The Effect of Auditor Cybersecurity Expertise on Audit Fees and Cyber Incidents

Feiqi (Freddy) Huang

Pace University

fhuang@pace.edu

He Li

Southwestern University of Finance and Economics, China

lihe_stanley@swufe.edu.cn

Zhengjie Sun

Southwestern University of Finance and Economics, China

zhengjie.sun@swufe.edu.cn

Preliminary version. Please do not cite without permission.

The Effect of Auditor Cybersecurity Expertise on Audit Fees and Cyber Incidents

Abstract

This study focuses on local audit offices' cybersecurity expertise and examines the effect of such expertise on non-breached clients' audit fees and future cyber incidents. Using data on cyber incidents from the Audit Analytics cybersecurity database and the Privacy Rights Clearinghouse for the period from 2006 to 2017, we observe a positive and significant association between auditor's cybersecurity experience and non-breached clients' audit fees. This suggests that auditors with greater cybersecurity experience consider cyber risk before any cyber incident has occurred. In addition, we find evidence that the increased audit fees charged by cybersecurity-experienced auditors are negatively associated with non-breached clients' future breaches and auditor's IT capability strengthens the association. Collectively, this finding suggests that auditor's cybersecurity experience is effective in helping clients preventing future cyber incidents and auditor's IT capability strengthens the effectiveness. Our results remain robust after a battery of sensitivity tests.

Keywords: audit fees; cyber incident; auditor cybersecurity expertise.

1. Introduction

Cybersecurity is becoming a great concern to our society after a series of notorious cyber incidents targeting large firms. For example, Marriott International, Inc., a mega hotel chain, was involved in one of the largest data breaches in history, with information such as customer name, address, credit card number, and travel history stolen for up to 500 million customers (Telford and Timberg 2018). According to the latest Data Breach Investigations Report (Verizon 2019), 71 percent of the breaches are financial motivated that are primarily carried out by outsiders (69 percent). More than 20 percent of impacted firms sustained significant loss of revenue and business opportunities (Cisco 2017). Moreover, recent report reveals that criminals who impersonate firm executives instructed employees to make unauthorized fund transfer, a type of cyber-enabled fraud that prompts the SEC to issue an investigative report (SEC 2018c). There is also evidence that attackers steal non-public sensitive information from firms with poor cybersecurity defense for illegal trading (Berkman et al. 2019). Therefore, CEOs exhibit great concern that cybersecurity issue may impede the economic growth of their firms (WSJ 2016). In response to the growing concern of cybersecurity risks, the SEC's Division of Corporation Finance issued cybersecurity disclosure guidance in 2011 and subsequently updated it in 2018, emphasizing the obligation of publicly traded firms to disclose cyber incidents and material risks regarding cybersecurity to investors (SEC 2011, 2018a). Although the SEC initially restrained its actions against firms, the establishment of "cyber unit" of the SEC's Division of Enforcement clearly indicates that the regulator is becoming more aggressive (Berman et al. 2019).

The ever-expanding cybersecurity risk also challenges the role of external auditors in understanding client's information technology environment (Yen et al. 2018). The Center for Audit Quality (2014) issued an alert to summarize external auditors' responsibilities regarding cybersecurity. The PCAOB (2014) has also formed a panel to discuss cybersecurity issues and the potential implications for financial reporting and auditing. In subsequent years, cybersecurity remains a key issue on each year's inspection report. For example, cybersecurity risk is listed as a key area of focus on PCAOB's inspections outlook for 2019 (PCAOB 2018a). Despite that auditors have very limited role related to cybersecurity under current standards, board member of the PCAOB has been calling on auditors to broadly consider cybersecurity risks that could have a material effect on firms' financial statements, and is questioning "*whether the PCAOB's auditing standards should or could require more*" (PCAOB 2019a).

In this paper, we examine the spillover effect of cybersecurity experience through auditor offices. Recent studies by Li et al. (2020), Yen et al. (2018) and Smith et al. (2019) have demonstrated that cyber incidents are positively associated with subsequent audit fees, supporting the argument that auditors are broadly considering the implications of cyber incidents on firms' financial reporting practice and control environment even if there is no explicit requirement. However, it is ex-ante not clear (1) whether auditors are simply responding to a negative event for satisfying regulator's expectation or are systematically considering cybersecurity risks, and (2) whether the experience of responding to cyber incidents can be leveraged to engagements for other clients. To that end, this study investigates the existence of cybersecurity experience spillover by testing the association between cybersecurity experience and audit fees of non-breached clients, and the usefulness of cybersecurity experience by testing the association between increases in audit fees by cyber-experienced auditor office and the likelihood of future cyber incidents for non-breached clients.

We capture auditor office's cybersecurity experience by using the extent that auditors are exposed to cyber incidents during their audit engagements in the past three years. By utilizing cyber incident data from the Audit Analytics cybersecurity database and the Privacy Rights Clearinghouse, we demonstrate that non-breached clients of cybersecurity-experienced auditor offices would have higher audit fees than clients of auditor offices without cybersecurity experience. Furthermore, the increased audit fees by cybersecurity-experienced auditor offices are associated with lower likelihood of subsequent cyber incidents, providing evidence that cybersecurity experience can successfully be transferred to non-breached clients to improve their cybersecurity risk management. In addition, auditor office's IT capability strengthens the association between audit fee increases for clients of cybersecurity-experienced auditor office and the likelihood of subsequent cyber incidents, revealing that the transfer of cybersecurity experience is contingent on auditor office's IT capability. Our results remain robust after a battery of sensitivity results.

The findings of this study provide several contributions to the literature. First, this paper contributes to the audit expertise literature. Prior studies have documented various types of audit expertise, including industry expertise (e.g., Ferguson et al. 2003; Chin and Chi 2009; Bae et al. 2018), multinational expertise (Gunn and Michas 2018), and IT expertise (Haislip et al. 2016). We enrich the audit expertise literature by identifying auditor cybersecurity expertise, which is developed through audit engagements of breached clients. We empirically demonstrate that such experience can be leveraged to other non-breached clients to improve their cybersecurity risk management and prevent future incidents. To our best knowledge, ours is the first study to investigate auditor cybersecurity expertise and its spillover effect to other audit engagements.

Second, different from prior literature (Lawrence et al. 2018; Smith et al. 2019; Li et al. 2020) that document auditor's responses to existing cyber incidents and its effect on future breaches of breached firms, our findings provide evidence that auditors with greater cybersecurity experience take cybersecurity risk into consideration before cyber incidents occur to clients. Also, the increased audit fees charged by cybersecurity-experienced auditors is associated with lower likelihood of future breaches. This suggests that actions taken by cybersecurity-experienced auditors are effective in preventing future cyber breaches. Therefore, this paper also extends the literature by highlighting auditors' role on firms' information security management.

Third, the findings of our study indicate that auditor with IT expertise is more capable of leveraging its cybersecurity experience in helping clients preventing future incidents. This adds value to the extant IT capability literature that identities firm's IT capability as an important factor in addressing cyber risks (e.g., Kwon et al. 2013; Higgs et al. 2016). Our findings that IT capability facilitates auditors to develop cybersecurity knowledge and to address cyber risks in audit engagements suggests that improving IT capability of audit firms is valuable. To the extent that current research primarily focuses on client firm's IT capability, results in this paper highlight the importance of shifting our attention to auditor's IT skills as well.

