

JOURNAL OF ACCOUNTANCY

TECHNOLOGY

Harnessing the power of the cloud

Experts advise caution as the profession exploits the great potential of emerging technologies.

BY JEFF DREW
APRIL 2014



Technology continues to transform the accounting profession. Cloud computing and mobile devices have untethered CPAs from their desks and desktops, allowing them to do work and access data on a virtually anytime, anywhere basis. Technology continues to break down geographic and market barriers, creating unprecedented opportunities for CPA firms and for CPAs in business and industry.

The internet also brings danger. Security breaches such as those at Target and Nieman Marcus show how cybercriminals are ready to exploit weaknesses to gain access to confidential financial information (see “Timeline: Target, Neiman Marcus Disclosures,” by Brian Acohido, *USA Today*, Feb. 6, 2014). CPAs leveraging the web for their business efforts need to be aware of the security concerns and protect themselves and their clients’ and companies’ data.

To help CPAs navigate the technological seas, the *JofA* gathered three of the top experts in accounting technology for a round-table discussion of the most crucial tech issues facing the profession. Participating in the discussion were David Cieslak, J. Carlton Collins, and Rick Richardson. An edited transcript of the conversation follows.

THE PANELISTS

- **David Cieslak**, CPA/CITP, CGMA, GSEC, principal and founder of Arxis Technology and a popular technology speaker known as Inspector Gadget.
- **J. Carlton Collins**, CPA, CEO of ASA Research and author of the *JofA*’s monthly Technology Q&A column.
- **Rick Richardson**, CPA/CITP, CGMA, founder and managing partner of Richardson Media & Technologies and a speaker on the future of technology.

Which technology trends will most affect the accounting profession and individual CPAs during the rest of 2014?

Cieslak: Cloud computing is changing the computing paradigm, and I think it has reached the tipping point in terms of folks saying, “You know what, I think I’m going to start looking to move certain services and things we do to the cloud.” I think we’re going to see a continuation of that and maybe even an acceleration around that movement.

Collins: In my opinion, the technology is all about maximizing productivity for CPAs. We want to get our job done better and faster. Moving forward, I think it will continue to be essential to provide employees with the best computers, the best handheld devices, faster internet, and proper training in these three areas. Further, I think that securing mission-critical data will continue to be a key.

And although this is not new, I believe CPAs should make it a priority to leverage the internet by updating their websites with more useful content and engaging videos. I think that most CPAs consider their website to be kind of a

fancy brochure, but that's the wrong way to look at it. A website for any company or CPA firm should be a reservoir of how-to information to help clients and customers.

Richardson: While people keep talking about the tax side of our business, I really think it's the accounting solutions that are going to get the biggest attention. Just so much is happening in that space, that I think people that haven't started making new decisions relative to where the software runs that supports the accounting side of their business are going to be looking toward the cloud.

What business opportunities are there for CPAs in the technology space?

Collins: I think that technology offers an abundance of great opportunities to expand your business. Cloud-based storage properly shared among company employees—that's basically an opportunity for a CPA firm to get into the game of mastering some type of cloud solution and helping companies implement that. A CPA firm could take the time and energy to master Amazon (Web Services, the world's top provider of cloud products and services) and then promote themselves as experts with the Amazon cloud.

I think security is another one. We know security's a problem, but who is it that is responsible for locking down the security measures and implementing all of the types of things we need to secure data? You might think that a computer technology company might make sense, but a CPA firm could make a lot of sense in this area. At least one of them that's just a dramatic, glaring problem is, according to PGP, Pretty Good Privacy, 95% of all emails are still not encrypted. That means that every day, more than 135 billion emails are basically naked and easily readable by hackers around the world. I believe a CPA firm could carve out a nice niche assisting businesses with locking down their emails using various email encryption products like PGP or DataMotion or Voltage or Proofpoint.

A third opportunity is training. Too often, I see companies that place too little emphasis on training. Their employees may go to one training per year or maybe none, and I think CPA firms could fill this void by providing technical and maybe nontechnical training to those employees in Excel and accounting systems, in email and work productivity, communication, project management topics, and things of that nature.

What are the baseline technology skills CPAs need to have today, and what will they need to have in the future?

Richardson: Today's CPA needs to be well-versed in a bunch of fields, but most importantly, mobile technology. CPAs need to be aware of its advantages and disadvantages with respect to communicating sensitive information to and from clients. CPAs today should also be comfortable discussing data ownership, transborder data flows, and be proactive advisers with their clients on how to protect both the privacy of their data and the intellectual property rights that are attached to it. I think in the future, the CPA's going to be called upon to assist clients with cloud services and potentially be in a position to interact with remote client systems.

Firms that have larger clients are going to increasingly be asked to evaluate alternative Big Data solutions being considered for implementation and in conjunction with existing client data collection systems, many of which, incidentally, go directly into financial systems we either attest to or are involved in reporting with.

