ONLINE EXCLUSIVE: 5 Ways to Keep Client Data Safe (https://tinyurl.com/2p82hvfc)

CPA Practice Advisor

Today's Technology for Tomorrow's Firm

OCTOBER/ NOVEMBER 2022

VOLUME 32
NUMBER 4

IN THIS ISSUE:

- Data Security
- Cyber Insurance
- 9 Tips to Thwart Cyber Thieves
- Your Firm and Your Cloud

2022 CPA Practice Advisor ENSURING SUCCESS

The Accounting Profession's Foremost Live Streaming Event

DEC. 14 & 15 2022

EARN UP TO 14 CPE CREDITS FOR FREE!

REGISTER TODAY

www.EnsuringSuccess.com

CPA Practice Advisor
Today's Technology for Tomorrow's Firm

OCT/NOV 2022
VOLUME 32
NUMBER 4

SPECIAL FEATURE

ISSUE FOCUS: DATA SECURITY

COLUMNS

FEATURES

MARKETING YOUR FIRM

20th ANNUAL WINNERS ANNOUNCED

40RTY UNDER 40RTY ACCOUNTING PROFESSIONALS

20NTY UNDER 40RTY INFLUENCERS

WEB EXCLUSIVES

CHECK OUT THE TECHNOLOGY LAB PODCASTS
www.cpapracticeadvisor.com/resource/podcast/

ACCOUNTING TOP 100 SOCIAL MEDIA LEADERBOARD
https://tinyurl.com/ycksm88x

ACCOUNTING STARTING SALARIES GET A BOOST
https://tinyurl.com/433kkwce

DEFERRED PAYROLL TAXES ARE COMING DUE SOON
https://tinyurl.com/5by9wjtt

ARCHIVED WEBCASTS www.CPAPracticeAdvisor.com/webinars

- Tax Prep and Customer Service in a Contactless World
- How Automation Helps You Build a More Scalable, Resilient Firm
- The Suite Life: Empowering Staff with Automated Processes
- Move Beyond the Borders of Your Current CAS Tech Stack

What's for Dinner?

IF YOU SHARE a home with someone, or even if you live alone, you likely hear, or ask, this question frequently. Unless you have planned and shopped for your meals in advance (as accountants, that concept is not foreign to us), you might find yourself turning to your go-to list of family favorites when it comes to dinner plans.

GAIL PERRY, CPA
Editor-in-Chief
gail.perry@cpapracticeadvisor.com
@gperrycpa

For me, it's spaghetti (my mom's recipe), tacos (a throwback to my college days), chili (that's when it's my husband's turn to cook), chicken stew, vegetable soup, and a few others. A big advantage is that I can usually count on finding all the necessary ingredients in the freezer and pantry, so there's no last-minute running to the grocery. (Of course, there's always, "Let's order pizza!" as a fallback.)

What does this have to do with accounting? I believe there are certainly days when we feel like we want to try something new, we're ready to get out of the regular grind. But often we jump into our workday and pull out the same familiar recipes. We look at our master schedule, take care of what is pressing and what is on the agenda for the day, make sure we're meeting deadlines, respond to client requests, make ourselves available to colleagues when necessary, attend required meetings, do whatever we need to do to get to the end of the day, set a similar schedule for tomorrow, and on and on.

Instead, it might be time to think like the meal planners who work out their week in advance, decide to try some new recipes, shop for the necessary ingredients, and add variety to the daily menus.

We can start with a bigger picture – what do you want to accomplish (or cook!) that you haven't tried in the past? Is it improving your skills? Adding a new service line? Reaching out to new potential clients? Updating your work-from-home policies? Cutting back in order to have more free time? Adding staff? Starting a client newsletter?

All of these seem like major tasks and thus often they get set aside and we stick to what we've been doing on a regular basis. In order to make a change in your business, consider breaking that change into small, manageable steps. I was moderating a webinar recently about adding CAS (Client Accounting Services) to an accounting firm, and the response from attendees was that the concept of adding a service line was overwhelming. Webinar participants cited problems like, our traditional partners don't want to change, we don't have the right staff, we can't find the right clients, we don't have the right technology in place. Confronting that list of problems was causing people to back away from adding the services even when they believe it would be good for the firm to do so.

Advance planning (the menu), knowing what's needed to add the service (the ingredients), and then setting up a step-by-step plan (the recipe), and assigning someone who will be in charge (the cook) is the way to get any large task accomplished. You may notice that this equates to the concept of a formal business plan, and that in itself might seem overwhelming, but you can create a plan much more easily when you think of what you want to accomplish in terms of the small tasks that make up the whole.

Adding small tasks to your daily project list is much easier than trying to deal with the overwhelming idea of making a major change. Try thinking about what changes you would like to make to your business or your regular routine, and use the concepts presented here to move forward. ■

CPA Practice Advisor
Today's Technology for Tomorrow's Firm

Published by Endeavor Business Media, LLC
1233 Janesville Ave. | Fort Atkinson, WI 53538 | 920-563-6388 | 800-547-7377
VOLUME 32, NUMBER 3

Publisher: Barry Strobel
Editor-in-Chief: Gail Perry, CPA
Managing Editor: Isaac M. O'Bannon
Senior Staff Writer: Jason Bramwell
Contributors: Ken Berry, J.D.
Jim Boomer, CPA.CITP
Kristy Short
Randy Johnston
Roman H. Kepczyk, CPA.CITP
Paul McDonald
Amy Vetter, CPA.CITP, CGMA
Becky Livingston
Garrett Wagner, CPA.CITP
Richard D. Alaniz, J.D.
Mary Girsch-Bock
Art Director: Rhonda Cousin
Site Manager: Lester Craft
Production Manager: Patricia Brown
Ad Services Manager: Carmen Seeber
Marketing Manager: Angie Gates
Audience Development Manager: Delicia Poole

ENDEAVOR BUSINESS MEDIA, LLC
CEO: Chris Ferrell
CRO/CMO: June Griffin
CFO: William Nurthen
COO: Patrick Rains
Chief Administrative and Legal Officer: Tracy Kane
EVP/Group Publisher: Lester Craft

ENDEAVOR BUSINESS MEDIA

Subscription Customer Service
Right Networks
888-417-4448
Attn: CPAPA Circulation
14 Hampshire Drive
Hudson, NH 03051

Article reprints:
reprints@endeavorb2b.com

List Rentals: Barry Strobel
203-395-0509
bstrobel@cpapracticeadvisor.com

PRINTED WITH SOY INK

Practice Advisor (USPS 017-576), (ISSN 2160-8725 print; ISSN 2160-8733 online) is published bi-monthly (April, June, August, October and December) by Endeavor Business Media LLC as *CPA Practice Advisor*. Periodicals postage paid at Fort Atkinson, WI 53538 and additional mailing offices. POSTMASTER: Send address changes to *Practice Advisor*, PO Box 3257, Northbrook, IL 60065-3257. Canada Post PM40612608. Return undeliverable Canadian addresses to: *Practice Advisor*, PO Box 25542, London, ON N6C 6B2.

Subscriptions: Individual subscriptions are available without charge in the U.S. to qualified subscribers. Publisher reserves the right to reject non-qualified subscriptions. Subscription prices: The basic annual rate is $3, based on qualifying associations of 10,000 or more public accountants that may also subscribe for all their public accountant members (certain restrictive covenants apply) for a basic subscription rate of $9 per member for a three-year subscription. One year subscription for all others: USA - $37; CAN $64+Tax GST; INT'L $91 GST. All subscriptions payable in U.S. funds, drawn on U.S. bank. Canadian GST#842773848. Back issue $10 prepaid, if available. Printed in the USA.

First Republic Bank

"First Republic provides exceptional service. They are the right fit for us and are able to meet the complex needs of clients."

West Rhode & Roberts, Certified Public Accountants

Christopher M. Roberts, CPA, Partner; Cheryl M. Rhode, CPA, Partner

firstrepublic.com | (888) 408-0288

YOUR FIRM AND YOUR CLOUD

RANDY JOHNSTON
EVP & Partner
K2 Enterprises &
CEO of Network Management Group, Inc.
randy.johnston@cpapracticeadvisor.com
@RPJohnston

CLOUD, CLOUD, CLOUD. That term seems to be a buzzword in the profession. But what does it mean to be "Your Cloud?" What works for you and your firm? In this column, I will talk about how cloud and mobile technology evolved, and the strategic benefit cloud methodology can bring to you, your firm, and your clients.

While you will see the theme and special report of this issue is data and cybersecurity, you should refer to my last column (https://tinyurl.com/bde7mmhm) to learn about security risks and to get your cybersecurity right. Here, I will focus on web-based cloud and mobile technologies that can help you build a cloud-first strategy. What am I learning "from the trenches" in my daily work with CPA firms, accounting VARs, and software publishers, and how can you leverage my experience?

WHAT WEB-BASED CLOUD AND MOBILE TECHNOLOGIES CAN YOU USE?

Cloud technology means many different things. In the early evolution of the cloud, I tended to be more of a purist. Centralizing data and running applications in a browser met my defini-

tion best as I assisted in designing accounting software tools such as Accounting Power, Acumatica, NetSuite, QuickBooks Online, Sage Intacct, Xero, Zoho, and more. This cloud computing style became known as Software-as-a-Service or SaaS.

However, limitations of internet speed, centralized computing power, and browser features made many of these early SaaS products seem pretty clunky. But the elegance of centralized updates to the software that could occur rapidly, leveraging the data to do more intelligent things, such as classification and coding, and having an automatic backup was beneficial. Clearly, this baby was evolving into a juvenile and had the promise of being an attractive and helpful adult.

Now, 25 years later, SaaS accounting software is maturing and becoming more valuable and convenient. Is it perfect yet? No. But how many people in their 20s are entirely mature and capable? Not many. Marc Benioff, cofounder of Salesforce, had the mission statement of "The End of Software," referring to the distribution of software on CD-ROM. Salesforce claims to be the first company to offer SaaS, renting software over the internet rather than installing programs on machines. SaaS is pure web-based software and should be part of your strategy.

Likewise, mobile technology means many different things. In the early evolution of the mobile, I tended to be more of an anywhere, anytime, any device (AAA) thinker. While I had run remote computing on mainframes in the 1970s and remote access over wide area networks (WANs) for banks in the 1980s, this AAA approach became effective when I started using Citrix Multiuser on OS/2 in 1991 before the company's evolution into Windows with my NMGI team.

I wanted to be able to run a computer or terminal from anywhere. I was less cellphone-centric even though I evolved with cellphones by starting with a car phone in my trunk in the 1980s and using cellphones to connect to computers as soon as the technology was available. I changed to mobile phones with the DynaTAC 8000X, Motorola 2900 bag phone, Motorola MicroTAC flip phone, Motorola StarTAC, and a parade of other cellphones, giving my K2 Enterprises team something new to discuss every year at events.

Cellphones and mobile technology continued to evolve through NTT DoCoMo's i-mode platform, BlackBerry, Nokia's Symbian platform, and Windows Mobile. Personal digital assistants like the PalmPilot, Apple Newton, and others served their purpose until the arrival of the smartphone, which combined mobile phone and computing functions. A popular smartphone, the iPhone, arrived in 2007. Touch screens, applications (There's an app for that), and the evolution of tablets like the iPad, Kindle (now Amazon Fire), Samsung Galaxy, and others allowed these mobile devices to become small, powerful, convenient computers.

Today, you and your clients expect the convenience of using your smartphone to access any information you care to look up in seconds. Why shouldn't business be transacted conveniently? Mobile technology is the freedom to run the technology you want securely and conveniently on any device, anywhere, at any time of day, and it should be part of your strategy.

WHAT CLOUD STRATEGIES CAN YOU USE?

The list of cloud technologies enables many cloud strategies. What is needed for your practice, your clients, and your life? What is your strategy as you position your tax, audit, CAS (client accounting services), advisory, wealth management, or any variety of vertical niche offerings? Is it cloud first? Is it about relationships? Integrity, independence, client service, team member experience, profitability, and more can be in your strategic plan. And what are your tactics? Convenience, client experience, automation, recurring revenue, and more can be in your tactical plan.

While *The Technology Lab Podcast (https://www.cpapracticeadvisor.com/resource/podcast)* can give you a tactical view of product solutions, co-host Brian Tankersley and I have many strategic discussions and thoughtfully advance individual solutions for your technology stack. Have you thought about your practice's future and what emerging technologies will bring? As mentioned in previous columns, Brian and I are rebuilding our technology stack recommendations across all practice areas.

You'll see more from us on this in the future as we remain independent recommenders and advisors, with a concern for vendor and monetary bias in stack recommendations. I'm particularly excited about my new designs for the business and accounting use of the Metaverse extending the thinking of Matthew Ball into our specialty.

