# Should Accountants Upskill? Evidence from Demand for Auditors with Cybersecurity Expertise

Musaib Ashraf
Michigan State University
musaib@msu.edu

Jennifer Puccia
PhD Candidate
Michigan State University
madden13@broad.msu.edu

We thank Ken Bills, Chris Hogan, Rani Hoitash, and Udi Hoitash for their feedback. We also thank the Eli Broad College of Business at Michigan State University for funding that enabled this study. Any errors are our own.

# Should Accountants Upskill? Evidence from Demand for Auditors with Cybersecurity Expertise

**Abstract:** Motivated by the forthcoming change to the CPA licensure exam that emphasizes non-traditional accounting skills like cybersecurity, we study whether audit clients have greater demand for auditors that possess cybersecurity expertise. Conceptually, we argue clients demand auditors with cybersecurity expertise because such auditors can help improve ex ante cybersecurity, help mitigate issues after a client is breached, or serve as a signaling mechanism to stakeholders that the client takes cybersecurity concerns seriously. Empirically, we find evidence consistent with our hypothesis: audit offices with cybersecurity expertise exhibit greater future market share, both in a levels analysis with audit office and year fixed effects and in a changes analysis. Inferences are robust to (i) calculating future market share based on either number of clients or fees and (ii) when studying future number of clients rather than future market share. We also find that audit offices with cybersecurity expertise are associated with lower future client cyber risk exposure, lower future likelihood of client information technology-related internal control material weaknesses, and greater future client audit fees. Overall, our evidence suggests that clients value auditors with cybersecurity expertise, implying that upskilling may benefit the accounting profession.

**Keywords:** audit, auditors, audit office market share, cybersecurity, cyber risk, information technology, internal controls, audit fees

**JEL classifications:** M40, M41, M42

All data used in the study is publicly available.

*"Today's CPAs need deeper skill sets, more competencies and greater knowledge of emerging technologies and their impact on tax, accounting and audit."*

– AICPA (2023)

# I. INTRODUCTION

One of the most significant changes in recent memory to the Certified Public Accountant (CPA) licensure process is the shift to requiring accountants to obtain 150 credit hours of education (Cumming and Rankin 1999). Debate continues whether this change benefited or harmed the accounting profession, with some evidence suggesting the increase to 150 credit hours produced little benefit (e.g., Lee, Liu, and Wang 1999; Barrios 2022) and some states debating whether they should roll back the requirement to 120 credit hours (Strickland 2023). A more recent, and perhaps similarly consequential, change to the CPA licensure process is a revamp of the CPA certification exam that is scheduled to take place in 2024.

Beginning in 2024, the CPA exam is no longer a four-part exam that all applicants take; rather, the CPA exam now follows a "Core + Discipline" model where all applicants must (i) pass three core sections in accounting, auditing, and tax and (ii) pick one of three disciplines for the fourth section (NASBA 2022). The argument behind this new model is that accountants need to upskill to stay relevant with the modern business environment, and part of this revamp includes a new emphasis on technology, including cybersecurity (AICPA 2023; Ho 2023). However, extant empirical evidence is limited on whether there is market demand for accountants to possess these traditionally non-accounting skills. We address this gap in the literature. Specifically, we study whether auditors with cybersecurity expertise are in demand by the audit client market.

Aside from allowing us to speak to the broad economic question regarding possible implications of the CPA exam revamp, studying market demand for auditors with cybersecurity expertise is important for two reasons. First, cybersecurity is a growing market-wide risk that concerns an increasing variety of stakeholders (e.g., US Treasury Department 2013; AICPA 2015;

Clayton 2018; and Depository Trust and Clearing Corporation 2018). Indeed, the Securities and Exchange Commission (2018) considers cyber risks to “pose grave threats to our capital markets”, and investors see cyber threats as the top-most threat to firm growth (PwC 2018). Despite the clear importance of cybersecurity, the literature does not agree whether cybersecurity threats are indeed material for firms and on how to mitigate them (e.g., Richardson et al. 2019; Kamiya et al. 2021; Ashraf and Sunder 2023). Our analysis allows us to bring a unique perspective to this increasingly critical debate: do clients consider cybersecurity important enough to demand that auditors possess such skills?

Second, there is extant literature on the types of skills and failures auditors are rewarded or punished for (e.g., Swanquist and Whited 2015; Berglund 2020; Chen et al. 2022; Cowle and Rowe 2022; and Ege and Stuber 2022). However, this literature has generally focused on traditional accounting tasks that are clearly related to GAAP. In contrast, extant literature on market demand for auditors’ non-GAAP skills is much more nascent, and we focus on an auditor skill that is, at least traditionally, non-GAAP (i.e., cybersecurity). Consequently, our study provides insights on whether clients value auditors’ non-GAAP skills. This insight is particularly relevant considering recent developments in the audit profession where at least one major CPA firm – Ernst & Young – is looking to bifurcate its audit practice from its consulting practice (Goldstein 2022), implying that the firm perceives the skills that fall under its consulting practice (such as cybersecurity) currently add little value to its audit clients.

Empirically, we study a panel of audit office-year observations and measure an audit office’s cybersecurity expertise as the cumulative number of data breaches experienced by the office’s clients (*CYBER_EXPERTISE*). The conceptual argument of why client data breaches proxy for an office’s cybersecurity expertise is based on experiential learning theory (Kolb 1984), which posits development of skills happens through experience (e.g., Ahn, Hoitash, and Hoitash 2020). When a client firm has a data breach, their auditor is likely intimately involved in post-breach processes (Center for Audit Quality 2020), which inherently includes assessing any impacts on the audit – but also assessing any impacts on financial reporting, the control environment, and disclosure implications (Center for Audit Quality 2014a; Tysiac 2014; Ashraf and Sunder 2023). This allows the audit office to develop cybersecurity expertise, both about the specific vulnerability the client experienced and about cybersecurity generally. For example, the National Institute of Standards and Technology Cybersecurity Framework notes that a firm's control environment is intricately linked to a firm's cybersecurity, and extant evidence suggests that firms change their internal controls when addressing cybersecurity (Ashraf 2022). Auditors must assess the operating effectiveness of any changes clients make to internal controls, and such assessments of a breached client's internal controls allows the auditor to develop expertise of underlying cybersecurity issues and vulnerabilities.

As we discuss in more detail in Section II, we argue that clients will want to hire auditors with cybersecurity expertise for three reasons: (i) to help improve the client's ex ante cybersecurity, such as through social learning (Bandura 1962); (ii) to help mitigate issues after a client is breached (Center for Audit Quality 2020); and (iii) to serve as a signaling mechanism to stakeholders that the client is taking cybersecurity concerns seriously (SEC 2011; PwC 2018). We find evidence consistent with our arguments. While controlling for audit office and year fixed effects and other commonly documented determinants of an audit office's MSA-level market share, we find *CYBER_EXPERTISE* is associated with greater future market share for the audit office (*OFFICE_MKTSHARE_CHG*$_{t+1}$).[1] This result is robust to a changes analysis and continues to hold if (i) we calculate *OFFICE_MKTSHARE_CHG*$_{t+1}$ based on fees rather than number of clients or (ii) we study an audit office's future number of clients rather than its future market share. In aggregate, our evidence suggests that clients have greater demand for auditors that possess cybersecurity expertise.

We conduct three additional analyses to reinforce our inferences. First, if clients are indeed hiring auditors for the auditor's cybersecurity expertise, then we should observe a reduction in a client's future cyber risk exposure. Empirically measuring cyber risk exposure is notoriously difficult and noisy. Nonetheless, using the cyber risk proxy developed by Florakis et al. (2022), we find *CYBER_EXPERTISE* is associated with lower *CLIENT_CYBER_RISK*$_{t+1}$. Similarly, an improvement in cybersecurity implies a reduction in cyber risk, and extant research has documented that an improvement in internal controls can proxy for a firm improving its cybersecurity (Ashraf 2022). We find *CYBER_EXPERTISE* is associated with lower likelihood of *CLIENT_IT_MATERIAL_WEAKNESS*$_{t+1}$. Finally, if cybersecurity expertise is truly in demand by clients, possessing cybersecurity expertise should give an audit office a competitive advantage relative to other audit offices, thereby allowing the audit office to charge clients higher audit fees. We find *CYBER_EXPERTISE* is associated with greater *CLIENT_AUDIT_FEES*$_{t+1}$. All three of these analyses are in a client firm-year panel with client firm fixed effects, year fixed effects, and relevant control variables.

We contribute to the literature in three ways. First, our evidence speaks to possible benefits of the recent revamp of the CPA certification exam. We find audit clients do appear to value

[1] To avoid potential confounds (e.g., Lawrence et al 2018; Smith et al. 2019), we study market share (and all other subsequent dependent variables) among non-breached clients only. In other words, all our analyses in this study exclude observations for clients that experienced a data breach.

auditors' non-GAAP skills, specifically cybersecurity. This suggests that upskilling may be advantageous for the accounting profession generally and auditors specifically. To our knowledge, we are the first to provide such evidence. Our insights are particularly important in the current climate where at least one major CPA firm has proposed splintering its consulting and audit practices (Goldstein 2022).

Next, we provide a unique perspective in the debate on whether data breaches are material for firms (e.g., Richardson et al. 2019; Kamiya et al. 2021; Ashraf and Sunder 2023). Our evidence implies that clients are concerned about data breaches to the point of employing auditors with cybersecurity expertise. Relatedly, there is some concern in the literature that firms may believe data breaches are inevitable and prefer to react to a breach after the fact rather than be proactive and implement preventative measures (e.g., Gordon, Loeb, Lucyshyn, and Zhou 2015; Sonnemaker 2019). Our evidence provides an alternative perspective to this concern: non-breached firms appear to be proactive and actively seek out auditors with cybersecurity expertise.

Finally, we contribute to the literature that studies auditor market share (e.g., Swanquist and Whited 2015; Berglund 2020; Chen et al. 2022; Cowle and Rowe 2022; and Ege and Stuber 2022). We differentiate from prior studies that focus on traditional accounting characteristics (e.g., restatements) by studying the role of a non-GAAP expertise – cybersecurity. Our findings cannot be extrapolated from extant literature because, as we discuss in Section II, the literature does not agree whether auditors are punished or rewarded for *GAAP-related* failures. Consequently, it is difficult to argue that our research question – which focuses on the impact of an auditor's *non-GAAP* expertise – has already been explored.

