Journal of Accounting and Public Policy xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Journal of Accounting and Public Policy

journal homepage: www.elsevier.com/locate/jaccpubpol

Full length article

The impact of audit firms' characteristics on audit fees following information security breaches

Ju-Chun Yen[a], Jee-Hae Lim[b,*], Tawei Wang[c], Carol Hsu[d]

[a] National Central University, Graduate Institute of Accounting, 300 Zhongda Rd, Zhoungli Dist., Taoyuan 32001, Taiwan
[b] University of Hawaii, Manoa, Shidler College of Business, 2404 Maile Way, Honolulu, HI 96822, United States
[c] DePaul University, Kellstadt Graduate School of Business, 1 East Jackson Blvd., DePaul Center 6028, Chicago, IL 60604, United States
[d] Tongji University, Department of Management Science and Engineering, Tongji Building A, Siping Road 1500, Shanghai 200092, China

ARTICLE INFO

Keywords:
Audit fees
Audit-firm industry expertise
Audit-firm tenure
Audit-firm size
Information security breach

ABSTRACT

Given the importance of auditors' assessing business risks and evaluating internal controls, we investigate whether an audit firm's industry expertise, tenure, and size can help its auditors better understand external and internal threats faced by the client with less effort. Using reported information security breach incidents from 2004 to 2013, we find that, consistent with prior studies, audit fees are higher after the occurrence of an information security breach. However, such an association is negatively moderated when the audit firm has industry-specific expertise, longer experience with the client, and is one of the Big 4 firms. Our results suggest that because of their better knowledge about a specific industry, increased familiarity with the client's operations, and more resources to understand a client's vulnerabilities and/or information security policies and procedures, these auditors are more capable of assessing the potentially changing information security risks implied by the occurrence of information security breach incidents. Our results are robust to a variety of sensitivity checks.

1. Introduction

Recent high-profile information security breaches such as Target and Yahoo! suggest that information security breaches affect a firm's operation and performance beyond financial losses. For instance, the cyber-attack on Sony in 2011, one of the biggest data breaches since the advent of the Internet, cost Sony around $1 billion, not to mention the impact on its brand image and all of its online networks of games, movies, and music.[1] According to Verizon's 2017 Data Breach Investigations Report (Verizon, 2017), 75% of breaches are related to outsiders and 73% of breaches are financially motivated. These breaches, according to IBM's 2016 Cost of Data Breach Study (IBM, 2016), cost $4 million on average globally with a 29% increase in total cost since 2013. The U.S. has the highest average per capita cost of data breaches at $221 in 2016 (IBM, 2016).

The upward trend of information security breaches has raised discussion about the importance of auditors' understanding clients' information technology environment. For example, the Center for Audit Quality (CAQ) released an alert to approximately 600 of its public company audit firm members that summarizes external auditors' duties with respect to cybersecurity (CAQ, 2014). In general, auditors are required to understand the client's environment, such as economic conditions, regulatory requirements, competitive environment, technological developments, and internal controls (AICPA, 2006), and to report the effectiveness of internal controls

* Corresponding author.
E-mail address: jeehae@hawaii.edu (J.-H. Lim).

[1] See http://money.cnn.com/2011/05/10/technology/sony_hack_fallout/ for an example of news articles about Sony's 2011 breach.

https://doi.org/10.1016/j.jaccpubpol.2018.10.002

over information systems (Boritz et al., 2012; Li et al., 2012). Such understanding could be critical because, on one hand, information technology (IT) enhances the timeliness and accuracy of information as well as reduces the chance that controls will be circumvented, both of which reduce the likelihood of misstatements and fraud (Bell et al., 1998; Messier et al., 2004). On the other hand, IT also poses information security risks, such as unauthorized access to data, destruction of or improper changes to data, and/or data unavailability for authorized use (AICPA, 2006), which has a significant impact on organizations and affects the reliability of financial reporting and the effectiveness and efficiency of operations (AICPA, 2006; Gordon et al., 2008).[2] Recently, Lawrence et al. (2018) have demonstrated that computer data breaches, as an operational control risk, are positively associated with financial reporting risk, as reflected in more restatements and SEC comment letters. Thus, to reduce audit risk *ex ante*, it is important for auditors to devote time and effort to understanding and assessing clients' information security risks. However, the extent of the time and effort that auditors devote may be conditional on several audit-firm characteristics, such as the specific knowledge about an industry, familiarity with the client's operations, and resources to understand information security risks.

In this study, we examine the impact of audit firms' characteristics on the association between audit fees and information security breach incidents. As information security breach incidents have been commonly used in other studies to proxy for the effectiveness of information security risk management (Kwon et al., 2013; Wang and Hsu, 2010b; Wang et al., 2013a), we first use the realization of a firm's information security risks (i.e., security breach incidents) to proxy for the level of the firm's information security risks. Second, to examine for auditors' efforts to understand and assess clients' information security risks and procedures, we use the audit fees charged to the client in the subsequent period of breaches.

To present empirical evidence, we collect reported information security breaches from *DataLossDB* (http://www.datalossdb.org) from 2004 to 2013. To supplement, we further conduct keyword searches of news articles from major media outlets through LexisNexis. Our empirical findings, first, are consistent with existing literature (Higgs et al., 2017; Li et al., 2017) that audit fees after the occurrences of information security breaches are on average 13.5% higher than those of firms without breaches. However, we find that this positive association between reported information security breaches and subsequent audit fees is negatively moderated by audit-firm characteristics, including industry expertise, tenure, and size. Specifically, as detailed in Section 4, industry expertise decreases the association between reported information security breaches and audit fees from 52.0% to 11.3%. Long audit tenure also decreases the association from 13.7% to −12.4%. Finally, audit-firm size, measured by Big 4 audit firms, decreases the association of reported breaches and audit fees from 64.5% to 15.4%. The overall results demonstrate that these audit firms' characteristics can help auditors better assess clients' information security risks and evaluate information security management processes with less effort.

Our study contributes to the literature in audit and information security risk management in the following ways. First, our study fills the gap of literature between auditing and information security. The literature and several anecdotal evidence in information security risk management have emphasized the threats brought to auditors by information technology. How auditors should response to these threats have been highlighted in auditing standards (e.g., SAS 70) and IT governance frameworks (e.g., COBIT 5). The ISACA's risk assessment program and the security management guidelines provided by the National Institute of Standards and Technology (NIST) have also pointed out the importance of understanding the client's environment, assessing risks as well as evaluating internal controls. In fact, although auditors are important external stakeholders of a firm, there is a lack of empirical research that examine the link between auditors and information security issues. For example, prior studies examine the association between the effectiveness of a firm's information security risk management and various internal and external stakeholders, including the board (Wang and Hsu, 2010b), the top management team (Kwon et al., 2013; Wang and Hsu, 2010a), and the change in regulations (Gordon et al., 2006). Different from these studies that focus on how stakeholders may affect a firm's management of information security risks, our study addresses that a client's information security and risk management should be an important factor for auditors to consider. Thus, we focus on how audit-firm characteristics affect auditors' efforts to understand and assess clients' information security risks.

Second, our study enriches the literature by connecting between audit fees and information security by examining the moderating effects of audit-firm characteristics. Two recent independent studies by Higgs et al. (2017) and Li et al. (2017) have examined the association between audit fees and information security breaches. Different from these studies, our study highlights the effort auditors devote to understanding and assessing clients' information security risks and provides further evidence by examining the moderating effects of audit-firm characteristics on the association between audit fees and security breaches.

Last, our study provides important policy implications. The high-profile information security breaches in recent years have raised concerns for the Securities and Exchange Commission (SEC), the Public Company Accounting Oversight Board (PCAOB), and the American Institute of CPAs (AICPA) as to whether firms should disclose information security management strategies, potential threats, and consequences such as reputation loss or even the continuity of business operations. Given that operating uncertainties and continuity of business operations are key factors auditors must consider, our analyses highlight the importance of auditors' understanding information security vulnerabilities, the emerging threats specific to a certain industry, and the possible corresponding controls based on existing information security program, standards, or guidance.

The remainder of the paper is organized as follows. We review relevant literature and develop hypotheses in Section 2. In Section 3, we discuss our research methodology. We present the results in Section 4 and conclude with limitations and future research avenues in Section 5.

[2] For example, see COBIT 5 for information security (https://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf) or the FFIEC IT Examination Handbook (https://ithandbook.ffiec.gov/media/222209/ffiec_itbooklet_informationsecurity-2006.pdf).