Finally, this paper provides timely insights to regulators. The PCAOB has identified cybersecurity threat as a topic of growing concern that warrants attention of public firms and auditors, and has highlighted the importance of cybersecurity risk assessment (PCAOB 2018a, 2018b). Then board members of the PCAOB stated in multiple occasions that auditor must consider any cybersecurity risks no matter whether or not a cyber-incident has occurred (PCAOB 2019a, 2019b). Our findings comfort, at least partially, regulators' concern by providing evidence that auditors with cybersecurity experience consider non-breached clients' cybersecurity risk and their responses are effectively eliminating cybersecurity risk.

The remainder of the study is organized as follows. The next section introduces the research background and develops hypothesis. The third section describes the research design and sample selection. Primary results and robustness tests are reported in the fourth section. The last section concludes this paper.

2. Background and Hypothesis Development

2.1 Background and literature review

The digital economy has made cybersecurity a top priority on regulator's agenda. The Division of Corporation Finance, a branch of the SEC that is responsible for the oversight of disclosure practices, issued a disclosure guidance that highlights the Division's view on disclosure requirement related to cybersecurity. Realizing that the prior guidance is non-authoritative, the commission itself further provided guidance in 2018 to expand and interpret the 2011 cybersecurity disclosure guidance (SEC 2018a, 2018d), with the intention to promote more transparent disclosure about cybersecurity risks and incidents to investors and to deter potential insider trading activities resulting from material, non-public cybersecurity information (EY 2018). Till today, the PCAOB has not yet issued any legislative rulings specific for cybersecurity, but is closely monitoring how engagement teams evaluate the risks of material misstatement and associated control issues following a cyber incident (PCAOB 2015, 2016). PCAOB's inspection outlook for 2019 also placed cybersecurity risks as one of the top 10 key areas of inspection focus (PCAOB 2018a). Kathleen M. Hamm, the then board member of the PCAOB, has urged auditors to "understand the methods used by the company to prevent and detect cyber-incidents that could have a material effect on the financial statements" (PCAOB 2019b).

Academic research on cybersecurity in the accounting and finance domain can be broadly categorized into three types. The first stream of research focuses on the economic consequence of cybersecurity breaches. Early studies that examine market reaction to publicly announced data breaches tend to find a negative impact (e.g., Campbell et al. 2003; Goel and Shawky 2009; Hinz et al. 2015). Ettredge and Richardson (2003) and Hinz et al. (2015) reveals that there exist spillover effects of data breaches. Share prices of firms in the same industry or similar firms are also negatively influenced. However, some research work fails to find such association (e.g., Hilary et al. 2016; Richardson et al. 2019). Both Gordon et al. (2011) and Richardson et al. (2019) argue that the inconsistent results can be explained by difference in sample, selection criteria, and research method. In addition to examining market valuation, a limited but growing number of studies are investigating the impact of cyber incidents on audit engagement. Lawrence et al. (2018) reveal that data breaches are positively associated with subsequent audit fees, restatement, SEC comment letters, and ICFR. Smith et al. (2019) find that increase in audit fees are driven only by data breaches that are initiated externally, and that the audit committees and board-level risk committees can mitigate the fee premium. Yen et al. (2018) suggests that the association between audit fees and cyber incidents are moderated by characteristics of the audit firm, including industry expertise, tenure, and whether the audit firm is one of the big 4. A more recent study by Li et al. (2020) systematically evaluates auditor’s effort in addressing cybersecurity risks and reports that auditors price cybersecurity risks ex-ante, respond to severe cyber incidents ex-post, and that such effort is negatively associated with subsequent cyber incidents.

The second stream of research concentrates on the mitigation of cybersecurity risks. Kwon et al. (2013) shows that the involvement of IT executives in the top management team and the relative pay status of IT executives can enhance firm’s IT governance and are negatively associated with cyber incidents. Similarly, Zafar et al. (2016) finds that placing CIO in the top management team can help firms better recover from the economic consequence of cyber incidents. Higgs et al. (2016) reports that firms with board-level technology committee are more likely to be breached, but the association is driving by relatively younger committees. In addition, the presence of technology committee can mitigate the negative market reaction following cyber incidents. Several studies particularly focus on the role of internal auditors in mitigating cybersecurity risks. By conducting interviews, Steinbart et al. (2012) concludes that the nature of relationship between internal audit function and information systems security function differs at different firms. The study is further extended by Steinbart et al. (2013), which shows that a good relationship between these two functions improves the perceived effectiveness of firm's cybersecurity management program. Using a unique dataset, Steinbart et al. (2018) empirically demonstrates that a good relationship between these two functions has a positive impact on the number of security incidents detected both before and after these incidents cause harm to the firm, suggesting that firms should cultivate a collaborative relationship between these two functions as an effective to improve cybersecurity.

The third stream of research centers on the disclosure of cybersecurity-related issues. Early empirical work by Gordon et al. (2006) provides evidence that voluntary disclosure of information security activities increased over 100 percent after the passage of SOX. A follow-up study by Gordon et al. (2010) demonstrates the market positively value the voluntary disclosure concerning information security. Specifically, disclosures of proactive security activities have the largest positive impact on market valuation, followed by the disclosure of security vulnerabilities. Wang et al. (2013) reveals that firms which voluntarily disclosed risk-mitigation themes are negatively associated with the likelihood of future data breaches, suggesting that firms disclosing countermeasures are indeed taking actions to address cybersecurity risks. A subsequent study by Li et al. (2018) examines the usefulness of cybersecurity-related risk factor disclosures and finds that both the presence and length of risk factor disclosures concerning cybersecurity in the Item 1A section of firm's annual reports are related to future reported cyber incidents, but the association between the presence of such risk factor disclosures and future incidents disappears after the passage of cybersecurity disclosure guidance, implying that the disclosure guidance may encourage firms with low cybersecurity risks to make such disclosures. Ettredge et al. (2018) identifies that firms mentioning the existence of trade secrets are more likely to be breached than other firms, especially for younger firms, firms with fewer employees, and firms in less concentrated industries. Amir et al. (2018) reports that managers will only disclose an existing cyber incident when investors are quite confident that an attack has happened. Furthermore, they find that withholding cyber incidents are severely punished by the market when the incident is subsequently discovered by sources other than the breached firms, while directly disclosing cyber-attacks are associated with a substantially lower decline of market value. Berkman et al. (2018) develops a measure to capture the extent and relevance of disclosure regarding cybersecurity, and empirically demonstrates that cybersecurity awareness is positively valued by the market. Finally, using the measure developed by Berkman et al. (2018), Berkman et al. (2019) discovers that a large portion of new earnings information is priced before the earnings announcement for firms with weak cybersecurity controls, indicating that weak cybersecurity risk mitigation may be exploited by attackers to gain unfair advantage in the financial market.