## II. RELATED LITERATURE & HYPTHESIS DEVELOPMENT

### *Related Literature*

Most relevant to our research question are two literatures – the cybersecurity literature and the auditor market share literature. The cybersecurity literature has generally focused on the determinants of experiencing a data breach and the consequences for (client) firms that are breached (e.g., Richardson et al. 2019; Kamiya et al. 2021; Huang and Kim 2021). There is some debate in this literature regarding whether data breaches are material for breached (client) firms. In particular, Richardson et al. (2019) argue that, although it is statistically significant, the effect of data breaches on firm value is not economically meaningful. In contrast, other research argues data breaches do materially decrease firm value (e.g., Kamiya et al. 2021; Amir et al. 2018). Further, extant evidence suggests that auditors increase audit fees for clients that experience data breaches (Lawrence et al. 2018; Smith et al. 2019). However, these manuscripts focus on the consequences of data breaches for the focal breached client firm. They do not address implications for auditor market share, nor do they document audit firm turnover events after a client is breached.

Further, some studies have examined implications beyond breached firms. For example, Ashraf (2022) finds non-breached peers enhance internal controls after a peer firm discloses a data breach; Ashraf and Sunder (2023) document that shareholders appreciate investments in cybersecurity, as proxied by lower cost of equity after passage of data breach disclosure laws; and Florakis et al. (2022) provide evidence that cyber risk is valued in the cross-section of firms. In aggregate, the cybersecurity literature is growing but, to our knowledge, prior literature has not examined whether there is demand for cybersecurity expertise in accountants in general and auditors in particular.

The auditor market share literature is vast. Generally, the literature finds that auditors are punished with lower market share after a GAAP failure. For example, Swanquist and Whited (2015) provide evidence that auditors are penalized for GAAP failures, as proxied by lower market share after a client restates audited financial statements. Chen et al. (2022) corroborate this evidence by documenting a similar punitive effect among audit partners in China. However, although some studies document a punitive effect for audit firms that experience audit failures, other studies find contradictory evidence. For example, Berglund (2020) does not find greater turnover for auditors that failed to issue a going concern opinion prior to a client going bankrupt. Interestingly, other research suggests that auditors can be penalized for *high*-quality audits and rewarded for *low*-quality audits: Cowle and Rowe (2022) note audit office growth declines as an audit office reports more internal control material weaknesses and Ege and Stuber (2022) find that auditors in the insurance industry are rewarded with increased market growth for leniency in the audit process. A key difference between these manuscripts and ours is that they study GAAP-related audit tasks whereas we study a non-GAAP skill: cybersecurity. Given that the literature does not agree about whether auditors are punished or rewarded for GAAP failures, it is even less uncertain whether auditors are rewarded for a non-GAAP skill.

### *Hypothesis Development*

Conceptually, clients may hire auditors with cybersecurity expertise for three not-mutually-exclusive reasons. First, clients may want to improve their cybersecurity. For example, Center for Audit Quality (2014b, p.1) notes: “Cybersecurity is one of the most complex and evolving issues facing public companies. All players in the financial reporting supply chain, including of course independent auditors, have an important role to play.” Auditors are generally prohibited from performing consulting services for their audit clients, so it is unlikely that auditors are formally advising their clients on cybersecurity measures. However, the literature (e.g., Fontaine and Pilote 2012) provides evidence that clients can – and often do – informally ask advice from their auditors that goes beyond core audit services, such as cybersecurity. Even if the client is not explicitly requesting cybersecurity advice from the auditor, social learning theory suggests that cybersecurity expertise is likely to transfer from the auditor to the client during the natural course of business. Social learning theory posits that people learn behaviors from their environment through observation (Bandura 1962; Wolfson et al. 2018). In our setting, client employees regularly interact with auditors, who are likely utilizing their cybersecurity knowledge during the normal course of the audit. Social learning theory predicts that the client employees will absorb at least some of the auditor's knowledge by observing it.[2] In short, client firms may perceive that having an auditor with cybersecurity expertise can enhance their cybersecurity through these informal learning channels.

Relatedly, while auditors may not perform consulting services for clients, auditors do assess clients' control environments. Prior literature (e.g., Lawrence et al. 2018; Ashraf 2022) has documented an intimate relation between cybersecurity and internal controls. Auditors are arguably able to impart their cybersecurity knowledge to the client through the process of evaluating a client's internal controls. For example, auditors often evaluate Information Technology General Controls (ITGCs). These controls involve assessing the design and evaluating the operating effectiveness of common firm-wide information technology processes, including but not limited to password security, how users obtain access to (and are removed access from) privilege systems, the process to develop and implement code changes, and data backups and recovery. Such assessments allow auditors to gain firsthand knowledge of a firm's information technology policies and procedures, including cybersecurity measures, and provide recommendations to management on how to correct weaknesses (when applicable). The

[2] For example, someone with cybersecurity knowledge will be hesitant to share flash drives among untrusted computers. Someone without cybersecurity knowledge can learn this behavior by observing the other person acting in this way.

recommendations that auditors share with management should impact the control environment, of course, but could also emanate throughout the organization as best practices – both of which should help achieve the client's desired outcome: reduction in overall cyber risk exposure. Indeed, numerous data breaches have been caused by weaknesses in the information technology functions that auditors test (Ashraf 2022; Irwin 2022; Kelly 2022). Thus, it follows that auditors with cybersecurity expertise should be able to help reduce a client's cyber risk exposure by identifying and providing recommendations for such weaknesses.

The second reason clients may hire auditors with cybersecurity expertise is as part of the client's contingency plan if the client were ever to be breached. Clients may prefer an auditor that has experience assisting other clients deal with post-data-breach cleanup and reporting procedures (e.g., Center for Audit Quality 2020; Ashraf and Sunder 2023). Given that data breaches are increasingly viewed as being inevitable (e.g., Sonnemaker 2019), even if a cybersecurity expert auditor is not actively helping improve a client's cybersecurity, they can assist should the client ever be breached. Auditors who have already been through the post-data-breach processes with other clients also likely have an active network of lawyers and consultants that a breached client can quickly leverage after a breach should the need arise.

Finally, clients may hire auditors with cybersecurity expertise as a mechanism to signal to concerned stakeholders that the client is taking cybersecurity seriously. Because investors consider cybersecurity risks a top concern (PwC 2018), firms may be motivated to signal their priority for this risk area. Besides investors, regulators have recently made cybersecurity a focal point. The SEC has campaigned for firms to enhance cybersecurity disclosure and practices (e.g., SEC 2011; SEC 2018). Additionally, the PCAOB has vowed to focus on cybersecurity risks (Center for Audit

Quality 2020). A client may view hiring an auditor with cybersecurity expertise as one way to help placate these clearly important stakeholders.

Given the above arguments, we state our hypothesis in its alternative form:

> **Hypothesis:** *Cybersecurity expertise for auditors is associated with greater future audit market share.*

While we make a directional prediction, it is possible that we observe no effect in our analyses. This is because, on the face of it, cybersecurity is a non-GAAP duty that would fall under consulting services for auditors – services that auditors are legally forbidden from performing for audit clients (see Sarbanes-Oxley Act of 2002). Consequently, clients may not demand any cybersecurity expertise from their auditors and rather rely on internal employees or external consultants for that particular expertise. This would suggest cybersecurity expertise for auditors should have no association with audit market share.

## III. RESEARCH DESIGN, DATA, AND SAMPLE SELECTION

We study our research question using the following ordinary least squares model in a panel of audit office-year observations:

$$\begin{aligned} \mathit{OFFICE\_MKTSHARE\_CHG}_{it+1} = {} & \alpha_i + \alpha_t + \beta_1 \mathit{CYBER\_EXPERTISE}_{it} \\ & + \textstyle\sum \beta_k \mathit{Control\ Variables}_{it} \\ & + e_{it}, \end{aligned} \tag{1}$$

where $i$ indexes audit office and $t$ indexes years. The dependent variable, $\mathit{OFFICE\_MKTSHARE\_CHG}_{t+1}$, is calculated for each audit office $i$ following Swanquist and Whited (2015):

$$\mathit{OFFICE\_MKTSHARE\_CHG}_{t+1} = [\mathit{OFFICE\_MKTSHARE}_{t+1} - \mathit{OFFICE\_MKTSHARE}_{t}] \div \mathit{OFFICE\_MKTSHARE}_{t}, \tag{2}$$

where *OFFICE_MKTSHARE* equals the number of clients audited by audit office *i* in year *t* scaled by the total number of clients audited by all audit offices in audit office *i*'s MSA *j* in year *t*.[3] Our test variable is *CYBER_EXPERTISE*, which equals the natural log of one plus the number of data breaches publicly disclosed by audit office *i*'s clients during or before year *t*. A positive coefficient on *CYBER_EXPERTISE* suggests that auditors with cybersecurity expertise experience greater market share – or premia facie evidence that clients demand this type of expertise from their auditors.

Our model includes audit office fixed effects to help eliminate the effect of time-invariant unobservable audit office and audit firm characteristics on our inferences. We also include year fixed effects to control for the effect of time-related factors (e.g., year-specific shocks and time trends). Further, we cluster robust standard errors at the audit office level to account for heteroskedasticity and correlated standard errors. Finally, we follow Swanquist and Whited (2015) and control for a vector of audit office-year characteristics that may impact an audit office's market share: *OFFICE_MKTSHARE_CHG*, *OFFICE_MKTSHARE*, *#_OFFICES_MSA*, *#_OFFICE_CLIENTS*, *M_GROWTH*, *M_ACC*, *M_INVREC*, *M_ROA*, *M_LOSS*, *M_LEV*, *M_CASH*, *M_SIZE*, *M_AQC*, *M_GC*, *M_MODOP*, *M_INITIAL*, *M_MISMATCH*, *M_EXPERT*, *M_ABFEES*, *M_SOX404*, *M_WEAK*, *M_RESTATE*, and *M_RESIGN_COUNT*. These variables are defined in Appendix A.

*Data and Sample Selection*

We present our sample selection in Table 1. We begin with 92,185 client firm-year observations between 2010 and 2020 with non-missing CIK.[4] We then exclude 28,225

[3] Audit offices are measured using the metropolitan statistical areas (MSA) taxonomy from the U.S. Census Bureau.
[4] Our sample begins in 2010 because that is when coverage starts in Audit Analytics' cybersecurity database (Audit Analytics 2023). We end in 2020 to enable calculation of *OFFICE_MKTSHARE_CHG*$_{t+1}$.

observations that are missing MSA data, 5,276 observations that belong to clients who are breached in our sample (to avoid confounds, e.g., Lawrence et al 2018 and Smith et al. 2019), 180 observations whose auditor's audit firm is part of an audit firm merger / acquisition or split event, 691 observations whose auditor's audit firm is deregistered with the PCAOB, and 2,478 observations with missing audit fees data. This results in a sample of 55,335 client firm-year observations, which we use to calculate our dependent, independent, and control variables. We then assign or aggregate (as applicable) the variables to 7,546 audit office-year observations that are associated with the 55,335 client firm-year observations. Of this 7,546, we exclude 1,030 observations for audit offices with no competitors, 610 observations with data missing for the variables in our model, and 105 singleton observations (Correia 2015), resulting in a main sample of 5,801 audit office-year observations.[5]

## IV. RESULTS

### *Descriptive Statistics and Pearson Correlations*

The descriptive statistics for our sample are presented in Table 2. The mean of *CYBER_EXPERTISE* is 0.165 logged and 0.179 unlogged (untabulated), meaning that the majority of audit offices' clients have not experienced a data breach in our sample. This is consistent with prior literature that finds roughly one percent of client firm-year observations have experienced a data breach (e.g., Lawrence et al. 2018). The mean of $OFFICE\_MKTSHARE\_CHG_{t+1}$ is -0.016, similar to Swanquist and Whited (2015). All control variables are also generally consistent with existing literature (e.g., Swanquist and Whited 2015).