2. Literature review and hypothesis development

2.1. Information security and auditors

In the current digital era, information security has been a critical concern for business operation (Gordon and Loeb, 2002a, 2010). Numerous studies have explored various information security risk management-related issues, such as information security investment (Gordon and Loeb, 2002a,b, 2006), sharing security information (Gal-Or and Ghose, 2005; Gordon et al., 2003), user security awareness programs (Dinev and Hu, 2007), the role of the top management team or the board (Hsu and Wang, 2014a,b; Wang and Hsu, 2013), the institutional factors that affect information security risk management (Hsu et al., 2012), adoption of information security standards (Hsu et al. 2016), and security policy (Hu et al., 2012). Other lines of study focus on information-security-related disclosures (Gordon and Loeb, 2010; Gordon et al., 2006; Wang et al., 2013a) and market reactions to security breaches (Acquisti et al., 2006; Campbell et al., 2003; Cavusoglu et al., 2004; Ettredge and Richardson, 2003; Garg et al., 2003; Gordon et al., 2011; Hovav and D'Arcy, 2003; Kannan et al., 2007; Wang et al., 2013b).

A security governance framework allows organizations to develop information security management processes and the associated measurements for evaluating the progress of implementation (Johnston and Hale, 2009; Nolan and McFarlan, 2005). Recent high-profile information security breaches have raised concerns for the SEC and PCAOB regarding whether firms should disclose potential threats and the consequences of information security risks, such as reputation loss or even the continuity of business operations (PCAOB, 2015; SEC, 2011). Given the importance of information security risks for business continuity, auditing standards (e.g., SAS 70) and the CPA's external audit responsibilities include the assessment of information security. For example, the Center for Audit Quality (CAQ, 2014) indicates that the auditor's responsibilities encompass an evaluation of financial statements, including the risk of material misstatements from unauthorized access to financial reporting-related IT systems and data:

> The financial statement audit and, where applicable, the audit of ICFR [*internal control for financial reporting*], include procedures with respect to a company's financial reporting systems, including evaluating the risks of material misstatement to a company's financial statements resulting from unauthorized access to such systems. The auditor is also responsible for evaluating a company's accounting for cybersecurity-related losses and for assessing the impact on a company's financial statements and disclosures, including items such as contingent liabilities or claims, as they relate to the audit of the financial statements taken as a whole and the impact on ICFR.
>
> (CAQ, 2014, para. 3)

In addition, the AICPA has introduced new guidance for auditors in thoroughly assessing a firm's information security risk management program. As the AICPA has developed the exam and guidance, large audit firms have already been gearing up to perform new services in assessing information security risks. Sandy Herrygers, a partner at Deloitte & Touche, notes that "It's [*the new guidance*] an attestation service that can be done to test the design and operating effectiveness of a firm's information security risk management controls" (Compliance Week, 2017, para. 2). This new guidance, which provides processes for detecting a firm's information security vulnerabilities, serves as a tool for auditors in taking a deeper look at clients' information security risks.

The increased effort to understand the client's information security risks when auditors perform assurance services may be reflected in audit fees.[3] Studies have shown that more audit effort is needed for clients with higher complexity, such as those with foreign subsidiaries or a higher number of subsidiaries or business segments (Hay et al., 2006). Audit efforts are also sensitive to client size and inherent risk (O'Keefe et al., 1994). These efforts to understand the inherent risk of the client may be reflected in higher audit fees. Given that a client's complicated and interwoven IT systems[4] increase the client's inherent risk and the auditor's efforts to understand the business and assess operating risks, audit fees may be expected to be higher. To the best of the authors' knowledge, two empirical research studies (Higgs et al. 2017; Li et al. 2017) have examined the direct association between audit fees and information security breaches, but not further examined how audit-firm characteristics may affect auditors' understanding and evaluation of information security risk. Specifically, Li et al. (2017) argue that a cybersecurity incident implies deficiencies in a firm's internal control over financial reporting and higher possibility of misstatements. Higgs et al. (2017) state that a cybersecurity breach risk may affect audit fees because of the increased audit cost and the increased premium that reflects potential future litigation risk. Different from these two studies, we focus on how audit-firm characteristics affect auditors' efforts to understand and assess clients' information security risks. In other words, we examine the moderating effects of audit-firm characteristics to provide evidence that an auditor's ability and effort matter when he/she assesses a client's information security risks.

[3] Audit fees may reflect auditors' efforts to perform services or premiums to compensate auditors for their litigation risk, or both (DeFond and Zhang, 2014; Simunic and Stein, 1996). Litigation risk is highly associated with clients' risk factors, such as operating losses, modified opinions, and weak governance. To mitigate or compensate for the litigation risk, auditors may take steps *ex ante* such as exerting additional effort or charging higher fees as a premium. This argument on litigation risk also results in a positive association between audit fees and *ex ante* estimated risks (Beatty, 1993; Francis and Simon, 1987; Palmrose, 1986; Simon and Francis, 1988; Simunic, 1980) from reported breaches. In our context, our main argument focuses on auditors' effort in understanding the clients' operational environment. The auditors' litigation risk is beyond our scope.

[4] The 2015 audit fee report by the Financial Executives Research Foundation (FERF, 2016) states, "Explaining that the audit fee is also multi-faceted, some audit partners expressed how a company is structured has an important impact on the audit fee. 'There are a number of companies that have multiple divisions that have different ERP systems, and in some cases, 50–100 different IT packages. This type of structure will require us to go and audit the system or at least understand the controls over the many systems at the important locations; whereas, other companies are designed much more efficiently where they have one or a few number of instances of a global ERP'" (p. 5).

2.2. The moderating effect of audit-firm industry expertise on the association between information security breaches and audit fees

PricewaterhouseCoopers (2002) argues that audit quality depends on the auditor's knowledge and understanding of the industry in which the client operates. Auditors obtain industry expertise through familiarity with the industry's accounting practices and risks in general and the experience of working with specific clients within an industry. Audit firms with industry expertise are likely to train their auditors with more industry-specific knowledge (Krishnan, 2003) and such auditors can better understand the environment in which their clients operate (Curtis et al., 2009; Tucker, 2001). Empirically, audit firm industry specialization is also shown to be positively associated with client disclosure quality, which is measured by analysts' evaluations in AIMR reports (Dunn and Mayhew, 2004), and negatively associated with financial fraud (Carcello and Nagy, 2004b). Audit firm industry specialization is associated with clients' larger earnings response coefficients and leads to lower levels of discretionary accruals (Balsam et al., 2003). Stanley and DeZoort (2007) find that audit firm industry specialization is negatively associated with restatement.

In our context, industry-specific knowledge includes the inherent information security risks, legislation and regulations about information security, and current trends in information security incidents.[5] We argue that such an understanding helps auditors better assess clients' inherent and control risks as stated in AICPA (2006) with less effort than is required from auditors without industry expertise. Therefore, given that auditors charge clients with reported breaches higher audit fees to reflect the increased effort they need to devote to the audit engagement (Higgs et al., 2017; Li et al., 2017), auditors with industry expertise may not charge audit fees that are as high as those charged by auditors without industry expertise. That is, there may be a negative moderating effect of industry expertise on the association between reported information security breaches and audit fees. This argument leads to the following hypothesis.

Hypothesis 1. Audit-firm industry expertise negatively moderates the positive association between information security breaches and audit fees.

2.3. The moderating effect of audit-firm tenure on the association between information security breaches and audit fees

Previous studies discuss audit-firm tenure from two opposite perspectives. As tenure increases, expert knowledge about the client's resources, operations, and risks increase (Finkelstein and Hambrick, 1990; Hsu and Wang, 2014b; Wang and Hsu, 2010a, 2013; Zajac and Westphal, 1996). Longer tenure increases auditors' competence as they are more familiar with the operation of the client and industry, which leads to a positive association with audit quality (Carcello and Nagy, 2004a; Geiger and Raghunandan, 2002; Ghosh and Doocheol, 2005; Johnson et al., 2002; Li, 2010; Lim and Tan, 2010; Myers et al., 2003). On the other hand, longer tenure also reflects the extent to which an individual is integrated into the networks of key stakeholders and obtains the resources and coalitions needed to "orchestrate, nurture, and support" (p. 654) his/her initiatives (Simsek, 2007), which may decrease auditor independence. For example, Congressman Richard Shelby stated, "How can an auditing firm remain independent when it has established long term personal and professional relationships with a firm by auditing the same firm for many years, some 10, 20, 30 years?" (U.S. House of Representatives, 1985). Auditors with longer tenure are more familiar with the management team, which may reduce their skepticism and objectivity (Carcello and Nagy, 2004a). Accordingly, longer tenure decreases auditor independence by increasing the tendency to compromise with the client, which leads to a negative association with audit quality (Davis et al., 2009).