Let's get to the core cloud offerings that I recommend that you consider, choose and use:

- SaaS software when it works for your firm and clients with tools like Accounting Power, AccountingSuite, Acumatica, NetSuite, QuickBooks Online, Sage Intacct, Spire Systems, Xero, or Zoho
- Collaborative tools with your clients, with tools like BizEKG from 4ImpactData, e-Courier, Liscio, PATH by Simplex Financials, or Suralink
- Accounting automation whenever possible with tools like Dext, Hubdoc, or Sage Autoentry
- Productivity Suites with Google Workspace, Microsoft 365 (particularly E5 for CPA firms), or Zoho One
- A modern, continuously updated website with a .CPA domain name as well as video and social media feeds
- Easy payment methods with services from Corpay One, CPACharge, or QuickFee
- Outsource for additional labor with services from AdvanceTrack, BooXkeeping, TOA Global, Taxfyle or Xpitax
- Hosting or private cloud deployments for legacy applications such as practice management, tax, audit, TValue, and QuickBooks desktop with suppliers like Ace Cloud Hosting, CETROM, Right Networks, or Network Management Group, Inc.
- Practice tools for your firm evolving to the cloud with choices such as Avii, Canopy, Clarity Practice Management, Corvee, Doc-It Suite Cloud, DoMore, Karbon, SmartVault, Tallyfor, Thomson Reuters ONVIO, TPS Cloud Axis, Verdocs, weintegrate, or Wolters Kluwer CCH Axcess
- Emerging technologies with your clients with choices such as Gilded, Ledgible by Verady, LukkaTax, and Vic.AI

SO, WHAT DO I DO NOW?

As you can see, web-based cloud and mobile technology opportunities abound. These tools can give you a competitive edge, particularly if you are a smaller firm. You can use most of the same technologies your competitors buy and leverage. You must be thoughtful about your strategy and tactics, carefully choosing your technology stack and where you spend your time. You can get leverage through more automation, outsourcing, and connecting cloud-based tools.

I have recommended ways to create your own strategic and tactical plans in various previous columns. It is time to review and update those plans. Your action plan and day-to-day activities must also evolve or quickly become obsolete. Finally, addressing cloud opportunities is not a project; instead, it is a process. If you need continuing guidance, watch this space. ■

The Pros and Cons of Offsite Data Storage

By Richard Bailey

Photo 142512492 © Siarhei Yurchanka | Dreamstime.com

ENTERPRISE-GRADE STORAGE IS the lifeblood of cloud computing. As a result, global businesses have an insatiable appetite for data storage, according to Cybersecurity Ventures, and it is estimated that there will be over 200 zettabytes of data by 2025. A zettabyte equals one billion terabytes.

Since the COVID-19 global pandemic, offsite storage has become the go-to place for data storage. Demand for centralized storage services has grown exponentially. Join us as we discover the pros and cons of offsite storage, learning why demand is so high along the way.

WHAT IS OFFSITE STORAGE?

Offsite storage is storage hardware relocated at a remote, geographically disparate location. Popular examples include:

- Leasing storage at a remote data center.
- Leveraging a managed service provider's data center.
- Consuming cloud storage from a cloud provider.

PROS:

Let's jump straight into the pros:

- **Scalability and Efficiency:** Offsite storage provides unlimited scalability; there is no cap on the amount of storage available, and you can consume as much or as little data as you desire. Automated schedules automatically archive data after a pre-defined period. For example, typical plans may include archiving all data over 90 days old. A computerized routine will copy the relevant data to archive storage, perhaps to another provider, to ensure data integrity.
- **Cost and Value:** Offsite and cloud storage is an affordable way to acquire enterprise-grade features (e.g., encryption and data protection); low cost is why users are switching to offsite storage en masse. Storage is often sold on a pay-as-you-go cost model, with free incentives to encourage users to join. There is no initial outlay for expensive storage hardware and no complex maintenance or support contracts to maintain.
- **Instant Availability:** Offsite and cloud data storage are available now. You can be up and running within a few clicks. Files can be uploaded or downloaded via a cloud console, a command line interface, or using an app created by the provider. With offsite cloud storage, the infrastructure is already in place, and the platform is already available. As a result, there are no extensive lead times when procuring the hardware and no waiting for employee availability to rack and install hardware. Instead, the client can plug directly into the cloud storage and start working immediately.
- **It's a Managed Service:** The storage solution is a managed service, so you expect everything to work perfectly as a consumer. These services have been around for several years, so the platforms have had time to bed in. Most cloud providers offer up to 100% service level agreements (SLAs) on cloud storage, enforcing the view that cloud storage reliability is exemplary. The managed service providers handle hardware failures and manage the complex operations needed to keep the service running efficiently. For example, engineers address problems at the storage layer and, if required, can allocate data between clients and devices on demand. In addition, the managed service provider is responsible for the storage lifecycle and upgrade planning.
- **Flexible Connectivity:** You only need an internet connection to access offsite storage; perhaps a dedicated virtual private network for added security. Data is easy to get to, private by default, and can be shared with whomever you like.

CONS:

- **Security and Privacy Concerns:** Although cloud storage is exceptionally secure, incorrectly configured solutions are possible. There are numerous examples of a misconfigured storage bucket exposing sensitive personal data. Protect offsite storage from unauthorized access and always encrypt.
- **Compliance and Data Governance:** There are complex data privacy laws to follow when securing or destroying data. General Data Protection Regulation (GDPR) and Cisco Certified Network Associate (CCNA) are just two examples. Consider the location of data; many businesses are forbidden to store sensitive data outside the U.S.
- **Long-Term Costs:** Offsite storage is often affordable; however, there may be a risk of vendor lock-in, so research the long-term costs.
- **Noisy Neighbors:** Choose wisely between dedicated or shared storage. Will there be contention for resources from yourself and other clients? Most good storage providers offer QOS, but this risk is vital to remember.

So that is our top pros and cons for offsite data storage. We are witnessing a paradigm shift toward cloud computing, and offsite cloud storage is making a real difference for business and personal users worldwide. ■

Richard Bailey is the Lead IT Consultant at Atlantic.Net, a growing and profitable cloud hosting company that specializes in HIPAA compliance.

Now's the Time to Engage in Thought Leadership as a CPA

By Patricia Wellmeyer, Ph.D, CPA, CGMA

THOUGHT LEADERSHIP IS often thought of as being the business of universities and academics. Indeed, academic research plays a significant and integral role in the advancement and attainment of new knowledge. What is not as widely recognized, however, is that CPAs and professional accounting firms can play an important role in the business of thought leadership as well.

Companies in today's accounting and reporting environment face an unprecedented number of new accounting and reporting challenges related to environmental, social, and governance issues, cryptocurrencies and digital assets, special purpose acquisition companies (SPACs), the Covid pandemic, inflation…to name only a few. In addressing these challenges, company managers, audit committees and stakeholders alike are increasingly turning to the professional accounting community for publications that disseminate timely information, perspective, and guidance helpful in understanding and dealing with today's issues.

If done with diligence, these thought leadership pieces can provide expert, quality data-rich content that is both informative and practical and, most importantly, quickly and easily accessible by interested users. They can also serve as vehicles for CPAs and accounting firms to showcase their strengths in expertise and professional capital to target audiences, providing additional support resources to existing clients and potential new ones.

SO, IF YOU'RE INTERESTED IN MAKING THOUGHT LEADERSHIP PART OF YOUR ACCOUNTING PRACTICE, WHAT SHOULD YOUR IMMEDIATE NEXT STEP BE?

Consider whether you have the time and resources to dedicate to this initiative- at its core, thought leadership in accounting is about producing and disseminating timely information that will be valuable to financial statement users and stakeholders in understanding and navigating through current reporting issues…and those to come. And providing value-added quality publishable content necessitates that you have both the time and expertise to add value on a particular topic. So, ask the hard question of yourself and those in firm leadership- is your firm willing and able to support and allocate resources to making thought leadership an important part of the firm's mission?

IF THE ANSWER TO THE QUESTION POSED ABOVE IS YES (CONGRATULATIONS!), HOW DO YOU GO ABOUT INCORPORATING THOUGHT LEADERSHIP INTO YOUR ACCOUNTING PRACTICE?

- Build thought leadership into firm strategy as its own KPI– identify how thought leadership activities may help support/achieve the core elements of the firm's strategic mission and positioning. In doing so, be sure to consider how thought leadership activities can help your firm achieve both tangible (e.g. additional client revenue) and intangible (e.g. enhanced reputation) outcomes.
- Make thought leadership part of firm culture– create and foster an environment that gives value to and supports thought leadership. It is important to build a culture where professional staff view engagement in professional development and knowledge sharing activities not just as a CPE check the box exercise, but as its own source of competitive advantage.
- Identify areas of expertise within firm and associated leading experts– build on the firm's current expertise/areas of strength and use planning for thought leadership activities as a means for identifying areas where expertise can/should be further developed.
- Allocate time to and reward experts for thought leadership activities– a successful thought leadership initiative takes commitment and a firm's reward system for professional staff should align with and incentivize that commitment.
- Identify platforms best suited for distributing your brand of thought leadership– give thought to which medium would be most impactful as a means of sharing your expertise and reaching your target audience. Podcast productions and panel participations work well if your brand of thought leadership is more conversational and/or opinion based. Practice articles and executive summaries tend to work well for data and fact rich thought leadership content.

Like a fine wine, a successful thought leadership initiative takes time to cultivate, but stay committed to the process and you will see how effectively you become known as a go-to expert! ■

Patricia Wellmeyer, PhD, CPA, CGMA, is an assistant professor at the Paul Merage School of Business, University of California, Irvine.

4ORTY UNDER 4ORTY

CPA Practice Advisor Announces 40 Under 40 and 20 Under 40 Award Winners

By Isaac M. O'Bannon, Managing Editor

CPA PRACTICE ADVISOR has announced the 2021 members of its "40 Under 40 Accounting Leaders" and "20 Under 40 Influencers" programs.

The awards recognize 40 professionals who are under 40, and have emerged as future leaders in the profession, and 20 who are leading the development of technology, education or services that enhance the profession.

The **40 Under 40 Awards** spotlight the top practicing public accountants, educators and thought leaders who are leading their profession by visibly and incrementally changing the accounting profession through their exemplary leadership, their innovative thinking, their collaborative efforts to provide unity to the profession across the generations, and their community outreach which extends the visibility of the profession outside the workplace.


LYDIA AHN, CPA – VSH CPAs


SUSAN ALLEN, CPA, CITP, CGMA – AICPA


DAVID ALMONTE, CPA, CGMA – Amica Mutual

ROSLYN BANKS, EA – Adelaide Rose LLC


MICHAEL BARTON, CPA – Sikich LLP


AARON BERSON, CPA – Fringe Advisory Co.


CHASE BIRKY, CPA – Dark Horse CPAs


KRISTIN BIVONA, CPA – GellerRagans CPAs


KENNETH BONUS, CPA – Bonus Accounting LLC


THOMAS CASTELLI, CPA, CFP – Hall CPA, PLLC


LINDSEY CURLEY, CPA, CGMA – AICPA


MICHAEL ECKSTEIN, EA – Eckstein Tax Services


LINCOLN FLEMING, CPA, CFP, PFS – Blackrock


ZACHARY GORDON, CPA – Propeller Industries


BRANDON HALL, CPA – Hall CPA, PLLC

HOLLY HAWK, Ph.D, CPA, CGMA – Clemson Univ.

KENNETH HEALY, CPA – Diversified Financial Solutions

CHRIS HERVOCHON, CPA, CVA – Hervochon CPA, CVA LLC

KARI HIPSAK, CPA, CGMA – AICPA + CIMA

KATHRYN HORTON, CPA CMA, CIDA, CFE – Horton CPA PA

JACKI JACOX, CPA – Mazars USA

CALEB JENKINS, EA, CQP – RLJ Financial Services

WASSIA KAMON, CPA, CMA, MBA- ACM Chemistries

JOSHUA LANCE, CPA, CGMA – Lance CPA Group

MATTHEW MARTIN, CPA – Citrin Cooperman

LIZ MASON, CPA – High Rock Accounting

CARL MAYES, CPA – AICPA

JESSICA MCCLAIN, CPA, CITP, CISA – Girls Scouts USA

JACKIE MEYER, CPA, CTC – Meyer Tax, Concierge CPA

GREG O'BRIEN, CPA – Go CPA LLC

JESSICA OFFER, CPA – Withum

TIM PETREY, CPA, CGMA – HD Davis CPAs

MATT ROETCISOENDER, CPA, CVA – VSH CPA

ALEXANDRIA ROMERO, CPA – Hervochon CPA

SEAN STEIN SMITH, Ph.D, CPA, CMA – CUNY Lehman

WILL TANEM, CPA – BPM LLP

HOWARD TELSON, CPA, MST – Crossborder Solutions

KATIE THOMAS, CPA – Leaders Online

ROBERT WESTLEY, CPA, PFS, CFP – Northern Trust

JEFF WILSON, CPA, PFS – The W2 Group

20NTY UNDER 40RTY INFLUENCERS

The **20 Under 40 Top Influencers** program similarly honors those who are leading the way in developing the constantly evolving technology and firm processes that allow practitioners to be more productive, efficient and profitable, as they build practices that will endure and thrive.