2.2 Hypothesis development

Our first hypothesis attempts to link the association between auditor cybersecurity experience and audit fees of non-breached clients. We argue that audit fees for non-breached clients would be higher when the auditor office has cybersecurity experience because (1) auditor offices with cybersecurity experience have incentives to charge a fee premium for being expertise on addressing cybersecurity risks, and because (2) cybersecurity-experienced offices are likely to expand their audit procedure to assess and reduce cybersecurity risks due to reputational concerns.

With respect to the first incentive, auditor offices can accumulate deep knowledge of cybersecurity risks and the proper response to those risks when their clients fall the victim of such attacks. For example, after an incident occurs, auditors need to understand the internal and external environment of cybersecurity, evaluate the potential access points into information systems, and identify firm's common practices that prevent and detect unamortized access to systems and information assets (PCAOB 2019b). Generally, audit firms modified their audit approaches or procedures to address the potential impact on relevant controls and the data generated by the company's IT systems and some audit offices have also established a group of cybersecurity experts to serve as specialist to address cybersecurity risks (PCAOB 2019d). The time and effort by the auditor office to understand the determinants and consequences of cyber incidents are arguably valuable for other clients as well because malicious hackers usually employ the same or similar methods to target different firms (PCAOB 2019c). Although it is likely that audit firms have internal trainings regarding how to respond to cybersecurity risks and incidents after the SEC and PCAOB repeatedly emphasized cyber threats (e.g., SEC 2018a; PCAOB 2019d), prior research has documented that offices primarily develop their expertise in directly serving clients. That is, indirect experience such as training and education is less effective than direct experience that is gained from interacting a breached client (Solomon et al. 1999; Zacks et al. 1982; Hasher and Zacks 1979). Therefore, auditor offices whose clients has experienced cyber incidents are likely to be expertise in addressing cybersecurity risks than other auditor offices. Since the auditing pricing literature indicates that office-level industry expertise generates an audit premium (Ferguson et al. 2003; Francis et al. 2005), it is thus reasonable to conjecture that auditor office's cybersecurity experience will result in fee premium in a similar way.

With respect to the second incentive, Kathleen M. Hamm, the board member of the PCAOB, states at the 18th Annual Financial Reporting Conference that auditors should remain professionally skeptical throughout the audit even if a specific cyber incident has not been identified because the average detection time is more than 6 months (PCAOB 2019b). Supporting the argument, both Li et al. (2020) and Smith et al. (2019) have revealed that auditors are evaluating cybersecurity risks before an actual event occurs. We argue that if client of a specific office has experienced cyber incidents, the office is under greater pressure to evaluate other firm's cybersecurity risks. Cyber incidents are considered to be realization of weakness in internal controls over operation, which could be indicative of weakness in internal control over financial reporting (Smith et al. 2019). The underlying reason is that controls for financial reporting and controls for operating activities are not separated. Instead they often reply on some shared controls. If one area is not well protected, it is possible that the other area is also compromised (Lawrence et al. 2018)[1]. In addition, weaknesses in internal controls over operation may suggest lack of commitment by management to develop a strong internal control environment, which is the basis for internal control practices identified by the COSO framework (COSO 2013). Since ICFR is the direct responsibility of the auditors, the occurrence of cyber incidents for one client may be perceived as audit failure of not properly evaluating ICFR, which could have implications for other clients of the same auditor office (Francis and Michas 2013). Indeed, there is argument by the practitioners that auditors should be held responsible after cyber incident happens (McKenna 2019). To that end, auditor office, after its client suffers cyber incident, is likely to pay greater

[1] A similar statement was also made by Rani Hoitash, Professor of Bentley University, to an interview by the MarketWatch. See https://www.marketwatch.com/story/equifax-auditors-are-on-the-hook-for-data-security-risk-controls-2017-10-02. In addition, the SEC is also pursuing firms after cyber incidents base on perceived shortcomings of breached firm's ICFR. See SEC Priorities and Enforcement Trends. Available at: https://m.acc.com/chapters/del/upload/2016-04-19_AkinGump_SEC_Trends-PPTX.pdf.

attention to other clients' cybersecurity risk and exert additional efforts to address such risk, leading to an increase in audit fees.

It is arguable that audit fees are not solely determined by auditors but reflect a negotiation between the management and the auditor (Abbott et al. 2003). In fact, anecdotal evidence suggests that auditors have difficulty raising audit fees due to intense completion for new clients (Richardson et al. 2019). However, as SEC has repeatedly emphasized cybersecurity (SEC 2011, 2018b, 2018a), firms are under greater pressure complying with SEC's cybersecurity disclosure guidance and also urgently demand assistance in evaluating cybersecurity controls[2]. Since auditors are more capable of identifying control issues than managers (Bedard and Graham 2011), their expertise may help the manager to improve the preparedness for cyberattacks (Li et al. 2020), it is therefore understandable that increase in audit fees resulting from cybersecurity risk evaluation would be acceptable for managers.

Despite the above arguments that would suggest a positive association between cybersecurity experience and audit fees of non-breached clients, Richardson et al. (2019) pointed out that these risks have long been known and thus have already been priced into audit fees regardless of cybersecurity experience. Furthermore, Yen et al. (2018) argues that industry expertise can help auditors better assess cybersecurity risks and evaluate cybersecurity management processes with less effort, which implies that we would expect a negative association. Therefore, we introduce our first hypothesis in the alternative form:

[2] There is even a bill introduced by Senator Ron Wyden proposing "jail executives who knowingly sign off on incorrect or inaccurate annual certifications of their firm's cyber security policies" (Chatterjee 2019). Should executives go to jail over cybersecurity breaches?

H1: Ceteris paribus, audit fees would be higher for non-breached clients of audit offices with cybersecurity experience than for those clients of audit offices without cybersecurity experience.

The second hypothesis focuses on the value relevance of increased audit fees for cybersecurity experience. That is, whether the increase in audit fees for non-breached clients of cyber-experienced auditor offices is associated with lower likelihood of future cyber incidents. Li et al. (2020) find that raise in audit fees for breached firm is associated with fewer subsequent incidents for the same breached firm, suggesting that the additional fees charged by auditors at least partially reflect audit effort that could address cybersecurity risks. However, it is ex-ante not clear whether the experience of directly responding to cyber incidents can be successfully transferred to engagements for other clients. Auditing literature has provided ample evidence that there is spillover effect of audit quality among clients of the same auditor offices (Li et al. 2015). Francis and Michas (2013) present that the audit failure for one client could be indicative of audit failure for other clients within the office. In other words, auditor office could serve as an effective channel, through which similar-quality audits spillover to other client firms within the same office due to similar office-level auditing procedure, quality-control standard, cognitive style, tolerance for aggressive accounting practices, and other unobserved factors (Francis and Michas 2013; Krishnan 2005).

Specific to cybersecurity, auditor offices are likely to train their employees with cyber-specific knowledge after interacting with breached clients, which can be used in other engagements. We therefore expect that:

H2: Ceteris paribus, increase in audit fees for clients of cybersecurity-experienced audit office is negatively associated with the likelihood of future cyber incidents.

