systems or workflow productivity tools, there are several security issues that users should be aware of.

Mar. 03, 2012

5 Things to Consider with Online Document Security

Last month (www.CPAPracticeAdvisor.com/10625996), I wrote about how I believe online backup of data, including client and firm data, is more reliable and safe than backing up files to another computer, device or CD, especially ones that are housed in the same office or building. It's also a lot easier and can even be automated, which removes the biggest factor for potential problems: Human error.

Whether using an online service for general data backup and recovery purposes, or

despite the occasional media story about a potential leak or hack of information, data stored on your own PC is still much more likely to be stolen or lost due to technical problems.

So, what should you think about dealing with paperless files? The answer is pretty much the same things you should be aware of when using any web-based systems. Fortunately, "awareness" doesn't mean you have to become an expert at these issues, just knowledgeable enough to ask some good questions.

Email

The most common mistake professionals can make is sending an email to a client with sensitive information (SSN, TIN, account numbers, etc.) in either the message of the email or in an attached file. Over the past 15 years, even novice technology users have come to rely on email for day-to-day business and personal communications, and it is invaluable for tasking, broad messaging, scheduling and other general tasks. **But never, ever (ever) email an official client document** to anybody, including the client or others in your firm unless you have a built-in Outlook plug-in like CPA SafeMail from cPaperless, or if your document management solution has a similar secure tie-in to your email program.

There is one exception to this, which is encrypting your client emails, but doing so manually and on a one-at-a-time basis is tedious, time consuming and prone to user error. What's the risk? Potential loss of client data, of course, but also potential fines, as many states ramp up digital protection laws. In Massachusetts, firms can be fined up to $10,000 for each breach of security.

You still need to deliver returns, reports and other documents to your clients, of course, and in the paperless world, this means using a secure portal or document management system that automatically encrypt files before they even leave your

computer, and stay that way until a client logs into their side. You can read our

Taxpayer ID and account numbers. There is rarely any reason for these numbers to be printed (paper or digitally) on a client's copy of tax returns or other documents, at least not in their entirety. Most modern practice management and tax systems have features that either mask sensitive information automatically, or have a user setting to do so (such as hiding all but the last four digits of an SSN, for example.)

Password Strategies

The most common way that the bad guys will get into your computer, server or mobile devices isn't through a virus or high-tech approach. They are much more likely to get in by guessing your password.

Unfortunately, most business professionals, and especially those in the accounting and tax space, interact with so many software programs and websites that require passwords, that trying to remember dozens or more different passwords at the recommended strength is a major challenge.

We all know we're not supposed to use the names of loved ones, birthdates and other generally accessibly information, but what else should you think about?

Good passwords should have six to eight characters, including upper and lowercase letters and numbers, while excellent passwords also include non alpha-numeric characters. And take it seriously. A recent report by information security provider Trustwave shows that far too many people are really lazy, with the most commonly used business system password being… "Password1," and other variations of the word are also common. Egads.

It just isn't possible to remember all of them if they are different, so most users have resorted to either using the same password on most technologies, or even worse, having a Post-It note or scrap of paper listing all of their passwords. The first method is at least a little better than the second, which is just so transparently dangerous.

Another option is to segregate your online accounts and programs into those that

passwords, and then only have to remember your password for that tool. Both of the systems then can automatically input your correct password into programs and online sites. CNET and PCWorld rated both programs as effective and secure.

~~SAS 70~~ SSAE 16

The AICPA's SAS 70 standard has been replaced by SSAE 16, the "Statement on Standards for Attestation Engagement, Reporting on Controls at a Service Organization." Is your firm required to use only SSAE-audited online technology vendors? No, but it can offer an easily-identifiable means of assurance that the document management or data backup service provider takes security issues seriously. Others to look for include SSL security credentials, such as VeriSign, Digicert and Thawte.

Paper and Digital Document Retention

If you're serious about being a paperless firm, then it takes more than just a scanner and a document management system to make that happen; it also requires a change in how you process your engagements. For tax returns, the best practices that have been developed focus on front-end scanning; that is, digitizing the documents right when they come in the door, then destroying the original or returning it to the client. The less paper retained in the office reduces the risk of loss, and also reduces the need for physical filing cabinets.

Just as with paper-based documents, digital files often have the same general retention requirements. Most advanced document management system, and some tax systems with built-in document management functions, include the ability to set retention policies, whereby files are automatically (or with prompting) deleted after a predetermined time frame, such as three years.

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.