"Without these creative minds, the accounting profession would not be where it is today - on the cutting edge of technology and innovation," said *CPA Practice Advisor*'s editor-in-chief Gail Perry, CPA. "All of this year's honorees are professionals who are not just thinking about the future, but are stepping forward and making significant changes in the accounting profession itself and the way in which our profession is perceived." ■


ANDREW ARGUE, CPA – Corvee


KIM AUSTIN – Avalara


KEVIN BONG – AuditFile


STEVEN BONG – AuditFile


JIN CHANG – Fieldguide


KATIE COHODES – Armanino LLP


BRYAN COMPTON, MBA – Blucora (TaxAct)


DAVID CRISTELLO – Jetpack Workflow


BRANDON GRAY, CPA – Firm360

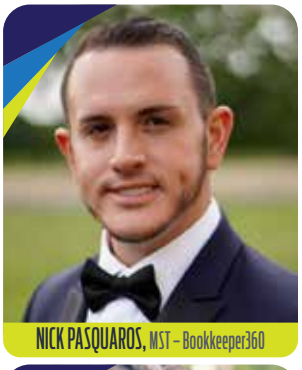

RICHARD LAVIÑA, CPA – Taxfyle


KALIL MERHIB – CPA.com


DAVE MUNDY – Audit Dashboard


AKMAL NASIMOV – Bloomberg Tax


SHALIN PARIKH, CA – Entigrity Solutions


NICK PASQUAROS, MST – Bookkeeper360


BRIAN RIVERA, CPA – Trader Tax CPA


NADIA RODRIGUEZ, CPA – Intuit


SCOTT SCARANO, EA – Padgett NC


DAVID TOTH – Winding River Consulting


SARAH YORK, EA – Keeper Tax

Nominations for the 2023 awards will open in March 2023.

Finance Pros Can Be a Powerful Defense Against Cybersecurity Threats

By Christina Quaine

A RECENT PWC survey found that rising cybersecurity threats are the number one concern for CEOs around the world. It's not surprising, as malware, ransomware, and phishing scams that provide criminals with access to sensitive customer and financial information can result in hefty financial loss and do irreparable damage to a firm's reputation.

As firms look to better protect themselves, payments remain a key area of concern. The 2022 AFP Payments Fraud and Control Survey found that 71 percent of organizations were victims of payments fraud attacks or attempts last year. Checks, still a primary payment source for many businesses, were the payment method most impacted by fraudulent activity, accounting for 66 percent of attacks.

Firms have powerful allies at their disposal to help protect against the growing threats—the finance and payments team. These professionals can leverage advanced technologies, including artificial intelligence (AI), and security best practices to keep a watchful eye and ward off potential attacks.

Here's a look at just how they can serve as an effective layer of defense, strengthening protection in their organizations from cybercrime that can have devastating effects:

TAKE A 360-DEGREE VIEW OF THE THREAT ENVIRONMENT AND UNDERSTAND THE RISKS

Understanding cybersecurity risks and generating awareness of them is the first step in training the finance and payments teams to help protect against them.

PwC reports that cybersecurity attacks haven't just multiplied, they've become more sophisticated, and ransom demands have become steeper. Remote and hybrid work environments have put organizations at increased risk for security breaches, as people are spending more time on their computers and often working on less secure networks and personal devices.

The record high labor shortage, including too few cybersecurity professionals to provide protection, is also to blame for creating a riskier business environment. Eighty-five percent of those finance pros surveyed in a global cybersecurity study by Trellix said they believe the current workforce shortage is making it difficult to secure increasingly complex information systems and networks.

Which department is most at risk? AFP's 2021 Survey shows that accounts payable (AP) departments are among the most susceptible. Fifty-eight percent of respondents report that their AP department was targeted by BEC fraud, a convincing approach where a criminal sends an email to an employee, pretending to be a senior executive with the company, and instructing the employee to approve a payment or release client data. Employees often fall for scams like this, unless they are made aware of them and on guard.

RELY ON ADVANCED TECHNOLOGY TO PROTECT FINANCIAL INFORMATION AND TRANSACTIONS

The majority of financial institutions surveyed by software provider VMWare plan to protect against the threats by increasing their cybersecurity budget by 20 percent to 30 percent this year.

One powerful place to allocate budget is to the team responsible for managing sensitive customer and financial data and handling mission critical financial transactions, including invoicing and payments—the AP team. Antiquated, error-prone tools and processes like spreadsheets and paper checks expose organizations to greater risk.

Automating risky manual invoicing and payments processes with AI-powered AP solutions can provide the controls and transparency organizations need to better detect fraudulent threats. It also enables organizations to offer vendors e-payments, a far safer payment method than paper checks.

Cloud-based automated AP solutions protect sensitive data by storing it in safe, electronic formations and putting controls in place to assure appropriate access to it. Embedded within the solutions, AI provides 24/7 fraud protection and malware and intrusion detection. It can identify, for instance, important missing invoice details, track unforeseen rises in invoice volumes, trace after-hours logins, and make it difficult to forge documents. The greater visibility also helps the finance team identify past payment transactions and behavioral patterns to better forecast future transactions.

ESTABLISH SECURITY PROTOCOLS AND TRAINING PROCEDURES TO SUPPORT THE FINANCE TEAM'S PROTECTION EFFORTS

In addition to creating awareness of risk and phasing out legacy equipment and processes that are becoming increasingly susceptible, organizations can protect against cybercriminal activity by establishing a strong safety culture.

That means sharing news updates and flagging pervasive issues, so workers are on guard, well prepared, and understand that safety and security are top priorities.

Together, departments can create and share policies and procedures that clarify expectations and define security protocols. Effective safety protocols include requiring remote workers to use company-owned devices, VPNs, and secure internal networks and firewalls to protect sensitive information; regularly updating company-owned software with security patches; and never leaving devices unattended.

LOOKING AHEAD

Alarmingly, more than half of respondents in the PwC's 2022 Global Digital Trust Insights survey expect to see an increase in cyberattacks. Undoubtedly, criminals will continue to take advantage of vulnerabilities as they emerge, evolving their methods and targets to outsmart prevention strategies.

While it's impossible to predict what new tactics may emerge, proactive prevention strategies and trusted technology partners remain the best defense. ■

Christina Quaine is chief information security officer and senior vice president of technology operations for AvidXchange. She is responsible for the company's cyber security program, leading efforts to reduce the risk of unauthorized access to sensitive data and personally identifiable information.

Maximize Your Security Posture with Proven IT Solutions

A global study, the IBM Cyber Security Intelligence Index Report (2021), researched thousands of IBM customers in 130 countries and concluded that "human error was a major contributing cause in 95% of all breaches." Clearly, human errors play a pivotal role in cybersecurity breaches.

Although totally eliminating human error is likely an impossible feat, CPA firms can take steps today to mitigate human errors that cause cybersecurity breaches.

- **Deploy Advanced Threat Protection.** Using tools such as Next Generation Antivirus (NGAV), Endpoint Detection & Response (EDR) and Managed Detection & Response (MDR) have proven instrumental in combating cyber threats.
- **Adopt Least Privilege Model.** Significantly reduce your risk by only granting access to networks, systems, and applications your staff need to execute their tasks.
- **Utilize a Multiple Backup Solution.** Multiple daily backups using different methodologies and stored off your network.
- **Enroll Multifactor Every Step of the Way.** Enroll MFA across all systems, solutions, etc. so you are prompted every step of the way - virtually eliminating weak entry points.
- **Create a Cybersecurity Culture.** CPA firms should create a culture of consistent security awareness to reduce the risk of cybersecurity breaches caused by human error. Also, employees should receive cybersecurity knowledge and training, so they have a philosophy of active cybersecurity decision-making.
- **Verified, Audited & Tested.** Ensure your team is regularly testing its Disaster Recovery Plan - printed, offsite, tested, and verified. Ensure your IT security solution or provider is SOC audited and verified through a third-party security auditor to ensure the most current security best practices are in place.

Finally, work with the experts! Cetrom is a proven Cloud Hosting Solutions provider with advanced support for CPA firms of all sizes. Just as businesses hire accounting firms to do taxes, enlist the help of the IT professionals to handle cloud hosting solutions and data security. Allow yourself the gift of time to focus on what you do best and leave IT to the experts. Contact Cetrom today to learn more about how they can help maximize your security posture with proven IT security solutions.

CETROM
www.cetrom.net

Do IT in Our Cloud

www.cetrom.net 866.364.1098

CPA Practice Advisor
Today's Technology for Tomorrow's Firm

INTUIT quickbooks®

At QuickBooks, we are on a mission to help all our customers succeed; and that focus on success starts with our partnership with the accounting community. In many ways, that partnership started 25 years ago when we launched the QuickBooks ProAdvisor Program, designed to celebrate the entrepreneurial spirit of accounting professionals with a focus on connecting them to small businesses using QuickBooks who need their help to thrive.

Today, alongside the 25th anniversary of the ProAdvisor Program, we celebrate the three million small businesses worldwide that are connected to accounting professionals through the QuickBooks platform. Accounting professionals are the driving force behind the QuickBooks platform that help small businesses succeed, leveraging the power of our initial desktop offering to today's robust online ecosystem that powers small businesses globally.

Through our online ecosystem, our priority is to provide accountants with the products and services they need, and by extension, their clients' needs, to succeed and grow. To do that, we continue to build our partnerships with the accounting community by listening to their feedback and using it to improve QuickBooks and its entire online product platform. Here are more details on how we are delivering for the community.

What is QuickBooks doing to help accountants and bookkeepers grow?

Our goal is to help power prosperity worldwide. This means ensuring that you and your small business customers are successful. Half of all small businesses fail within the first five years. We're on a mission to decrease that failure rate. We can help decrease that failure rate by connecting every small business on our platform to an accounting professional. We firmly believe that small businesses are more successful when they work with an accounting professional, and more specifically, a ProAdvisor. It's this shared mission that connects us: linking more small businesses to accounting professionals coupled with the power of the integrated QuickBooks platform can have a real, tangible impact on helping small businesses, and you, succeed in the long term.

What are your priorities for the QuickBooks platform?

We're prioritizing improvements across our ecosystem in several ways. This includes improvements to QuickBooks Online Advanced to better meet the needs of mid-market businesses, with commerce accounting capabilities, such as inventory management, to help product-based businesses manage their omnichannel strategies. Across the platform, we're also focused on personalization, automation, and ease-of-use features and functionality to help small businesses better navigate QuickBooks, ultimately helping you be more efficient when working on your clients' books. We're also prioritizing our QuickBooks Desktop migration efforts. Small business adoption of QuickBooks Online grew significantly during the pandemic as small businesses required and realized the benefits of working online. Our integrated QuickBooks Online platform unlocks the power and value of what we deliver for accountants and your clients, from payroll to payments, to capital to inventory management, and more. Finally, we're digging deeper into how best to combine the power of QuickBooks and Mailchimp so you and your clients can find and nurture new and existing customers. We're excited for the future of the QuickBooks Online ecosystem and how it will continue to serve you and your clients.

What's next for the ProAdvisor Program?

In addition to the commitment to connect an accountant, and more specifically, a ProAdvisor, to small businesses using the QuickBooks platform, we have some exciting efforts on the horizon for the ProAdvisor Program. We're getting ready to launch a redesigned ProAdvisor training portal to make it easier to identify and find the training ProAdvisors are looking for. We're also building out even more personalized learning paths based on what ProAdvisors tell us they want to learn, including educational content on serving growing mid-market businesses. Furthermore, we're looking at how we can improve the program overall with more impactful benefits and ProAdvisor-only access to discounts and services that help them better serve clients.

As our most valued partners, we will continue to listen, learn, and create an ecosystem that contributes to the success of all accounting professionals on the QuickBooks platform.

QuickBooks Online Payroll

A payroll system should make the life of an accounting pro easier. And, more importantly, it should make your client's life easier.

Make your life easier with a payroll solution that can help give you time back, offer more control, and provide expert help so that you can confidently and holistically advise your clients.

To learn more, visit
quickbooks.com/accountantpayroll

> The time I get back allows me to focus on what really matters—my clients.
>
> *– Accountant QuickBooks Online Payroll User*

INTUIT quickbooks®

For Accounting Professionals

CLOUD ACCOUNTING

The Right Time to Move to the Cloud

For a lot of small firms and accounting professionals, moving their business to the cloud feels overwhelming and often gets deprioritized when stacked against the deluge of everyday tasks. The truth is… you can't afford to wait any longer to make the move. We have all heard about the rising security risks the accounting profession is facing, and one of the best ways to protect yourself and your clients is by moving to the cloud.

For Darren Root, Chief Strategist at Right Networks, the cloud is an important component of any security strategy. Here, Darren takes time to answer the most common questions he hears when working with accounting firms and small businesses.

Darren Root, CPA, CITP, CGMA, is the Founder of Rootworks and serves as Chief Strategist for Right Networks. Darren has over 30 years of experience as a CPA and in management within the profession. He has vast accounting expertise and a passion for helping firm owners modernize and transform their practices into thriving, sustainable enterprises.

Darren has earned numerous awards and continues to contribute to the profession with books, articles, podcasts and shows that educate and inform the industry in all areas of firm operations, industry trends and business models.