Given that a firm's information security risk is idiosyncratic,[6] an auditor's understanding of the client's IT operations and business processes can critically affect the auditor's competency for assessing and understanding information security risks, as has been emphasized in the ISO 27000 series standards regarding information security management systems. Based on the competency argument, we expect that the longer the tenure, the better the auditor can evaluate which information security clause or category is important to the client or how it can be applied to various business processes. Given that auditors will charge clients with reported breaches higher audit fees to reflect the increased effort they need to devote to the audit engagement (Higgs et al., 2017; Li et al., 2017), auditors who are more competent and have more experience with the client may not need to increase their effort as much as do those less competent. Thus, there might be a negative moderating effect of audit-firm tenure on the association between audit fees and reported information security breach incidents. On the other hand, we do not find any existing literature discussing the role of auditor independence in the context of information security risk management. Therefore, we state our second hypothesis based on the argument of competence as follows.

Hypothesis 2. Audit-firm tenure negatively moderates the positive association between information security breaches and audit fees.

[5] These factors are highlighted in the ISACA's risk assessment program and security management guidelines provided by National Institute of Standards and Technology (NIST). See https://www.isaca.org/journal/archives/2010/volume-1/pages/performing-a-security-risk-assessment1.aspx.

[6] According to the Basel II framework, IT risks are classified as an operational risk type (BCBS, 2001). Because operational risks "tend to be idiosyncratic to a particular institution" (Herring, 2002, p. 43), their assessment is also difficult.

2.4. The moderating effect of audit-firm size on the association between information security breaches and audit fees

The gap between Big N audit firms and non-Big N audit firms is getting larger since the mergers of audit firms in 1989 (Wolk et al., 2001; Wootton et al., 1994). Despite debate and regulators' discouragement, the audit market continues to be dominated by large auditors. Several studies have shown that clients pay higher audit fees to Big N auditors (Fafatas and Sun, 2010; Ireland and Lennox, 2002; Palmrose, 1986; Vermeer et al., 2009), which is consistent with the argument that Big N auditors provide higher audit quality.

We argue that in the context of information security, audit-firm size also has a role.[7] Large auditors usually have more experience and resources through their business scale of both audit and advisory services. They may utilize their experience and resources to better understand clients' vulnerabilities and better assess information security risks that would influence business operations. Therefore, given that auditors will charge clients with reported breaches higher audit fees to reflect the increased effort they need to devote to the audit engagement (Higgs et al., 2017; Li et al., 2017), large auditors, measured by the Big 4, may not need to increase their effort to understand the risks as much as do small auditors. Following this line of argument, we expect to observe a negative moderating effect of audit-firm size on the association between reported information security breaches and audit fees as follows.

Hypothesis 3. Audit-firm size negatively moderates the positive association between information security breaches and audit fees.

3. Research design

3.1. Sample and data collection

We first extract all information security breaches collected by *DataLossDB*[8] for the period from 2004 to 2013. *DataLossDB* is a not-for-profit organization that collects details of information security breach incidents from news feeds, blogs, and websites on a daily basis and verifies incidents by requesting breach notification documents from the U.S. State governments.[9] In order to enhance the completeness and accuracy of our data, we also conduct a subsequent manual search on LexisNexis for key words such as (1) security breach, (2) hacker, (3) cyber attack, (4) virus or worm, (5) computer break-in, (6) computer attack, (7) computer security, (8) network intrusion, (9) data theft, (10) identity theft, (11) phishing, (12) cyber fraud, and (13) denial of service in the *Wall Street Journal*, *USA Today*, the *Washington Post*, and the *New York Times*, as in prior studies (e.g., Campbell et al., 2003; Wang et al., 2013a). The final sample includes all major information security incidents collected through this two-step process.[10]

Table 1 shows the sample selection procedure. An initial list of reported breach incidents has 7518 organization-breach observations. After eliminating non-publicly traded firms, government agencies, and universities that do not have publicly available information and CIK, a total of 310 incidents remain. A subsequent cross-match with *Compustat* and *Audit Analytics* results in a sample of 22,467 firm-year observations, including 248 firm-year observations with reported breaches versus 22,219 firm-year observations without reported breaches (denoted as the full sample). At the firm level, there are 3246 firms with available financial data for analysis, where 164 firms have one or more reported breaches and 3082 firms have no reported breaches during the sample period.

In addition to the full sample, we construct a matched-pair control group using the propensity score matching (PSM) approach to generate a sample of control firms that most resemble our sample firms with reported breaches based on several firm-level characteristics (Armstrong et al., 2010; Rosenbaum and Rubin, 1983). The PSM procedure allows us to efficiently match along multiple dimensions at the firm level. In particular, we establish a one-to-ten matched sample, as we notice that information security breaches are rare events. This one-to-many matching approach allows us to improve bias reduction in the matching process as stated in Ming and Rosenbaum (2000) and to have enough degrees of freedom when performing the analysis. First, at the firm level, we use the PSM approach based on firm size (average total assets of a firm during the sample period) and industry to match each of the treatment firms (firms which have one or more reported breaches during the sample period; 164 firms in total) to ten control firms (firms which have no reported breaches during the sample period; 3082 firms in total).[11] Next, we include all firm-year observations of these treatment firms and matched control firms in the sample (denoted as the PSM sample). Therefore, the PSM sample consists of 248 firm-years with reported breaches and 12,460 firm-years without reported breaches.

Table 2 presents the sample distribution. Panels A and B demonstrate the distributions by year of the full sample and the PSM sample, respectively. From the second column, which shows the by-year distribution of the breach events, we notice that most breaches happen in 2008, 2009, 2011, and 2012 (about 56% of the total sample). At the firm-year level, Panels A and B show that

[7] In our study, we do not consider the small audit firms that specialize in information security management, nor do we consider the scope of the engagement.

[8] *DataLossDB* (http://datalossdb.org/) has been used as the main data source in prior studies (e.g., Kwon et al., 2013; Sen and Borle, 2015; Sullivan, 2010).

[9] Most of information security breach incidents are reported by news media. We notice that the firms with breaches seldom report breach incidents actively.

[10] Information security incidents can be categorized into three not-mutually-exclusive types: confidentiality, integrity, and availability. Confidentiality-type incidents refer to unauthorized disclosure or access to sensitive firm information. Integrity-type incidents refer to improper authorization, inaccuracy, incompleteness, and delay of data process. Availability-type incidents refer to unavailability of a system that fails to meet operational and contractual obligations (e.g., denial of service attacks). Our final sample consists of only confidentiality type incidents. We acknowledge it as a limitation of the study.

[11] We execute the one-to-one no-replacement PSM ten times to make sure no control firms are matched multiple times. The adjusted Pseudo R^{2}s range from 0.115 to 0.782, with an average of 0.480.

Table 1
Sample selection.

	# of incidents	# of firm-years	# of firms
Information Security Breach Data			
DataLossDB	7518		
Minus: Missing CIK	(5944)		
No matched CIK	(1264)		
Total	310		
Full Sample			
Compustat (2004–2013)		70,273	20,731
Minus: Missing variables		(25,764)	
Missing CIK		(5037)	
Subtotal		39,472	11,343
Minus: Missing in *Audit Analytics*		(17,005)	
Total		22,467	3,246
Total (with breaches)		248	164
Total (without breaches)		22,219	3,082

there are more observations in later years than earlier years (1805 firm-years in 2004 versus 2606 firm-years in 2013), which is likely caused by fewer missing variables in *Audit Analytics* in later years.

Panels C and D of Table 2 demonstrate the distributions by the one-digit SIC of the full sample and the PSM sample, respectively. Panel C shows that the service industry (one-digit SIC codes 7 and 8) and the manufacturing industry (one-digit SIC codes 2 and 3) have the most firm-year observations with reported breaches (85 and 60 observations, respectively). They are only 2.10% and 0.55% of firm-years within the specific industry (85 of 4054 and 60 of 10,876, respectively). On the other hand, the agriculture industry (one-digit SIC code 0), the public administration industry (one-digit SIC code 9), and the mining and construction industry (one-digit SIC code 1) have the fewest firm-year observations with reported breaches (1, 2, and 4 observations, respectively). This is expected because of the lower IT intensity and the nature of the business in these industries. In terms of percentage, the mining industry has the smallest percentage (0.20% of firm-years with reported breaches). However, 5% of firm-years in the public administration industry have reported breaches, which is the largest among all industries. One possible reason is that there are only 40 firm-years in the public administration industries in our sample. Based on the PSM sample, Panel D shows similar results with larger percentages of firm-years with reported breaches in industries, as we exclude several firm-years without reported breaches from the full sample.

