Cybersecurity in Focus

FICPA Research Results

Sponsored by COAXIS

About the Researchers

Dr. Valrie Chambers *(Ph.D., University of Houston; CPA, Texas*) is an Associate Professor and Beights Fellow for Research and past Chair of the M.E. Rinker, Sr., Institute of Tax and Accountancy and an Associate Professor of Accounting at Stetson University in Deland, Florida. Prior to receiving her Ph.D. with a concentration in taxation in 2000, she had more than a decade of public accounting experience as owner/partner-in-charge of a CPA firm in Houston. Dr. Chambers has published articles in the Journal of Business Ethics, Journal of State Taxation, Strategic Finance, Journal of Accountancy, Tax Notes and Tax Adviser. She has served on the American Taxation Association's Family Tax Policy subcommittee, been cited by National Taxpayer Advocate Nina Olson in her 2004 Annual Report to Congress, developed continuing education courses for accounting professionals, and coordinated an extracurricular simulation set with the Internal Revenue Service for students interested in careers curbing financial crimes. She has also volunteered in several capacities for the American Institute of CPAs (AICPA) and has served on the Board of Directors for the Florida Institute of CPAs (FICPA) and other not-for-profit boards.

Dr. William Sause *(Ph.D., Nova Southeastern University)* is an Assistant Professor of Practice in the Department of Business Systems and Analytics at Stetson University's School of Business. He has more than 15 years of professional experience as a software developer at corporations such as Lockheed Martin and McKesson. His areas of research include virtual environments for e-business and e-learning, data visualization, and software development. During the COVID-19 pandemic, Dr. Sause served as the Brown Center Fellow for Digital and Remote Learning, where he consulted with faculty colleagues on the transition to online delivery of classes and promoted faculty development in digital and remote learning.

Carrie Summerlin *(MNM, University of Central Florida)* is the Chief Growth and Innovation Officer for the FICPA. She has more than 20 years of professional experience serving in association and nonprofit management, overseeing membership, marketing, professional development, fundraising, academic engagement, publication, and research functions. Summerlin has led research initiatives focused on an array of topics, including professional standards, fraud, internal audit, business resilience, ESG, DEI, and more.

Introduction and Methodology

A 2021 survey of FICPA members revealed that issues related to cybersecurity, such as keeping up to date with changing technology and the security of clients' financial data, ranked among the top five industry challenges faced by Florida CPAs. In December 2022, to further understand these challenges, the FICPA partnered with Dr. Valrie Chambers and Dr. William Sause of Stetson University to launch a second online survey: Cybersecurity in Focus.

This survey, targeted to firm leaders, sought to answer two key questions:

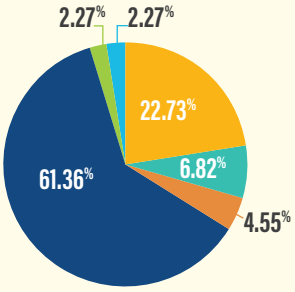
1. How prepared are CPA firms to mitigate their firms' cybersecurity risks?

2. To what extent are CPA firms – particularly sole proprietors, small, and mid-sized CPA firms – preparing to consult in cybersecurity?

The 20-question survey conducted from Dec. 4, 2022, through Jan. 15, 2023, received 75 responses. Firm sizes ranged from sole proprietors to those with as many as 2,000 employees.

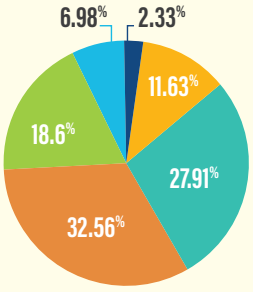
The research team analyzed the data and presented the academic paper, *Analysis of Cybersecurity Preparedness of FICPA Members*, at the 2023 ORLANDO International Multidisciplinary Academic Conference in May. The following whitepaper, sponsored by Coaxis International, explores key findings from the study.