Q: I am not a big company. Why should I consider the cloud?

A: Any size business can benefit from using the cloud it is not just for the big firms. In fact, a lot of small businesses greatly benefit from the secure, anytime, and anywhere access the cloud enables for their team.

Q: Is the cloud secure?

A: The cloud is, in fact, more secure than most CPA firms' and small businesses' current in-house IT environments. There are cloud service providers that use the highest level of encryption technology to give users bank-level security.

Q: I don't have time to train myself let alone my team on something new. How long will the onboarding process take?

A: Once you're in the cloud, there's actually very little onboarding involved, since getting employees up to speed mostly just requires implementing new login names and passwords. Applications remain the same and run securely in the cloud, rather than on individual workstations or the office server.

Q: I am running a hybrid model, some of my team is at home, and some are in the office. Can they collaborate in real-time using the cloud?

A: Working in the cloud saves time and enables you and your staff to continue serving your clients without missing a beat. Plus, most tax applications running in the cloud are updated automatically for extra efficiency.

Q: How do I choose the right cloud provider?

A: When selecting a service provider ensure your data is protected in a private cloud hosted at data centers offering the highest tier of security. Also, select a provider that employs enterprise-grade intrusion detection and can deliver U.S.-based 24/7/365 support from a team with accounting industry expertise.

The cloud can deliver an extensive array of benefits to large and small businesses including securing your data and thus significantly improving business continuity and recoverability. Simply put, it is quickly becoming too costly not to be in the cloud.

Right Networks®
RightNetworks.com

Right Networks®

Cloud hosting • Security solutions • Firm IT outsourcing

Powering the new way firms work.

The world and the people who make it work have changed forever. Right Networks gives you the solutions to enable a remote workforce and attract and retain top talent. We offer cloud hosting with bank-level security for QuickBooks® and more than 3,000 applications in the accounting ecosystem that help people work anywhere and simplify everything.

Talk to us, and let's empower your firm for the new way the world works.

rightnetworks.com | 888.417.4448

2022 Digital Security and Cybercrime Update

By Mary Girsch-Bock

IN 2021, CYBERCRIME cost U.S. businesses almost $7 billion, yet today, only 50% of U.S. businesses report having a cybersecurity plan in place.

ThoughtLab, a leadership and economic research firm recently conducted a cybersecurity benchmarking study. The study, Cybersecurity Solutions for a Riskier World analyzed cybersecurity strategies, with 1,200 large organizations in 16 countries participating in the study.

According to the study, material breaches rose 20.5% from 2020 to 2021, with cybersecurity budgets rising as a direct result of those breaches. But increased budgets do not necessarily equate with preparedness, with 29% of CEOs and 40% of chief security officers admitting that their organizations remain unprepared for a large-scale cyberattack. Their reasons varied:

- 44% cited supply chain issues
- 41% cited the fast pace of digital innovation
- 28% cited inadequate cybersecurity budgets and lack of executive support
- 24% cited a shortage of talent versed in cybersecurity

How do these facts impact your firm? Keep in mind that in some states, CPA firms are held liable for any data breaches that impact their client's personal data. But even if you're not legally responsible, a cybercrime committed against your firm will directly impact your current client list as well as those looking to contract with your firm for services.

Though cybercrime threats vary, today, ransomware and phishing are considered the two top threats to businesses nationwide. If you're not exactly sure what ransomware and phishing are and the impact they can have on your business, read on.

RANSOMWARE AND MALWARE

Ransomware is a type of malware that is used most often, infiltrating your computer system and encrypting the files so that you're unable to access the system unless a ransom is paid. If the ransom is paid, the company receives an encryption key that will allow them to access their files once again.

In many cases, businesses have resorted to paying ransom to gain access to their files. Unfortunately, paying the ransom is no guarantee that the hackers will give you access to your files.

PHISHING

In years past, phishing attempts were clumsy and fairly easy to detect. That's not the case today, with counterfeit communications difficult to identify. Today, there are over 150 million phishing emails sent daily.

Phishing typically lures victims in by email, with the request made to look like communication from a trusted institution such as a bank or government agency. A link is always included in the initial contact email or text, which takes you not to the site indicated, but to the hacker's site, where your personal information can be easily compromised. Because of the level of sophistication available to hackers, it can be difficult to determine the legitimacy of an email or text.

One way to check for the legitimacy of a link is to place your mouse over the link itself. This will display the hyperlink and allow you to see exactly where the link will take you.

Of course, the best way to prevent phishing is to not click on any link sent to you until you've verified it. It's also important to never respond to an email or text that requests personal information or asks for a password.

Whether your firm is small or you have offices around the world, you're vulnerable to cyberattacks. Taking the proper precautions will help keep your firm and your client data safe. ■

Mary Girsch-Bock began her career as an accountant and later made the switch to writing full time, concentrating on software reviews. A former QuickBooks beta tester, Girsch-Bock currently specializes in business and technology with a focus on small businesses. Her work has appeared in The Motley Fool, The Blueprint, Property Manager.com and she currently writes a monthly business and technology-related blog for PLANERGY, a Procure-to-Pay platform designed for mid-market organizations.

PAUL McDONALD
Senior Executive Director
Robert Half
paul.mcdonald@cpapracticeadvisor.com

Struggling to Recruit Top Talent?

Start Re-Recruiting!

THE "GREAT RESIGNATION" has handed American employers an immense challenge. Many professionals enjoyed increased flexibility and improved work-life balance during the acute phase of the COVID-19 pandemic, and this led them to re-evaluate their jobs and careers. Not everyone liked what they found, and plenty began looking for greener pastures. All told, some 47.8 million Americans had quit their jobs by the end of 2021.

Virtually every employment sector, including finance and accounting, has been affected by the "Great Resignation." And virtually every manager has been asking the same question: How can I keep my best employees from leaving? The answer may be as straightforward as re-recruiting.

WHAT IS RE-RECRUITING?

Put simply, re-recruiting is recruiting your current employees all over again. It's about reminding and showing them they are valued and their contributions further your mission and contribute to firm goals.

The major advantage to re-recruiting is that you're also helping head off potential turnover. When you view your best employees as top job candidates, you keep them more satisfied, lessening the likelihood that they'll burn out and leave.

STRATEGIES FOR RE-RECRUITING

It's important to note that there is no one-size-fits-all approach to re-recruiting. To an extent, offerings will need to be personalized to each employee's unique needs and circumstances, so listening is key. With this in mind, here are some ways you can re-recruit your employees.

■ Improve Compensation

Salary and total compensation are key. Many accounting professionals may be lured away by better pay. In fact, there's a widening gap between pay increases for taking new jobs and those offered for staying in a role.

Inflation is also a driver of employee frustration. In May, the U.S. annualized inflation rate was at 9.1%, the highest it's been since 1981. Workers are feeling this in rising costs for groceries, utilities and gas. Standard raises are no longer enough and inflation undercuts their value. Instead, use the rate of inflation as a benchmark, and increase salaries 1-2% above that.

Other ways to retain employees through compensation include bonuses and improving pay equity. Make sure salaries are commensurate with experience across the board — men, women and employees from traditionally underserved groups should be paid on the same scale.

Above all, don't make your employees ask. If they come to you for a pay increase, it's a clear indicator they're already unhappy and may be looking elsewhere. If budget is an issue, take some of your recruiting dollars and use that to focus on retention. After all, retaining a standout employee will be less expensive than hiring and onboarding a new one.

■ Increase Flexibility

As a result of the pandemic, employees are no longer asking for flexibility — they expect it. And if you can't provide it, they'll look elsewhere. Everyone wants a healthier work-life balance and employees who can achieve one are happier, more productive and more likely to stay.

The most obvious way to increase flexibility is by offering some form of remote work. At the height of the pandemic, almost every accounting firm went remote in one way or another. Chances are, your employees don't need to come into the office every day to work effectively, which is why hybrid schedules (some days in, some days out) can be a win-win for firms and their workforces.

Consider making fully remote and hybrid work a permanent fixture and allowing employees to do their jobs wherever they are most comfortable and productive. You can also let employees customize their work hours by offering compressed workweeks. All this makes it easier for workers to balance the demands of their work and personal lives, leading to less stress and more productivity and engagement.

You can also provide additional days off outside of standard holidays. Some firms may do Summer Fridays, or provide extra time away after tax season.

■ Evaluate your benefits

Making sure you offer competitive benefits is another critical step in retaining talent, and keeping your finger on the pulse of what your employees want is especially important in your re-recruiting discussions.

In the wake of the pandemic, more employers are offering mental health benefits, such as employee assistance programs (EAPs), which provide access to counselors. However, don't make assumptions about what your workforce wants or needs. If people prefer employee discounts to mindfulness courses, it's not wise management to tell them they're wrong.

Financial planning benefits are also rising in popularity, as companies seek to help employees achieve budgetary goals. These can include planning sessions or even student loan assistance.

Childcare support is another in-demand benefit, particularly during the summer months. Some companies are partnering with services that connect their employees with vetted childcare providers so, if they get in a pinch, they have someone to watch their children.

Explain during your employee discussions that you're reworking your benefits package, including evaluating your competition to make sure you fill in any gaps.

■ Encourage Professional Development

If you want to keep your employees, it's important that they can see a future at your firm, so you need to focus on professional development. When looking to fill an open position, consider internal candidates first. Promoting from within shows all your employees that growth is possible.

Mentoring programs are another effective way of investing in your employees, and recognizing their achievements — even if it's a simple "thank you" — can go a long way in making them feel valued.

All the talk of the "Great Resignation" may leave some CPA managers feeling like they're at the mercy of market forces. But remember: quitting is rarely an easy decision for professionals, regardless of how talented they are. By re-recruiting them to your firm and getting them excited about the next leg of their career journey, you can make the decision to move on even harder. ■

AMY VETTER, CPA.CITP, CGMA
Mindful Technologist &
Keynote Speaker
@AmyVetterCPA

THE CLOCK IS ticking for the 9-to-5 work schedule. Many workers have begun to demand more flexible work schedules. Those with families generally want the option of working from home at least one day a week. Employee morale is better when workers can work from home on their schedule, and employees who can work only part-time have struggled to find employers that will accommodate their schedule.

The reason is simple: businesses often fear what these changes could mean for workplace productivity and profitability. Here are five alternative work schedules that offer a range of options for both companies and their employees:

CORE HOURS

With core hours, a company chooses set days and times when all employees are expected to work, for example, 10 a.m. to 2 p.m. Monday-Thursday. Between those times, all employees are present in the office and working. They can schedule the rest of their hours for whenever works best for them. This is ideal for companies with a busy workload that requires teams to be together in one place at certain times. It also helps with team dynamics because everyone is present during core hours.

FLEXTIME

Flextime allows employees to choose when they want to start their day as long as it doesn't interfere with deadlines or client needs. Iif a staff member has regular client work later in the day, she shouldn't set her flex schedule so that she leaves early every day and misses crucial client opportunities.

Because flextime varies based on individual needs and preferences, it's ideal for those with other commitments outside work, such as children or elderly relatives who need caretaking. Many firms offer this option to attract new talent because it appeals to those looking for flexibility in their jobs.

TELECOMMUTING

Telecommuting allows staff to work regularly from home or some other location outside of the office and is increasingly popular with companies. Employees can also choose to come into the office on a part-time basis. Firms can also set mandatory in-office days or times. This flexibility allows a company to save money by paying for less space and equipment, while at the same time giving employees more control over their schedule.

Telecommuting is an excellent way to boost productivity and reduce your environmental impact. It also serves as an opportunity for employees to increase their skills by working independently on projects.

COMPRESSED WORKWEEK

A compressed work schedule allows employees to work a traditional 35-40 hour workweek less than the conventional number of workdays. For example, a full-time employee scheduled for 40 hours per week could work four 10-hour days instead of five 8-hour days. This arrangement can benefit both employers and employees by increasing productivity while reducing stress levels by providing more days off during the week.

JOB SHARING

Job sharing is a flexible work arrangement in which two people work part-time schedules to complete the work one person would do in a single full-time job. The two employees share all responsibilities (including pay) and split the total hours. Each employee typically works half the full-time hours (for example, 20 hours per week).

Job sharing can benefit both employers and employees because it allows companies to retain experienced workers looking for greater work-life balance. Meanwhile, job sharers benefit from having more free time than they would if they worked alone on full-time duties.

It's important to mention that if your firm isn't yet ready for a shift in schedule, you don't have to implement a complete change right away. Try implementing the alternatives, then assess how it worked and determine how to move forward. ■

4 Steps to Successfully Implement and Manage Change in the Workplace

By Clayton Crouch and Carla Caldwell

AS HUMAN BEINGS, it's natural to be averse to change. So it's no surprise that when you introduce new initiatives in the workplace, it can often become a battle for time, attention, and buy-in from employees.

Whether it's starting a workflow, introducing technology or migrating your business to the cloud, inertia often gets in the way of successfully implementing a new routine. This is especially true during tax season, when even the most structured practices have to prioritize urgent tasks that leave no time for new initiatives.

