a common and misplaced expectation that technology would somehow automatically prevent such problems as embezzlement and identity theft.

Jun. 01, 2006

From the June/July 2006 Issue

When automated accounting and banking programs were first introduced, there was a common and misplaced expectation that technology would somehow automatically
prevent such problems as embezzlement and identity theft. As we move further into the computer age, though, it's becoming obvious that the human factors involved in working with automated systems are essential to minimizing thefts and managing risks.

The most common embezzlement scenario in the small business world involves a business owner who is so busy running the operation that the control of financial matters is entrusted to an employee with an accounting software program. The program enables one person to perform all of the cash-related functions of the business, thereby bypassing basic internal controls such as the separation of the duties of receiving and disbursing funds, writing and signing checks, and reconciling bank accounts. In such a scenario, technology actually facilitates the perpetration of fraud.

At the same time, accountants are expected by clients, the general public and (all too often) jurors, to always detect fraud and advise and warn clients about their exposures to fraud. The expectation to always detect fraud can be extremely difficult to meet, but the expectation to advise and warn is much less difficult. And by advising and warning clients of their exposures, accountants can reduce liability stemming from the expectation to detect fraud.

technology typically includes a checklist such as the following:
Essentially, anyone with enough knowledge about computer programs and bookkeeping
can conceal just about anything unless a business has controls in place to prevent embezzlement.

Electronic Information Security
As more people are victimized by identity theft, accountants need to pay more attention to the secure transmission and storage of documents containing social security numbers, bank and credit card account numbers, driver's license numbers, birth dates, and medical information. Personal identity information should be protected at all times in computer programs and in transmissions via the Internet. Tax and accounting firms should try to obtain computer software that provides adequate security features. This can be a challenge in light of the fact that some popular programs provide little in the way of security features. (Click here for
draft standards.)

Operating systems and software programs should provide "restricted user" or "restrictions to user" modes to offer basic protection of information.
Such modes keep users from having any more rights or access to a system or program than they need, also known as the "least privilege" concept. "Local administrator" modes offer little protection from users damaging the system or breaching security.

Accountants should never e-mail tax returns or other personal information documents without client consent. Nor should they do so without a layer of encryption,
a digital certificate, password protection or other means of protecting sensitive information (e.g., Adobe Acrobat can provide password protection for its *.PDF

files). When client personal identity information is transmitted via the Internet,

- Whether the third-party provider has obtained an independent security attestation
  regarding their systems.

Third-party providers can use various measures and computer protections that prevent downloading, printing, scanning or copying client information. Some use nondisclosure agreements with employees and incorporate firewall security measures to help prevent outsiders from hacking into the system.
More information on firm privacy issues can be found at www.aicpa.org/privacy.

Electronic Media & Record Retention
The use of technology by accounting firms to render client services has resulted in more than 90 percent of all business documents being created electronically. And only 30 percent of those documents are ever committed to paper, according to Kroll Ontrack, Inc. (www.krollontrack.com),
a company specializing in computer forensics and the collection and production of electronic and paper evidence.

All data and information that exist on a firm's backup storage systems and computers (which may also include personal and laptop computers from home) are subject to discovery in a lawsuit, resulting in large increases in the volume of litigation documents. With discovery typically representing 50 percent of litigation costs in an average case, firms have cause for concern.

A firm will want to address the use of electronic documents and establish guidelines for document management, which includes document storage and disposal,
file organization, naming conventions, archiving and control of software application
versions (version control). All software applications should enable users to

record when and by whom documents are created, changed or imaged. Applications

accountant's office with the client records. The two versions and environments may then become out of sync with each other.

Changes to the software or data bring up the issue of version control (i.e., matching the updated version in one environment to the outdated version in another
environment). Another issue is data validation, or ensuring that both environments produce the same records and numbers. The Sarbanes-Oxley Act and subsequent SEC rules have provided guidance in the realm of publicly held company audits (see "Top
Ten Tips for Effective Electronic Data Management"), but other areas of law and accounting are still evolving.

For example, in September 2005 the U.S. Judicial Conference approved amendments to the Federal Rules of Civil Procedures (the "playbook" for civil litigation in the U.S. federal court system). The amendments are designed to address the impact of electronically stored information on civil litigation, but the Rules are projected to take effect on Dec. 1, 2006, after the U.S. Supreme Court promulgates them and Congress approves them, according to Kroll Ontrack, Inc.

Certain states have also implemented statutes and rules relating directly to the discovery of electronic documents. Accounting firms will want to stay current on the rules in the states where they do business, either through legal counsel or other resources such as those listed
here.

E-mail messages are subject to discovery and therefore should be addressed by an e-mail usage policy that defines the circumstances under which e-mail use is authorized and not authorized. Guidelines should also be established

for deleting or retaining e-mail messages, according to the nature of the e-mail

as secure as e-mail. Nor is it recommended as a form of documentation for storage and retrieval. All significant communications should be put in writing to facilitate clear communication with clients and to preserve a clear record of advice provided and decisions made. Recorded telephone conversations tend to fall in the same category as voicemail, but state laws vary so widely on the subject that an attorney should be consulted before recording any telephone conversation.

Instant Messaging (IM) is also subject to discovery in a lawsuit but is another method of communication that is not considered secure or recommended for retaining
and storing information pertaining to firm clients. Most documents that are created electronically are accepted by courts into evidence records as long as the document can be authenticated as an unaltered original, does not amount to hearsay, and comes with evidence establishing its contents, who created it, and how it was created. Some software providers have had legal analyses prepared on the admissibility into evidence of documents that have been duplicated or stored by their systems. Accounting firms should obtain a copy of such analyses and have an attorney with expertise on rules of evidence review them in light of legal considerations.

Hard Drive & Server Cleansing

Accounting firms are also responsible for securing adequate disk cleansing processes before recycling or selling computers and servers. The Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), and other regulations
require enterprises to employ secure data sanitization procedures in order to minimize the risk of stolen personal identity information.

Some approaches to protecting personal identity information on a drive before

offer the following:

- On-site destruction of hard drives;
- Acertificate of data destruction, which should verify adherence to EPA guidelines;
- An audit or paper trail of the serial-numbered inventory and a description of the equipment, method of disposal, and date of disposal, in the event the accounting firm faces an audit, litigation, investigation or other inquiry; and
- Indemnification for improper data disclosures.

Firms choosing to outsource data sanitization and drive disposal should perform appropriate and thorough due diligence before contracting with a provider, as firms should with any third-party provider that will be handling confidential client data. Contractual agreements with third-party service providers should contain language indicating that the third-party provider will treat any client data it receives as confidential and will not allow any unauthorized disclosures or use of the information; and the provider will be financially responsible for any unauthorized disclosures or use that it commits.

The use of technology has brought with it new liability exposures as well as the need for accounting firms to establish risk management processes to address those exposures. Firms that commit the time to succeed in managing the risks will find themselves much more insurable than they would otherwise be and will more fully reap the significant benefits technology has to offer. □

Ric Rosario, CPA, CFE, is vice president of risk management services with CAMICO Mutual Insurance Company.

A Certified Fraud Examiner with experience in public accounting and private

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.