Our last hypothesis concentrates on the effect of auditor office's IT capability on the transfer of cybersecurity experience. Auditor's IT capability is defined as auditor's expertise in firm's financial reporting environments that heavily dependent on IT (Haislip et al. 2016). Prior studies consistently find that client's IT capability is an important factor in addressing cyber risks. For example, firms are less likely to experience cyber incidents when there is a CIO position in the firm, when the IT manager has greater power, and when there are more established technology committees (Kwon et al. 2013; Higgs et al. 2016). In addition, IT ability of a peer firm can moderate the contagion effect of a cyber incident (Kashmiri et al. 2017). To our context, auditors with greater IT knowledge including the understanding of information security will better assess client's control systems, especially IT-related elements. Given cyber breaches are inherently related to firms' IT related controls, we expect that auditor offices with better IT capability to be more successful in applying knowledge of interacting with breached clients to other non-breached clients. This leads to our third hypothesis:

H3: Ceteris paribus, the association between increase in audit fees for clients of cybersecurity-experienced auditor office and the likelihood of future cyber incidents is moderated by auditor office's IT capability.

3. Research Design

3.1 Model specification

Since auditors are required to assess the nature and extent of the incident for breached firms and evaluate its impact on firm's operations and financial performance (PCAOB 2019), auditor office with more clients experiencing cyber incidents would accumulate greater expertise on cybersecurity. Therefore, we proxy auditor's cybersecurity experience by using the extent that auditors are exposed to cyber breaches during their audit engagements following the logic that auditor industry expertise is developed through audits within an industry (e.g., Ferguson et al. 2003; Chin and Chi 2009). In addition, suggested by prior literature that IT-related capability may be developed over time and auditors' IT expertise is measured using the previous three years' experience (Haislip et al. 2016; Huang et al. 2018), we define auditor cybersecurity experience as the total number of times that clients of an audit office experienced cyber incidents in the previous three years, scaled by the total number of clients of that audit office[3].

In addition, we capture auditor cybersecurity experience at the local office level for two reasons. First, prior literature has well documented that the office-level characteristics including audit quality and expertise exhibit significant variation. Second, the local office has significant autonomy and is largely responsible for personnel assignments, audit engagements administering, and many other strategic functions. This is also consistent with recent literature that focuses on audit quality and audit expertise at the local office level (e.g., McGuire et al. 2012; Swanquist and Whited 2015; Gunn and Michas 2018)

$$\begin{aligned} LogAuditFees_t & \\ = {} & CyberExp_t + OfficeSize_t + OfficeMS_t + OfficeInd_t + Size_t \\ & + Growth_t + Btm_t + ROA_t + InvRec_t + Segment_t + Foreign_t \\ & + Merger_t + Special_t + Loss_t + Leverage_t + Quick_t \\ & + GoingConcern_t + Restatement_t + ICW_t + Big4_t + Initial_t \\ & + YearFE + AuditorOfficeFE + FirmFE \end{aligned} \tag{1}$$

We test our first hypothesis using an audit fees model based on prior literature (e.g., Stanley 2011; Elliott et al 2013; Doogar et al 2015; Li et al 2019). To mitigate concerns about endogeneity, we follow Li et al (2019) to control for firm fixed effects that transforms the level model into a difference-in-difference (DID) design, which is suitable for identifying causal effects (Armstrong

[3] In addition to the measure based on the number of client, we use audit fee based measure as an alternative proxy for auditor cybersecurity experience. Untabulated results show that the results are comparable to the results of our main models.

et al. 2012)[4].The variable of interest is $CyberExp$, which captures auditor cyber-incident experience. A positive coefficient of $CyberExp$ will support H1 and suggest that auditors with higher cybersecurity experience charge higher audit fees compared with non-experienced peers.

Audit office controls include office size (*OfficeSize*), office market share (*OfficeMS*), and office industry expertise (*OfficeInd*). Firm characteristics are firm size (*Size*), sales growth (*Growth*), book to market ratio (*Btm*), and return on assets (*ROA*). In addition, other controls include firm complexity variables (*InvRec*, *Segment*, *Foreign*, *Merger*, and *Special*), risk-related factors (*Loss*, *Leverage*, *Quick*, *GoingConcern*, *Reseatement*, and *ICW*) and auditor related variables (*Big4* and *Initial*).

To examine the second hypothesis, we adopt a logit model from Wang et al. (2013), Higgs et al. (2016), and Li et al. (2019).

$$\begin{aligned} P(CyberIncident_{t+1} = 1) \\ &= CyberExp_t \times \Delta LogAuditFees_t + CyberExp_t + \Delta LogAuditFees_t \\ &+ OfficeSize_t + OfficeMS_t + OfficeInd_t + Size_t + Growth_t \\ &+ ROA_t + Segment_t + Loss_t + Leverage_t + ICW_t + YearFE \\ &+ IndustryFE + AuditorOfficeFE. \qquad (2) \end{aligned}$$

Our focus is the interaction term *CyberExp**$\Delta LogAuditFees$. A negative coefficient would suggest that higher audit fees charged by auditors with cybersecurity experience are associated with a lower likelihood of future cyber incidents, demonstrating the spillover effect of experience in cybersecurity. Appendix A presents detailed definitions of all variables.

[4] We do not use two-stage model or propensity score matching as our main tests, because Lennox et al (2012) suggested that two-stage model is fragile and propensity score matching can’t control for the endogeneity issue raised from unobservable factors. Nevertheless, we rerun our model using propensity score matched sample and report the results in the robustness tests section.

3.2 Sample selection

The cyber incident data is obtained from the Audit Analytics cybersecurity database and the Privacy Rights Clearinghouse, covering the period from 2006 to 2017 and containing 739 cyber incidents. After joining to the Compustat and the Audit Analytics database and keeping only the first incident for firms experiencing multiple cyber breaches in a single fiscal year, 375 cyber breaches are included. Then, firms audited by foreign auditors are excluded because of the lacking of U.S. Metropolitan Statistical Areas (MSAs) data and firms in the financial industry (SIC 6000-6999) are removed due to the different audit fees structure. Since our model requires data of cyber incidents in the prior three years (to measure cybersecurity experience) and data of cyber incidents in the subsequent year (to measure future incident), sample from year 2006 to year 2008 and year 2017 are also deleted. Since Smith et al. (2019) and Li et al. (2020) have recently documented that auditors charge higher audit fees for firms experienced cyber incidents, we further exclude observations experienced cyber breaches in current or previous years to avoid the confounding effect of breaches on audit fees. Finally, after eliminating observations with missing values for the variables used in our test, 21991 observations are included in the final sample, which consists of 3955 firm-year observations audited by auditors with cyber-incident experience and 18036 observations audited by auditors without cyber-incident experience. Table 1 presents the sample selection process.