Despite these challenges, change is necessary to stay competitive and efficient, especially as new technologies continue to emerge. Here are four management tips for change that can help you successfully adopt new tools and help your firm thrive.

IT'S NOT JUST ANOTHER NEW INITIATIVE

When thinking about communicating an upcoming change to employees, it's crucial to start by establishing why the change is important in the first place. You want to differentiate the initiative from other optional activities that can be disregarded. This way, your entire firm can embrace the new program despite their busy days and deadlines.

The easiest and most important way to do this is through messaging. If you're rolling out a new technology, for example, make sure to reiterate its potential impacts in all meetings, not just those that are specifically about the tool. You want everyone involved in the process, so position this technology as a priority whenever possible so it permeates your firm's identity.

At smaller practices, it's important when establishing a change not to take your foot off the gas because you think "everyone knows" about upcoming adjustments. At larger firms, you'll want to bring in key players to help you disseminate the information to the full team.

IDENTIFY THE OWNER

From start to finish, all successful initiatives need a distinct owner who can lead the change with authority within your firm. Whether it's a new policy or an application that's being installed on work devices, you need someone to be the face of the operation. Look for someone who can learn the ins and outs of the subject matter, understands the resources available and makes the best decisions for when, where and how to implement change.

This person should become synonymous with the initiative, and be prepared to act as a liaison between employees, management, and any third-party vendors involved. Over time, they can coach fellow employees to create redundancy for the times they are unavailable.

ACCEPT THE HICCUPS

Just because your initiative is being prioritized and you have a dedicated owner doesn't mean problems won't arise along the way. The reality is that with any change there will be hiccups that are not anticipated, and responding to them promptly is another piece of change management. During these times, remember that not everything is going to be done exactly the way you would do it and that even with specific processes in place, everyone does things differently.

There will always be pitfalls throughout any project, so make sure to schedule check-ins so that all necessary parties are communicating, and empower your project owner to have the authority and tools to address each situation individually.

CELEBRATE ACHIEVEMENTS ALONG THE WAY

One of the most overlooked pieces of successful change management is the importance of celebrating your wins. As accounting practitioners, it's often "off we go" when moving onto the next step of a project. As busy people, it's easy to forget to celebrate achievements and recognize the individuals who contributed to a new service or application. But taking a moment to be thankful and express gratitude for the work is key to keeping spirits high and the ball rolling.

Not everyone needs to give a speech at every milestone, but remember to stop and celebrate what the team has accomplished.

INTEGRATING NEW IDEAS

Even with the most adaptable of employees, change management takes time, dedication and, above all, repetition. As technology changes along with staffing and the rise of remote work, these skills will benefit firms of all shapes and sizes.

It takes practice, but approaching change as a positive force rather than an insurmountable task will ultimately lead to more efficiency and better outcomes for your employees, clients, and practice. ■

Clayton Crouch, MBA is an Intuit Senior Solution Specialist who helps tax and accounting firms understand and implement the right solutions based on their needs. Carla Caldwell runs Caldwell Consulting & Training, LLC, which strategically guides accounting teams to become modern practices.

Converting an S Corp to a C Corp

By Nellie Akalp

MANY FACTORS DETERMINE what kind of business structure your clients choose when starting their businesses. But whatever structure your clients launched with, at some point, for various reasons, changing structures may become a valid consideration. Although typically, clients choose to convert from a C Corp to an S Corp to avoid the C Corp's double taxation, there are reasons to convert in the opposite direction. Here's more to know about S Corp to C Corp entity conversions so you can help your clients make an informed decision.

WHY A C CORP?

Your C Corp clients likely went in that direction for the liability protections and 21% flat tax rate inherent with the C Corp legal entity. Once a C Corp registers with the state, it is considered a separate legal entity with independent financial and legal responsibilities. C Corp owners are employees/shareholders and receive salaries and dividends when (and if) dividend profits are distributed. Owners are not responsible for the corporation's financial debts and legal liabilities as employees.

In addition, the Tax Cuts and Jobs Act of 2018 reduced the corporate tax rate to a flat 21%, which makes it attractive for some companies, although organizational requirements may seem cumbersome. A C Corp must have an elected board of directors responsible for all critical business decisions. Also, a C Corp must file articles of incorporation and bylaws with the state, meet regularly, keep shareholder board minutes, and comply with the Secretary of State's requirements for C Corps in each state where they conduct business.

Tax considerations also make C Corps stand apart from other legal structures. Because the corporation is a separate legal entity from the owners, the C Corp is responsible for filing and paying its own taxes. Then the owners pay taxes on their salaries and dividends, causing "double taxation." Some companies prefer to file taxes as an S Corp to avoid double taxation.

WHY AN S CORP?

An S Corp is a "pass-through entity" under Subchapter S of the Internal Revenue Code. S Corps, therefore, are not separate taxable entities; the profits and losses are "passed-through" and reported on the personal tax returns of shareholders.

Generally, an S Corp is exempt from paying federal income tax other than taxes on some capital gains and passive income. S Corp shareholders can save on taxes by dividing income into wages and dividends. Also, the business owner/employee must pay Social Security and Medicare taxes. Your clients who are employees of S Corps are only responsible for part of these taxes, and the company pays the balance. However, when your clients organize as an S Corp, they have the flexibility to classify some of the business's income as salary and some as dividend distribution. That means your clients will still be subject to self-employment taxes on the wage portion of their income but pay only income tax on the dividend portion. Depending on how they divide their income, filing as an S Corp could save your clients a significant amount on self-employment taxes.

WHY CONVERT TO A C CORP?

Typically, S Corp business owners converting to a C Corp tax status do so because their companies no longer meet IRS requirements for an S Corp.

Qualifications for the S Corp election include:

- The company must file Form 2553, Election by a Small Business Corporation, promptly—no more than two months and 15 days after the beginning of the tax year. S Corp status will begin the next calendar year if the business misses the deadline.
- Tax Form 2553 must be signed by all shareholders
- The company must be filed as a U.S. corporation
- Can maintain only one class of stock
- Limited to 100 shareholders or less
- Shareholders must be individuals, estates, or certain qualified trusts
- Requires each shareholder to have a U.S. Social Security number
- All shareholders must be U.S. citizens
- The corporation must have a tax year ending on December 31

Consequently, if any of these requirements are not met, your clients must convert the company's tax status. For example, your clients may want to bring on more than 100 shareholders, shareholders who are not U.S. citizens, or offer different kinds of stock. C Corps do not have limitations on the type of stock offered, the number of shareholders, or on the citizenship of shareholders.

Another reason for conversion is that the IRS tends to keep a close eye on S Corp returns, as the possibility for abuse is high. Business owners must be careful to portion themselves a "reasonable salary" consistent with position and responsibility—and not hide from payroll taxes by issuing excessive dividends.

CONVERTING THE S CORP TO A C CORP

Fortunately, your clients can convert their S Corp to a C Corp at any time and with relative ease. The business must submit a "statement of revocation" to the state service center where their annual return is filed.

The revocation statement must state that the company wishes to revoke the election made under Section 1362(a). In addition, the statement should include:

- Name of the shareholder(s)
- Address of the shareholder(s)
- Federal Tax ID Number of the corporation
- Social Security numbers of the shareholder(s)
- The number of shares of stock owned by the shareholder(s)
- The date (or dates) on which the stock was acquired
- The name of the S Corp
- The effective date of the revocation (or prospective date)

Finally, the statement must be signed by all shareholders who own more than 50% of the corporation's issued and outstanding stock (whether the shares are voting or non-voting).

To have the conversion take effect on the first day of the company's taxable year, your clients must submit the statement by the 15th day of the third month of the tax year, in other words, by March 15.

Entity conversions may seem like a complex decision for your clients; however, with your expertise and advice, the process can be accomplished seamlessly and win you a client for life. ■

Nellie Akalp is the CEO of CorpNet.com, a resource and service provider for business incorporation, LLC filings, and corporate compliance services in all 50 states. CorpNet recently launched a partner program for accountants, lawyers, and business professionals to help them serve their clients.

Change is Hard

GARRETT WAGNER, CPA
CEO/Founder, C3 Evolution Group
garrett.wagner@cpapracticeadvisor.com

IF WE CAN all agree on just one small detail after the past few years, it may simply be that change is hard. It doesn't matter if that change is planned on, desired, or force upon us, change in any shape or fashion is hard to do both at the individual level and at the organizational level. As a profession, we have been called many things when it comes to our pace of change: slow, stuck in the past, old-fashioned, or my favorite, inexorable.

AVOIDING CHANGE

No matter what you call it, accountants' actions are governed by the old saying: If it ain't broke, don't fix it.

According to Wikipedia, this phrase originated in the early 1970s, and was popularized by Bert Lance, who was the director of the Office of Management and Budget under President Jimmy Carter.

Lance believed like many accountants that the secret to success was to avoid change; you know he would have been a huge friend of SALY too. Under this mantra, you avoid change on most occasions under the view that you will have more success doing the same thing as the day before versus adapting to the challenge tomorrow brings.

AVOIDING HARM

Now while Lance's saying has gotten a lot of attention and certainly could be a rallying cry for accountants, another famous saying should be getting our attention in these modern times. U.S. Navy Rear Admiral Grace Hopper has been credited with the most dangerous phrase in the English language: "We've always done it this way."

Think about that for a minute. While Lance's phrase is easy, Hopper hits the nail on the head. She recognized in her brilliance that while change is hard and difficult, it is unavoidable. While we may wish for things to stay the same and for tomorrow to be like today, the truth is that the world, our lives, our clients, our schedule change each day. That is one of the undeniable truths of existence, tomorrow will be different than today. Before we run away from the idea of change, we need to acknowledge that one of the main reasons most people avoid change is due to fear. Fear of the unknown, fear of doing things differently, and fear that what we change may not make things better.

FEAR

You see, one of the things that Hopper understood which eluded Lance, was that despite our fears, change isn't about always having the right answer. Change is about adapting to the world around us and having the courage and strength to try something different. In addition to being a rear admiral, Hopper was a computer scientist and her career is filled with tales of her innovation, adapting, and breakthroughs. She was not without fear and caution, but she was always looking to solve that next problem in her work, and that is the core principle we see in her famous saying, that push to overcome fear of failure and reach for success.

BABY STEPS

As we move closer to yet another year, we need to leave old Lance's mindset in the past and realize the future is coming no matter what. But this doesn't mean we need to overwhelm ourselves; instead we can take it slow. You see, change doesn't mean massive broad sweeping change, change can simply mean one small change to get started on the path. Instead of getting all excited by this article and deciding to change everything and then feeling overwhelmed, take a step back and try this instead.

Write down five things that you want/should change right now. Now instead of tackling the hardest or the most impactful first, I want you to do something different. Look at your list and pick the one that will be the easiest change to make. Allow yourself an easy win, an easier fear to overcome and then build upon that success.

POSSIBILITY

While accounting as a whole may not be broken, one thing is clear, it is undergoing major change in all aspects. We cannot allow ourselves to bury our heads in the sand any longer with our buddy Lance. We need to do something different tomorrow than we have done today, because what other choice do we have? We can overcome our fears, and if we start small we can build upon our success at making change happen and stop being afraid. Just image if you were not struggling today with all the challenges you are faced with, because you had already been adapting to the future. ■

REVIEW YOUR EXEMPT EMPLOYEES: Manager and Supervisor Pay

RICHARD D. ALANIZ
Senior Partner
Alaniz Schraeder Linker Faris Mayes, L.L.P.
ralaniz@alaniz-schraeder.com

THE FAIR LABOR Standards Act (FLSA) is the federal law governing employee compensation in U.S. workplaces. Some states also apply their own, more rigorous wage and hour laws. The FLSA requires employers to pay employees a minimum wage for all hours worked and a time-and-a-half overtime rate for all hours worked over 40 in a workweek.

However, the FLSA provides certain exemptions from minimum wage and overtime requirements. The so-called "white collar" exemptions to minimum wage and overtime requirements refer to the executive, administrative, professional, computer, and outside sales exemptions. To qualify an exemption, employees must receive a predetermined salary not subject to reduction based on hours worked or quality of work, and the salary must meet the minimum FLSA threshold of $684 per week or $35,568 annually. In addition, employees must satisfy duties tests set out by the FLSA to fit into one of the exemptions.