Respondent Demographics



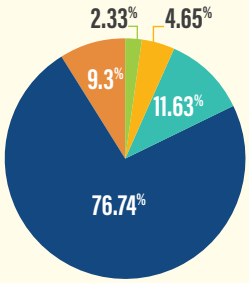
POSITION

- Partner/Shareholder/Owner
- Managing Partner
- Senior Accountant
- Director/Manager
- Staff Accountant
- Other



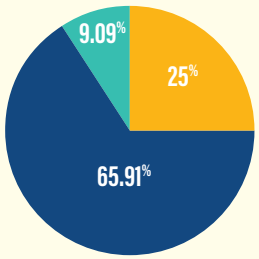
AGE RANGE

- 30-39
- 40-49
- 50-59
- 60-69
- 70-79
- 80-89



ETHNICITY

- White/Caucasian
- Black or African American
- Hispanic, Latino/a, or of Spanish origin
- Asian or Pacific Islander
- Prefer not to answer



GENDER

- Male
- Female
- Prefer not to answer

TOP 5 TIPS FOR CPA AND ACCOUNTING FIRMS TO PROTECT THEIR FIRMS FROM DATA BREACHES:

1. Implement a strong password policy
Encourage your employees to use complex passwords, change them frequently, and avoid reusing passwords across multiple accounts. Consider using a password manager to securely store and manage passwords.

2. Use multifactor authentication
Implement multifactor authentication for all remote access to your network and cloud-based systems. This adds an extra layer of protection against unauthorized access.

3. Regularly update and patch software
Make sure all software and applications are up to date with the latest security patches to prevent vulnerabilities from being exploited by attackers.

4. Provide regular cybersecurity training
Educate your employees about cybersecurity best practices and the latest threats, including phishing and social engineering attacks. Consider conducting simulated phishing attacks to test employee awareness and effectiveness of training.

5. Penetration Testing
Perform regular penetration testing to ensure your network can withstand a cybersecurity attack. Cybersecurity measures are put in place to protect you from hackers. Spending money on cybersecurity defense without testing it is money wasted.

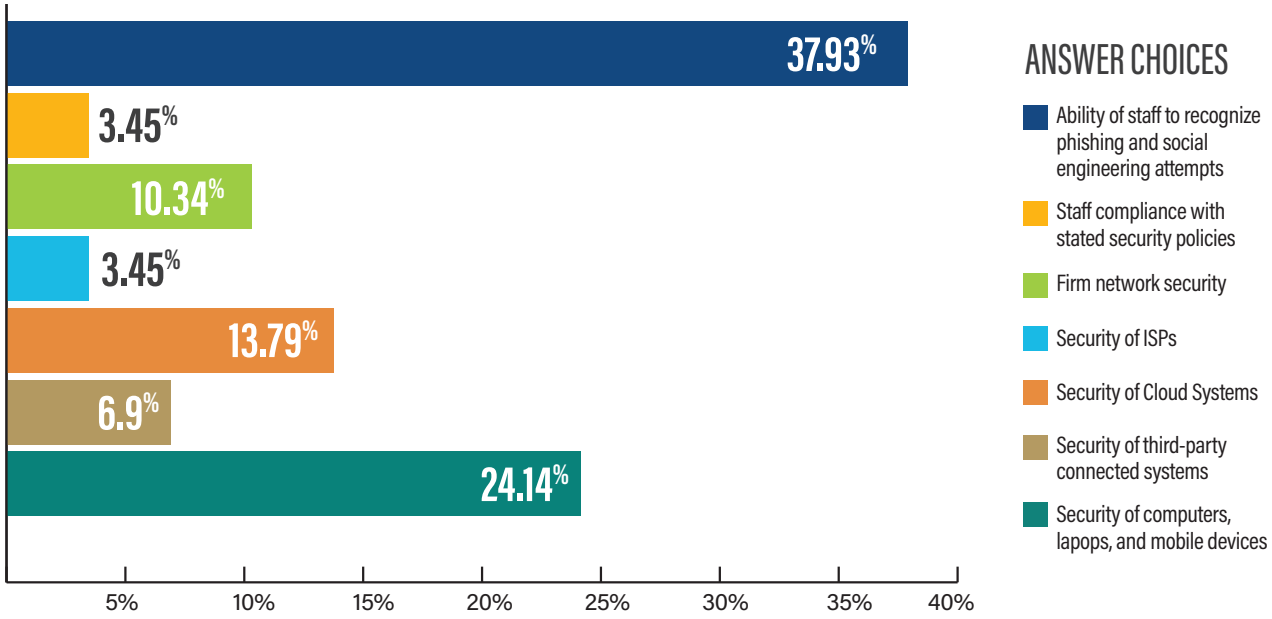
CPA Firms at Heightened Risk

Accounting practices of all shapes and sizes are of particular interest to hackers, who are eager to access the sensitive client information firms keep on file. Just as digitization and paperless work environments have increased efficiency, so too have they exposed firms to additional security risks. As cyber schemes evolve and bad actors continue to look for new ways to steal valuable information, firms need to be equally committed to updating their defenses and planning for a potential attack.