We plot our test variable by time, client industry, and MSA in Figures 1, 2, and 3 respectively. *CYBER_EXPERTISE* is increasing in over time, which is consistent with an increase

[5] All continuous variables are winsorized at the 1st and 99th percentile.

in the number of data breaches over time (Identity Theft Resource Center 2017). Further, while there is variation in *CYBER_EXPERTISE* across client industries, there does not appear to be any significant outliers. Lastly, as expected, we observe *CYBER_EXPERTISE* is concentrated in larger MSAs.

Pearson correlations for our sample are presented in Table 3. *CYBER_EXPERTISE* is positively correlated with $OFFICE\_MKTSHARE\_CHG_{t+1}$. However, this correlation is marginally insignificant (*p*-value = 0.14; untabulated). We further explore the relation between our test and dependent variable in subsequent multivariate analyses.

*Main and Sensitivity Analyses*

We present the results of our main analysis in Table 4. The coefficient on *CYBER_EXPERTISE* is positive and significant (*p*-value ≤ 0.01). A one standard deviation increase in *CYBER_EXPERTISE* is associated with a 2.3 percent *increase* in future market share, compared to the average sample *decrease* of 1.9 percent. This result holds when we conduct a changes analysis in Table 5 (*p*-value ≤ 0.01), rather than the levels analysis in Table 4, and also when we calculate audit office market share using fees (rather than number of clients) in Table 6 (*p*-value ≤ 0.05).[6] Inferences continue to remain consistent when, instead of studying market share, we study the number of clients at an audit office in Table 7 (*p*-value ≤ 0.01). Altogether, these results suggest that auditors' cybersecurity expertise is in demand by clients.

*Additional Analyses*

We reinforce our main finding with three additional analyses. We motivate our hypothesis with the notion that clients may hire an auditor with cybersecurity expertise in order to use the auditor's cybersecurity knowledge to improve the client's cybersecurity or, conversely, lower the

[6] $OFFICE\_MKTSHARE\_CHG\_FEES_{t+1}$ is calculated following Swanquist and Whited (2015).

client's cyber risk exposure (see hypothesis development in Section II). We now empirically test this argument with our first additional analysis.

We use a panel of client firm-year observations and the cyber risk measure from Florakis et al. (2022) to estimate the relation between *CYBER_EXPERTISE* and *CLIENT_CYBER_RISK*$_{t+1}$ (defined as client firm *k*'s Cybersecurity Risk Index in year *t*+1, where higher values indicate greater cyber risk exposure).[7] We present the results of this analysis in Table 8.[8,9] Consistent with our arguments, the coefficient on *CYBER_EXPERTISE* is negative and significant (*p*-value ≤ 0.05).

Empirically measuring a client firm's cyber risk exposure is difficult. We use Florakis et al. (2022)'s measure that, although noisy, directly captures the construct we are interested in. To ensure our inferences are not idiosyncratic to their measure, for our second additional analysis, we study the association between *CYBER_EXPERTISE* and *CLIENT_IT_MATERIAL_WEAKNESS*$_{t+1}$ (equals one if client firm *k* possesses an IT-related internal control material weakness in year *t* [zero otherwise], where a material weakness is IT related following the definition in Ashraf et al. 2020). This analysis is predicated on the fact that extant literature (e.g., Ashraf 2022) has documented that improvements to cybersecurity can manifest as improvements to internal controls, particularly IT-related internal controls. Thus, if auditors with cybersecurity expertise are indeed helping improve a client's cybersecurity, we should observe an improvement in IT-related internal controls. Further, although *CLIENT_IT_MATERIAL_WEAKNESS*$_{t+1}$ is a less direct proxy than *CLIENT_CYBER_RISK*$_{t+1}$ of the client's cyber risk exposure construct, the variable is also

[7] We thank Michael Weber for sharing the data with us.

[8] The control variables in Table 8 are based on Ashraf and Sunder (2023)'s cybersecurity model.

[9] The sample selection criteria in Tables 8, 9, and 10 is the same as described in Table 1 (including excluding observations for breached clients), and the difference in observations across these tables is due to data availability for the particular variables in each model.

relatively clean and less noisy. We present the results of this analysis in Table 9. As predicted, the coefficient on *CYBER_EXPERTISE* is negative and significant ($p$-value ≤ 0.05).[10]

For our final analysis, we study the association between *CYBER_EXPERTISE* and $CLIENT\_AUDIT\_FEES_{t+1}$ (defined as the log of audit fees paid by client firm *k* in year *t*). If clients are truly demanding auditors with cybersecurity expertise as our analyses thus far suggest, then that should give audit offices with such expertise a competitive advantage and greater bargaining power, thereby enabling these offices to extract greater rents from clients. This argument predicts a positive association between *CYBER_EXPERTISE* and $CLIENT\_AUDIT\_FEES_{t+1}$. We find such a relation in Table 10 ($p$-value ≤ 0.01).[11,12]

## V. CONCLUSION

In this study, we investigate whether there is market demand for auditors with cybersecurity expertise. Our research question is motivated by the recent push by the accounting profession for CPAs to develop not-traditionally-accounting skills like cybersecurity (NASBA 2022; Ho 2023). However, we also speak to extant literature which studies the effect of data breaches on capital markets and organizational behavior (e.g., Richardson et al. 2019; Kamiya et al. 2021) and the literature on auditor market share (e.g., Swanquist and Whited 2015).

[10] The control variables in Table 9 are based on internal control models used by extant literature (Ashbaugh-Skaife et al. 2007; Doyle et al. 2007; Ashraf 2022).

[11] The control variables in Table 10 are based on the common control variables identified by DeFond and Zhang (2014).

[12] Asthana, Kalelkar, and Raman (2021) find lower audit fees for non-breached clients after an audit office's client publicly discloses a breach. We differentiate from Asthana et al. (2021) in the following ways. First, conceptually, we are interested in possible benefits of accountants upskilling as suggested by the revised CPA exam. Consequently, we focus on market share for auditors with cybersecurity expertise, and our analysis of audit fees is ancillary to our main contribution. In contrast, Asthana et al. (2021) focus on audit fess and do *not* study audit office market share. Second, empirically, it is difficult to reconcile our ancillary finding of higher audit fees with Asthana et al. (2021)'s main finding of lower audit fees because of different research designs. For example, Asthana et al. (2021) do not control for numerous confounding factors, such as time trends, year-specific shocks, or a firm's unobservable characteristics – whereas we do, vis-à-vis firm and year fixed effects.

Focusing on an audit office-year panel and using client data breaches to proxy for an audit office's level of cybersecurity expertise, we find auditor cybersecurity expertise is associated with greater future MSA-level market share. This result holds both in a levels analysis with audit office and year fixed effects and in a changes analysis. Our finding is robust to measuring market share using three different dependent variables. Further, consistent with our argument that clients are interested in hiring auditors for their cybersecurity expertise, we also find that auditor cybersecurity expertise is associated with lower future client cyber risk, lower future likelihood of client IT-related material weaknesses, and higher future audit fees in a client firm-year panel.

Overall, our analyses provide evidence which suggests that accountants in general and auditors in specific may benefit from the upskilling that is suggested by the new CPA exam (which is set to go live in 2024). Our findings should be of interest not just to academics but also to any practitioner, investor, and regulator who is interested in accounting, auditing, or cybersecurity. Notably, we cannot speak to whether CPA firms will be "better off" by bifurcating their non-GAAP consulting expertise and GAAP audit expertise, such as what is proposed by Ernst & Young (Goldstein 2022). However, our evidence does suggest that clients reward auditors that possess at least some non-GAAP expertise – cybersecurity, in our setting.

# APPENDIX A
# Variable Definitions

**Variable** **Definition [Data Source]**

*#_MSA_OFFICES* = Natural log of one plus the number of unique audit offices in MSA *j* in year *t* [Audit Analytics]

*#_OFFICE_CLIENTS* = Natural log of one plus the number of audit client's audit office *i* in year *t* [Audit Analytics]

$\#\_OFFICE\_CLIENTS_{t+1}$ = Natural log of one plus the number of audit client's audit office *i* in year *t*+1 [Audit Analytics]

*ABFEES* = Following Swanquist and Whited (2015), *ABFEES* is the residual from the following model:

$$Ln\_Fees_{it} = \beta_0 + \beta_1 SIZE_{it} + \beta_2 GROWTH_{it} + \beta_3 ROA_{it} + \beta_4 LOSS_{it} + \beta_5 LEV_{it} + \beta_6 NEWAUDITOR_{it} + \beta_7 MSAOFFICES_{it} + \beta_8 WEAK_{it} + \beta_9 SOX404_{\mathrm{it}} + \beta_{10} BIG4_{\mathrm{it}} + Year\_FE + Ind\_FE + \varepsilon_{\mathrm{it}}$$

*ACC* = Following Swanquist and Whited (2015) and Kothari, Leone, and Wasley (2005), *ACC* is the absolute value of the residual from the following regression, estimated on all industry-years with a minimum of ten observations:

$$TA = \lambda_0 + \lambda_1(\Delta REV - \Delta REC) + \lambda_2 PPE + \lambda_3 NI$$

*TA* = total accruals (income before extraordinary items - cash flows from operations + depreciation)
*ΔREV* = change in revenue
*ΔREC* = change in receivables
*PPE* = gross property, plant, and equipment
*NI* = net income

Each term is calculated at the client firm-year level and scaled by lagged total assets.