(Insert Table 1 here)

Table 2 presents descriptive statistics for our sample. $LogAuditFees_t$ has a mean value of 13.512, corresponding to \$1.13 million dollars. The mean value of $Restatement_t$ is 0.113, highlighting that 11.3 percent of firms disclose restatements over a two-year period. ICW_t has a mean value of 0.036, indicating that 3.6 percent of firm-years have a SOX 404 internal control weaknesses over financial reporting. Column 7 - 12 of Table 2 present the means and medians of variables for subsamples audited by auditors with or without cyber-incident experience. As the results show, auditors with cyber-incident experience charge higher audit fees, have more clients, have greater industry expertise, and are more likely to be the Big 4 auditors. In addition, many firm characteristics are significantly different. For instance, firms audited by cyber incident experts have larger size, higher ROA, and are more likely to issue restatement and have material internal control weaknesses.

(Insert Table 2 here)

4. Empirical Results

4.1 Main models

Table 3 presents the results of the model (1). The coefficient on *CyberExp* is positive and significant ($p<0.01$), suggesting that *CyberExp* are positively associated with audit fees. Consistent with our first hypothesis, the result indicates that auditors with greater cybersecurity experience charge higher audit fees to non-breached clients. Control variables are mainly significant as predicted. Specifically, *Size*, *InvRec*, *Segments*, *Foreign*, *Merger*, *Special*, *Loss*, *Leverage*, *GoingConcern*, *Restatement*, *ICW*, *Big4* lead to audit fees, while *ROA*, *Quick* and *Initial* are negatively associated with audit fees.

(Insert Table 3 here)

Table 4 presents the test of H2 regarding the likelihood of future breaches. The interaction term *CyberExp**$\Delta LogAuditFees$ is significantly negative ($p<0.05$), indicating that increased audit fees charged by auditors with more cybersecurity experience are negatively associated with cyber breaches in the following year. This suggest that auditor's cybersecurity experience is effective on preventing future breaches, supporting our second hypothesis.

(Insert Table 4 here)

Third hypothesis measures the moderating effect of auditor IT expertise. We follow Haislip et al. (2016) to proxy auditor IT expertise using the InformationWeek database, which identifies clients' IT capability (e.g., Santhanam and Hartono 2003; Chae et al. 2014; Huang et al. 2018). Because with more clients having greater IT capability, auditors are exposed to more IT integrated systems and have a greater understanding of IT through the clients that they audit. Specifically, auditor IT expertise, *ITExp*, is the total number of clients who are identified as high-IT-capability firms, scaled by the total number of clients of each local office per year. Table 5 presents the moderating effect of auditor IT capability on future breaches. The interaction term $CyberExp*\Delta LogAuditFees*ITExp$ is negative and significant ($p<0.05$), demonstrating that auditor with IT expertise is more capable of leveraging its cybersecurity experience in helping clients preventing future incidents. The results support our third hypothesis. Collectively, the results of Table 5 imply that auditor's IT expertise is the driving force for the spillover of cybersecurity experience. Although we don't expect any moderating effect on the association of cybersecurity expertise and audit fees, untabulated results show a positive but non-significant coefficient on *CyberExp**ITExp*, implying that cybersecurity-experienced auditors raise audit fees at similar levels regardless of their IT expertise.

(Insert Table 5 here)

4.2 Robustness tests

4.2.1 Propensity score match

To address the potential selection bias that clients audited by auditors with greater cyber experience may exhibit firm-specific characteristics that drive our results, we use a propensity score matched sample to evaluate our main results. Suggested by Shipman et al. (2017), all control variables in model (1) are included in the matching procedure. Within the caliper distance of 0.001, the treatment observation is matched with the nearest control observation. Results estimated using PSM sample are presented in Table 6. Panel A shows the results of H1 and Panel B displays that of H2. The variable of interest are positive (negative) and significant (p<0.10) for H1 (H2). However, the moderating effect of auditor IT expertise is only marginally significant (p=0.14). Overall, the results using PSM sample are weaker in statistical significance but mainly consistent with our main models.

(Insert Table 6 here)

4.2.2. Alternative measures

Instead of measuring auditor cybersecurity experience based on the number of clients who had cyber incidents, we use alternative proxy based on total audit fees of clients who had cyber incidents in past three years, scaled by total audit fees for each audit office. Untabulated results are robust to our main findings.

Although we believe that auditor cybersecurity experience may be developed over time and it is measured based on three years' experience, we calculate alternative measures based on one- or two-year experience and rerun our models. Generally, we observe statistically weaker but similar results, which consistent with our expectation that auditor's cybersecurity experience is accumulated over time.

5. Concluding Remark

Cybersecurity threat is a topic of growing concern among public companies, investors, regulators, auditors, and others. This study focuses on auditor's cybersecurity experience at the local office level and examines the effect of such experience on audit engagements. Using data on cyber incidents from the Audit Analytics cybersecurity database and the Privacy Rights Clearinghouse for the period from 2006 to 2017, we measures auditor cybersecurity experience as the total number of times that clients of an audit office experienced cyber incidents in the previous three years, scaled by the total number of clients of that audit office. Then, we observe a positive and significant association between auditor's cybersecurity experience and non-breached clients' audit fees. This suggests that auditors with greater cybersecurity experience consider cyber risk before any cyber incident has occurred. In addition, our findings provide evidence that the increased audit fees charged by cybersecurity-experienced auditors are negatively associated with future breaches, implying that such experience is effective in helping clients preventing future incidents. Finally, auditor's IT capability strengthens the association between audit fee increases for clients of cybersecurity-experienced auditor office and the likelihood of subsequent cyber incidents. This finding suggests that auditor's IT expertise is the driving force for the spillover of cybersecurity experience.

Our study is subject to several limitations. First, since we consider only publicly available cyber incidents, our sample size for cyber incidents is small. It is possible that some cyber breaches are not disclosed to the public or not are not discovered by the victim itself. Additional cyber breaches dataset might be helpful to supplement our findings. Second, although we believe that auditors accumulate experience through prior audit engagements and charge higher audit fees due to their cybersecurity expertise, our empirical study cannot completely rule our other reasons. Other type of research such as interview or case study may help us build a comprehensive understating.

Refereces

Abbott, L. J., S. Parker, G. F. Peters, and K. Raghunandan. 2003. The association between audit committee characteristics and audit fees. *Auditing: A Journal of Practice & Theory* 22 (2):17-32.

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.

Armstrong, C. S., K. Balakrishnan, and D. Cohen. 2012. Corporate governance and the information environment: Evidence from state antitakeover laws. *Journal of Accounting and Economics* 53 (1-2):185-204.

Bae, G. S., S. U. Choi, and J. E. Lee. 2018. Auditor industry specialization and audit pricing and effort. *Auditing: A Journal of Practice & Theory* 38 (1):51-75.

Bedard, J. C., and L. Graham. 2011. Detection and severity classifications of Sarbanes-Oxley Section 404 internal control deficiencies. *The Accounting Review* 86 (3):825-855.

Berkman, H., J. Jona, G. Lee, and N. Soderstrom. 2018. Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy* 37 (6):508-526.

Berkman, H., J. Jona, G. Lee, and N. S. Soderstrom. 2019. Digital insiders and informed trading before earnings announcements. *Working paper.*

Berman, S., I. Roffman, and M. Todman. 2019. Year in review: the SEC and cybersecurity.