Collins: If I were to tell you what I think that the baseline skills are, I would just go back to five simple answers: Word, Excel, Outlook, Windows, and your smartphone. Probably every CPA should master a few additional applications that are relevant to their specific job functions, such as tax preparation or audit software if they're an auditor, or an accounting system.

Where do we stand today with the cloud, where is the cloud at as a technology, and how should CPAs be using the cloud?

Cieslak: We describe going to the cloud as a journey. For those firms that have a substantial investment in on-premise IT today, they're going to be moving in bits and pieces. The way we're observing that happening today is around horizontal applications first—so email, backing up their systems, making a redundant copy of key data out to some kind of secure backup repository out in the cloud, so you have basically a good backup of your data in case of catastrophe. Data collaboration tools and whether it's Dropbox or Box or Google Drive or OneDrive (formerly known as SkyDrive), both internally coming up with a strategy for internal collaboration and sharing, as well as client portals, which are something that have been around for a number of years, but really continuing to get that all locked down and make all of that available in the cloud.

Collins: Last year's revelations that cloud hosting companies and the federal government are capturing, reading, and storing our cloud-based data are keeping a lot of CPAs from moving to the cloud, and rightfully so. I think because CPAs deal with critical company and client data, privacy concerns trump cloud benefits. Therefore, my advice to CPAs is, embrace the cloud's casual applications, like Triplt, but keep your mission-critical company and client data out of the cloud for now, at least until new developments pop up that ensure its privacy.

Richardson: I'm not sure I totally concur with not having accounting apps in the cloud; I think the level of security we've seen from at least the three or four major providers thus far would be enough to allow me to make a decision to go to the cloud for it. But I would say this: I think it's essential that the firm has a written set of policies that surround client data and cloud use—so if people within the firm are using consumer-based services like Dropbox or Box or OneDrive that they understand they're not to be putting any kind of firm-confidential or client-confidential information into those services. Instead, they should use only secure portals or secured facilities, such as a ShareFile kind of system.

What do you see as the future of mobile devices for the next couple of years, and how will that evolution affect CPAs?

Collins: When I ask how many people have the latest smartphones, most CPAs in my audiences seem to do a good job of grabbing that technology. Probably what they need to do a better job of is adding and learning to use the various apps that will make their lives easier. For example, I've got five screens on my Android device filled with apps, but a lot of people out there barely have one screen filled up with apps.

And so there are a lot of apps out there, cloud-based apps. Cloud-based contact management would be a good example, and maybe your calendar, as well.

As stories continue to emerge, revealing a lot of security issues related to using smartphones and smartphone apps, CPAs need to be more diligent in password-protecting their devices, backing up their devices, and maybe installing anti-virus protection on the devices.

Richardson: I have heard from a number of senior management people at—I'll call them Tier 2, Tier 3 firms—all of whom are trying to figure out where a good place would be to start finding the leadership talent in the Gen Y folks they've hired. I think getting those people involved in the firm's overall direction and use of technology, and in particular, mobile, would be just an excellent opportunity to get these people knee-deep into where the future's going, how they can help with that process, how we make more money using this technology and stay secure. If we could do that, I'll tell you, these Gen Y kids will stick around.

Another thing that might help some of the Gen Y professionals stick around is bring your own device (BYOD). How widespread is the use of BYOD, and is it working well?

Richardson: Research firm Webroot did a study late last year. Seventy-three percent of U.S.-based companies have BYOD policies in place, and they forecast that number to get close to 90% by the end of 2014. The real issue is, with the advent of better mobile device management systems that allow companies' IT departments to control these devices, they now have the ability to provide access to enterprisewide single sign-in. And that's going to allow users to present their corporate credentials across a secure bridge to get at apps that are either in the cloud or even potentially local, and do them from their own mobile device. So I think, between the growing trend of just adoption and policymaking in BYOD and this mobile device management systems software cycle, which seems to have caught on well, we're in pretty good space.

Collins: The key trade-off is the user freedom for your employees versus corporate control of the technology. My philosophy is, you really want to strive to accommodate your employees as much as possible by allowing them to work with the tools that make them most productive. Now, this approach causes more security and setting headaches for your IT professionals, but making your employees more productive seems to trump providing a bed of roses to your IT staff. That's what those IT staff get the big bucks for. Let them deal with controlling a disparate brand set of devices. Let's keep your employees happy and working as productively as possible. That would be my recommendation.

Cieslak: For some organizations, the way they've gone about solving this is they said, "Look, you're welcome to continue to work with your own personal device; that's fine, but our policy is, no corporate data, no corporate anything on your personal device. But instead, we will issue you a company-based cellphone or smartphone or company-

based tablet.” And then from there, they’re able to go ahead and lock that down, put their monitoring and security software on there, because part of the struggle with BYOD is, folks are using these as personal devices with obviously personal communication going on and, at the same time, wanting just the right amount of access to corporate information as well. So I can appreciate some organizations that said, “You know what, we’ll issue you a separate mobile device,” so it’s not uncommon.

What’s the best approach smaller firms can take in handling BYOD and other issues related to IT when they are not big enough to have a full IT department?