*ALTMANZ* = 0.717 * [(current assets - current liabilities) / total assets] + 0.847 * [retained earnings / total assets] + 3.107 * [earnings before interest and taxes / total assets] + 0.42 * [book value of equity / total liabilities] + 0.998 * [sales / total assets], where all terms are calculated for client *k*'s year *t* (Altman 1983) [Compustat]

*AQC* = One if client *k* has had an acquisition in the year *t* or year *t*-1 (zero otherwise) [Compustat]

*BIG4* = One if client *k*'s auditor in year *t* is a Big 4 auditor (zero otherwise) [Audit Analytics]

*CASH* = Client *k*'s cash and short term investments in year *t* scaled by client *k*'s total assets for year *t* [Compustat]

$CLIENT\_AUDIT\_FEES_{t+1}$ = Natural log of one plus client *k*'s audit fees for year *t*+1 [Audit Analytics]

*CLIENT_CYBER_RISK*$_{t+1}$ = Client firm *k*’s Cybersecurity Risk Index in year *t*+1, where the Cybersecurity Risk Index is from Florakis et al. (2022) [Florakis et al. 2022]

*CLIENT_IT_MATERIAL_WEAKNESS*$_{t+1}$ = One if client *k* in year *t*+1 has an IT-related material weakness in internal control over financial reporting (SOX 404A or SOX 404B) (zero otherwise), where IT-related material weakness is calculated following Ashraf et al. (2020) [Audit Analytics]

*CURRENT_ASSETS* = Current assets for client *k*'s year *t* scaled by total assets for client *k*'s year *t* [Compustat]

*CYBER_EXPERTISE* = Natural log of one plus the number of data breaches publicly disclosed by audit office *i*’s clients during or before year *t* [Audit Analytics]

*DECEMBER* = One if client *k*'s fiscal year end in year *t* is in December (zero otherwise) [Compustat]

*EXPERT* = One if client *k*'s auditor *i* in year *t* is both the local and national leader (i.e., most audit fees) in client k’s industry-year (zero otherwise) [Audit Analytics]

*FIRM_AGE* = The age of client *k* in year *t* [Compustat]
*FOREIGN* = One if client *k* in year *t* has non-zero pre-tax foreign income (zero otherwise) [Compustat]

*GC* = One if client *k* receives a going concern opinion from their external auditor in the year *t* (zero otherwise) [Audit Analytics]

*GROWTH* = Client *k*’s total assets in year *t* minus client *k*’s total assets in year *t*-1, all scaled by client *k*’s total assets in year *t*-1 [Compustat]

*INITIAL* = One if auditor *i* in new to client *k* in year *t* (zero otherwise) [Audit Analytics]

*INST_OWN* = The percentage of client *k* owned by institutional investors in year *t* [Thomson Reuters]

*INV* = Total inventory for client *k*'s year *t* scaled by total assets for client *k*’s year *t* [Compustat]

*INVREC* = Client *k*’s inventory in year *t* plus client *k*’s receivables year *t*, all scaled by client *k*’s total assets for year *t* [Compustat]

*LEV* = Client *k*’s total liabilities in year *t* scaled by client *k*’s total assets for year *t* [Compustat]

*LOSS* = One if client *k*’s net income in year *t* is negative (zero otherwise) [Compustat]

*M_{X}* = The mean of variable *{X}* for all of audit office *i*'s audit clients *k* during year *t*, where the *M_{X}* variables are:
*M_GROWTH*
*M_ACC*
*M_INVREC*

*M_ROA*
*M_LOSS*
*M_LEV*
*M_CASH*
*M_SIZE*
*M_AQC*
*M_GC*
*M_MODOP*
*M_INITIAL*
*M_MISMATCH*
*M_EXPERT*
*M_ABFEES*
*M_SOX404*
*M_WEAK*
*M_RESTATE*
*M_RESIGN_COUNT*

*MISMATCH* = One if client *k* is mismatched with its auditor *i* in year *t* (zero otherwise)

Following Swanquist and Whited (2015), Shu (2000), and Landsman et al. (2009), mismatch is determined by first estimating the probability that a client is misaligned using the following regression for each year:

$$Big4_{it} = \beta_0 + \beta_1 Size_{it} + \beta_2 Acquisition_{it} + \beta_3 ExFinance_{it} + \beta_4 Profitability_{it} + \beta_5 MktBk_{it} + \varepsilon_{it}.$$

We use coefficient estimates from the regression to estimate the probability that client *k* has a Big 4 auditor in year *t*. The observations are divided into 20 quantiles based on the estimated probability for each year. The lowest quantile at which 50 percent of clients have a Big 4 auditor is the cutoff. Above the cutoff, clients employing a non-Big 4 auditor are classified as mismatched. Below that cutoff, clients employing a Big 4 auditor are classified as mismatched.

*Big4* = indicator for having a Big 4 auditor
*Size* = natural log of total assets
*Acquisition* = acquisitions scaled by average total assets
*ExFinance* = total debt and stock issuances scaled by average total assets
*Profitability* = income before extraordinary items scaled by average total assets
*MktBk* = market value of equity scaled by book value of common equity

Each term is calculated at the client firm-year level.

*MODOP* = One if client *k* receives a modified opinion from their external auditor in the year *t* for any reason other than going concern (zero otherwise) [Compustat]

*OFFICE_MKTSHARE* = Number of clients audited by audit office *i* in year *t* scaled by the total number of clients audited by all audit offices in audit office *i*'s MSA *j* in year *t* [Audit Analytics]

*OFFICE_MKTSHARE_CHG* = $OFFICE\_MKTSHARE_t$ for audit office *i* minus $OFFICE\_MKTSHARE_{t-1}$ for audit office *i*, all scaled by $OFFICE\_MKTSHARE_{t-1}$ for audit office *i* [Audit Analytics]

*OFFICE_MKTSHARE_CHG_FEES* = *OFFICE_MKTSHARE_FEES*$_t$ for audit office *i* minus *OFFICE_MKTSHARE_FEES*$_{t-1}$ for audit office *i*, all scaled by *OFFICE_MKTSHARE_FEES*$_{t-1}$ for audit office *i* [Audit Analytics]

*OFFICE_MKTSHARE_CHG_FEES*$_{t+1}$ = *OFFICE_MKTSHARE_FEES*$_{t+1}$ for audit office *i* minus *OFFICE_MKTSHARE_FEES*$_t$ for audit office *i*, all scaled by *OFFICE_MKTSHARE_FEES*$_t$ for audit office *i* [Audit Analytics]

*OFFICE_MKTSHARE_CHG*$_{t+1}$ = *OFFICE_MKTSHARE*$_{t+1}$ for audit office *i* minus *OFFICE_MKTSHARE*$_t$ for audit office *i*, all scaled by *OFFICE_MKTSHARE*$_t$ for audit office *I* [Audit Analytics]

*OFFICE_MKTSHARE_FEES* = Total fees paid by all of audit office *i*'s audit clients in year *t* scaled by total fees paid by all audit clients in audit office *i*'s MSA *j* in year *t* [Audit Analytics]

*QUICK_RATIO* = Current assets for client *k*'s year *t* minus inventory for client *k*'s year *t*, all scaled by current liabilities for client *k*'s year *t* [Compustat]

*RESIGN* = One if the external auditor for client *k* resigned between nine months prior to the fiscal year-end to three months after fiscal year-end for year *t* (following Ashbaugh-Skaife et al. 2007) (zero otherwise) [Audit Analytics]

*RESIGN_COUNT* = Number of auditors that resigned from client *k*'s audit in year *t* [Audit Analytics]

*RESTATE* = One if client *k* in year *t* discloses a restatement (zero otherwise) [Audit Analytics]

*RESTRUCTURE* = One if client *k* in year *t* has non-zero restructuring costs (zero otherwise) [Compustat]

*ROA* = Client *k*'s net income in year *t* scaled by client *k*'s total assets for year *t*-1 [Compustat]

*SALES_GROWTH* = Sales for client *k*'s year *t* minus sales for client *k*'s year *t*-1, all scaled by sales for client *k*'s year *t* [Compustat]

*SEGMENTS* = Natural log of one plus client *k*'s number of business segments in year *t* [Compustat Segments]

*SIZE* = Natural log of client *k*'s total assets for year *t* [Compustat]

*SOX404* = One if client *k* in year *t* receives a SOX 404 audit from their auditor (zero otherwise) [Audit Analytics]

*WEAK* = One if client *k* in year *t* receives an adverse SOX 404 opinion from their auditor (zero otherwise) [Audit Analytics]

# REFERENCES

Ahn, J., R. Hoitash, and U. Hoitash. 2020. Auditor task-specific expertise: The case of fair value accounting. *The Accounting Review* 95 (3): 1–32.

American Institute of Certified Public Accountants (AICPA). 2015. Security Regains Place as Top Technology Priority for CPAs, North American Survey Finds. https://www.aicpa.org/press/pressreleases/2015/security-regains-place-as-top-technology-priority-for-cpas-north-american-survey-finds.html.

American Institute of Certified Public Accountants (AICPA). 2023. AICPA Unveils Blueprints for Redesigned CPA Exam. https://www.aicpa-cima.com/news/article/aicpa-unveils-blueprints-for-redesigned-cpa-exam.

Amir, E., S. Levi, and T. Livne. 2018. Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies* 23 (3): 1177–1206.

Ashbaugh-Skaife, H., D. W. Collins, and W. R. Kinney. 2007. The discovery and reporting of internal control deficiencies prior to SOX-mandated audits. *Journal of Accounting and Economics* 44 (1–2): 166–192.

Ashraf, M. 2022. The Role of Peer Events in Corporate Governance: Evidence from Data Breaches. *The Accounting Review* (Forthcoming).

Ashraf, M., and J. Sunder. 2023. Can shareholders benefit from consumer protection disclosure mandates? Evidence from data breach disclosure laws and the cost of equity. *The Accounting Review* (Forthcoming).

Bandura, A. 1962. *Social learning through imitation*. Oxford, England: University of Nebraska Press.

Barrios, J. M. 2022. Occupational Licensing and Accountant Quality: Evidence from the 150-Hour Rule. *Journal of Accounting Research* 60 (1): 3–43.

Berglund, N. R. 2020. Do Client Bankruptcies Preceded by Clean Audit Opinions Damage Auditor Reputation?*. *Contemporary Accounting Research* 37 (3): 1914–1951.

Center for Audit Quality. 2014. CAQ Alert #2014-3. https://www.thecaq.org/wp-content/uploads/2019/03/caqalert_2014_03.pdf.

Center for Audit Quality. 2014. Center for Audit Quality Issues Cybersecurity Member Alert Ahead of SEC Roundtable. https://www.thecaq.org/news/center-audit-quality-issues-cybersecurity-member-alert-ahead-sec-roundtable/.

Center for Audit Quality. 2020. The Role of Auditors in Company-Prepared Cybersecurity Information: Present and Future. https://thecaqprod.wpenginepowered.com/wp-content/uploads/2020/10/caq-role-of-the-auditor-cybersecurity-2020-Oct.pdf.

Chen, K. C. W., T. Y. Chen, W. Han, and H. Yuan. 2022. Auditors Under Fire: The Association Between Audit Errors and the Career Setbacks of Individual Auditors. *Journal of Accounting Research* 60 (3): 853–900.

Clayton, C. J. 2018. SEC Rulemaking Over the Past Year, the Road Ahead and Challenges Posed by Brexit, LIBOR Transition and Cybersecurity Risks. https://www.sec.gov/news/speech/speech-clayton-120618.

Correia, S. 2015. *Singletons, Cluster-Robust Standard Errors and Fixed Effects: A Bad Mix*.

Cowle, E. N., and S. P. Rowe. 2022. Don't Make Me Look Bad: How the Audit Market Penalizes Auditors for Doing Their Job. *The Accounting Review* 97 (3): 205–226.