3.2. Regression models

To establish the base model for the association between audit fees and information security breaches, we estimate the following regression model, Eq. (1):

$$\begin{aligned} lnAUDIT\_FEES_{i,t+1} = {} & \alpha_0 + \alpha_1\, breachvar_{i,t} + \alpha_2\, MTB_{i,t} + \alpha_3\, lnAT_{i,t} + \alpha_4\, DEBTR_{i,t} + \alpha_5\, CRTR_{i,t} + \alpha_6\, ROI_{i,t} + \alpha_7\, QCKR_{i,t} \\ & + \alpha_8\, LOSS_{i,t} + \alpha_9\, SEG_{i,t} + \sum^{\alpha} Years + \sum^{\alpha} Industries + \varepsilon_{i,t} \end{aligned} \tag{1}$$

where $lnAUDIT\_FEES_{t+1}$ is the natural log of audit fees charged to the firm for the audit service performed for the following year, $t + 1$. We examine audit fees in year $t + 1$ instead of year t in order to examine the results of audit fee negotiation *after* the occurrence of breaches in year t.[12] In Eq. (1), the variable of interest, *breachvar*, is one of the following: *BREACH*, an indicator denoted as one if one or more reported information security breaches occurred during year t, and zero otherwise. *NBREACH* is the number of reported information security breaches during year t. In the base model, we expect a positive coefficient for *breachvar* ($\alpha_1 > 0$), indicating higher audit fees following reported breaches (*BREACH* or *NBREACH*), compared to firms without breaches, all else being equal. Stated another way, a positive coefficient for *BREACH* suggests that the auditor charges higher fees if a client has one or more information security breaches reported in the prior year, and a positive coefficient for *NBREACH* suggests that the audit fees increase with the number of breaches reported in the prior year.

To isolate the effect of breaches on audit fees from the effect of other variables, we control for firm-specific variables that are known as audit fee determinants following the recommendation of Ferguson et al. (2003). Since higher fees are related to larger clients, measured by market-to-book ratio (*MTB*) and the natural log of total assets (*lnAT*), we expect positive signs for these variables. Since higher audit fees are associated with higher audit risk, we expect positive signs for debt ratio (*DEBTR*), which is long-term debt over total assets, and current ratio (*CRTR*), which is current assets over total assets. Similarly, we expect negative signs for return on investment (*ROI*), which is the earnings before interest expenses and taxes over total assets, and the quick ratio (*QCKR*), which is current assets (minus inventories) over current liabilities. We include *LOSS*, an indicator denoted as one if there is a net loss in any of the past three years, and zero otherwise. *LOSS* may represent audit risk, which leads to a positive association with audit fees. However, *LOSS* may also reflect the client's ability to pay the fees, which results in a negative association with audit fees. Finally, we

[12] We also perform a robustness test using audit fees in year $t + 2$ as it is possible that the fees in year $t + 1$ were predetermined in year t, and our un-tabulated results remain similar.

Table 2
Sample distribution.

Year	Total number of breaches	Firm-years		
		With breaches	Without breaches	Total
Panel A. Full sample by year				
2004	2	2	1,803	1,805
2005	11	10	1,943	1,953
2006	34	23	2,023	2,046
2007	38	31	2,082	2,113
2008	46	37	2,191	2,228
2009	43	34	2,154	2,188
2010	34	27	2,328	2,355
2011	41	32	2,494	2,526
2012	43	34	2,613	2,647
2013	18	18	2,588	2,606
Total	310	248	22,219	22,467
Panel B. Propensity score matching sample by year				
2004	2	2	1,055	1,057
2005	11	10	1,109	1,119
2006	34	23	1,151	1,174
2007	38	31	1,175	1,206
2008	46	37	1,239	1,276
2009	43	34	1,211	1,245
2010	34	27	1,294	1,321
2011	41	32	1,357	1,389
2012	43	34	1,439	1,473
2013	18	18	1,430	1,448
Total	310	248	12,460	12,708

One-digit SIC	Total number of breaches	Firm-years		
		With breaches	Without breaches	Total
Panel C. Full sample by industry				
0: Agriculture, Forestry, and Fishing	1	1 (1.37%)	72	73
1: Mining and Construction	4	4 (0.20%)	1,989	1,993
2 & 3: Manufacturing	69	60 (0.55%)	10,816	10,876
4: Transportation and Utilities	60	47 (1.54%)	3,011	3,058
5: Wholesale and Retail Trade	31	25 (1.74%)	1,409	1,434
6: Finance, Insurance, and Real Estate	35	24 (2.56%)	915	939
7 & 8: Services	106	85 (2.10%)	3,969	4,054
9: Public Administration	4	2 (5.00%)	38	40
Total	310	248 (1.10%)	22,219	22,467
Panel D. Propensity score matching sample by industry				
0: Agriculture, Forestry, and Fishing	1	1 (1.64%)	60	61
1: Mining and Construction	4	4 (0.51%)	779	783
2 & 3: Manufacturing	69	60 (1.69%)	3,483	3,543
4: Transportation and Utilities	60	47 (2.05%)	2,248	2,295
5: Wholesale and Retail Trade	31	25 (2.52%)	968	993
6: Finance, Insurance, and Real Estate	35	24 (2.56%)	915	939
7 & 8: Services	106	85 (2.10%)	3,969	4,054
9: Public Administration	4	2 (5.00%)	38	40
Total	310	248	12,460	12,708

Panels A and C present the distribution of the full sample, which includes all firm-year observations. Panels B and D present the distribution of the propensity score matching sample, which includes the observations of the treatment firms (firms which have breaches during the sample period) and the matched control firms (firms which have no breaches during the sample period). The second column of each panel shows the distribution of the total number of breaches reported, and the remaining columns show the distribution of firm-year observations with/without breaches. In Panels C and D, the percentages of firm-years with reported breaches over total firm-years of the industry are in the parentheses.

include the number of business segments or operating segments (if business segments are not reported) (*SEG*) to capture audit complexity, as the higher the complexity, the higher the audit fees. The model includes year and industry (one-digit SIC code) fixed effects, and the standard errors of coefficients are clustered by firms. To minimize the influence of outliers, we winsorize all continuous variables at the top and the bottom 1%.[13] See the Appendix A for detailed variable definitions.

To test Hypothesis 1, the moderating effect of the audit-firm industry expertise on the relationship between breaches and audit

[13] The empirical results of our tests are qualitatively the same when using un-winsorized data.

fees, we estimate the following regression model, Eq. (2):

$$\begin{aligned} lnAUDIT\_FEES_{i,t+1} = {} & \alpha_0 + \alpha_1\, breachvar_{i,t} + \alpha_2\, EXPERTISE_{i,t} + \alpha_3\, EXPERTISE^{*}_{i,t} breachvar_{i,t} + \alpha_4\, MTB_{i,t} + \alpha_5\, lnAT_{i,t} \\ & + \alpha_6\, DEBTR_{i,t} + \alpha_7\, CRTR_{i,t} + \alpha_8\, ROI_{i,t} + \alpha_9\, QCKR_{i,t} + \alpha_{10}\, LOSS_{i,t} + \alpha_{11}\, SEG_{i,t} + \sum \alpha Years \\ & + \sum \alpha Industries + \varepsilon_{i,t} \end{aligned} \tag{2}$$

where *breachvar* is either *BREACH* or *NBREACH* as in Eq. (1). *EXPERTISE* is an indicator denoted as one if the audit firm has the largest or more than 10% of market share in the industry (measured by total assets of firms) in which the client operates, and zero otherwise.[14] Auditors with industry expertise (or industry specialists) may charge higher fees as a premium to provide high quality service because of their better knowledge of the industry than non-specialists or their higher reputational capital (DeFond and Zhang, 2014; Dopuch and Simunic, 1982). Thus, we expect a positive coefficient for *EXPERTISE* ($\alpha_2 > 0$), suggesting that auditors with industry expertise charge higher fees. For the variable of interest, we use an interaction term (*EXPERTISE*breachvar*) in Eq. (2) in order to examine whether the association between reported breaches and audit fees is conditioned upon whether firms engage with auditors with expertise versus those without expertise. Hypothesis 1 translates into the expectation of a negative coefficient for *EXPERTISE*breachvar* ($\alpha_3 < 0$), suggesting that the association between audit fees and reported breaches is reduced for clients whose auditors have expertise in the industry in which the client operates, compared to those whose auditors have no expertise. All other variables are as explained in relation to Eq. (1).

