4-2000

Members in Small Local Public Accounting Firms, April 2000

American Institute of Certified Public Accountants (AICPA)

Members in Small·Local Accounting Firms

April 2000

AICPA

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

Highlights

AICPA Tips for Warding Off E-Commerce Hackers

technology

When hackers disrupted the activity of numerous major Web sites in Feb., the AICPA took a leadership role in offering tips to e-commerce sites to help protect them and their customers against similar threats. The tips, which were released to the press, demonstrate the profession's important role in e-commerce—particularly through its *CPA WebTrust* program—and can also help firms and their clients plan strategies to keep hackers at bay.

Here are the Institute's tips for Internet sites:

1. Conduct a risk assessment of your Internet business. This should be done before implementing specific technical controls, allowing the client and the CPA to identify possible security vulnerabilities and decide what enhancements are necessary. The greatest threat will come from the weakest links in the company's defenses, so the risks will change as security solutions evolve.

2. Develop security standards. Criminal hackers exist inside and outside an organization, and experts recommend that online businesses must protect against both threats. A security policy based on technical standards and procedures must underpin any technical solutions. The company security policy must be clearly communicated to employees so that they are aware of their responsibilities, the penalties for misuse and what to do in the event of a suspected security breach.

3. Test defenses. Check physical security systems to prevent an attack by an outsider who may have very little knowledge of the company but who is capable of using either information or a physical product to hack into the system. Test remote access to systems using specialist tools to get at resources through e-mail, the Internet and telephone systems. Also test for unauthorized attacks by employees. Conduct an entire system audit, testing security—especially firewalls—to identify breaks.

4. Develop procedures for prevention and use independent third parties to test them. Fraud prevention depends on having robust procedures, strict controls and strong audit capabilities. Independent third parties, such as CPAs, can help to test and verify a site's security and safety.

5. Limit the number of people who can access controls to an e-commerce business. Access should be granted to the minimum number of people for the minimum possible number of systems and for the minimum amount of time required to do the job. Use authentication methods such as passwords, smart cards, PIN numbers or fingerprint scans for systems access. Digital certificates should be used to verify electronic identities. Encryption can render data unintelligible to unauthorized users who do not have access to the decryption key. Also use anti-virus software and keep it up-to-date. Software should be installed on individual client machines, servers or firewalls.

6. Use firewalls. Firewalls intelligently isolate one network from another by passing messages through a control point where the system can check whether their transmission conforms to the site's security policy. Firewalls can be implemented in various ways, the most typical involving a combination of devices, including routers and servers running appropriate software.

7. Use surveillance tools. These make it possible to monitor employees to quickly identify if they are abusing legitimate access to the system. Products in this category normally act by "sniffing" the network cable and logging actions, raising alerts if certain criteria are matched. The detailed logs produced by such tools can be used as documentary evidence in legal proceedings. Among the choices are:

- *Security management tools* can help administrators to enforce security policies

continued on page C2

continued from page C1—**AICPA Tips**

consistently across the various technical environments within a site and simplify or even automate the process of managing user privileges.

- *E-mail security tools* intercept and scan e-mail automatically to determine if it presents a security risk. These tools can review content, access authorizations and sensitivity of information.

8. Monitor networks for unusual activity. If it is discovered, monitor important systems using intrusion detection software or services. This can help mitigate the attack by discovering actions that can be taken (e.g. installing security patches, expanding RAM to maintain performance during denial-of-service attacks). It can also help detect signs that this attack is more than a nuisance. For example, it can determine that a denial-of-service attack is being waged to distract attention from an actual system takeover. If other organizations are under particular attack, clients should check their systems for similar signs of attack.

9. Contact the Internet Service Provider. If the site uses an ISP, it should be contacted to determine the level of protection already in place. In addition, it is possible that the ISP can take action to block the attacks before they reach a client's computer systems.

10. Report computer violations to the proper law enforcement authorities. There may be other organizations under attack, and the authorities may be able to provide technical assistance or contacts to help response efforts. CPAs and their clients can also help law enforcement efforts by collecting system log information from target systems, which may contain important evidence to be used in enforcement actions. It is critical that this information be collected and protected before it is accidentally or deliberately erased.

AICPA/CICA WebTrust℠™ Principles and Criteria for Certification Authorities, Version 1.0

To increase consumer confidence in the Internet as a vehicle for conducting e-commerce and in the application of public key infrastructure (PKI) technology, the profession has developed and is promoting a set of principles and criteria for certification authorities (CAs), referred to as the *AICPA/CICA WebTrust Principles and Criteria for Certification Authorities*. CPA firms and practitioners who are specifically licensed by the AICPA/CICA can provide assurance services to evaluate and test whether the services provided by a particular CA meet these principles and criteria.

The document was publicly exposed through Mar. 31, 2000, and once released in final form (expected during Apr. 2000) may be downloaded from www.aicpa.org/webtrust/index.htm. The document provides a framework for licensed *CPA WebTrust* practitioners to assess the adequacy and effectiveness of the controls employed by CAs, the importance of which will continue to increase as the need for third-party authentication increases to provide assurance with respect to e-commerce business activities. As a result of the technical nature of the activities involved in securing e-commerce transactions, this document also provides a brief overview of PKI using cryptography, trusted third-party concepts and their increasing use in e-commerce.