Turning to the data, two-thirds of our respondents (66.2%) answered that they were actively involved in assessing, mitigating, or remediating cybersecurity threats. From this same group, 27% indicated that their firm has experienced a cyber-related incident. Fortunately, 89% of those individuals reported that their response plans were "effective to extremely effective" in addressing the issue.

With cybercrime on the rise and CPA firms in the crosshairs, the question is no longer if a firm will be attached – but when. When an incident does inevitably occur, the severity of the breach will depend on the effectiveness of your advanced preparation and staff training.

Greatest Areas of Cyber-Related Concerns for Florida CPAs



Phishing for People

While CPA firms are generally under threat, it's firm employees who are often the specific target.

Our survey revealed the greatest area of concern for firm leaders is the ability of staff to recognize phishing and social engineering attempts (37.93%). This feedback aligns with data from CISCO's 2021 Cybersecurity Threat Trends report indicating that approximately 90% of data breaches are a result of phishing.

It's also vital to note that many of these phishing attacks go unnoticed, either for months after the breach or altogether. While only a quarter of the respondents mentioned in the previous section confirmed that they have experienced a cyber-related incident, the number is likely much higher. A 2018 IT Professionals Security Report Survey reported that 76% of its participants experienced a phishing attack that year. This would seem to indicate that a great many of our FICPA members, including the respondents of our survey, have in fact been victims of a phishing attack, with real threats going undetected and underreported.

While cybersecurity software plays a key role in protecting your firm, Christophe Reglat, the President and CEO of Coaxis Hosting and a member on the FBI's Counterintelligence Task Force, reminds firms to stay just as focused on educating and equipping staff members.

"Empowering your staff to recognize phishing and social engineering attempts is like giving them a digital shield to protect themselves and your organization," Reglat advises. "It's not just about technology; it's about people. Train and educate your staff, and together, you'll build a stronger line of defense against cyber threats."

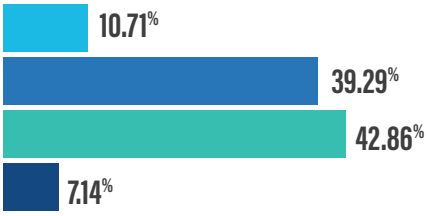
Written Information Security Plans

Of course, having a response plan for a potential incident is more than just best practice; it's the law. Under the Gramm-Leach-Bliley Act, the Federal Trade Commission requires all preparer tax identification number (PTIN) holders to have a Written Information Security Plan (WISP). Bear in mind, there is no one-size-fits-all WISP; plans are meant to be tailored to a firm's unique size, needs and exposure. Crucially for CPAs in Florida, a detailed WISP can also help firms navigate other non-cyber events that can disrupt business, including natural disasters – like hurricanes.

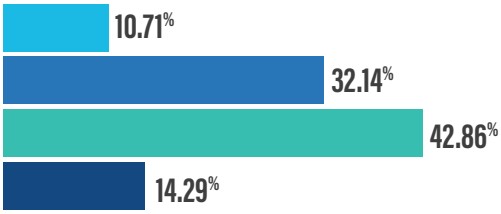
FICPA survey respondents were asked to indicate the level to which they already had or wanted to implement certain elements of effective WISPs. More than 50 percent of respondents indicated they have a plan in place with "no changes needed" with respect to their plan purpose (64.29%), access policy (50%), the and the identification of responsible parties (50%). Firm leaders indicated at the highest frequency that they have a plan but "would look to improve" cybersecurity and awareness training with staff (44.44%). This latter response aligns with the firm leader's aforementioned concerns about staff members' being able to recognize phishing and social engineering attempts.

Overall, survey respondents expressed confidence in their firm's cybersecurity program, adherence to policies, and ability to detect incidents.

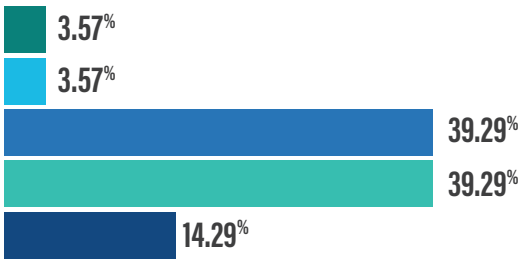
How confident are you in your firm's ability to identify and appropriately respod to a phishing or social engineering attempt?