Richardson: Regardless of the size of the firm, looking into mobile device management systems is an important ingredient in providing at least the base level of combination of access and security to be able to find a phone if you have to, wipe it clean, to be able to segregate data on the phone, depending on its architecture. Most of these mobile device management systems today cover, at a minimum, Android and iOS, and most of them have now begun to include Windows Phone, and most of them, I think—probably half—still cover BlackBerry as an alternative, and you’ve covered 97, 98% of the market with those. So the ability to be able to have those devices used without requiring the firm buying a second device—products like Good Technology, their mobile device manager is reasonably priced, so that even a four-, five-, six-person firm could easily afford it.

What are the biggest security threats to the accounting profession and individual CPAs, and how should CPAs respond to those threats?

Cieslak: This is going to be a pretty easy question for 2014 because of Windows XP reaching end of life in April. Windows XP has been around for a very long time for many organizations. It may or may not be the operating system that you’re using on your primary machine today right now, but there probably is a machine in a back room somewhere running an older version of QuickBooks; there might be a machine that you occasionally access to run an older piece of software still running Windows XP. And what Microsoft has said is that they are no longer going to be providing security patches for the Windows XP operating environment. And so some folks have said, “Well, that’s not a big deal. It’s not my primary machine. It’s not something I’ve been routinely using for my day job,” but the reality is that as compromises are discovered in whatever operating system in the Microsoft lineup—that is Windows 7, Vista—for those who may have attempted to use that, even Windows 8—as those flaws are detected and addressed and patched by Microsoft, those patches are no longer going to be made available to Windows XP users.

As a result, those machines become the high-risk threat vector for any of those unpatched, but known, vulnerabilities that hackers can exploit. We’ve been telling folks for years now that it’s time to move on from Windows XP, at least to Windows 7 if you don’t have an appetite to move on to Windows 8. But you absolutely need to be thinking about those machines that are in the back of the shop and not just those that are maybe primarily on users’ desktops.

We’re seeing more situations when malware does breach the wall, come over the top, and penetrate an organization. We’re seeing more situations where systems are compromised, networks are compromised, and end users aren’t aware of it. Not only are they not aware of it immediately, they may not be aware of it for quite some time. And so it’s these undetected compromises that we think are going to continue to pose a very substantial threat to organizations.

Richardson: I’m a bugaboo about nonsecure communications with clients. To me, the issue of making certain you have either a secure portal or some means of encrypted mail is going to be so crucial in the future, because a CPA someplace is going to get taken to court because they just used Hotmail or Gmail or anything else, and maybe they didn’t send the entire set of tax returns, but they commented on 22 lines in a review, and that review memo is sitting in the open text space with all of the data that somebody could use to reconstruct the entire income statement for a client. So there’s this whole issue of secure communications and realizing that we, as a husbandry function, have a responsibility to keep that stuff secure. And so the more we can do to make certain everybody’s aware of that, I think the better off we’re going to be.

Collins: One thing that people don’t seem to quite understand is where all these breaches come from. If you look at the Privacy Rights Clearinghouse at a list of all the breaches that have occurred since 2006, the majority of them are either stolen laptops that go missing out of the trunks of cars, overhead bins on airplanes, out of offices and out of homes, or inside employees that are copying data and selling it. We need to look at the people inside our organizations, unfortunately, and we need to secure those laptops better, and do a good job by putting whole-disk encryption, or at least encrypting folders with the data on the laptops. And then there are a lot of other common-sense things, like not having smartphones that have passwords saved in them but no PIN protecting the smartphone.

Jeff Drew is a JofA senior editor. To comment on this article or to suggest an idea for another article, contact him at jdrew@aicpa.org or 919-402-4056.

AICPA RESOURCES

JofA articles

- "Checklist: Five Apps for CPAs," April 2014, page 18
- "Tech Talk: What CPAs Need to Know," April 2013, page 42

Publication

10 Steps to a Digital Practice in the Cloud: New Levels of CPA Firm Workflow Efficiency (#PTX1204P, paperback; and #PTX1204E, ebook)

CPE webcast

2014 North America Top Technology Initiatives Survey Webcast, June 18, 2–3:30 p.m. EDT (#WBC140211)

Conferences

- Practitioners Symposium and Tech+ Conference, June 9–11, Las Vegas
- Digital CPA Conference, Dec. 8–10, Washington

For more information or to make a purchase or register, go to cpa2biz.com or call the Institute at 888-777-7077.

Information Management and Technology Assurance (IMTA) Section and CITP credential

The Information Management and Technology Assurance (IMTA) division serves members of the IMTA Membership Section, CPAs who hold the Certified Information Technology Professional (CITP) credential, other AICPA members, and accounting professionals who want to maximize information technology to provide information management and/or technology assurance services to meet their clients' or organization's operational, compliance, and assurance needs. To learn about the IMTA division, visit aicpa.org/IMTA. Information about the CITP credential is available at aicpa.org/CITP.