CPA WebTrust Update

- *H.D. Vest Is Granted* CPA WebTrust *Seal*. H.D. Vest, Inc., a publicly traded company that provides extensive investment and tax services, became the recipient of the first *CPA WebTrust* Seal to be awarded to a U.S.-based online tax preparation site, www.hdvest.com. The company said it wants to increase customer confidence in its online services by providing security, privacy protection and peace of mind.
- *International News*. Germany now joins England, France, Scotland, Ireland and Wales in the European Union in offering *CPA WebTrust*, which has distinguished itself as the sole global, comprehensive seal of assurance. *CPA WebTrust* is also available in Australia, New Zealand, Canada and Puerto Rico. Negotiations are under way with other European and Asian countries to offer *CPA WebTrust*.

CPA Performance View Plus Training Developed by the AICPA and Mentor Plus

Members can tap into the most comprehensive training available on the AICPA's assurance service—CPA Performance View—with a comprehensive three-day training workshop plus a system for developing and delivering performance measures consulting services.

Here are the dates and locations of upcoming training sessions:

- May 22–24, 2000—Las Vegas.
- June 19–21, 2000—Washington, D.C.
- July 10–12, 2000—Chicago.

CPA Performance View offers a tremendous opportunity to the CPA community. It is a step-by-step process for delivering consistent business performance measurement services to clients. Providing additional value to clients through performance measures consulting not only increases a client's loyalty to their CPA, but it opens up new revenue streams for CPAs. And there is no better place to learn about CPA Performance View than with the AICPA's CPA Performance View PLUS Training Program.

This innovative program provides three days of interactive technical instruction on how to develop and deliver performance measures consulting services, including in-depth case study work to deepen your understanding of performance measures. Participants will walk away with superb training plus a systems-oriented approach and accompanying tools for delivering performance measures consulting services. It's possible to become a more valued business adviser to clients by offering this dynamic new service.

To order, contact Member Satisfaction (No. G50095CLA04):


888/777–7077


www.aicpa.org


memsat@aicpa.org

Published for AICPA members in small firms. Opinions expressed in this supplement do not necessarily reflect policy of the AICPA.
Anita Dennis, supplement editor
973/763–2608; fax 973/763–7036; e-mail: adennis20@aol.com

Ellen J. Goldstein, *CPA Letter* editor
212/596–6112; egoldstein@aicpa.org

The CPA Letter and Member Supplements Earn High Ratings from Members, Survey Shows

This supplement continues to meet readers' needs, according to ratings from *The CPA Letter*'s fifth readership survey. More than 4,000 questionnaires were mailed to randomly selected members in all membership segments last fall. Here are some of the key findings of the comprehensive research effort.

- Nine in 10 readers believed the member segment supplements were a worthwhile addition to *The CPA Letter*. (That's up from 85% in the 1997 survey).
- 89% found the supplement they receive contains useful information.
- 84% believed the articles in their supplement were relevant to members in their field.
- 83% believed the supplements addressed issues that were important to them as CPAs.

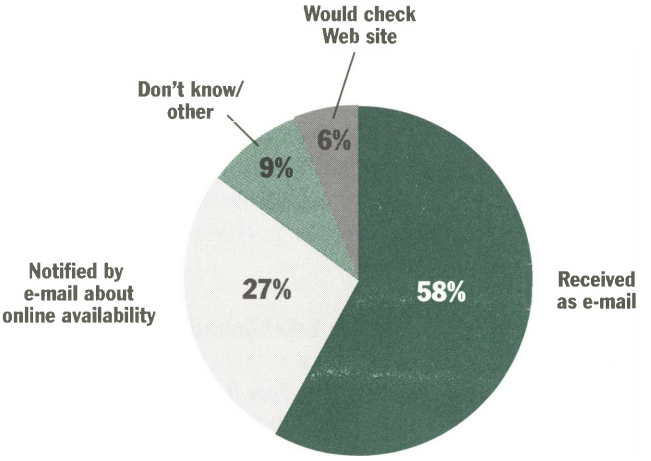
In rating individual articles, 82% thought the length of a supplement was about right, while 83% thought they contained the right amount of detail. Nearly 60% wanted to continue to receive their supplements seven times a year.

In general, members found the public practice supplements to be relevant to their firm size, timely, useful in pinpointing trends and well-focused on practice management issues. The topics of greatest interest to readers in this segment were:

- Practice management.
- Tax issues.
- Technology.
- Comparative peer data, billing records.
- Audit issues.
- OCBOA financial statements.
- Small business consulting, smaller firm issues.
- Computer security.

Information Online

How would members like to receive *The CPA Letter* if it were distributed online only? (*The CPA Letter* and its supplements are currently available online at www.aicpa.org as well as in print.)