- To qualify for the **executive exemption**, which covers most managers and supervisors, an employee's primary duty must be management of the enterprise or a recognized subdivision or department thereof. The fundamental requirement is that the employee must regularly direct the work of two or more subordinate employees.
- The **administrative exemption** covers many office managers, financial consultants, sales directors, production planners, inspectors, insurance agents, and human resources employees and requires an employee's primary duty be office or non-manual work directly related to management or general business operations. In particular, the duties must include the exercise of discretion and independent judgment regarding matters of significance.
- The **professional exemption** can be broken up into two categories – learned professionals and creative professionals. Learned professionals' primary duty must involve advanced knowledge in a specialized field of science or learning, generally acquired through prolonged study – often a college degree. Engineers, pharmacists, medical technologists, nurses, dental hygienists, physician assistants, and accountants are common examples. Creative professionals include editorial writers, journalists, graphic artists, actors, and artistic painters.
- The **computer employee exemption** generally excludes IT support employees who install and maintain workstation software and similar functions. The exemption requires both theoretical and practical knowledge in systems analysis, programming, or software engineering and duties that consist generally of designing, testing, and/or implementing software or hardware systems. While the same minimum salary of $684 per week is required if paid on a salary basis, the FLSA also permits payment of an hourly rate of at least $27.63 per hour to qualify.
- In addition to a duties test, common among each white collar exemption, the **outside sales exemption** requires a location test. However, in contrast to the other exemptions, it requires no minimum salary. As the name suggests, to qualify, an employee's primary duty must be making sales away from the employer's place or places of business, which of course excludes inside sales employees, unless they qualify separately for the executive or administrative exemption.

The DOL has raised the salary threshold numerous times over the years in response to economic conditions. The most recent increase in the minimum salary became effective on January 1, 2020, rising from $455.00 per week ($23,660 annually) to $684.00 per week ($35,568 annually). In 2016, the Obama administration proposed an increase from $455.00 per week to $913.00 per week ($47,476 annually).

Numerous business associations, as well as a number of states immediately challenged this proposal in federal court. The court blocked implementation of the Obama administration's proposed increase, and it remained blocked until the Trump administration withdrew it. It is estimated that if the Obama proposal had gone into effect four to five million more workers would have become overtime eligible.

The Biden administration announced several months ago that it plans to issue a proposed increase in the salary threshold in October 2022. If the increase proposed during the Obama administration is any guide, we may see a near doubling of the current $684.00 per week to about $1,300.00 per week. Many small and even medium-sized employers may struggle to afford such a dramatic increase, with as many as 10 million workers becoming entitled to overtime pay if the FLSA's salary threshold doubles. Whatever the increase turns out to be, its implementation will almost certainly be delayed by court challenges.

Nonetheless, now is the time for employers to carefully review the specific duties and number of hours worked each week by their exempt-classified employees. A thorough review can confirm whether the employee's primary duties are sufficient for exempt status. Unfortunately, misclassification is a common problem that can create substantial liability.

Reviewing the hours worked will also help determine whether an exempt position requires more than 40 hours, such that converting it from salaried to hourly may not result in a difference in cost due to the need to pay substantial overtime. This review could also help confirm whether a consolidation of exempt duties and/or positions could be an option.

Beyond additional overtime costs, employers should consider the effect on employee morale and productivity if an employee's position is reclassified from salaried to hourly. A supervisor who rose through the ranks of hourly jobs to ultimately become a salaried supervisor may see going back to an hourly position as a demotion.

Since an increase in the salary threshold, perhaps a substantial one, is virtually certain, even if delayed by court action, these are the types of issues that proactive employers should be seriously considering in anticipation of any salary threshold increase. ■

Intuit Tax Advisor Delivers Innovative Tax Planning and Tax Strategies

HAVING HELPFUL, ALWAYS-ON tools to give your clients the information they need to make more-informed decisions is a key component of delivering advisory services to your clients. With the new Intuit Tax Advisor (ITA), the process is easier than ever—and right at your fingertips.

Thanks to the seamless integration between ITA and Intuit ProConnect Tax and Lacerte Tax, you'll get vital insights and strategies to help your clients. Bringing tax prep and advisor tools under one roof, ITA allows you to create personalized tax planning that offers value-added services to your clients, including tax savings and powerful, straightforward reports.

"When more and more people are in need of advisory services to help them make significant financial decisions, ITA can help tax professionals differentiate their services and power prosperity with industry-leading change," said Barry Pennett, senior vice president and general manager of Intuit ProConnect Group. "There is a clear need and appetite for creating more value for clients and firms, and ITA is designed to do just that."

To get a sense of the value and impact this tool can have, here are some of the biggest benefits regarding ITA.

AUTOMATED DATA + POWERFUL INTEGRATION = TIME SAVINGS AND ACCURATE TAX PROJECTIONS

With the integration between Lacerte and ProConnect Tax, client data is automatically mined to bring significant time savings to your practice and more accurate tax projections for your clients. In the process, all legislated tax law updates are incorporated into the software's planning and projections, with built-in compliance.

All of this not only reduces audit risk, but also eliminates the time it takes to perform cumbersome tasks that keep you from helping your clients run and grow their businesses.

"Based on customer feedback, we designed Intuit Tax Advisor to help advisors save time and scale their planning services to more of their staff," said Jorge Olavarrieta, vice president of product management and design at Intuit ProConnect Group. "Tax professionals can simplify proactive tax planning and advisory services with ITA to replace the current process of cobbling together tax planners, spreadsheets, and reporting applications."

PERSONALIZED TAX PLANNING STRATEGIES

Packed inside ITA is an endless number of strategies that can take your practice—and your clients—to the next level.

For example, ITA gives you hundreds of potential triggers in your clients' tax data that show smart strategies for you to implement for your clients. Whether you choose to use them or dismiss them is your call, but you can also create your own strategy in minutes, and save and modify your strategies at any time. In addition, you can try different tax scenarios to see their implications, as well as explore the ITA's library of strategies, where you can plug and play everything from hiring your kids to 401(k) contributions.

CUSTOMIZABLE, CLIENT-FRIENDLY REPORTS

As you gather these recommended tax strategies and estimated tax savings projections for your clients, they will be automatically populated in a customizable, client-friendly report for you to share with your clients. This allows you to illustrate your personalized tax planning strategies and estimated savings plan for them, turning something complex into something easy to understand.

Before sending out the report, you can customize it in a professional way with your firm brand. Choose logos and colors that represent your practice, and update it year-round as things change or you're feeling creative.

SIMPLE PRICING

When it comes to pricing for ITA, it's simple. To start generating custom tax plans for a client, customers just need to purchase a client credit. One client credit equals unlimited tax plans for that client within a calendar year. Customers are eligible to reserve three free client credits.

MORE RESOURCES TO GET YOU STARTED

ITA is a win-win for you and your clients. With ITA, you get the foundation to offer transformational tax advisory services that help your clients save time, save money, and strategize for long-term growth. In doing so, these value-added services will boost profits and productivity for your practice, while also bringing measurable savings and more accurate planning to your clients.

To check out the new tax advisory resources library for a step-by-step guide to offer tax advisory in your practice, visit https://intuit.me/3EobAjh. And for more information on Intuit Tax Advisor, visit https://tinyurl.com/3pcm267n. ■

CYBER INSURANCE FOR ACCOUNTING FIRMS:
Coverage Options and Provider Expectations

By Stan Sterna, J.D.

CYBER INCIDENTS CONTINUED their upward trajectory in 2022 – once again breaking records and setting the stage for an even more active 2023, with geopolitical events contributing to an already heightened threat level. And in this environment, CPA firms – which accelerated their digital transformation during the pandemic – are particularly vulnerable to an attack.

The motivation and rationale behind a cyber criminal can vary, from securing ransom payments to selling confidential data on the dark web. This fluid environment is challenging firms to sharpen their focus on not just creating, but also continually enhancing, their security strategy – and considering securing cyber insurance coverage.

TARGETING CPAS

In recent years, hackers have been shifting their focus – moving beyond just the big name, headline-making targets that were synonymous with breaches in the past, to focusing on smaller, "under the radar" victims. For example, based on emerging patterns, it seems like some cyber criminals may be avoiding larger organizations for ransomware attacks so they don't evoke national political or law enforcement response.

According to Sherry Bambrick, senior underwriter for the AICPA Member Insurance Programs, this evolving strategy has serious implications for CPAs.

"Hackers have always found CPA firms particularly attractive because they are, in essence, aggregators of data - both financial and PII or personal identifiable information," Bambrick said. "This trending focus on smaller organizations, coupled with the level of PII a firm potentially holds, quite simply increases the risk they face."

Beyond the data, hackers also tend to target CPA firms because they frequently have access to client funds. Cyber criminals may also assume that mid-size and smaller firms do not have strong information security preparedness strategies in place because their leaders believe they are too small to be targeted.

COMPLYING WITH INSURERS' EXPECTATIONS

Many insurers are demanding more from firms in terms of cyber resilience, so firms should expect rigorous questioning about their cybersecurity protocol when they seek coverage.

It's not unusual for an insurer to review a firm's cybersecurity efforts in a few key areas. In general, insurers review whether a firm is:

SOFTWARE

- Installing patches within 30 days of release.
- Tagging external emails to alert employees that the message originated from outside the organization.
- Implementing software to help protect against phishing messages.
- Utilizing web filtering to block access to known malicious websites.

CLASSIFYING DATA

- Segmenting network based on the classification level of information stored on its systems.

SYSTEMS

- Confirming it does not utilize any end-of-life operating systems or platforms (those being phased out by the manufacturer and no longer receiving security patches). This includes systems using an extended service contract from the manufacturer.
- Utilizing an advanced endpoint detection and response (EDR) tool on all endpoints and servers. EDR tools proactively address threats after they have penetrated an organization's endpoints, but before they cause damage.
- Having a process to decommission unused systems.

TRAINING & TESTING

- Conducting regular security awareness training and penetration testing.
- Ensuring access to information and resources is only provided to employees who need it for a legitimate purpose.
- Require multi-factor authentication for:
  - Remote access to the network, including web-based email
  - To protect privileged user accounts
  - For all cloud resources like Office365
  - For all remote desktop protocol (RDP)
  - Virtual desktop instances (VDI) accessible from the internet

BACKUPS & SECURITY PLANNING

- Taking the following steps to help protect data from ransomware:
  - Perform full and incremental backups of business data regularly.
  - Test backups for restorability.
  - Ensure backups are stored physically offsite.Ensure backups are stored offline to safeguard from infection.
  - Put in place an annually-tested incident response plan that includes the ability to quickly contain an incident.
  - Have formal, annually-tested disaster recovery and business continuity plans.
  - Implement a formal vendor management program that inventories and classifies the type of data and level of access each vendor has.

Reviewing these areas before any discussions with an insurer can help facilitate the process of securing cyber coverage. ■

Stan Sterna is a vice president with Aon Insurance Services, the broker and national administrator for the AICPA Member Insurance Programs, the nation's largest professional liability program for CPAs and the pioneer of cyber coverage for CPAs.

Data Security: What Could Go Wrong?

By Christopher Stark

THE REALITY IS, when it comes to data security, zero risk does not exist. There is nothing on the market today that can 100% protect you from a cyberattack unless you completely disconnect yourself from the internet.

In 2021, IBM reported that the average size of a data breach is 25,575 records, with each record costing the company $165 on average, and the total cost to a company averaging over $4.24 million. It is critical that firms implement proactive IT strategies using a multifaceted approach to protect data. Before we dig into the preventative strategies to combat threats, we need to understand what methods cyber criminals are taking to try and penetrate systems.

WHAT'S THE CYBER CRIMINAL'S END GAME?

Cyber criminals have countless reprehensible methods of conducting cybercrime, as noted below:

- **Send out phishing emails.** A phishing scam is when a bad actor sends an email which appears to be from a reliable source. The hacker asks for personal identifying information, then uses the information to access existing accounts or open new accounts.
- **Collect personal information.** The cyber criminal's goal is to gather personal information to be used for other types of identity theft such as credit card or insurance fraud.
- **Infect a computer with ransomware.** The cyber criminal infects a computer with malicious malware which prevents access to files, systems, or networks, and requires payment of a ransom for their return.
- **Access further accounts within an organization.** Account takeovers can morph from a personal attack on a singular computer as an entry to compromise an entire system or network.

The threat of account takeovers continues to evolve as the scenarios cyber criminals use to gain access to victim's accounts also evolve. It is important for C-suite executives and tech experts to understand their cybersecurity vulnerabilities.

WHY WOULD GLOBAL CYBER CRIMINALS TARGET CPA FIRMS?

CPA firms are prime targets because of the sensitive, confidential, financial information accounting firms amass. Hackers target CPA firms for explicit information and then use the data to steal assets, ransom it, or sell the data to the highest bidder.

- **Obtain confidential, personal data.** Cyber criminals seek client data from CPA firms such as birthdays, Social Security numbers, and other personal information. The data is used to target and steal from specific clients or to sell the data to other criminals who specialize in identity theft.
- **Attain financial information.** Cyberattacks on accounting firms seek specific account numbers, tax records, credit card information, and employee identification numbers.
- **Gain tax records.** Cyber criminals file fraudulent tax returns from information obtained from CPA firms. They steal tax returns and use the information for additional identity theft.