Campbell, K., L. A. Gordon, M. P. Loeb, and L. Zhou. 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security* 11 (3):431-448.

Center for Audit Quality. 2014. CAQ member alert: Cybersecurity and the external audit.

Chae, H.-C., C. E. Koh, and V. R. Prybutok. 2014. Information technology capability and firm performance: contradictory findings and their possible causes. *MIS Quarterly* 38 (1):305-326.

Chatterjee, D. 2019. Should executives go to jail over cybersecurity breaches? *Journal of Organizational Computing and Electronic Commerce* 29 (1):1-3.

Chin, C. L., and H. Y. Chi. 2009. Reducing restatements with increased industry expertise. *Contemporary Accounting Research* 26 (3):729-765.

Cisco. 2017. Annual cybersecurity report.

COSO. 2013. Internal Control — Integrated Framework (2013).

Ettredge, M., F. Guo, and Y. Li. 2018. Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy* 37 (6):564-585.

Ettredge, M. L., and V. J. Richardson. 2003. Information transfer among internet firms: the case of hacker attacks. *Journal of Information Systems* 17 (2):71-82.

EY. 2018. SEC reporting update.

Ferguson, A., J. R. Francis, and D. J. Stokes. 2003. The effects of firm-wide and office-level industry expertise on audit pricing. *The Accounting Review* 78 (2):429-448.

Francis, J. R., and P. N. Michas. 2013. The contagion effect of low-quality audits. *The Accounting Review* 88 (2):521-552.

Francis, J. R., K. Reichelt, and D. Wang. 2005. The pricing of national and city-specific reputations for industry expertise in the US audit market. *The Accounting Review* 80 (1):113-136.

Goel, S., and H. A. Shawky. 2009. Estimating the market impact of security breach announcements on firm values. *Information & Management* 46 (7):404-410.

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and T. Sohail. 2006. The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy* 25 (5):503-530.

Gordon, L. A., M. P. Loeb, and T. Sohail. 2010. Market value of voluntary disclosures concerning information security. *MIS quarterly*:567-594.

Gordon, L. A., M. P. Loeb, and L. Zhou. 2011. The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security* 19 (1):33-56.

Gunn, J. L., and P. N. Michas. 2018. Auditor multinational expertise and audit quality. *The Accounting Review* 93 (4):203-224.

Haislip, J. Z., G. F. Peters, and V. J. Richardson. 2016. The effect of auditor IT expertise on internal controls. *International Journal of Accounting Information Systems* 20:1-15.

Hasher, L., and R. T. Zacks. 1979. Automatic and effortful processes in memory. *Journal of experimental psychology: General* 108 (3):356.

Higgs, J. L., R. E. Pinsker, T. J. Smith, and G. R. Young. 2016. The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems* 30 (3):79-98.

Hilary, G., B. Segal, and M. H. Zhang. 2016. Cyber-Risk Disclosure: Who Cares? *Georgetown McDonough School of Business Research Paper* (2852519).

Hinz, O., M. Nofer, D. Schiereck, and J. Trillig. 2015. The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management* 52 (3):337-347.

Huang, F., H. Li, and T. Wang. 2018. Information technology capability, management forecast accuracy, and analyst forecast revisions. *Accounting Horizons* 32 (3):49-70.

Kashmiri, S., C. D. Nicol, and L. Hsu. 2017. Birds of a feather: intra-industry spillover of the Target customer data breach and the shielding role of IT, marketing, and CSR. *Journal of the Academy of Marketing Science* 45 (2):208-228.

Krishnan, J. 2005. Audit committee quality and internal control: An empirical analysis. *The Accounting Review* 80 (2):649-675.

Kwon, J., J. R. Ulmer, and T. Wang. 2013. The association between top management involvement and compensation and information security breaches. *Journal of Information Systems* 27 (1):219-236.

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

Li, H., W. G. No, and J. E. Boritz. 2020. Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice & Theory*, forthcoming.

Li, H., W. G. No, and T. Wang. 2018. SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems* 30:40-55.

McGuire, S. T., T. C. Omer, and D. Wang. 2012. Tax avoidance: Does tax-specific industry expertise make a difference? *The Accounting Review* 87 (3):975-1003.

McKenna, F. *Equifax auditors are on the hook for data security risk controls.* 2019.

Public Company Accounting Oversight Board (PCAOB). 2014. Standing advisory group meeting.

———. 2015. Staff inspection brief. Information about 2015 inspections.

———. 2016. Staff inspection brief. Information about 2016 inspections.

———. 2018a. Inspections outlook for 2019.

———. 2018b. Standing advisory group meeting.

———. 2019a. Cybersecurity: a holistic approach.

———. 2019b. Cybersecurity: where we are; what more can be done? A call for auditors to lean in.

———. 2019c. "Keep calm and carry on": The role of regulators in cybersecurity and resiliency.

———. 2019d. Staff Preview of 2018 Inspection Observations.

Richardson, V., M. W. Watson, and R. E. Smith. 2019. Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches. *Journal of Information Systems*.

Santhanam, R., and E. Hartono. 2003. Issues in linking information technology capability to firm performance. *MIS Quarterly*:125-153.

Securities and Exchange Commission (SEC). 2011. CF disclosure guidance: Topic No. 2.

———. 2018a. Commission statement and guidance on public company cybersecurity disclosures.

———. 2018b. Public companies should consider cyber threats when implementing internal accounting controls.

———. 2018c. Report of investigation pursuant to Section 21(a) of the Securities Exchange Act of 1934 regarding certain cyber-related frauds perpetrated against public companies and related internal accounting controls requirements.

———. 2018d. Statement on cybersecurity interpretive guidance.

Shipman, J. E., Q. T. Swanquist, and R. L. Whited. 2017. Propensity score matching in accounting research. *The Accounting Review* 92 (1):213-244.

Smith, T. J., J. L. Higgs, and R. E. Pinsker. 2019. Do auditors price breach risk in their audit fees? *Journal of Information Systems* 33 (2):177-204.

Solomon, I., M. D. Shields, and O. R. Whittington. 1999. What do industry-specialist auditors know? *Journal of Accounting Research* 37 (1):191-208.

Steinbart, P. J., R. L. Raschke, G. Gal, and W. N. Dilla. 2012. The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems* 13 (3):228-243.

———. 2013. Information security professionals' perceptions about the relationship between the information security and internal audit functions. *Journal of Information Systems* 27 (2):65-86.

———. 2018. The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society* 71:15-29.

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.

Telford, T., and C. Timberg. 2018. Marriott discloses massive data breach affecting up to 500 million guests. . *Washington Post*.

Verizon. 2019. Data breach investigations report (2019).

Wang, T., K. N. Kannan, and J. R. Ulmer. 2013. The association between the disclosure and the realization of information security risk factors. *Information Systems Research* 24 (2):201-218.

WSJ. 2016. Cybersecurity and the board: 8 issues keeping directors up at night. *Wall Street Journal*.

Yen, J.-C., J.-H. Lim, T. Wang, and C. Hsu. 2018. The impact of audit firms' characteristics on audit fees following information security breaches. *Journal of Accounting and Public Policy* 37 (6):489-507.