To test Hypothesis 2, the moderating effect of the audit-firm tenure on the relationship between breaches and audit fees, we estimate the following regression model, Eq. (3):

$$\begin{aligned} lnAUDIT\_FEES_{i,t+1} = {} & \alpha_0 + \alpha_1\, breachvar_{i,t} + \alpha_2\, TENURE\_short_{i,t} + \alpha_3\, TENURE\_long_{i,t} + \alpha_4\, TENURE\_short_{i,t} {*} breachvar_{i,t} \\ & + \alpha_5\, TENURE\_long_{i,t} {*} breachvar_{i,t} + \alpha_6\, MTB_{i,t} + \alpha_7\, lnAT_{i,t} + \alpha_8\, DEBTR_{i,t} + \alpha_9\, CRTR_{i,t} + \alpha_{10}\, ROI_{i,t} \\ & + \alpha_{11}\, QCKR_{i,t} + \alpha_{12}\, LOSS_{i,t} + \alpha_{13}\, SEG_{i,t} + \sum^{\alpha} Years + \sum^{\alpha} Industries + \varepsilon_{i,t} \end{aligned} \tag{3}$$

where *breachvar* is either *BREACH* or *NBREACH* as in Eq. (1). *TENURE* captures the auditor-client relationship (Krishnan, 1994; Krishnan and Krishnan, 1997). To consider the potentially non-liner effect of tenure, as discussed in Carcello and Nagy (2004a), we follow the literature and employ two indicators: *TENURE_short(long)* is equal to one if the incumbent audit firm has audited the client for four years or fewer (thirteen years or more), and zero otherwise. The two indicators split the sample into three groups: long tenure (*TENURE_long* = 1 and *TENURE_short* = 0), medium tenure (*TENURE_long* = 0 and *TENURE_short* = 0), and short tenure (*TENURE_long* = 0 and *TENURE_short* = 1). Thus, in Eq. (3), our variables of interest are the interaction terms, *TENURE_short*breachvar* and *TENURE_long*breachvar*. Hypothesis 2 translates into the expectation of a negative coefficient of *TENURE_long*breachvar* ($\alpha_5 < 0$), suggesting that the association between breaches and audit fees is less pronounced for clients with long tenure with the incumbent auditors than for those with medium tenure. In addition, if such a reduction also holds for clients with long tenure compared to those with short tenure, we should observe a statistically more negative coefficient of *TENURE_long*breachvar* than that of *TENURE_short*breachvar* ($\alpha_5 < \alpha_4$). However, we do not have an expectation for the direction of the coefficient of *TENURE_short*breachvar*. All other variables are as explained in relation to Eq. (1).

To test Hypothesis 3, the moderating effect of Big 4 vs. non-Big 4 audit firms on the relationship between breaches and audit fees, we estimate the following regression model, Eq. (4):

$$\begin{aligned} lnAUDIT\_FEES_{i,t+1} = {} & \alpha_0 + \alpha_1 breachvar_{i,t} + \alpha_2\, BIG4_{i,t} + \alpha_3\, BIG4^{*}_{i,t} breachvar_{i,t} + \alpha_4\, MTB_{i,t} + \alpha_5\, lnAT_{i,t} + \alpha_6\, DEBTR_{i,t} + \alpha_7\, CRTR_{i,t} \\ & + \alpha_8\, ROI_{i,t} + \alpha_9\, QCKR_{i,t} + \alpha_{10}\, LOSS_{i,t} + \alpha_{11}\, SEG_{i,t} + \sum Years + \sum Industries + \varepsilon_{i,t} \end{aligned} \tag{4}$$

where *breachvar* is either *BREACH* or *NBREACH* as defined in Eq. (1). *BIG4* is an indicator denoted as one if the client is audited by one of the Big 4 audit firms, and zero otherwise. Several studies have found evidence that Big N auditors charge higher fees (Francis, 1984; Francis and Stokes, 1986; Palmrose, 1986; Simon and Francis, 1988). The higher fees charged by the Big N auditors may represent higher audit quality, a risk premium, or monopoly pricing for their market power (DeFond and Zhang, 2014), which suggests a positive coefficient for *BIG4* ($\alpha_2 > 0$). For the variable of interest, we use an interaction term, *BIG4*breachvar* in Eq. (4) to examine whether the association between breaches and audit fees is conditioned on whether firms engage with Big 4 versus non-Big 4 auditors. Hypothesis 3 translates into the expectation of a negative coefficient for *BIG4*breachvar* ($\alpha_3 < 0$), suggesting that the association between security breaches and audit fees is reduced for firms audited by one of the Big 4 auditors compared to those audited by one of the non-Big 4 auditors. All other variables are as explained in relation to Eq. (1).

4. Empirical results

4.1. Descriptive statistics

Table 3 presents the descriptive statistics of the variables in our analyses. Panels A and B show the statistics of the full sample and

[14] We use the 10% cutoff to capture a minimum level of experience in an industry that an auditor needs to perform the service (Neal and Riley, 2004).

Table 3
Descriptive statistics.

Panel A. Full sample (N = 22,467)

Variable	*BREACH* = 1 (N = 248)					*BREACH* = 0 (N = 22,219)					Diff in mean	Diff in median
	Mean	S.D.	p25	p50	p75	Mean	S.D.	p25	p50	p75		
NBREACH	1.25	0.73	1.00	1.00	1.00							
AUDIT_FEES (in millions)	8.90	8.40	2.70	5.30	13.00	2.40	4.20	0.38	0.97	2.30	6.50***	4.33###
EXPERTISE	0.90	0.30	1.00	1.00	1.00	0.64	0.48	0.00	1.00	1.00	0.26***	0.00###
TENURE_short	0.17	0.38	0.00	0.00	0.00	0.37	0.48	0.00	0.00	1.00	−0.20***	0.00###
TENURE_long	0.08	0.27	0.00	0.00	0.00	0.05	0.21	0.00	0.00	0.00	0.03***	0.00###
BIG4	0.95	0.22	1.00	1.00	1.00	0.76	0.43	1.00	1.00	1.00	0.19***	0.00###
MTB	3.54	4.20	1.53	2.50	4.07	3.15	5.62	1.27	2.10	3.69	0.39	0.40###
AT (in billions)	28.83	37.13	3.12	10.05	37.18	5.55	16.22	0.11	0.56	2.87	23.28***	9.49###
DEBTR	0.19	0.16	0.08	0.16	0.26	0.17	0.19	0.00	0.11	0.27	0.02*	0.05###
CRTR	0.4	0.21	0.23	0.36	0.55	0.48	0.26	0.27	0.47	0.69	−0.08***	−0.11###
ROI	0.1	0.08	0.06	0.10	0.14	0.00	0.30	0.00	0.07	0.12	0.10***	0.03###
QCKR	1.54	1.68	0.85	1.17	1.70	2.60	3.29	0.98	1.52	2.77	−1.06***	−0.35###
LOSS	0.21	0.40	0.00	0.00	0.00	0.46	0.50	0.00	0.00	1.00	−0.25***	0.00###
SEG	3.82	2.10	2.00	4.00	5.00	2.62	1.97	1.00	2.00	4.00	1.20***	2.00###

Panel B. Propensity score matching sample (N = 12,708)

Variable	*BREACH* = 1 (N = 248)					*BREACH* = 0 (N = 12,460)					Diff in mean	Diff in median
	Mean	S.D.	p25	p50	p75	Mean	S.D.	p25	p50	p75		
NBREACH	1.25	0.73	1	1	1							
AUDIT_FEES (in millions)	8.90	8.40	2.70	5.30	13.00	3.70	5.10	0.84	1.80	4.20	5.20***	3.50###
EXPERTISE	0.90	0.30	1.00	1.00	1.00	0.77	0.42	1.00	1.00	1.00	0.13***	0.00###
TENURE_short	0.17	0.38	0.00	0.00	0.00	0.31	0.46	0.00	0.00	1.00	−0.14***	0.00###
TENURE_long	0.08	0.27	0.00	0.00	0.00	0.06	0.23	0.00	0.00	0.00	0.02	0.00
BIG4	0.95	0.22	1.00	1.00	1.00	0.88	0.33	1.00	1.00	1.00	0.07***	0.00###
MTB	3.54	4.20	1.53	2.50	4.07	3.12	5.26	1.33	2.14	3.66	0.42	0.36###
AT (in billions)	28.83	37.13	3.12	10.05	37.18	9.61	20.78	0.48	2.16	7.62	19.22***	7.89###
DEBTR	0.19	0.16	0.08	0.16	0.26	0.20	0.19	0.02	0.17	0.31	−0.01	−0.01
CRTR	0.40	0.21	0.23	0.36	0.55	0.41	0.24	0.21	0.38	0.58	−0.01	−0.02
ROI	0.10	0.08	0.06	0.10	0.14	0.07	0.17	0.04	0.08	0.13	0.03***	0.02###
QCKR	1.54	1.68	0.85	1.17	1.70	1.97	2.45	0.89	1.30	2.09	−0.43***	−0.13###
LOSS	0.21	0.40	0.00	0.00	0.00	0.34	0.47	0.00	0.00	1.00	−0.13***	0.00###
SEG	3.82	2.10	2.00	4.00	5.00	3.10	2.14	1.00	3.00	4.00	0.72***	1.00###

Panels A and B present the descriptive statistics of the full sample and the propensity score matching sample, respectively. The propensity score matching sample consists of the observations of the treatment firms (firms which have breaches during the sample period) and the matched control firms (firms which have no breaches during the sample period). See the Appendix A for variable definitions. *AUDIT_FEES* and *AT* are audit fees and total assets before log transformation. ***, **, and * represent significance levels at 1%, 5%, and 10%, respectively, based on two-tailed t-tests. ###, ##, and # represent significance levels at 1%, 5%, and 10%, respectively, based on two-tailed z-tests in the Wilcoxon rank-sum test.

the PSM sample, respectively. In both panels, we show the statistics of the observations with *BREACH* = 1 and *BREACH* = 0 separately and compare the means and medians.