HOW TO MINIMIZE YOUR RISK OF A CYBERATTACK

CPA firms, regardless of size, must have vigorous cybersecurity protections in place. The risk of cyberattacks is disproportionally higher for smaller and medium-sized organizations, which tend to be much more reactive than proactive. Below are steps to help protect you from possible cyberattacks:

- **Have a good backup strategy.** Hackers tend to go for your backups first, making you more vulnerable during the attack. Firms should have multiple backups using different technologies and be physically removed from the network, so in case of a malware infection, the backup data does not become infected.
- **Implement multifactor authentication for everything.** By requiring multiple login factors to prove your identity, you can drastically reduce the chance of unauthorized access.
- **Train employees about cybersecurity risks.** Educating employees about cybercrime such as phishing, malware, and ransomware attacks is an effective strategy. CPA firms should create a culture of consistent security awareness to reduce the risk of cybersecurity breaches caused by human errors.
- **Use Advanced Threat Prevent Technologies.** Leverage Next Generation Antivirus (NGAV), Endpoint Telemetry Data, DNS Filtering, Intrusion Prevention Systems, Reputation Based Threat Prevention, Data Encryption – the more the better! These technologies learn users' habits and daily activities using behavioral detection, machine learning algorithms, and exploit mitigation so known and unknown threats can be anticipated, blocked, and immediately prevented.
- **Patch all systems.** Focus on patching any and all known, exploitable vulnerabilities.
- **Store data and information in encrypted databases.** Storing data in an encrypted database can deter cyber criminals from accessing the information.
- **Prepare your organization.** Have a cyber incident response and business continuity plan ready so as to ensure critical functions and operations can remain running if technology systems are disrupted. If your IT systems go down, how will day-to-day account management and communication continue with personnel and clients? Make sure important contacts are up to date and test it regularly!

Accounting firms are prime targets for cybercrime for specific reasons due to all the sensitive, confidential, and potentially lucrative information they have in their systems.

HOW CPA FIRMS CAN SHIFT THEIR RISK

Accounting firms have significant responsibilities to protect client information from potential cybercriminals. Adhering to the Cybersecurity & Infrastructure Security Agency (CISA) guidelines is an important, proactive plan for CPA firms. More specific cybersecurity strategies are examined below:

- **Review cybersecurity insurance.** C-suite executives should determine if specific cybercrime insurance coverage includes state-sponsored cyberattacks such as what might be initiated by outside threats. Check for first-party versus third-party insurance coverage, ransomware coverage, and employ an attorney who understands cybersecurity review your cyber insurance coverage.
- **Encourage a "security mindset" in employees.** Require multifactor authentication, training on data security policies and procedures, and remind personnel that phishing is still the most common cyberattack modality.
- **Enlist the help of IT security professionals.** Engage with cybersecurity experts who can help reduce your level of risk through deploying stronger security technologies, preventative solutions, help guide and enforce evolving security best practices. Having a cybersecurity team available 24/7/365 monitoring threats is a great peace of mind.

At the end of the day, cyberattacks can have a detrimental impact on firms. Don't wait until it's too late to develop an effective data security plan. ■

Christopher Stark is president & CEO of Cetrom.

9 TIPS to Thwart Cyber Thieves Coming For Your Firm's Data

By Jason Bramwell

IT HAS BEEN more than two years since the coronavirus pandemic forced accountants to leave their work cubicles behind for their new home away from home—which was, well, their homes. And even though many public accounting firms and corporate accounting and finance departments are starting to make their employees come back to the office and become familiar with their cubicles again, a lot of these same companies are continuing to allow their staffs to work from home two or three days a week under a hybrid work model—and others have gone the remote route permanently.

But the continued remote work environment has cyber criminals licking their chops, as they look to exploit vulnerabilities in companies' security infrastructures and target employees through phishing emails and other schemes in order to gain access to their login information.

"When you move to remote work, anything that was a potential weakness in your internal control system or your security architecture or your cybersecurity plan now becomes completely apparent; that's when it becomes abundantly clear that you have gaps, either on the functional side or on the security side," Darren Guccione, CEO and co-founder of Keeper Security Inc., said during a recent webinar (https://tinyurl.com/2epr7t96). "Because at the start of it, cyber criminals are always looking for ways to capture login credentials. One of the easiest and lowest technology methods of stealing login credentials is through a phishing attack."

According to a 2022 survey of C-suite leaders by HelpSystems, 29% of respondents cited business email compromise or phishing as their greatest concern, but 43% said the biggest danger to their company and data is ransomware or malware designed to steal data or extort money.

RANSOMWARE REARS ITS UGLY HEAD

After getting an employee's login credentials, cyber criminals can move within a network to find sensitive data, such as financial accounts and

client information. That data can then be sold to identity thieves on the dark web or held for ransom against the victimized firm.

A ransom cyber incident was brought to light recently when two accounting firms were among several victims of a large-scale computer hacking scheme in the United States conducted by three Iranians between October 2020 and August 2022. The three men now face federal charges of conspiracy to commit fraud, intentional damage to computers, and transmitting demands, according to an indictment unsealed in September.

In one instance, the hackers launched an encryption attack last February and March, causing a New Jersey accounting firm's network to connect with their server. The cyber criminals demanded a ransom of $50,000 and allegedly told the firm, "If you don't want to pay, I can sell your data on the black market. This choice is yours." It is unknown whether the accounting firm paid the ransom, but federal authorities said some of the victims did pay ransoms, while others contacted the FBI or local law enforcement.

According to Verizon (https://tinyurl.com/2pajax4c), the average cost of a data breach for companies increased to $21,659 per incident last year, with most incidents ranging from as little as $800 to more than $650,000. But 5% of successful ransomware, phishing, and other attacks cost businesses $1 million or more.

Ransomware breaches increased by 13% within the last year—representing a jump greater than the past five years combined, according to a 2022 report from Verizon. In addition, external bad actors are approximately four times more likely to cause breaches in an organization than internal personnel.

The Verizon report also revealed that people are the weakest link in an organization's cybersecurity defenses. When you include human errors and misuse of privilege, the human element accounts for 82% of analyzed breaches over the past year, rather than cyber thieves exploiting flaws in computer systems.

In addition, cyber criminals have used the pandemic as an opportunity to capitalize on people's strong interest in coronavirus-related news by luring people to fake malicious websites, clicking on malicious links, or providing personal information online or over the phone under the guise of COVID-19. Many of these scams attempt to impersonate legitimate organizations, such as the Center for Disease Control or the World Health Organization, by offering fake informational updates and even promises of access to vaccines—all for a price. These so-called social engineering attacks accounted for 25% of total breaches in 2022, according to Verizon.

"When there is a mass amount of movement or migration to remote work environments and a greater number of endpoints, as well as a greater level of anxiety, this is as much about the physical and the psychological as it is about just general architecture. It involves everything," Guccione said. "There's a state of panic, there's a state of uncertainty, there's transitioning—there's so much going on that cyber criminals really gravitate toward situations like this because they always want to attack the lowest-hanging fruit and any companies they view as a potential weakness."

MOST COMMON ENTRY POINTS FOR CYBERATTACKS

Changes in information technology infrastructure brought about by remote work, such as a move to cloud solutions, has shifted the focus of cyberattacks, according to a new report from Hiscox and Atlas VPN.

Cloud servers is now the No. 1 way in for cyberattacks, with 41% of companies reporting it as the first point of entry—a 10% increase from the year before. Cloud servers has replaced corporate-owned servers, which was the leading attack entry point, or vector, in 2021.

Corporate-owned servers now occupies the third spot on the list, according to the report, with 37% of businesses reporting this as the main cyberattack entry method. Meanwhile, the second spot now belongs to business emails, as 40% of companies named it the main access point for attackers.

"If you get a spam email or an email that looks legit but is asking you to do something like upload some information or change a password or even transfer funds, make sure you have a policy in place to make a verbal verification for that," according to Bobby Garrett, IT director at CPA firm Gray, Gray & Gray. "No client is going to be upset if you call them and say, 'Did you really want me to transfer $10,000 to this account?' Because if you do it and you don't call, they are going to be upset if it's not a real request because there's no getting that money back. It'll be gone."

Employee-owned mobile devices are another common entry point for cyberattacks at 29%, an increase of 6% from the previous year, according to the Hiscox and Atlas VPN report. Others include remote access servers at 31% and distributed denial of service (DDoS) attacks at 26%.

"When we all go remote, a lot of traditional internal control policies become less effective and they become dilutive when it comes to exploiting or capturing security vulnerabilities," Guccione said. "And so now as we all move to this much larger endpoint landscape and geometry, we now have to figure out, well, what do we need to do to make sure that we're tracking and monitoring every endpoint—smartphone, tablet, computer—across every employee in the organization? What can we do to track that down and make sure that on the prevention side of cybersecurity that we're doing what we need to do to protect our environment?"

STRATEGIES FOR SECURING DATA WHILE WORKING REMOTELY

In the two and a half years since the pandemic began in the U.S., companies have been able to fine-tune their cybersecurity processes for remote workers. But the continued number of cyberattacks in the U.S. means IT professionals cannot let their guard down—and neither can a firm's employees.

The following are best practices compiled from articles, reports, and webinars on how to reduce the risk of a data breach in a remote work environment. (Note: This is not an all-inclusive list and the best practices are not numbered in terms of importance.)

1. **Ensure you have a modern cybersecurity plan that covers remote work environments:** Firms need to make sure endpoint security and enterprise password security software is running on all employee devices, Guccione said.

"We know password security is the trojan horse into your business. So at the end of the day, you could have the best antivirus protection and you could have the best privileged access management system running, but if you do not put a cloak of armor around your password security and your password internal controls and enforcement policies, you are in real serious trouble because this is where the cyber criminals know exists the lowest-hanging fruit. This is where it's at," he added.

2. **Use a Wi-Fi password:** But do not use the default password, Jim Bourke, a partner at CPA firm Withum and managing director of the firm's Advisory Services practice, said in a video for the American Institute of CPAs.

"If you're using the default password on your Wi-Fi device, change the default password. Go into your Admin settings and make that change," he said.

Bourke also recommends changing your service set identifier (SSID). "What is your SSID? That is your

Wi-Fi network name. So change your SSID, make it generic. It will be less likely to be hacked," he said.

3. Install antivirus and internet security software at home: One of the most common—and effective—security strategies for working from home is to invest in a comprehensive antivirus suite for your company and your employees.

Antivirus suites offer automatic remote work security against a host of threats, including:

- Zero-day attacks (viruses taking advantage of security gaps before they are patched);
- Malware, spyware, and viruses;
- Trojans and worms; and
- Phishing schemes, including those sent via email.

Nowadays, comprehensive antivirus and internet security software automatically updates itself to stay on top of new and emerging threats.

4. Use a VPN: Virtual private networks (VPNs) add an extra layer of protection to internet use from home. They cannot on their own be relied upon to prevent cyberattacks, but they can be a useful barrier against one.

According to antivirus provider Kaspersky, VPN security can be enhanced by using the most robust possible authentication method. Many VPNs use a username and password, but firms might want to think about upgrading to the use of smart cards. Companies can also enhance their encryption method for VPN access, for example, by upgrading from a Point-to-Point Tunneling Protocol to a Layer Two Tunneling Protocol.

But no matter how strong your VPN is, if an employee's password is compromised, it will give hackers an easy way in. So Kaspersky recommends that employees update their passwords regularly. Employees should also be reminded to only use the VPN when they need it, switching it off if they are on their work devices for personal use in the evenings or on weekends.

5. Define clear procedures for reporting and responding to security incidents: "This is so important because if everyone is remote and there's an anomaly or an incident with somebody's email system or somebody in your organization believes that there's been a breach, you want to make sure that they have a well-defined incident response plan so that they can identify, mitigate, and reduce the cost of the cyberattack," Guccione said. "Most importantly, we want to make sure that every person in the organization knows what to do if they think there's been a breach. They need to know who to report it to, how to report it, and what to do. So making sure that you have this plan in place is of paramount importance."

6. Set up two-factor or multifactor authentication: By now, we've all used two-factor or multifactor authentication when logging into something, whether on work computers or mobile devices. Cybersecurity experts say it is an effective and fairly easy-to-understand extra layer of security.

When used with single sign-on solutions, multifactor authentication makes logging in easier because it allows users to pass through many security measures at once.

"When you sit in front of a system that's protected with multifactor authentication, you present a username and password—something you know—and then you provide a PIN from a security token—something you have. This can be a hard token, a soft token, or a smart card," Steve Tcherchian, chief product officer and chief information security officer at XYPRO Technology, said during a webinar. "If you don't have that token, you won't have that PIN. And that PIN, in most cases, will rotate every 30 seconds. So even if your username and password were stolen, unless the attacker has that token along with your username and password, what your PIN was at that moment in time, your username and password is useless to them."

7. Make sure critical applications utilize zero knowledge, zero trust, and end-to-end encryption: Zero knowledge is "the premise that only the user of your application has full knowledge of your master password and complete control over and domain of, in terms of ownership, your encryption key that's used to encrypt and decrypt your information," Guccione said.

"When you buy these products, you want to make sure that any encryption or decryption is done client-side, meaning it is done at the client device level. It is not done at the vendor level," he added. "The vendor should never be generating those keys for you, and they should never have the ability to decrypt and view your information. This is really important."

The premise of zero trust is "the idea around privileged access that you want to make sure in a very simple world you can trust, but you always must verify," Guccione said.