Cumming, J., and L. J. Rankin. 1999. 150 hours: A look back. *Journal of Accountancy* 187 (4): 53–58.

DeFond, M., and J. Zhang. 2014. A review of archival auditing research. *Journal of Accounting and Economics* 58 (2–3): 275–326.

Depository Trust and Clearing Corporation. 2018. The Next Crisis Will Be Different. http://www.dtcc.com/~/media/Files/Downloads/WhitePapers/Systemic-Risk-White-Paper-962018.pdf.

Doyle, J., W. Ge, and S. McVay. 2007. Determinants of weaknesses in internal control over financial reporting. *Journal of Accounting and Economics* 44 (1–2): 193–223.

Ege, M. S., and S. B. Stuber. 2022. Are auditors rewarded for low audit quality? The case of auditor lenience in the insurance industry. *Journal of Accounting and Economics* 73 (1).

Florackis, C., C. Louca, R. Michaely, and M. Weber. 2022. Cybersecurity Risk. *Review of Financial Studies*. Forthcoming.

Fontaine, R., and C. Pilote. 2012. Clients' preferred relationship approach with their financial statement auditor. *Current Issues in Auditing* 6 (1): 1–6.

Goldstein, M. 2022. EY, the accounting and consulting firm, will split into two businesses. *The New York Times*. https://www.nytimes.com/2022/09/08/business/ey-ernst-young-split.html.

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and L. Zhou. 2015. The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy* 34 (5): 509–519.

Ho, S. 2023. AICPA Publishes Blueprints for New CPA Exams. https://tax.thomsonreuters.com/news/aicpa-publishes-blueprints-for-new-cpa-exams.

Huang, H. H., and C. Wang. 2021. Do banks price firms' data breaches? *The Accounting Review* 96 (3): 261–286.

Identity Theft Resource Center. 2017. ITR Data Breach Overview 2005 to 2017. https://www.idtheftcenter.org/images/breach/Overview20052017.pdf.

Irwin, L. 2022. The 5 most common causes of data breaches. https://www.itgovernance.eu/blog/en/the-most-common-causes-of-data-breaches-and-how-you-can-spot-them.

Kamiya, S., J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz. 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics* 139 (3): 719–749.

Kelly, E. 2022. Everything you need to know about ITGC SOX. https://securityboulevard.com/2022/12/everything-you-need-to-know-about-itgc-sox/.

Kolb, D. 1984. *Experiential Learning: Experience as the Source of Learning and Development*. New Jersey: Prentice-Hall.

Lawrence, A., M. Minutti-Meza, and D. Vyas. 2018. Is operational control risk informative of financial reporting deficiencies? *Auditing* 37 (1): 139–165.

Lee, C.-W. J., C. Liu, and T. Wang. 1999. The 150-hour rule. *Journal of Accounting and Economics* 27: 203–228.

National Association of State Boards of Accountancy (NASBA). 2022. Transition Policy Announced for the 2024 CPA Exam Under the CPA Evolution Initiative. https://nasba.org/blog/2022/02/25/transition-policy/.

PricewaterhouseCoopers (PwC). 2018. 2018 Global Investor Survey. https://www.pwc.com/gx/en/ceo-survey/2018/deep-dives/pwc-global-investor-survey-2018.pdf.

Richardson, V. J., R. E. Smith, and M. W. Watson. 2019. Much Ado About Nothing: The (Lack of) Economic Impact of Data Privacy Breaches. *Journal of Information Systems* 33 (3): 227–265.

Securities and Exchange Commission (SEC). 2011. CF Disclosure Guidance: Topic No. 2. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

Securities and Exchange Commission (SEC). 2018. Commission Statement and Guidance on Public Company Cybersecurity Disclosures. https://federalregister.gov/d/2018-03858.

Smith, T., J. Higgs, and R. Pinsker. 2018. Do Auditors Price Breach Risk in Their Audit Fees? *Journal of Information Systems*.

Sonnemaker, T. 2019. Facing inevitable data breaches and new privacy laws, companies shift focus to response. *Medill Reports Chicago*. https://news.medill.northwestern.edu/chicago/facing-inevitable-data-breaches-and-new-privacy-laws-companies-shift-focus-to-response/.

Strickland, B. 2023. NASBA upholds 150-hour education requirement for CPA licensure. https://www.journalofaccountancy.com/news/2023/feb/nasba-upholds-150-hour-education-requirement-for-cpa-licensure.html.

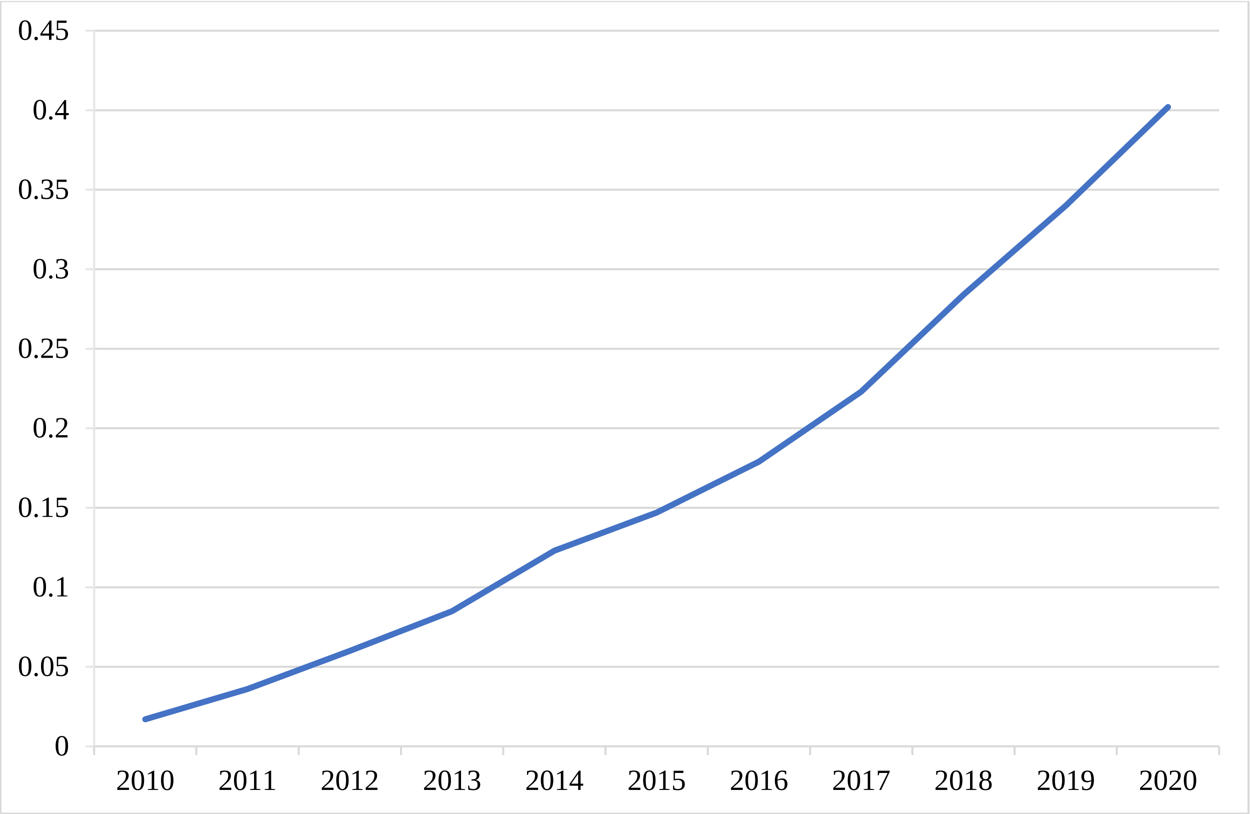
Swanquist, Q. T., and R. L. Whited. 2015. Do clients avoid "contaminated" offices? The economic consequences of low-quality audits. *The Accounting Review* 90 (6): 2537–2570.

Tysiac, K. 2014. Auditors have important role in cybersecurity. *Journal of Accountancy*.

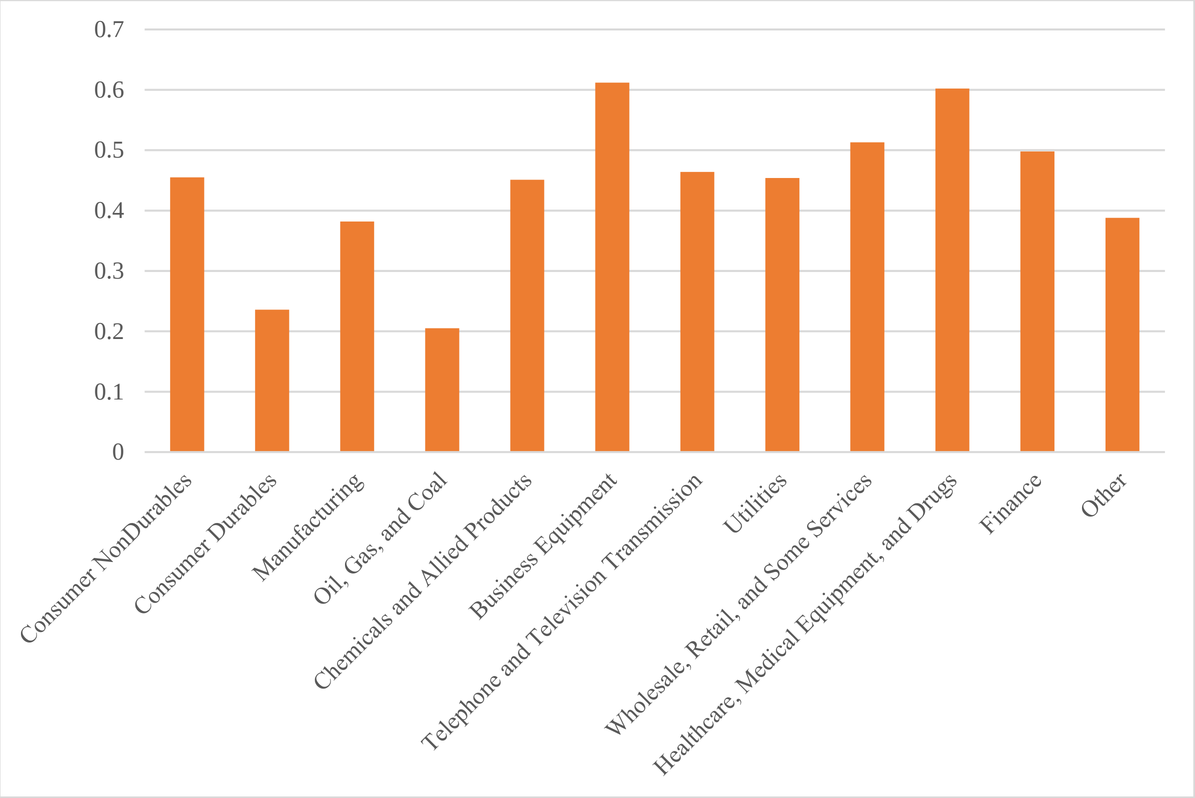
US Treasury Department. 2013. Report to the President on Cybersecurity Incentives Pursuant to Executive Order 13636. https://www.treasury.gov/press-center/Documents/Supporting Analysis Treasury Report to the President on Cybersecurity Incentives_FINAL.pdf.