First, for those firm-years with reported breaches, the average number of breaches during the year is 1.25. Second, the mean of audit fees (before log transformation) for observations with reported breaches (*BREACH* = 1) is 8.90 million, which is significantly larger than those for observations without reported breaches (*BREACH* = 0) in both the full sample and the PSM sample (means of 2.4 million and 3.7 million, respectively). Focusing on *EXPERTISE*, about 90% of observations with reported breaches include auditors with industry expertise, which is significantly more than observations without reported breaches (64% and 77% in the full sample and the PSM sample, respectively). Moreover, the statistics for *TENURE_short* show that in about 17% of observations with reported breaches, firms engage with the incumbent auditors for four years or fewer, while in observations without reported breaches, 37% do (31% in the PSM sample). For *TENURE_long*, the statistics show that in 8% of observations with reported breaches, firms engage with the incumbent auditors for 13 years or more, which is similar to the statistics for those without reported breaches (5% and 6% in the full sample and the PSM sample, respectively).[15] Finally, for *BIG4*, firms engage with Big 4 auditors in about 95% of observations with reported breaches, which is significantly larger than the statistics for those without reported breaches (76% and

[15] We further examine whether the audit firm is retained after a client has an information security breach incident. In our sample, only 2 of the 248 breach incidents (0.8%) are followed by an auditor switch in a three-year post-breach period. The reason for the switch requires further investigation as it may or may not be related to the breach and such an investigation is beyond our scope. We thank the anonymous reviewer for this suggestion and leave this question for future research.

Table 4
Pearson correlations.

Full sample	PSM sample														
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)
(1) *lnAUDIT_FEES*	1	0.12***	0.11***	0.41***	−0.24***	0.11***	0.50***	−0.06***	0.86***	0.17***	−0.24***	0.25***	−0.31***	−0.22***	0.46***
(2) *BREACH*	0.13***	1	0.86***	0.04***	−0.04***	0.01	0.03***	0.01	0.11***	−0.01	−0.01	0.03***	−0.02***	−0.04***	0.05***
(3) *NBREACH*	0.12***	0.86***	1	0.04***	−0.04***	0.01	0.03***	0.01	0.11***	−0.01	−0.01	0.03***	−0.02*	−0.04***	0.04***
(4) *EXPERTISE*	0.49***	0.06***	0.05***	1	−0.21***	0.08***	0.68***	−0.01	0.40***	0.08***	−0.12***	0.15***	−0.12***	−0.12***	0.15***
(5) *TENURE_short*	−0.28***	−0.04***	−0.04***	−0.27***	1	−0.17***	−0.29***	0.02**	−0.26***	−0.04***	0.09***	−0.12***	0.10***	0.14***	−0.14***
(6) *TENURE_long*	0.13***	0.02***	0.01	0.10***	−0.17***	1	0.08***	0.00	0.10***	0.02**	−0.01*	0.03***	−0.02*	−0.07***	0.04***
(7) *BIG4*	0.56***	0.05***	0.04***	0.75***	−0.34***	0.11***	1	−0.03***	0.52***	0.14***	−0.19***	0.25***	−0.18***	−0.19***	0.19***
(8) *MTB*	−0.05***	0.01	0.01	−0.01	0.03***	−0.01	−0.01	1	−0.10***	−0.08***	0.16***	0.05***	0.06***	−0.05***	−0.08***
(9) *lnAT*	0.88***	0.13***	0.12***	0.48***	−0.29***	0.12***	0.54***	−0.08***	1	0.27***	−0.46***	0.32***	−0.33***	−0.32***	0.44***
(10) *DEBTR*	0.26***	0.01*	0.01*	0.13***	−0.06***	0.02***	0.16***	−0.08***	0.33***	1	−0.51***	0.02*	−0.23***	0.07***	0.08***
(11) *CRTR*	−0.33***	−0.03***	−0.03***	−0.19***	0.11***	−0.03***	−0.20***	0.12***	−0.51***	−0.48***	1	−0.10***	0.37***	0.12***	−0.20***
(12) *ROI*	0.36***	0.04***	0.03***	0.18***	−0.13***	0.04***	0.22***	−0.03***	0.47***	0.07***	−0.26***	1	−0.07***	−0.40***	0.11***
(13) *QCKR*	−0.32***	−0.03***	−0.03***	−0.11***	0.10***	−0.03***	−0.11***	0.06***	−0.31***	−0.26***	0.38***	−0.15***	1	0.09***	−0.18***
(14) *LOSS*	−0.31***	−0.05***	−0.05***	−0.15***	0.13***	−0.08***	−0.18***	0.01	−0.40***	−0.02**	0.21***	−0.45***	0.18***	1	−0.13***
(15) *SEG*	0.49***	0.06***	0.05***	0.20***	−0.16***	0.06***	0.21***	−0.08***	0.49***	0.14***	−0.27***	0.23***	−0.22***	−0.22***	1

The lower left side of the table presents the Pearson correlations based on the full sample. The upper right side of the table presents the Pearson correlations based on the propensity score matching sample, which consists of the observations of the treatment firms (firms which have breaches during the sample period) and the matched control firms (firms which have no breaches during the sample period). See the Appendix A for variable definitions. ***, **, and * represent significance levels at 1%, 5%, and 10%, respectively.

88% in the full sample and the PSM sample, respectively).

For other variables, on average, observations with reported breaches have significantly larger values in *AT*, *ROI*, and *SEG* and significantly smaller values in *CRTR, QCKR*, and *LOSS*. We find no significant differences between observations with and without breaches in *MTB* and *DEBTR*. We also observe similar results when we compare medians between observations with *BREACH* = 1 and *BREACH* = 0. These results provide initial evidence that firm-years with the occurrence of information security breaches are fundamentally different from those without breaches.

Table 4 displays the Pearson correlations between variables. The lower left and upper right sides present the results of the full sample and the PSM sample, respectively. From the table, we first observe that *lnAUDIT_FEES* is positively correlated to *BREACH* in both samples. The audit-firm characteristics (*EXPERTISE, TENURE_long,* and *BIG4*) are positively correlated to *lnAUDIT_FEES* as well. These results are consistent with prior studies about audit fees. Second, we do not find high correlations between *breachvar* (*BREACH* or *NBREACH*) and other control variables; the highest correlation ratio is 0.13 between *BREACH* and *lnAT* in the full sample. This result does not show evidence of a potential multicollinearity problem.[16]

4.2. Regression results: the base model

Before we report the tests of our hypotheses, we first present the results of the base model, which regresses *lnAUDIT_FEES* on *BREACH* or *NBREACH*. Columns (1) and (2) of Table 5 show the results using the full sample, and Columns (3) and (4) show the results using the PSM sample. In Columns (1) and (2), the coefficients of *BREACH* and *NBREACH* are both significantly positive (0.127 and 0.087, respectively; both with $p < 0.01$). The estimated coefficients mean that audit fees in the next year are on average 13.5% ($e^{0.127} - 1$) higher for firms with breaches than for firms without breaches, all else being equal. Also, audit fees in the next year increase by 9.1% ($e^{0.087} - 1$) on average per breach, all else being equal. These results indicate that audit fees in year $t + 1$ are higher with the occurrence of an information security breach in year *t*. However, the results may come from the effect of firm size, that is, the fees are originally higher for larger firms, which may also have a higher possibility of being attacked.

To reduce the size effect, we run Eq. (1) using the PSM sample. Columns (3) and Column (4) show that the coefficients of both *BREACH* and *NBREACH* remain significantly positive (0.142 and 0.101, respectively; both with $p < 0.01$). In sum, the overall main results are similar across different samples and models. These results are consistent with the findings of Higgs et al. (2017) and Li et al. (2017) and provide initial evidence on the association between audit fees and the occurrence or the number of information security breaches. With respect to the control variables, the signs of coefficients are mostly consistent with prior literature. The audit fees are higher when the client size is larger (*lnAT*), when the audit case is more complex (*SEG*), and when the audit risk is higher, as reflected in higher debt ratio (*DEBTR*), higher current ratio (*CRTR*), lower return on investment (*ROI*), lower quick ratio (*QCKR*), and previous losses (*LOSS*).