"At the end of the day, you should know through event logging and reporting what every single user on your system on every device is doing, what they're accessing, and who they are transacting with," he continued. "And you should have those internal controls, those role policies, those enforcement policies, the reporting, and the logging, and the auditing capability in that ecosystem to make sure you can lock everything down if there is an incident, whether by a rogue employee or an external adverse third party or bad actor. You can lock down that device and make sure that you maintain the integrity of your organization."

End-to-end encryption is really important to have for sensitive information, such as personal identifiable information, business assets like a business plan or a financial model, tax returns, or wiring instructions to a bank account, he said.

"If you're transacting over any type of … application, you want to make sure all of that information is completely encrypted from point A to point B, and that means from one user device to and through the internet, down into that device and into their screen from A to Z. You want to make sure that you practice full end-to-end encryption," Guccione said. "These three things are so critical because they're intrinsic and existential elements of any great productivity and security application."

8. Provide cybersecurity awareness training that includes threats and best practices: Guccione said it is extremely important that every single person in the organization who uses a computing device is trained on things like phishing scams, cybersecurity awareness, the dark web, and credential stuffing attacks. He added that phishing simulations "are one of the best tools that you can utilize in a company to prevent against a password-related data breach."

9. Keep family members away from work devices: Kaspersky recommends reminding your staff to not allow other household members to access their work laptops, mobile devices, and other forms of hardware. They should also be reminded of the importance of password protecting their devices to prevent third parties from accessing sensitive files.

Bourke recommends setting up a separate network in your home for guests. "Do your work under your secure Wi-Fi network that you have in your house, and if you bring guests over, set up a guest network. Guests should use that network and have that password. It keeps things totally separate," he said. ■

Jason Bramwell is senior staff writer for CPA Practice Advisor. He has nearly 25 years of professional writing experience, the last nine covering the accounting profession. He most recently was a staff writer and editor at Going Concern, and he previously spent five years as a staff writer and editor at AccountingWEB. He can be reached by email at jbramwell@cpapracticeadvisor.com.

Boost Firm Efficiency With Proposal Software

By Becky Livingston

IF YOU HAVE spent time writing a client proposal, you know it's not easy. It's downright tedious. You might start from an outline, collect prospect information, and include relevant graphs from various departments. I am here to tell you that there is an easier way.

Rather than manually writing each proposal or taking bits and pieces of Word documents of previously-crafted slide decks and creating new documents, leverage a proposal software tool.

WHY USE PROPOSAL SOFTWARE

In addition to the amount of data you can collect, such as metrics, pipeline views, interactive pricing tables, and more, here are 10 additional benefits:

- Simplifies the sales process
- Speeds up negotiation and objection handling
- Seamlessly collaborates and tracks the process in a CRM
- Updates documents and proposals quickly
- Revives inactive deals
- Grows revenue
- Saves time with templates
- Increases your document hit rate
- Accepts secure and legally-binding electronic signatures
- Sets automatic reminders for clients and prospects

TRIED-AND-TRUE PROPOSAL SOFTWARE TOOLS

HubSpot recently shared its list of favorite proposal software tools. None are free. Each has unique features.

- PandaDoc: easily create customized, on-brand proposals through collaboration tools, integrations with several CRMs, and a content library.
- RFPIO: using artificial intelligence, it suggests responses from your content library that best answers the RFP.
- FastSpring IQ: easily incorporates videos, customer testimonials, and other supporting assets, acting as a modern alternative for lengthy slide decks and PDFs.
- Proposify: easily add different sections to your document, customize a proposal with an InDesign-like editor, add text, images, and videos.
- Venngage: an extensive library of proposal templates with a drag-and-drop editor to create eye-catching proposals in minutes.
- Qwilr: embed interactive content, such as video, maps, interactive dashboards, and Google Sheets, while tracking what people view and click.
- Bidsketch: create proposals by combining sections or using the company's sample proposal language; plus, indicate optional fees to take advantage of upselling and cross-selling opportunities.
- Loopio: pull from your content library to auto-populate a proposal and integrate it with tools, including Salesforce, Microsoft Dynamics 365, Google Drive, OneDrive, Slack, and many more.
- Proposable: use drag-and-drop creation tools, email and SMS notifications, and analytics for a deeper understanding of your sales pipeline.
- RFP360: centralize requests for proposal (RFP) answers in a knowledge library, saving you time and effort by importing RFPs and using AI to suggest responses.
- Prospero: its drag-and-drop interface for images, videos, icons, backgrounds, and texts, plus an easy signature method.

PROPOSAL TABLE OF CONTENTS

PandaDoc provides a sample proposal template that you can download for free. It includes the following sections.

- Cover letter
- Sender/Company Background
- Service(s)Bookkeeping
- Payroll
- Financial Analysis
- Tax Preparation
- Regulatory Compliance
- Financial Consulting
- Pricing
- Acceptance

FINAL TIPS

Hinge Marketing offers these proposal tips for professional services firms:

- Use fewer words
- Organize content for easy skimming
- Never use words when a picture will do, e.g., graphs
- Propose a better way for the client to achieve their goals (versus what they asked for)
- Consider video to capture case studies, client evaluations, or testimonials
- Surprise them with industry research and backup assertions with data
- Offer something extra

When it comes to proposals, do you want to spend time writing them or signing the prospect? Now is the time to invest in a proposal tool that will take your firm to the next level and increase its efficiency. ■

Becky Livingston is the President and CEO of Penheel Marketing, a NJ-based firm specializing in social media and digital marketing for CPAs. Learn more about Becky and her firm at https://Penheel.com.

AICPA News is a round-up of recent announcements from the institute.

AICPA Comments on Tax Provisions in Senate Reconciliation Legislation

The AICPA submitted a letter to Senate Finance Committee and House Ways and Means Committee leadership regarding tax policy issues in the Senate reconciliation legislation released July 27 (the Inflation Reduction Act of 2022). The letter highlights some of the key issues the AICPA has identified, including with regard to:

- Sec. 10101. Corporate Alternative Minimum Tax
- Sec. 10201. Modification of Rules for Partnership Interests Held in Connection with the Performance of Services (Carried Interest)
- Sec. 10301. Enhancement of Internal Revenue Service Resources

The AICPA believes that the Corporate Alternative Minimum Tax proposal contained in Section 10101 violates numerous elements of good tax policy and may result in unintended consequences that must be carefully considered. However, if the tax is enacted, the AICPA recommends that the effective date is delayed until after the later of taxable years beginning after December 31, 2023, or the date Treasury issues proposed regulations to provide taxpayers with the needed time to fully analyze and comply.

While the AICPA is not taking a position on the adoption of the modification of the carried interest rules in Section 10201, should Congress move forward with the carried interest changes, we suggest several technical clarifications or modifications. The suggested changes are outlined in the letter. In its letter, the AICPA urges Congress to commit, in a bipartisan manner, to determine the appropriate level of service necessary for the IRS and provide adequate resources for the agency to meet those goals – either as part of a reconciliation package or in a separate vehicle. ■

AICPA & CIMA RECOGNIZE THREE CPAS FOR WORK IN GOVERNMENT

The AICPA and CIMA have presented **Elaine M. Howle**, CPA, of El Dorado Hills, Calif., with its 2022 Outstanding CPA in Government Career Contribution Award, honoring her dedication to the accounting profession.

The AICPA & CIMA also presented their 2022 Outstanding CPA in Government Impact Award at the state and local level to:

Joseph R. Morrissette, CPA, of Bismarck, N.D., with the 2022 Outstanding CPA in Government Impact Award at the state level.

Charles W. Warren, CPA, CGMA, of Fort Smith, Ark., with the 2022 Outstanding CPA in Government Impact Award at the local level. ■

AICPA ADDRESSES LEVEL OF SERVICE WITH PRACTITIONER PHONE LINE

The AICPA submitted a letter to the Internal Revenue Service (IRS) addressing the plummeting level of service for the Practitioner Priority Service (PPS) telephone line and providing recommendations for improvement. Despite recent efforts by the IRS to ease the burden the backlog has caused for taxpayers and practitioners, the AICPA notes that service levels for the practitioner priority service phone line had been in continuous decline for several years.

The AICPA submitted comments on the specific PPS line challenges and provided suggestions for improving the experience for tax practitioners and IRS customer service representatives in the following areas:

- Power of Attorney (POA) Issues
- Transcripts
- Accounts Management versus Automated Collection System
- General Recommendations

AICPA strongly urges the IRS to consider implementing these recommendations as part of their plan to reduce the backlog and improve services and believe that doing so will have a significant positive impact on services provided by the IRS. ■

AICPA SUBMITS COMMENTS RELATED TO REMOTE WORK

The American Institute of CPAs (AICPA) submitted comments to the Department of the Treasury and the Internal Revenue Service (IRS) requesting updated guidance in several key areas related to employees working remotely and offering recommendations regarding the taxation of payments related to remote work.

The AICPAs comments and recommendations focus on the following areas:

- Principal Place of Business
- Work Arrangements: Employer-Location Based, Remote, and Hybrid Definitions of Employer Location-Based, Remote and Hybrid Work Arrangements to Define Employee's Tax Home
- Facts and Circumstances Test for use in the Classification of a Remote Employee and Defining a Hybrid Employee's Tax Home
- Safe Harbor for Use in Defining a Remote Worker
- Employee-Employer Arrangement
- Pursuit of a Trade or Business
- Non-Travel Expenses Incurred While Working Remotely
- Examples

As a result of the pandemic, many companies are redefining their respective work structures – while some are moving to fully remote, others are offering their employees a hybrid structure. Many employees prefer the work-from-home format, particularly as it relates to commuting. Additionally, many employers recognize the increased productivity and note the value of decreased office maintenance costs. Many revenue rulings and interpretations of case law are outdated, which creates unnecessary confusion and stress. ■

SANDRA WILEY
President, Boomer Consulting, Inc.
sandra.wiley@cpapracticeadvisor.com

Exploring New Roles and Positions in Your Firm

A COMMON COMPLAINT from firm leaders these days is, "We can't find any CPAs to hire!"

If you're in that boat, I wish I had a quick fix for you. But the truth is that there's a shortage of CPAs and CPA candidates, and the situation isn't going to improve anytime soon.

THE CPA SHORTAGE

Fewer college students are pursuing accounting degrees, and those who do aren't necessarily interested in working in a CPA firm or pursuing a CPA license.

Among accounting graduates who do not plan to become CPAs, the top reasons for not pursuing the credential include not seeing value or relevance to their careers (32%) and not seeing the return on investment (28%).

Meanwhile, Baby Boomers are retiring—taking a lot of institutional knowledge with them—and many accountants are shifting into industry or leaving accounting altogether as they reevaluate their professional lives post-pandemic.

At a time when 96% of firm leaders say they're taking steps to grow the business in the next three to five years, the ability to attract and hire talent will be the most significant factor for a firm's future success.

So whom will you hire? It's time to start looking for people who aren't CPAs.

NEW TALENT FOR NEW JOBS

Today's workforce demands we focus on the unique abilities of individuals and plug them into where they're needed the most. Our focus can't be solely on education, experience or letters after a name, but on who can do the work that needs to be done.

That's going to require firm leaders and recruiters to seek out different types of people than they've ever looked at before.

Consider your tax and audit team members. While there are certainly aspects of their job that require an accounting degree and CPA license, they likely spend a good portion of their time on non-CPA tasks, including:

- Marketing
- Business development
- Data analytics
- Consulting
- Project management
- Content creation
- Wealth management
- Training others

And more!

In the past, when your tax and audit team members were out of capacity to take on additional work, you would simply hire another tax accountant or auditor member.

Today, that's not always an option. Rather than trying to hire another accountant, consider which tasks your tax and audit team members perform that don't necessarily need to be done by a CPA. Then you have three options:

- Automate the work
- Outsource it to an independent contractor
- Hire a non-CPA with the unique skill set to handle that part of the job

Many of the firms we work with have had a lot of success with this approach. Some of the tasks we've seen them offload to other employees, automate, or outsource include:

- Conducting initial pre-screening conversations with potential clients that come in from referrals, phone calls, social media platforms, or website contact forms
- Performing data analysis as part of assurance, advisory or consulting engagements
- Consulting with clients on technology, growth, leadership, human resources, wealth management and other non-accounting areas
- Writing blog and newsletter content for the firm
- Managing non-client-facing projects

PROFILING, RECRUITING AND HIRING CHANGES

If hiring non-CPAs is part of your strategy, you must change whom you're looking for. Start by creating new candidate profiles. What is the job description for new employees? What skills do they need? What personality traits would help them be successful in the role? What experience or certifications (other than in accounting) should they have?

Now that you know whom you're looking for, you can acquire talent from all over the world. The pandemic proved that employees don't have to be on-site 100% of the time to be productive, and there are many aspects of the work your team does that don't require them to be in the same physical location or even in an overlapping time zone.

Talent is the most critical asset in any CPA firm, and while accounting professionals are still vital, they're not the only type of talent you should be looking for. When you open your mind to hiring beyond accounting professionals—when and where it makes sense—you'll enjoy greater stability on your bench, more room to grow organically, and a diverse team that generates the creativity and innovation to move forward into the future. ■