Wolfson, M. A., S. I. Tannenbaum, J. E. Mathieu, and M. T. Maynard. 2018. A cross-level investigation of informal field-based learning and performance improvements. *Journal of Applied Psychology* 103 (1): 14–36.

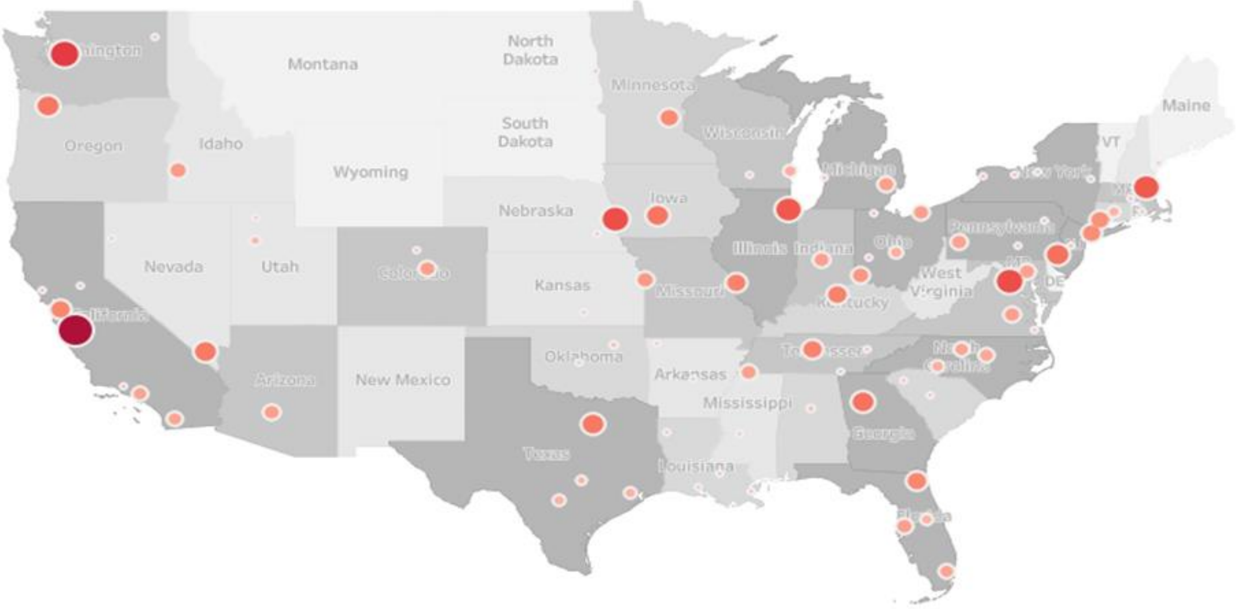
**FIGURE 1**
**Temporal Variation in *CYBER_EXPERTISE***



## FIGURE 2
## Variation in *CYBER_EXPERTISE* by Client Fama-French 12 Industries



## FIGURE 3
## Geographic Variation in *CYBER_EXPERTISE*



## TABLE 1
## Sample Selection

**Panel A: Client-Year Sample for Calculation of Variables**

| | Obs. |
|---|---|
| Client-year observations from 2010 to 2020 with non-missing CIK and fiscal year (Compustat) | 92,185 |
| Less: Observations missing MSA data (Audit Analytics) | (28,225) |
| Less: Observations for client firms that are breached (Audit Analytics) | (5,276) |
| Less: Observations whose auditor had a merger / acquisition or split (Audit Analytics) | (180) |
| Less: Observations whose auditor deregistered with the PCAOB (Audit Analytics) | (691) |
| Less: Observations missing fees data (Audit Analytics) | (2,478) |
| Client-year observations for calculation of our variables | 55,335 |

**Panel B: Audit Office-Year Sample for Empirical Analyses**

| | Obs. |
|---|---|
| Unique audit office-year observations associated with 55,335 client-year observations | 7,546 |
| Less: Observations with no competitors | (1,030) |
| Less: Observations missing data to calculate variables | (610) |
| Less: Observations that are singletons (Correia 2015) | (105) |
| Sample of audit office-year observations for empirical analyses | 5,801 |

## TABLE 2
## Descriptive Statistics for Audit Office-Year Sample (N = 5,801)

| Variable | Mean | Std. Dev. | 25% | Median | 75% |
|---|---|---|---|---|---|
| *Test Variable* | | | | | |
| *CYBER_EXPERTISE* (logged) | 0.165 | 0.447 | 0.000 | 0.000 | 0.000 |
| *Dependent Variable* | | | | | |
| *OFFICE_MKTSHARE_CHG$_{t+1}$* | -0.016 | 0.402 | -0.143 | 0.000 | 0.109 |
| *Control Variables* | | | | | |
| *OFFICE_MKTSHARE_CHG* | 0.095 | 0.394 | -0.092 | 0.010 | 0.150 |
| *OFFICE_MKTSHARE* | 0.123 | 0.136 | 0.024 | 0.077 | 0.167 |
| *#_MSA_OFFICE* (logged) | 2.558 | 0.688 | 2.079 | 2.565 | 2.890 |
| *#_OFFICE_CLIENTS* (logged) | 1.788 | 0.888 | 1.099 | 1.609 | 2.303 |
| *M_GROWTH* | 0.300 | 0.763 | -0.003 | 0.090 | 0.279 |
| *M_ACC* | 0.198 | 0.320 | 0.049 | 0.091 | 0.192 |
| *M_INVREC* | 0.260 | 0.164 | 0.148 | 0.234 | 0.342 |
| *M_ROA* | -0.744 | 1.986 | -0.355 | -0.028 | 0.035 |
| *M_LOSS* | 0.454 | 0.359 | 0.143 | 0.400 | 0.750 |
| *M_LEV* | 1.397 | 2.519 | 0.487 | 0.629 | 0.832 |
| *M_CASH* | 0.212 | 0.175 | 0.081 | 0.160 | 0.302 |
| *M_SIZE* | 4.998 | 2.682 | 3.103 | 5.468 | 7.224 |
| *M_AQC* | 0.320 | 0.300 | 0.000 | 0.289 | 0.500 |
| *M_GC* | 0.175 | 0.298 | 0.000 | 0.000 | 0.250 |
| *M_MODOP* | 0.143 | 0.235 | 0.000 | 0.000 | 0.214 |
| *M_INITIAL* | 0.094 | 0.214 | 0.000 | 0.000 | 0.083 |
| *M_MISMATCH* | 0.226 | 0.335 | 0.000 | 0.000 | 0.333 |
| *M_EXPERT* | 0.061 | 0.155 | 0.000 | 0.000 | 0.000 |
| *M_ABFEES* | -0.026 | 0.386 | -0.249 | -0.006 | 0.200 |
| *M_SOX404* | 0.455 | 0.384 | 0.000 | 0.500 | 0.800 |
| *M_WEAK* | 0.028 | 0.084 | 0.000 | 0.000 | 0.000 |
| *M_RESTATE* | 0.074 | 0.163 | 0.000 | 0.000 | 0.083 |
| *M_RESIGN_COUNT* | 0.071 | 0.302 | 0.000 | 0.000 | 0.000 |

This table presents descriptive statistics for the audit office-years sample. Continuous variables are winsorized at the 1st and 99th percentiles. All variables are defined in Appendix A.