4.3. Regression results: the moderating effect of audit-firm industry expertise

Table 6 presents the regression results of the test of Hypothesis 1. Columns (1) and (2) show the results using the full sample, and Columns (3) and (4) show the results using the PSM sample. Compared to the base model, we include *EXPERTISE* and *EXPERTISE*BREACH* (or *EXPERTISE*NBREACH*) in the regression. In Column (1), the main effect of *EXPERTISE* is significantly positive on *lnAUDIT_FEES* (0.195 with $p < 0.01$), which is consistent with results in prior studies. The coefficient of *BREACH* remains significantly positive (0.419 with $p < 0.01$). Moreover, the coefficient of *EXPERTISE*BREACH* in Column (1) and that of *EXPERTISE*NBREACH* in Column (2) are both significantly negative (-0.312 and -0.254, respectively; both with $p < 0.01$). These results are consistent when using the PSM sample, i.e., -0.242 in Column (3) and -0.195 in Column (4) (both with $p < 0.05$). The results in Column (1), as an example, mean that among firms whose auditors have no industry expertise, the audit fees are on average 52.0% ($e^{0.419} - 1$) higher for firms with breaches than for firms without breaches, all else being equal. However, the difference is only 11.3% ($e^{0.419–0.312} - 1$) on average among firms whose auditors have industry expertise. In addition, the signs of all control variables are consistent with our expectations. In sum, the negative coefficients of *EXPERTISE*breachvar* support Hypothesis 1; that is, the positive association between audit fees and the occurrence or the number of information security breaches is negatively moderated when firms engage with auditors who have industry expertise. This result may occur because less incremental effort is needed by audit firms with industry expertise, compared to those without expertise, to estimate clients' information security risks in future operations.

4.4. Regression results: the moderating effect of audit-firm tenure

Table 7 shows the results of the test of Hypothesis 2. In Column (1), the coefficient of *BREACH* is significantly positive (0.128 with $p < 0.05$). The coefficient of *TENURE_long*BREACH* is, as expected, significantly negative (-0.260 with $p < 0.01$), while that of *TENURE_short*BREACH* is statistically insignificant (0.108). These results show that among firms with medium audit-firm tenure, audit fees are on average 13.7% ($e^{0.128} - 1$) higher for firms with breaches than for firms without breaches, all else being equal. However, among firms with long audit-firm tenure, audit fees are reduced, on average, by 12.4% ($e^{0.128–0.260} - 1$) for firms with breaches, compared to those without. The results are similar when we consider the number of breaches, i.e., Columns (2) and (4), or

[16] We also calculate variance inflation factors (VIFs) after running the regressions to detect a potential multicollinearity problem and do not find any VIF above the suggested threshold of 10. *lnAT* has the highest value of VIF at 2.78 and the mean VIF is 1.58.

Table 5
Base model: Audit fees and information security breaches.

	Predicted sign	Full sample		Propensity score matching sample	
		(1)	(2)	(3)	(4)
Dependent variable:		*lnAUDIT_FEES*	*lnAUDIT_FEES*	*lnAUDIT_FEES*	*lnAUDIT_FEES*
breachvar:		*BREACH*	*NBREACH*	*BREACH*	*NBREACH*
breachvar	+	0.127***	0.087***	0.142***	0.101***
		(0.048)	(0.032)	(0.049)	(0.032)
MTB	+	0.005***	0.005***	0.003	0.003
		(0.001)	(0.001)	(0.002)	(0.002)
lnAT	+	0.574***	0.574***	0.557***	0.557***
		(0.006)	(0.006)	(0.009)	(0.009)
DEBTR	+	0.174***	0.174***	0.196***	0.196***
		(0.052)	(0.052)	(0.074)	(0.074)
CRTR	+	0.767***	0.767***	0.939***	0.939***
		(0.051)	(0.051)	(0.077)	(0.077)
ROI	−	−0.280***	−0.280***	−0.217***	−0.217***
		(0.029)	(0.029)	(0.070)	(0.070)
QCKR	−	−0.033***	−0.033***	−0.033***	−0.033***
		(0.002)	(0.002)	(0.005)	(0.005)
LOSS	?	0.124***	0.124***	0.124***	0.124***
		(0.016)	(0.016)	(0.020)	(0.020)
SEG	+	0.050***	0.050***	0.057***	0.057***
		(0.005)	(0.005)	(0.006)	(0.006)
Intercept		9.550***	9.549***	9.396***	9.392***
		(0.139)	(0.139)	(0.282)	(0.280)
Year fixed effects		Included	Included	Included	Included
Industry fixed effects		Included	Included	Included	Included
Observations		22,467	22,467	12,708	12,708
Adjusted R-squared		0.832	0.832	0.810	0.810

Columns (1) and (2) present the results based on the full sample, including the first breach of a firm-year and all breaches, respectively. Columns (3) and (4) present the results based on the propensity score matching sample, including the first breach of a firm-year and all breaches, respectively. The propensity score matching sample consists of the observations of the treatment firms (firms which have breaches during the sample period) and the matched control firms (firms which have no breaches during the sample period). See the Appendix A for variable definitions. ***, **, and * represent significance levels at 1%, 5%, and 10%, respectively. In parentheses are the standard errors of coefficients, which are clustered by firms. All regressions include dummy variables to control for year fixed effects and industry fixed effects (one-digit SIC).

when we use the PSM sample, i.e., Columns (3) and (4).

Since the coefficient of *TENURE_long***breachvar* only represents the difference between long tenure and medium tenure effects, we further test the difference between the coefficients of *TENURE_short***breachvar* and *TENURE_long***breachvar* to examine whether the effects of long and short audit-firm tenures are statistically indifferent. The *F* test results are listed at the bottom of Table 7. In Column (1), the *F* value is 7.334, which rejects the hypothesis that the two incremental effects of tenure are no different at the significance level of 1%. The result is similar, albeit weak statistical significance, using *NBREACH* ($p < 0.10$). The results are also similar using the PSM sample, except for Column (4). In sum, our results support Hypothesis 2. That is, auditors who have long tenure with current clients may already have experience and be competent to better estimate clients' potential information security risks with less effort. Therefore, the audit fees they charge their clients with reported breaches may not be as high as the fees charged by auditors with short or medium tenure.

4.5. Regression results: the moderating effect of audit-firm size

The results of Hypothesis 3 are shown in Table 8. As seen in Column (1), the coefficient of *BREACH* is significantly positive (0.498 with $p < 0.01$). Furthermore, as expected in Hypothesis 3, the coefficient of *BIG4***BREACH* is significantly negative (−0.355 with $p < 0.05$). The negative coefficient of the interaction term means that the association between audit fees and the occurrence of breaches is smaller for firms audited by one of the Big 4 auditors than for those audited by non-Big4 auditors. Specifically, among firms engaging with Big 4 auditors, audit fees are only, on average, 15.4% ($e^{0.498-0.355}-1$) higher for firms with breaches than for firms without breaches, compared to 64.5% ($e^{0.498}-1$) among firms engaging with non-Big 4 auditors, all else being equal. The results are similar when we consider the number of breaches (*NBREACH*) instead of the occurrence of breaches (*BREACH*) in the model, i.e., Columns (2) and (4), or when we use the PSM sample, i.e., Columns (3) and (4). The signs of control variables are mostly consistent with our expectations.

4.6. Endogeneity consideration

Several factors may affect audit fees and the occurrence of information security breaches simultaneously, we consider the

Table 6
The moderating effect of audit-firm industry expertise.