Zacks, R. T., L. Hasher, and H. Sanft. 1982. Automatic encoding of event frequency: Further findings. *Journal of Experimental Psychology: Learning, Memory, and Cognition* 8 (2):106.

Zafar, H., M. S. Ko, and K.-M. Osei-Bryson. 2016. The value of the CIO in the top management team on performance in the case of information security breaches. *Information Systems Frontiers* 18 (6):1205-1215.

Appendix A Variable Definitions

Variable	Definition
Audit office level variables	
$CyberExp_t$	The total number of times that clients of an audit office experienced cyber incidents in the previous three years, scaled by the total number of clients of the audit office of year t.
$OfficeSize_t$	The nature log of total number of clients audited by the audit office of year t.
$OfficeMS_t$	The total number of clients for an audit office divided by the total number of clients for all offices in the MSA in year t.
$OfficeInd_t$	Indicator variable equal to 1 if the audit office is the MSA-level industry expert on an audit engagement in year t, and 0 otherwise. A MSA industry expert charges the largest amount of total audit fees within an industry-year in the same MSA. Industries are classified at the two-digit SIC level.
$ITExp_t$	Indicator variable equal to 1 if the audit office's IT capability is higher than the median value in year t, and 0 otherwise. Audit office's IT capability is the total number of clients listed on InformationWeek500 of an audit office, scaled by the total number of clients of the audit office.
Firm level variables	
$LogAuditFees_t$	The nature log of audit fees.
$Size_t$	The nature log of total assets.
$Growth_t$	The one-year growth rate of sales.
Btm_t	The book value divided by market value.
ROA_t	The operating income after depreciation scaled by total assets.
$InvRec_t$	The sum of inventories and accounts receivable divided by total assets.
$Segment_t$	The number of business segments.
$Foreign_t$	Indicator variable equal to 1 if the firm has foreign operations, and 0 otherwise.
$Merger_t$	Indicator variable equal to 1 if the firm reports merger activities, and 0 otherwise.
$Special_t$	Indicator variable equal to 1 if the firm reports special items, and 0 otherwise.
$Loss_t$	An indicator variable that equals to 1 if the firm has net loss, and 0 otherwise.
$Leverage_t$	The total liabilities divided by total assets.
$Quick_t$	The current assets minus inventories scaled by total assets.
$GoingConcern_t$	Indicator variable equal to 1 if the auditor issue a going-concern opinion in year t, and 0 otherwise.
$Restatement_t$	Indicator variable equal to 1 if the firm reports a restatement in year t or year t+1, and 0 otherwise.
ICW_t	Indicator variable equal to 1 if the firm has at least one weakness in internal controls in year t, and 0 otherwise.
$Big4_t$	Indicator variable equal to 1 if the firm is audited by a Big4 auditor in year t, and 0 otherwise.

$Initial_t$ Indicator variable equal to 1 if it is an initial-year audit, and 0 otherwise.

$CyberIncident_{t+1}$ Indicator variable equal to 1 if the firm experiences a cyber incident during year t, and 0 otherwise.

Table 1 Sample selection

Firm-years with auditor cybersecurity experience available	43,056
Less: observations audited by foreign auditors	(1,525)
Less: observations that are in the financial industries	(11,055)
Less: observations experienced cyber breaches in current or previous years	(609)
Less: observations with missing variables	(8,876)
Final sample	21,991

Table 2 Descriptive statistics

	Full Sample					$CyberExp_t > 0$			$CyberExp_t = 0$		
Variables	**N**	**mean**	**median**	**p25**	**p75**	**N**	**mean**	**median**	**N**	**mean**	**median**
$LogAuditFees_t$	21991	13.512	13.657	12.543	14.506	3955	14.373	14.311	18036	13.323	13.431
$CyberExp_t$	21991	0.012	0	0	0	3955	0.066	0.051	18036	0	0
$OfficeSize_t$	21991	2.658	2.639	1.946	3.434	3955	3.447	3.497	18036	2.485	2.485
$OfficeMS_t$	21991	0.165	0.129	0.059	0.228	3955	0.198	0.170	18036	0.158	0.118
$OfficeInd_t$	21991	0.840	1	1	1	3955	0.971	1	18036	0.811	1
$Size_t$	21991	5.749	5.989	4.134	7.616	3955	7.046	7.052	18036	5.465	5.702
$Growth_t$	21991	0.141	0.041	-0.073	0.170	3955	0.103	0.043	18036	0.149	0.041
Btm_t	21991	0.356	0.404	0.181	0.709	3955	0.394	0.364	18036	0.348	0.414
ROA_t	21991	-0.195	0.093	-0.012	0.149	3955	0.060	0.105	18036	-0.250	0.089
$InvRec_t$	21991	0.240	0.206	0.084	0.348	3955	0.219	0.190	18036	0.244	0.210
$Segment_t$	21991	1.936	1	1	3	3955	2.048	1	18036	1.912	1
$Foreign_t$	21991	0.307	0	0	1	3955	0.392	0	18036	0.288	0
$Merger_t$	21991	0.268	0	0	1	3955	0.385	0	18036	0.243	0
$Special_t$	21991	0.695	1	0	1	3955	0.784	1	18036	0.675	1
$Loss_t$	21991	0.404	0	0	1	3955	0.330	0	18036	0.421	0
$Leverage_t$	21991	0.948	0.519	0.324	0.714	3955	0.559	0.525	18036	1.033	0.517
$Quick_t$	21991	2.244	1.429	0.871	2.473	3955	2.361	1.555	18036	2.218	1.401
$GoingConcern_t$	21991	0.101	0	0	0	3955	0.023	0	18036	0.118	0
$Restatement_t$	21991	0.113	0	0	0	3955	0.137	0	18036	0.108	0
ICW_t	21991	0.036	0	0	0	3955	0.046	0	18036	0.034	0
$Big4_t$	21991	0.628	1	0	1	3955	0.971	1	18036	0.553	1
$Initial_t$	21991	0.058	0	0	0	3955	0.027	0	18036	0.065	0

Table 3 Auditor cyber-incident experience and audit fees

Variables	**DV: $LogAudFees_t$**
$CyberExp_t$	0.238*** (3.18)
$OfficeSize_t$	-0.021* (-1.78)
$OfficeMS_t$	-0.067 (-1.25)
$OfficeInd_t$	0.022** (2.35)
$Size_t$	0.282*** (56.76)
$Growth_t$	-0.001 (-0.45)
Btm_t	-0.002 (-0.93)
ROA_t	-0.058*** (-16.60)
$InvRec_t$	0.190*** (6.88)
$Segment_t$	0.010*** (4.63)
$Foreign_t$	0.043*** (5.15)
$Merger_t$	0.045*** (9.01)
$Special_t$	0.022*** (4.67)
$Loss_t$	0.041*** (7.91)
$Leverage_t$	0.018*** (9.28)
$Quick_t$	-0.012*** (-10.84)
$GoingConcern_t$	0.038*** (3.42)
$Restatement_t$	0.020*** (3.41)
ICW_t	0.186*** (19.46)
$Big4_t$	0.416** (2.37)
$Initial_t$	-0.027*** (-3.38)
Year Fixed Effects	Included
Audit Office Fixed Effects	Included
Firm Fixed Effects	Included
N	21,991
$Adj\ R^2$	84.2%

*, **, *** Indicate significance (two-tailed) at the 0.10, 0.05, and 0.01 levels, respectively.