# TABLE 3
# Pearson Correlations for Audit Office-Year Sample

| | | (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) | (9) | (10) | (11) | (12) | (13) | (14) | (15) | (16) | (17) | (18) | (19) | (20) | (21) | (22) | (23) | (24) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| (1) | OFFICE_MKTSHARE_CHG$_{t+1}$ | 1.00 | | | | | | | | | | | | | | | | | | | | | | | |
| (2) | CYBER_EXPERTISE | 0.02 | 1.00 | | | | | | | | | | | | | | | | | | | | | | |
| (3) | OFFICE_MKTSHARE_CHG | **0.05** | **-0.08** | 1.00 | | | | | | | | | | | | | | | | | | | | | |
| (4) | OFFICE_MKTSHARE | 0.00 | **0.12** | -0.02 | 1.00 | | | | | | | | | | | | | | | | | | | | |
| (5) | #_MSA_OFFICE | **-0.02** | **0.05** | 0.02 | **-0.64** | 1.00 | | | | | | | | | | | | | | | | | | | |
| (6) | #_OFFICE_CLIENTS | 0.01 | **0.44** | **-0.04** | **0.25** | **0.23** | 1.00 | | | | | | | | | | | | | | | | | | |
| (7) | M_GROWTH | 0.01 | -0.01 | **0.08** | **-0.08** | **0.13** | **0.04** | 1.00 | | | | | | | | | | | | | | | | | |
| (8) | M_ACC | -0.01 | **-0.10** | **0.09** | **-0.15** | **0.20** | **-0.02** | **0.37** | 1.00 | | | | | | | | | | | | | | | | |
| (9) | M_INVREC | -0.02 | **-0.09** | -0.01 | 0.00 | **-0.05** | **-0.09** | **-0.14** | **-0.10** | 1.00 | | | | | | | | | | | | | | | |
| (10) | M_ROA | 0.01 | **0.11** | **-0.09** | **0.16** | **-0.24** | 0.02 | **-0.48** | **-0.68** | **0.16** | 1.00 | | | | | | | | | | | | | | |
| (11) | M_LOSS | **-0.04** | **-0.11** | **0.10** | **-0.23** | **0.24** | **-0.07** | **0.17** | **0.37** | **-0.21** | **-0.44** | 1.00 | | | | | | | | | | | | | |
| (12) | M_LEV | -0.02 | **-0.11** | **0.07** | **-0.13** | **0.23** | **-0.04** | **0.09** | **0.50** | **-0.08** | **-0.66** | **0.34** | 1.00 | | | | | | | | | | | | |
| (13) | M_CASH | 0.01 | 0.00 | **0.03** | **-0.16** | **0.17** | 0.02 | **0.20** | **0.27** | **-0.29** | **-0.24** | **0.30** | **0.13** | 1.00 | | | | | | | | | | | |
| (14) | M_SIZE | **0.07** | **0.32** | **-0.14** | **0.37** | **-0.33** | **0.30** | **-0.20** | **-0.50** | **0.07** | **0.57** | **-0.58** | **-0.56** | **-0.42** | 1.00 | | | | | | | | | | |
| (15) | M_AQC | **0.05** | **0.14** | **-0.06** | **0.16** | **-0.19** | **0.12** | **-0.03** | **-0.23** | **0.04** | **0.24** | **-0.26** | **-0.22** | **-0.28** | **0.49** | 1.00 | | | | | | | | | |
| (16) | M_GC | **-0.05** | **-0.17** | **0.12** | **-0.22** | **0.26** | **-0.12** | **0.21** | **0.50** | **-0.15** | **-0.61** | **0.57** | **0.60** | **0.18** | **-0.70** | **-0.32** | 1.00 | | | | | | | | |
| (17) | M_MODOP | 0.01 | **0.27** | -0.02 | **0.16** | **-0.07** | **0.22** | **-0.04** | **-0.14** | **-0.06** | **0.16** | **-0.12** | **-0.15** | **-0.08** | **0.31** | **0.12** | **-0.24** | 1.00 | | | | | | | |
| (18) | M_INITIAL | **0.05** | **-0.10** | **0.55** | **-0.13** | **0.13** | **-0.10** | **0.10** | **0.13** | -0.01 | **-0.16** | **0.20** | **0.14** | **0.06** | **-0.26** | **-0.10** | **0.22** | **-0.07** | 1.00 | | | | | | |
| (19) | M_MISMATCH | 0.01 | **-0.14** | -0.01 | **-0.11** | -0.02 | **-0.06** | **-0.03** | **-0.10** | **0.17** | **0.16** | **-0.13** | **-0.16** | **-0.07** | **0.15** | **0.10** | **-0.20** | **-0.04** | -0.02 | 1.00 | | | | | |
| (20) | M_EXPERT | **0.03** | **0.18** | **-0.07** | **0.32** | **-0.16** | **0.23** | **-0.08** | **-0.15** | **-0.05** | **0.14** | **-0.24** | **-0.12** | **-0.19** | **0.40** | **0.16** | **-0.21** | **0.12** | **-0.12** | **-0.20** | 1.00 | | | | |
| (21) | M_ABFEES | **0.03** | 0.02 | 0.01 | -0.02 | **-0.07** | **0.05** | **-0.05** | -0.01 | **0.04** | **0.07** | 0.02 | **-0.06** | -0.01 | **0.07** | **0.17** | -0.02 | **0.06** | 0.01 | **0.15** | 0.00 | 1.00 | | | |
| (22) | M_SOX404 | **0.08** | **0.23** | **-0.15** | **0.31** | **-0.31** | **0.22** | **-0.17** | **-0.34** | **0.03** | **0.37** | **-0.48** | **-0.32** | **-0.28** | **0.78** | **0.48** | **-0.51** | **0.19** | **-0.22** | **0.14** | **0.31** | **0.10** | 1.00 | | |
| (23) | M_WEAK | -0.01 | **0.05** | 0.00 | 0.02 | **-0.04** | **0.03** | 0.00 | **-0.06** | 0.00 | **0.06** | -0.02 | **-0.07** | **-0.05** | **0.14** | **0.14** | **-0.08** | **0.07** | **0.02** | **0.06** | **0.03** | **0.05** | **0.24** | 1.00 | |
| (24) | M_RESTATE | **-0.03** | 0.00 | **0.04** | **-0.02** | **0.03** | -0.02 | 0.02 | 0.01 | **-0.02** | **-0.04** | **0.07** | **0.02** | **-0.04** | -0.02 | 0.01 | **0.07** | 0.00 | **0.06** | **-0.04** | 0.01 | **0.05** | 0.00 | **0.12** | 1.00 |
| (25) | M_RESIGN_COUNT | **-0.23** | 0.02 | **-0.04** | **-0.04** | **0.11** | **0.11** | **0.05** | **0.09** | -0.02 | **-0.10** | **0.11** | **0.08** | **0.07** | **-0.13** | **-0.07** | **0.12** | **-0.02** | 0.00 | **-0.03** | **-0.05** | **-0.03** | **-0.11** | 0.00 | 0.01 |

This table presents Pearson correlations for the audit office-years sample. Bold values indicate significance at the 0.10 level or lower.

## TABLE 4
## Main Analysis: The Effect of Auditor's Cybersecurity Expertise on Audit Market Share

| **Independent Variables** | **Pr.** | **Dependent Variable:** ***OFFICE_MKTSHARE_CHG***$_{t+1}$ | | | | | |
|---|---|---|---|---|---|---|---|
| | | **(1)** | | **(2)** | | **(3)** | |
| *Test Variable:* | | *Coef.* | *t-stat* | *Coef.* | *t-stat* | *Coef.* | *t-stat* |
| *CYBER_EXPERTISE* | + | 0.0174*** | 2.69 | 0.0720*** | 4.34 | 0.0504*** | 2.92 |
| (*p*-value) | | | (≤0.01) | | (≤0.01) | | (≤0.01) |
| | | | | | | | |
| *Control Variables:* | | | | | | | |
| *OFFICE_MKTSHARE_CHG* | ? | | | | | 0.0277 | 1.32 |
| *OFFICE_MKTSHARE* | - | | | | | -0.5376*** | -2.26 |
| *#_MSA_OFFICE* | + | | | | | 0.1368*** | 2.32 |
| *#_OFFICE_CLIENTS* | - | | | | | -0.2977*** | -7.66 |
| *M_GROWTH* | ? | | | | | 0.0025 | 0.20 |
| *M_ACC* | ? | | | | | -0.0144 | -0.39 |
| *M_INVREC* | ? | | | | | -0.0632 | -0.70 |
| *M_ROA* | ? | | | | | -0.0031 | -0.37 |
| *M_LOSS* | ? | | | | | 0.0030 | 0.10 |
| *M_LEV* | ? | | | | | -0.0052 | -0.97 |
| *M_CASH* | ? | | | | | -0.0110 | -0.12 |
| *M_SIZE* | ? | | | | | 0.0047 | 0.29 |
| *M_AQC* | ? | | | | | 0.0058 | 0.17 |
| *M_GC* | - | | | | | -0.0682 | -1.20 |
| *M_MODOP* | - | | | | | -0.0865** | -2.42 |
| *M_INITIAL* | ? | | | | | 0.1068** | 2.42 |
| *M_MISMATCH* | ? | | | | | 0.0017 | 0.04 |
| *M_EXPERT* | ? | | | | | -0.0428 | -0.60 |
| *M_ABFEES* | - | | | | | -0.0633** | -1.94 |
| *M_SOX404* | ? | | | | | -0.0326 | -0.71 |
| *M_WEAK* | - | | | | | -0.0465 | -0.58 |
| *M_RESTATE* | - | | | | | -0.0147 | -0.34 |
| *M_RESIGN_COUNT* | - | | | | | -0.2988*** | -12.62 |
| | | | | | | | |
| Audit Office Fixed Effects | | NO | | YES | | YES | |
| Year Fixed Effects | | NO | | YES | | YES | |
| N | | 5,801 | | 5,801 | | 5,801 | |
| Adjusted R-squared | | 0.02% | | 8.22% | | 19.16% | |

This table presents the analysis of the effect of an audit office's cybersecurity expertise on its future MSA-level audit market share. The sample consists of audit office-year observations. Column 1 excludes all fixed effects and all control variables. Column 2 includes all fixed effects but excludes all control variables. Column 3 includes all fixed effects and all control variables. All variables are defined in Appendix A. The model in all columns is an ordinary least squares regression with robust standard errors clustered by audit office. ***, **, and * indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests if the coefficient sign is consistent with the predicted direction (when a directional prediction is made) and two-tailed tests otherwise.

## TABLE 5
## Sensitivity Analysis: The Effect of Auditor's Cybersecurity Expertise on Audit Market Share in a Changes Model

| **Independent Variables** | **Pr.** | **Dependent Variable: *ΔOFFICE_MKTSHARE_CHG$_{t+1}$*** | |
|---|---|---|---|
| | | **(1)** | |
| *Test Variable:* | | *Coef.* | *t-stat* |
| *ΔCYBER_EXPERTISE* | + | **0.1118***** | 4.26 |
| (*p*-value) | | | (≤0.01) |
| | | | |
| *Control Variables:* | | | |
| *ΔOFFICE_MKTSHARE_CHG* | ? | -0.1639*** | -7.22 |
| *ΔOFFICE_MKTSHARE* | - | -1.4466*** | -4.79 |
| *Δ#_MSA_OFFICE* | + | 0.2374*** | 3.25 |
| *Δ#_OFFICE_CLIENTS* | - | -0.7481*** | -12.14 |
| *ΔM_GROWTH* | ? | -0.0147 | -1.25 |
| *ΔM_ACC* | ? | -0.0208 | -0.69 |
| *ΔM_INVREC* | ? | -0.0082 | -0.08 |
| *ΔM_ROA* | ? | -0.0001 | -0.01 |
| *ΔM_LOSS* | ? | 0.0050 | 0.16 |
| *ΔM_LEV* | ? | -0.0108** | -2.21 |
| *ΔM_CASH* | ? | 0.1150 | 1.21 |
| *ΔM_SIZE* | ? | 0.0103 | 0.57 |
| *ΔM_AQC* | ? | -0.0053 | -0.14 |
| *ΔM_GC* | - | -0.0566 | -0.99 |
| *ΔM_MODOP* | - | -0.0985*** | -2.74 |
| *ΔM_INITIAL* | ? | 0.1115*** | 2.36 |
| *ΔM_MISMATCH* | ? | 0.0495 | 1.08 |
| *ΔM_EXPERT* | ? | -0.0383 | -0.51 |
| *ΔM_ABFEES* | - | -0.0553* | -1.61 |
| *ΔM_SOX404* | ? | -0.0212 | -0.44 |
| *ΔM_WEAK* | - | -0.0081 | -0.11 |
| *ΔM_RESTATE* | - | -0.0089 | -0.23 |
| *ΔM_RESIGN_COUNT* | - | -0.1726*** | -8.93 |
| | | | |
| Year Fixed Effects | | YES | |
| N | | 4,908 | |
| Adjusted R-squared | | 32.77% | |

This table presents the analysis of the effect of an audit office's cybersecurity expertise on its future MSA-level audit market share in a changes model. The sample consists of audit office-year observations. All variables are defined in Appendix A. The model is an ordinary least squares regression with robust standard errors clustered by audit office. ***, **, and * indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests if the coefficient sign is consistent with the predicted direction (when a directional prediction is made) and two-tailed tests otherwise.