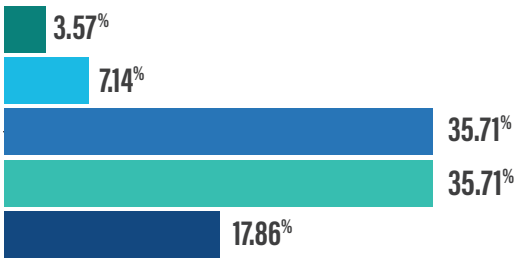
Understanding that today hackers are gaining access to targeted networks and laying undetected and dormant for over 200 days, how confident are you that your firm has not ben hacked/breached?



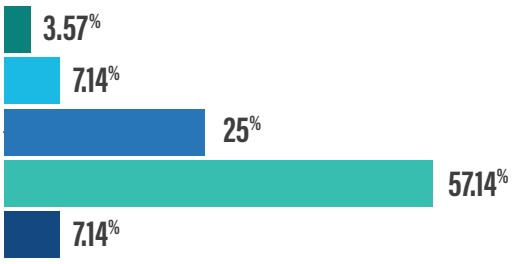
How confident are you that your current cybersecurity training is preparing your employees to identify the various social engineering tactics deployed by hackers?

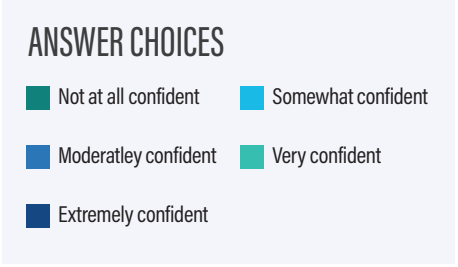


How confident are you that your firm adheres to your firm's data destruction policy?



Today, how confident are you that your current IT has the right IT tools in place to detect a dormant hacker in your network?





"Having a data plan in place is a necessity for a modern firm," says W.G. Spoor, Past Chair of the FICPA and Partner at Spoor Bunch Franz in St. Petersburg. "Beyond the practical benefits, there's genuine peace of mind in knowing that you've taken advance action in the event of an incident. Whether we're responding to a potential cyber breach or a natural disaster, CPAs must plan in advance for the good of the firm and the good of the client."

For those firms who do not have a plan in place or who would like to improve their existing plan, the Internal Revenue Service released Publication 5708, *Creating a Written Information Security Plan (WISP) for your Tax & Accounting Practice*, in October 2022. The document, prepared by the Security Summit – a partnership of the IRS, state tax agencies, private-sector tax groups and tax professionals – is "intended to provide sample information and to help tax professionals, particularly smaller practices, develop a WISP". It can be accessed at *www.irs.gov/pub/irs-pdf/p5708.pdf*.

CPAs as Cyber Advisors?

CPAs are trusted advisors who provide insights to their clients on a broad range of issues and topics.

But what about cybersecurity?

Only 24% of survey respondents indicated they would potentially advise clients on the quality of their cybersecurity programs, if asked. A slightly higher number (27%) indicated they would be more inclined to offer System and Organization Controls (SOC) for cybersecurity assurance services rather than advisory services to help strengthen cybersecurity risk management program.

Nearly 80% of respondents indicated their staff did not possess any technology or cybersecurity related credentials. This could play a factor in the low percentage of firms advising in this space, owing to a lack of specialized knowledge within the firm.

Key Takeaways

CPAs are expected and tax preparers are required to have strong cybersecurity controls on their systems and data.

Our research revealed that survey respondents generally believe their current cybersecurity measures are sufficient, and that only a small number believed their firm has been the target of an attack – even if the reality is likely different.

Although our respondents feel confident about the plans they have in place, they are less willing to enter the cybersecurity space as advisors themselves.

About the FICPA

The Florida Institute of Certified Public Accountants serves as the premier professional association for CPAs and accountants in the state of Florida. Founded in 1905, the FICPA continues to advance the accounting profession, advocating on behalf of 18,500 members who actively work in public accounting, private industry, government or education, making the FICPA one of the largest CPA organizations in the United States.
To learn more about the FICPA, visit www.ficpa.org.

About the Research Sponsor, COAXIS

Coaxis International (Coaxis), an experienced provider of managed data hosting (cloud computing) solutions, through its Coaxis CPA Program provides a fully hosted and managed network solution designed to remove the complexities of federal and industry compliances, curb the demands of information technology infrastructure, and greatly minimize the threat of cybercrime. The Coaxis team has extensive experience in hosting and supporting a broad range of tax and financial reporting software applications. A Florida corporation since 2002, Coaxis operates a privately owned, single-tenant, Tier 4 Data Center in Tallahassee.
To learn more about Coaxis and their FICPA Endorsed program, visit https://www.coaxiscloud.com/ficpa/.