Table 4 Auditor cyber-incident experience and future breaches

Variables	**DV: $\boldsymbol{Breach_{t+1}}$**
$CyberExp_t$*$D.LogAudFees_t$	-19.123** (-2.10)
$CyberIncidentExp_t$	-13.300*** (-4.16)
$D.LogAudFees_t$	1.651*** (3.35)
$OfficeSize_t$	-1.027 (-1.40)
$OfficeMS_t$	-1.899 (-0.46)
$OfficeInd_t$	0.648 (0.93)
$Size_t$	0.701*** (8.96)
$Growth_t$	-1.120** (-2.13)
ROA_t	0.276 (0.45)
$Segment_t$	-0.061 (-0.98)
$Loss_t$	-0.279 (-1.05)
$Leverage_t$	0.231 (0.93)
ICW_t	-1.930* (-1.71)
Year Fixed Effects	Included
Audit Office Fixed Effects	Included
Industry Fixed Effects	Included
N	7,719
$Pseudo\ R^2$	26.9%

*, **, *** Indicate significance (two-tailed) at the 0.10, 0.05, and 0.01 levels, respectively. Standard errors are clustered at the firm level.

Table 5 Moderating effect of auditor IT expertise

Variables	DV: $\boldsymbol{Breach_{t+1}}$
$CyberExp_t$*$D.LogAudFees_t$*$ITExp_t$	-40.467** (-2.28)
$CyberExp_t$	-17.780*** (-3.23)
$D.LogAudFees_t$	0.976 (1.53)
$ITExp_t$	0.135 (0.37)
$OfficeSize_t$	-0.953 (-1.28)
$OfficeMS_t$	-2.211 (-0.52)
$OfficeInd_t$	0.692 (1.00)
$Size_t$	0.707*** (8.97)
$Growth_t$	-1.075** (-2.10)
ROA_t	0.238 (0.39)
$Segment_t$	-0.060 (-0.95)
$Loss_t$	-0.275 (-1.04)
$Leverage_t$	0.232 (0.92)
ICW_t	-2.048* (-1.72)
$D.LogAudFees_t$*$ITExp_t$	1.216 (1.47)
$CyberExp_t$*$D.LogAudFees_t$	12.347 (0.81)
$CyberExp_t$*$ITExp_t$	5.118 (0.91)
Year Fixed Effects	Included
Audit Office Fixed Effects	Included
Industry Fixed Effects	Included
N	7,719
$Pseudo\ R^2$	27.2%

*, **, *** Indicate significance (two-tailed) at the 0.10, 0.05, and 0.01 levels, respectively. Standard errors are clustered at the firm level.

Table 6 PSM sample

Panel A Auditor cyber-incident experience and audit fees

Variables	**DV: $\boldsymbol{LogAudFees_t}$**
$CyberExp_t$	0.195*
	(1.95)
$OfficeSize_t$	-0.026
	(-0.83)
$OfficeMS_t$	0.080
	(0.63)
$OfficeInd_t$	0.098**
	(2.06)
$Size_t$	0.367***
	(35.49)
$Growth_t$	0.002
	(0.28)
Btm_t	0.019***
	(3.32)
ROA_t	-0.020
	(-0.85)
$InvRec_t$	0.382***
	(5.37)
$Segment_t$	0.009***
	(2.70)
$Foreign_t$	0.046***
	(3.61)
$Merger_t$	0.047***
	(6.00)
$Special_t$	0.023***
	(2.68)
$Loss_t$	0.058***
	(6.69)
$Leverage_t$	0.069***
	(5.92)
$Quick_t$	-0.022***
	(-9.79)
$GoingConcern_t$	0.092***
	(2.97)
$Restatement_t$	0.023**
	(2.47)
ICW_t	0.187***
	(12.95)
$Big4_t$	0.009
	(0.03)
$Initial_t$	-0.057***
	(-2.93)
Year Fixed Effects	Included
Audit Office Fixed Effects	Included
Firm Fixed Effects	Included
N	6890
$Adj\ R^2$	57.2%

*, **, *** Indicate significance (two-tailed) at the 0.10, 0.05, and 0.01 levels, respectively.

Panel B Auditor cyber-incident experience and future breaches

Variables	**DV: $Breach_{t+1}$**
$CyberExp_t$*$D.LogAudFees_t$	-20.449*
	(-1.95)
$CyberExp_t$	1.478*
	(1.81)
$D.LogAudFees_t$	-11.888**
	(-2.09)
$OfficeSize_t$	0.727***
	(4.66)
$OfficeMS_t$	-0.035
	(-0.29)
$OfficeInd_t$	2.305
	(0.87)
$Size_t$	-1.466
	(-1.30)
$Growth_t$	-0.567
	(-1.30)
ROA_t	0.879
	(1.55)
$Segment_t$	-1.013
	(-0.84)
$Loss_t$	-1.217
	(-0.61)
$Leverage_t$	5.014
	(0.41)
ICW_t	-0.539
	(-0.37)
Year Fixed Effects	Included
Audit Office Fixed Effects	Included
Industry Fixed Effects	Included
N	2584
$Pseudo\ R^2$	36.2%

*, **, *** Indicate significance (two-tailed) at the 0.10, 0.05, and 0.01 levels, respectively. Standard errors are clustered at the firm level.

Panel C Moderating effect of auditor IT expertise

Variables	**DV:** $\boldsymbol{Breach_{t+1}}$
$CyberExp_t$*$D.LogAudFees_t$*$ITExp_t$	-39.121
	(-1.46)
$CyberExp_t$	-21.405**
	(-2.55)
$D.LogAudFees_t$	0.962
	(1.31)
$ITExp_t$	0.230
	(0.31)
$OfficeSize_t$	-0.400
	(-0.19)
$OfficeMS_t$	4.966
	(0.42)
$OfficeInd_t$	-1.150
	(-0.70)
$Size_t$	0.742***
	(4.61)
$Growth_t$	-1.235
	(-1.12)
ROA_t	2.658
	(0.96)
$Segment_t$	-0.030
	(-0.24)
$Loss_t$	-0.488
	(-1.13)
$Leverage_t$	0.870
	(1.53)
ICW_t	-1.052
	(-0.84)
$D.LogAudFees_t$*$ITExp_t$	0.927
	(0.56)
$CyberExp_t$*$D.LogAudFees_t$	11.482
	(0.58)
$CyberExp_t$*$ITExp_t$	11.799
	(1.45)
Year Fixed Effects	Included
Audit Office Fixed Effects	Included
Industry Fixed Effects	Included
N	2,584
$Pseudo\ R^2$	36.8%

*, **, *** Indicate significance (two-tailed) at the 0.10, 0.05, and 0.01 levels, respectively. Standard errors are clustered at the firm level.