# TABLE 6
## Sensitivity Analysis: The Effect of Auditor's Cybersecurity Expertise on Audit Market Share Calculated Using Fees

| Independent Variables | Pr. | Dependent Variable: *OFFICE_MKTSHARE_CHG_FEES$_{t+1}$* | |
|---|---|---|---|
| | | **(1)** | |
| *Test Variable:* | | *Coef.* | *t-stat* |
| *CYBER_EXPERTISE* | + | **0.0484**** | 1.99 |
| (*p*-value) | | | (0.023) |
| | | | |
| *Control Variables:* | | | |
| *OFFICE_MKTSHARE_CHG_FEES* | ? | -0.0743*** | -3.32 |
| *OFFICE_MKTSHARE_FEES* | - | -0.7287*** | -3.46 |
| *#_MSA_OFFICE* | + | 0.2688*** | 2.83 |
| *#_OFFICE_CLIENTS* | - | -0.3940*** | -7.52 |
| *M_GROWTH* | ? | 0.0446** | 2.17 |
| *M_ACC* | ? | -0.0503 | -0.77 |
| *M_INVREC* | ? | -0.1315 | -0.91 |
| *M_ROA* | ? | -0.0094 | -0.63 |
| *M_LOSS* | ? | -0.1003** | -2.18 |
| *M_LEV* | ? | -0.0060 | -0.59 |
| *M_CASH* | ? | 0.1113 | 0.74 |
| *M_SIZE* | ? | -0.1516*** | -5.73 |
| *M_AQC* | ? | -0.0384 | -0.76 |
| *M_GC* | - | 0.0347 | 0.40 |
| *M_MODOP* | - | -0.1605*** | -3.05 |
| *M_INITIAL* | ? | 0.2763*** | 3.84 |
| *M_MISMATCH* | ? | -0.0263 | -0.43 |
| *M_EXPERT* | ? | 0.1992** | 2.20 |
| *M_ABFEES* | - | -0.5684*** | -8.97 |
| *M_SOX404* | ? | -0.1353** | -2.11 |
| *M_WEAK* | - | -0.2572*** | -2.39 |
| *M_RESTATE* | - | -0.0741 | -1.08 |
| *M_RESIGN_COUNT* | - | -0.2776*** | -7.93 |
| | | | |
| Audit Office Fixed Effects | | YES | |
| Year Fixed Effects | | YES | |
| N | | 5,801 | |
| Adjusted R-squared | | 18.92% | |

This table presents the analysis of the effect of an audit office's cybersecurity expertise on its future MSA-level audit market share, where audit market share is calculated using fees instead of number of clients. The sample consists of audit office-year observations. All variables are defined in Appendix A. The model is an ordinary least squares regression with robust standard errors clustered by audit office. ***, **, and * indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests if the coefficient sign is consistent with the predicted direction (when a directional prediction is made) and two-tailed tests otherwise.

## TABLE 7
## Sensitivity Analysis: The Effect of Auditor's Cybersecurity Expertise on the Number of Audit Clients

| **Independent Variables** | **Pr.** | **Dependent Variable: *#_OFFICE_CLIENTS*$_{t+1}$** | |
|---|---|---|---|
| | | **(1)** | |
| *Test Variable:* | | *Coef.* | *t-stat* |
| *CYBER_EXPERTISE* | + | **0.0413*** ** | 2.91 |
| (*p*-value) | | | (≤0.01) |
| | | | |
| *Control Variables:* | | | |
| *OFFICE_MKTSHARE_CHG* | + | 0.0547*** | 3.62 |
| *OFFICE_MKTSHARE* | + | 0.1017 | 0.55 |
| *#_MSA_OFFICE* | + | -0.0171 | -0.38 |
| *#_OFFICE_CLIENTS* | + | 0.7232*** | 24.37 |
| *M_GROWTH* | ? | 0.0071 | 0.78 |
| *M_ACC* | ? | -0.0228 | -0.76 |
| *M_INVREC* | ? | -0.0873 | -1.34 |
| *M_ROA* | ? | -0.0060 | -0.87 |
| *M_LOSS* | ? | -0.0022 | -0.10 |
| *M_LEV* | ? | -0.0011 | -0.27 |
| *M_CASH* | ? | -0.0348 | -0.52 |
| *M_SIZE* | ? | -0.0029 | -0.25 |
| *M_AQC* | ? | -0.0028 | -0.12 |
| *M_GC* | - | -0.0741** | -1.91 |
| *M_MODOP* | - | -0.0455*** | -1.99 |
| *M_INITIAL* | ? | 0.0645** | 2.08 |
| *M_MISMATCH* | ? | -0.0154 | -0.54 |
| *M_EXPERT* | ? | -0.0365 | -0.81 |
| *M_ABFEES* | - | -0.0489*** | -2.10 |
| *M_SOX404* | ? | 0.0095 | 0.30 |
| *M_WEAK* | - | -0.0580 | -0.93 |
| *M_RESTATE* | - | 0.0030 | 0.11 |
| *M_RESIGN_COUNT* | - | -0.3804*** | -11.18 |
| | | | |
| Audit Office Fixed Effects | | YES | |
| Year Fixed Effects | | YES | |
| N | | 5,801 | |
| Adjusted R-squared | | 91.21% | |

This table presents the analysis of the effect of an audit office's cybersecurity expertise on its future MSA-level number of audit clients. The sample consists of audit office-year observations. All variables are defined in Appendix A. The model is an ordinary least squares regression with robust standard errors clustered by audit office. ***, **, and * indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests if the coefficient sign is consistent with the predicted direction (when a directional prediction is made) and two-tailed tests otherwise.

# TABLE 8
## Additional Analysis: The Effect of Auditor's Cybersecurity Expertise on Client's Cyber Risk Exposure

| Independent Variables | Pr. | Dependent Variable: *CLIENT_CYBER_RISK$_{t+1}$* | |
|---|---|---|---|
| | | (1) | |
| *Test Variable:* | | *Coef.* | *t-stat* |
| *CYBER_EXPERTISE* | - | **-0.0079**** | -1.65 |
| (*p*-value) | | | (0.049) |
| | | | |
| *Control Variables:* | | | |
| *SIZE* | ? | 0.0208*** | 4.62 |
| *LEV* | ? | 0.0043 | 0.79 |
| *ROA* | ? | -0.0026 | -0.96 |
| *MTB* | ? | 0.0002 | 1.05 |
| *FIRM_AGE* | ? | 0.0153 | 1.17 |
| *INST_OWN* | ? | 0.0194** | 2.26 |
| *LN_SEGMENTS* | ? | 0.0052 | 0.59 |
| *FOREIGN* | ? | 0.0137 | 1.57 |
| *AQC* | ? | -0.0027 | -0.68 |
| *RESTRUCTURE* | ? | 0.0040 | 1.09 |
| *BIG4* | ? | 0.0149 | 1.33 |
| | | | |
| Client Firm Fixed Effects | | YES | |
| Year Fixed Effects | | YES | |
| N | | 14,578 | |
| Adjusted R-squared | | 71.79% | |

This table presents the analysis of the effect of an audit office's cybersecurity expertise on client's future cyber risk exposure. The sample consists of client firm-year observations. All variables are defined in Appendix A. The model is an ordinary least squares regression with robust standard errors clustered by client firm. ***, **, and * indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests if the coefficient sign is consistent with the predicted direction (when a directional prediction is made) and two-tailed tests otherwise.

## TABLE 9
## Additional Analysis: The Effect of Auditor's Cybersecurity Expertise on Propensity for Client to Exhibit Information Technology-Related Internal Control Material Weaknesses

| Independent Variables | Pr. | Dependent Variable: *CLIENT_IT_MATERIAL_WEAKNESS$_{t+1}$* | |
|---|---|---|---|
| | | (1) | |
| *Test Variable:* | | *Coef.* | *t-stat* |
| *CYBER_EXPERTISE* | - | **-0.0092**** | -2.29 |
| (*p*-value) | | | (0.011) |
| | | | |
| *Control Variables:* | | | |
| *SIZE* | ? | 0.0180 | 1.48 |
| *SEGMENTS* | ? | -0.0206** | -2.08 |
| *FOREIGN* | ? | 0.0104** | 2.29 |
| *AQC* | ? | -0.0064 | -1.45 |
| *RESTRUCTURE* | ? | 0.0002 | 0.02 |
| *FIRM_AGE* | ? | 0.0015 | 0.53 |
| *SALES_GROWTH* | ? | -0.0392 | -0.64 |
| *INV* | ? | 0.0067 | 1.39 |
| *LOSS* | ? | -0.0014*** | -2.93 |
| *ALTMANZ* | ? | 0.0470** | 2.31 |
| *RESIGN* | ? | 0.0030 | 0.46 |
| *RESTATE* | ? | -0.0369*** | -3.99 |
| *INST_OWN* | ? | 0.0273* | 1.94 |
| *BIG4* | ? | 0.0180 | 1.48 |
| | | | |
| Client Firm Fixed Effects | | YES | |
| Year Fixed Effects | | YES | |
| N | | 27,913 | |
| Adjusted R-squared | | 50.73% | |

This table presents the analysis of the effect of an audit office's cybersecurity expertise on propensity for client to exhibit information technology-related internal control material weaknesses in the future. The sample consists of client firm-year observations. All variables are defined in Appendix A. The model is a linear probability model with robust standard errors clustered by client firm. ***, **, and * indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests if the coefficient sign is consistent with the predicted direction (when a directional prediction is made) and two-tailed tests otherwise.

# TABLE 10
# Additional Analysis: The Effect of Auditor's Cybersecurity Expertise on Client's Audit Fees

| **Independent Variables** | **Pr.** | **Dependent Variable: *CLIENT_AUDIT_FEES$_{t+1}$*** | |
|---|---|---|---|
| | | **(1)** | |
| *Test Variable:* | | *Coef.* | *t-stat* |
| *CYBER_EXPERTISE* | + | **0.0221***** | 3.21 |
| (*p*-value) | | | (≤0.01) |
| | | | |
| *Control Variables:* | | | |
| *SIZE* | + | 0.2797*** | 30.25 |
| *LEV* | + | 0.0321*** | 8.25 |
| *LOSS* | + | 0.0055 | 0.86 |
| *ROA* | - | 0.0035 | 1.07 |
| *CURRENT_ASSETS* | + | 0.0951*** | 2.80 |
| *QUICK_RATIO* | - | -0.0176*** | -9.60 |
| *FOREIGN* | + | 0.0930*** | 5.51 |
| *SEGMENTS* | + | 0.0634*** | 3.49 |
| *DECEMBER* | + | 0.0896* | 1.40 |
| *GC* | + | 0.0355** | 2.05 |
| *BIG4* | + | 0.3208*** | 14.63 |
| | | | |
| Client Firm Fixed Effects | | YES | |
| Year Fixed Effects | | YES | |
| N | | 27,913 | |
| Adjusted R-squared | | 96.68% | |

This table presents the analysis of the effect of an audit office's cybersecurity expertise on client's future audit fees. The sample consists of client firm-year observations. All variables are defined in Appendix A. The model is an ordinary least squares regression with robust standard errors clustered by client firm. ***, **, and * indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests if the coefficient sign is consistent with the predicted direction (when a directional prediction is made) and two-tailed tests otherwise.