



nerej

Appraisal recordkeeping, security and data storage: Surviving the paperless office

November 13, 2014 - Appraisal & Consulting

While drowning in information, digital and otherwise, I've been thinking about surviving in the paperless office of the future. Many of us, as well as other financial professionals, have worked in a paper/digital environment for some time now. With the advent of cheap and easy cloud storage, inexpensive large format monitors, and the ability to access data anytime and anywhere, making the transition to a paperless environment is a foregone conclusion.

With an office in the cloud, many of our problems regarding access, clutter, storage, and communication are all eased. But are they? Consider some of the issues as they relate to USPAP and appraisal practice.

There is a large scale issue as to how appraisal data should be stored. The Recordkeeping Rule instructs that a "workfile must be stored in a medium that is retrievable by the appraiser over the prescribed record retention period." Thus, appraisers need to ensure that their storage medium, whether it is a manila folder, some sort of removable disk, the web, the cloud, or some combination of media, meets those requirements.

Despite our protestations, appraisal offices fall into the same category as financial institutions, and our security requirements must meet those requirements.

USPAP 2014 redefines Assignment Results to underscore the appraiser's obligation to "act in good faith with regard to the legitimate interests of the client in the use of confidential information and in the communication of assignment results."

USPAP also advises, in the Confidentiality Section of the Ethics Rule, that an "appraiser must protect the confidential nature of the appraisal-client relationship." Further, laws and regulations relating to confidentiality apply in assignments.

What are the downsides to operating in this environment?

The cloud, while convenient, is far from being immune to casual or determined malicious activity. Appraisers should exercise care, just as with on-line bank and brokerage accounts, to maintain password security and to perform regular due diligence to ascertain that the cloud service used is reasonably secure.

As the financial sector implements more stringent requirements regarding protection of consumer information, so will appraisers, as third party vendors, be held to higher security standards. As the Confidentiality Rule notes, "an appraiser must be aware of and comply with all confidentiality laws and regulations applicable in an assignment." Clearly, data security falls under this requirement.

Financial institutions ultimately have responsibility for the activities of their vendors. Thus, they will be looking at their vendors' data management practices more carefully and, in the event of a vendor problem, will be asking questions about the extent and efficacy of vendor systems.

What needs to be done?

Most appraisers do not have IT departments. Most appraisers are their IT department. Appraisers, however, must make intelligent business decisions to secure data and minimize exposure in the event of data breaches.

Take seriously those financial institution documents that you sign every year. Read and understand them. Put enhanced measures into place. Make sure your cloud storage is secure, or secure enough (any system can be compromised), and make sure staff acts in a safe and consistent manner where data is concerned. Email is not really very secure. Consider adopting more secure ways of transmitting reports and other sensitive information. To the extent possible, strive to keep separation between personal and business web activity. Explore ways of adopting better solutions ways to manage passwords and access to websites. Back up your data. Find simple, practical ways to secure the office environment that you and your staff will actually follow.

Appraisers are not unique in facing the challenges of business in the cloud. All businesses are tasked with adapting to positives and negatives of technology. Solutions will evolve; issues will get worked out.

While technology evolves, take reasonable care to protect not only against threats and intrusion, but for professional and legal liability that might result from compromised data. Work to stay on top of the issue. Develop guidelines in writing, and adhere to them. Much of what you can do to protect data comes down to common sense. It's just a matter of exercising it.

William Pastuszek, MAI, SRA, MRA heads Shepherd Associates, Newton, Mass.

New England Real Estate Journal - 17 Accord Park Drive #207, Norwell MA 02061 - (781) 878-4540