files to see if they are done according to the policy, and finally review the overall system security of the client to see if their systems can be relied on (www.aicpa.org/webtrust/transsec.htm).

The third major criterion of review for the CPA firm involves system access. System access is a very detailed and encompassing area to review for assurance. The AICPA has outlined numerous criteria checks that a CPA firm should review. For the purposes of this paper, not all requirements can be discussed, however, a good overview will be presented. The CPA firm should determine if the client has security procedures to establish new users and authenticate authorized users. The client can do this by giving new users a unique secure session in which they can provide their new user information, or for authenticated users require a user ID and password specific to that user. The client should also have procedures to safeguard important passwords of which should only be know by a select few. The client should have procedures that protect idle machines. For example, a logoff mechanism should be in place when there is inactivity. Remote access should be supervised and authenticated. The system should maintain a good security structure with limited security holes. The client should log and review port activity and eliminate unneeded port services. The client should update their software to make sure the most recent and safe software is running on all machines. The CPA firm can review the companies use of encryption and make sure that they are using 128 bit encryption technology. The CPA firm also checks and makes sure that the client protects their systems from viruses and uses the most updated technology in this respect. Finally, the CPA

firm will review the setup of physical access to firewalls and servers verifying only authorized personnel have access (www.aicpa.org/webtrust/transsec.htm).

The forth and final area of security procedures relates to monitoring. This is a very basic check but one of great importance. The CPA firm makes sure that the client has procedures for their own monitoring of their systems. This includes using software such as COPS, Tripwire, and SATAN. The client should maintain and document the server logs on a regular basis. The client should also maintain and update their security policy habitually. Finally, the client should have procedures in place in case disaster strikes. The client should be able to recover backups and act quickly when security breaches occur. The CPA firm can review all of these procedures and verify that the company does have these safeguards in place. The CPA firm can verify that meetings are held on a continuing basis in which new security issues are addressed, and can make an overall assessment that the client is committed to having strong security (www.aicpa.org/webtrust/transsec.htm).

Concluding Thoughts:

"A CPA WebTrust seal tells potential customers that a CPA has evaluated a web site's business practices and controls and that the web site meets all the CPA WebTrust criteria (www.microsoft.com/europe/industry/ecommerece/features/946.htm)." The CPA WebTrust service can be of great value when the program is fully developed. The AICPA is committed to making the CPA WebTrust seal valuable and the only way that consumers and the market will look at it as adding value is if the principles and criteria for certification are encompassing and trustworthy. With new, focused, principles and criteria additions such as the one discussed in this paper, the services provided by CPA WebTrust will be very valuable. As one can see the criteria for security alone is very well laid out and if CPA firms or similar firms can provide the necessary skills as outlined by the AICPA then WebTrust will become very valuable.

References:

1. Crowe, Elizabeth. "Watchdogs on the Web." Net Surfer. 22 September 1998. URL: http://www.microsoft.com/europe/industry/ecommerece/features/946.htm
2. "Highlights of Recent Action- Electronic Commerce." AICPA Digest of Washington Issues, Winter/Spring 1999. URL: http://www.mocpa.org/leg_federal.html
3. "Overview of the WebTrust 3.0 Program." CPA WebTrust Organization. 2000. URL: http://www.cpawebtrust.org/onlnover.htm
4. "Security Principles and Criteria." AICPA Organization. 16 October 2000. URL: http://www.aicpa.org/webtrust/transsec.htm
5. "VeriSign Secure Server Ids for the WebTrust Program- Frequently Asked Questions." 2000. URL: http://www.verisign.com/webtrust/faq.html