Source: *The CPA Letter* Readership Survey

Where to Find It

If you'd like to receive a copy of the report's "Summary of Findings," contact Joe Bass in AICPA Public Relations:

jbass@aicpa.org 212/596–6116

We appreciate your input and support of this supplement and of *The CPA Letter*. If you have story ideas or suggestions for improvement, please contact the supplement editor.

adennis20@aol.com 973/763–2608

The Scoop on *The CPA Letter*

As has been the case in previous surveys, more than 8 in 10 members gave *The CPA Letter* itself an overall rating of excellent or good. Nearly one-third found it more useful to them now than it was two years ago, with another 43% saying it remains as useful as before.

Online Internet Submission of the SF-FAC

Do you have government clients? Online Internet submission of the OMB Circular A-133 Data Collection Form (SF-SAC) is now available through the Federal Audit Clearinghouse (FAC) Web site. The site provides instructions on electronic submission, which users are urged to read carefully. A hard copy of the form (which can be a printout of the online submission) still must be signed and sent in along with the required number of reporting packages. (Note that the hard-copy form submitted must include original signatures.)

One main benefit of the online submission is a built-in edit function that can help prevent errors before submission. To use the online option:

http://harvester.census.gov/sac

Questions about the submission can be addressed to:

800/253–0696

fac@census.gov

AICPA Revises Peer Review Standards for Firms that Do Not Audit SEC Registrants

The AICPA has revised its peer review performance and reporting standards for firms that do not audit SEC registrants. The new standards become effective Jan. 1, 2001.

"These standards were designed to improve the quality of financial reporting for non-SEC registrants and to protect the public that uses and relies on those reports," said Susan Coffey, AICPA Vice-President of Self-Regulation and the SEC Practice Section. "In addition, we believe that significant efficiencies will be achieved in the way the peer reviews are conducted and administered."

Three Peer Review Categories Established

The new standards establish three categories of peer review for firms that are enrolled in the AICPA Peer Review Program:

- *System.* This type of peer review is required for firms that perform engagements under the Statements on Auditing Standards (SAS) or examinations of prospective financial information under the Statements on Standards for Attestation Engagements (SSAEs). The system review is designed to review and issue an opinion on the firm's system of quality control.
- *Report.* This type of peer review is for firms that only perform compilations that omit substantially all disclosures with the objective of enabling the reviewed firm to improve the overall quality of its compilation practice. There is no review of or opinion issued on the firm's system of quality control. The report review is ordinarily performed at a location other than the reviewed firm's office.
- *Engagement.* This type of peer review is required for firms that do not have a system review or are ineligible for a report review. The objectives of the engagement review are to determine (1) whether the financial statements or information and the related accountant's report conform in all material respects with the requirements of professional standards and (2) whether the firm's working paper documentation conforms with the requirements of SSARS and the SSAEs applicable to those engagements in all material respects. Similar to a report review, there is no review of or opinion issued on the reviewed firm's system of quality control and the review is generally performed at a location other than the reviewed firm's office.

Last May, the AICPA Peer Review Board issued its exposure draft to revise the AICPA *Standards for Performing and Reporting on Peer Reviews*. The draft included nine proposals for revised standards.

More Information Available

"The board considered all of the approximately 300 comment letters received on the exposure draft," Coffey said, "and believes it addressed most of the respondents' concerns in concluding on the final revised standards." Over 40,000 firms participate in the AICPA peer review program.

A discussion point summary on the revised standards is available on the AICPA Web site:


www.aicpa.org

Advisory Council on Government Auditing Standards

David M. Walker, Comptroller General of the United States and head of the U.S. General Accounting Office, has named six new members to the Advisory Council on Government Auditing Standards who will provide advice and guidance on government auditing standards.

The Advisory Council works with GAO to keep the auditing standards current through the issuance of revisions and guidance.

The Comptroller General first issued standards for government auditing in 1972; major revisions were made in 1981, 1988, and 1994. Two amendments to the 1994 revision were issued in 1999 affecting the auditor's responsibility for conducting and reporting on financial statement audits. Certain laws, regulations and contracts require auditors to follow generally accepted government auditing standards (GAGAS) promulgated by the Comptroller General of the United States.

To meet the demands for more responsive and cost-effective governments, policymakers and managers need reliable financial and performance information. The credibility that auditors add about that information, as well as the systems producing it, is a critical component of fiscal integrity and accountability. GAGAS are a fundamental necessity to guide auditors and evaluators and allow others to rely on their work.

The six new members will replace those whose term has expired. They will join the 14 members previously appointed to serve on the council. The new members, selected from nominations received from relevant professional organizations, will serve for three-year terms to provide continuity in membership.

The six new members are:

- Ralph Campbell, Jr., State Auditor, State of North Carolina.
- Bert T. Edwards, Chief Financial Officer, U.S. Department of State.
- Dr. Jesse W. Hughes, private consultant, retired as Professor Emeritus of Accounting, College of Business and Public Administration at Old Dominion University.
- Auston G. Johnson, Utah State Auditor.
- Sam M. McCall, City Auditor, Tallahassee, Florida.
- Jacquelyn L. Williams-Bridgers, Inspector General for State Department, Arms Control and Disarmament Agency, and the U.S. Information Agency.