	Predicted sign	Full sample		Propensity score matching sample	
		(1)	(2)	(3)	(4)
Dependent variable:		*lnAUDIT_FEES*	*lnAUDIT_FEES*	*lnAUDIT_FEES*	*lnAUDIT_FEES*
breachvar:		*BREACH*	*NBREACH*	*BREACH*	*NBREACH*
breachvar	+	0.419***	0.332***	0.365***	0.286***
		(0.083)	(0.075)	(0.087)	(0.076)
EXPERTISE	+	0.195***	0.195***	0.151***	0.151***
		(0.019)	(0.019)	(0.028)	(0.028)
EXPERTISE*breachvar	(H1) -	−0.312***	−0.254***	−0.242**	−0.195**
		(0.098)	(0.082)	(0.101)	(0.083)
MTB	+	0.004***	0.004***	0.002	0.002
		(0.001)	(0.001)	(0.002)	(0.002)
lnAT	+	0.550***	0.550***	0.542***	0.542***
		(0.006)	(0.006)	(0.009)	(0.009)
DEBTR	+	0.176***	0.176***	0.190***	0.191***
		(0.051)	(0.051)	(0.073)	(0.073)
CRTR	+	0.744***	0.744***	0.918***	0.918***
		(0.050)	(0.050)	(0.077)	(0.077)
ROI	−	−0.264***	−0.263***	−0.224***	−0.223***
		(0.029)	(0.029)	(0.068)	(0.069)
QCKR	−	−0.033***	−0.033***	−0.033***	−0.033***
		(0.002)	(0.002)	(0.005)	(0.005)
LOSS	?	0.116***	0.116***	0.124***	0.123***
		(0.015)	(0.015)	(0.020)	(0.020)
SEG	+	0.051***	0.051***	0.057***	0.057***
		(0.005)	(0.005)	(0.006)	(0.006)
Intercept		9.567***	9.568***	9.440***	9.437***
		(0.136)	(0.136)	(0.275)	(0.273)
Year fixed effects		Included	Included	Included	Included
Industry fixed effects		Included	Included	Included	Included
Observations		22,467	22,467	12,708	12,708
Adjusted R-squared		0.835	0.835	0.812	0.812

Columns (1) and (2) present the results based on the full sample. Columns (3) and (4) present the results based on the propensity score matching sample. The propensity score matching sample consists of the observations of the treatment firms (firms which have breaches during the sample period) and the matched control firms (firms which have no breaches during the sample period). See the Appendix A for variable definitions. ***, **, and * represent significance levels at 1%, 5%, and 10%, respectively. In parentheses are the standard errors of coefficients, which are clustered by firms. All regressions include dummy variables to control for year fixed effects and industry fixed effects (one-digit SIC).

potential endogeneity issue resulting from unobserved factors. For example, auditors may charge large clients higher fees because more effort is needed. Large firms may be more likely to become the target of information security attacks. Missing these factors in the regression model may lead to an endogeneity issue, which violates the assumption of the OLS model that $\mathrm{E}(\epsilon\ \mathrm{X}) = 0$.

One way to address this issue is to run a two-stage least squares regression with instrumental variables (IVs). However, it is theoretically and empirically difficult to find a suitable IV. Furthermore, there is a dilemma that the better the IVs are correlated with the endogenous factors, the more difficult it is to claim that they are uncorrelated with the disturbances (Greene, 2000). Therefore, in our context, we need to find a way to statistically address this issue even though no strong instrumental variables can be identified. We adopt a method provided by Lewbel (2012), which generates IVs from existing variables based on higher moments and heteroscedasticity.[17] We generate IVs based on the following equation, Eq. (5):

$$IV_j = (X_j - \bar{X})\ \epsilon \tag{5}$$

where X is each of the exogenous variables in our main model, i.e., *MTB*, *lnAT*, *DEBTR*, etc.; $\bar{X}$ is the mean of the exogenous variable; and ϵ is the residual from the auxiliary regression of *BREACH* (or *NBREACH)* on all exogenous variables (*MTB, lnAT*, etc.). Thus, we generate as many IVs as the number of exogenous variables in our main model. Next, we use these generated IVs to run two-stage least squares regressions based on our main models with *BREACH* (or *NBREACH*) as the endogenous variable.

The empirical results are qualitatively similar to those of the main tests. Table 9 presents the results of the base model using *BREACH*. In the full sample and the PSM samples, the coefficients of *Predicted_BREACH* from the second stage are positive with a weak significance (0.104 and 0.125, respectively; both with $p < 0.10$). The un-tabulated results are also similar using *NBREACH* as the

[17] Lewbel's approach is to identify the coefficients by restricting the correlations of the product of residuals and the exogenous variables ($\mathrm{E}(\epsilon\epsilon^{'}\ \mathrm{X}) = 0$) and by the heteroscedasticity of residuals (Lewbel, 2012). Since the identification is based on higher moments, the estimates are likely to be noisier and less reliable than those based on standard exclusion restrictions. However, they may be useful when traditional instruments are weak or nonexistent.

Table 7
The moderating effect of audit-firm tenure.

		Full sample		Propensity score matching sample	
Dependent variable: breachvar:	Predicted Sign	(1) lnAUDIT_FEES BREACH	(2) lnAUDIT_FEES NBREACH	(3) lnAUDIT_FEES BREACH	(4) lnAUDIT_FEES NBREACH
breachvar	+	0.128^{**}	0.097^{***}	0.146^{***}	0.113^{***}
		(0.055)	(0.034)	(0.055)	(0.034)
TENURE_short	?	-0.064^{***}	-0.063^{***}	-0.037^{*}	-0.036^{*}
		(0.013)	(0.013)	(0.019)	(0.019)
TENURE_long	?	0.141^{***}	0.141^{***}	0.111^{***}	0.111^{***}
		(0.020)	(0.020)	(0.024)	(0.024)
$TENURE\_short^{*}breachvar$	?	0.108	−0.003	0.066	−0.028
		(0.099)	(0.079)	(0.099)	(0.075)
$TENURE\_long^{*}breachvar$	(H2) -	-0.260^{***}	-0.222^{***}	-0.210^{**}	-0.173^{*}
		(0.100)	(0.085)	(0.104)	(0.089)
MTB	+	0.005^{***}	0.005^{***}	0.003	0.003
		(0.001)	(0.001)	(0.002)	(0.002)
lnAT	+	0.569^{***}	0.569^{***}	0.555^{***}	0.555^{***}
		(0.006)	(0.006)	(0.009)	(0.009)
DEBTR	+	0.178^{***}	0.178^{***}	0.199^{***}	0.199^{***}
		(0.052)	(0.052)	(0.074)	(0.074)
CRTR	+	0.765^{***}	0.766^{***}	0.938^{***}	0.939^{***}
		(0.051)	(0.051)	(0.077)	(0.077)
ROI	−	-0.277^{***}	-0.277^{***}	-0.222^{***}	-0.221^{***}
		(0.029)	(0.029)	(0.070)	(0.070)
QCKR	−	-0.033^{***}	-0.033^{***}	-0.033^{***}	-0.033^{***}
		(0.002)	(0.002)	(0.005)	(0.005)
LOSS	?	0.129^{***}	0.129^{***}	0.128^{***}	0.128^{***}
		(0.015)	(0.016)	(0.020)	(0.020)
SEG	+	0.050^{***}	0.050^{***}	0.056^{***}	0.056^{***}
		(0.005)	(0.005)	(0.006)	(0.006)
Intercept		9.621^{***}	9.622^{***}	9.436^{***}	9.430^{***}
		(0.136)	(0.135)	(0.281)	(0.278)
Year fixed effects		Included	Included	Included	Included
Industry fixed effects		Included	Included	Included	Included
Observations		22,467	22,467	12,708	12,708
Adjusted R-squared		0.833	0.833	0.811	0.811
F test: $TENURE\_short^{*}breachvar = TENURE\_long^{*}breachvar$					
F value		7.334	3.468	3.981	1.515
p value		0.007	0.0627	0.046	0.219

Columns (1) and (2) present the results based on the full sample. Columns (3) and (4) present the results based on the propensity score matching sample. The propensity score matching sample consists of the observations of the treatment firms (firms which have breaches during the sample period) and the matched control firms (firms which have no breaches during the sample period). See the Appendix A for variable definitions. ***, **, and * represent significance levels at 1%, 5%, and 10%, respectively. In parentheses are the standard errors of coefficients, which are clustered by firms. All regressions include dummy variables to control for year fixed effects and industry fixed effects (one-digit SIC).

major independent variable (0.068 and 0.082, respectively; both with $p < 0.05$). Next, to test the moderating effects of audit-firm characteristics, we divide the sample by the three audit-firm characteristics and run the two-stage regressions separately (un-tabulated). Using the subsample with industry expertise, the coefficients of *BREACH* and *NBREACH* are both significantly positive (0.115 with $p < 0.10$ and 0.077 with $p < 0.05$, respectively) and, consistent with Hypothesis 1, are smaller than those using the subsample without industry expertise (0.359 and 0.270, respectively; both with $p < 0.01$). Using the subsample with long audit-firm tenure, the coefficients of *BREACH* and *NBREACH* are both statistically insignificant (−0.085 and −0.082, respectively), while those using the subsample without long audit-firm tenure are significantly positive (0.121 and 0.077, respectively; both with $p < 0.05$), which is consistent with Hypothesis 2. Finally, using the subsample with Big 4 audit firms, the coefficients of *BREACH* and *NBREACH* are both positive (0.128 and 0.084, respectively; both with $p < 0.05$) and, consistent with Hypothesis 3, are smaller than those using the subsample without Big 4 audit firms (both 0.512 with $p < 0.01$).

4.7. Additional tests

The first additional test is to control for the three audit-firm characteristics simultaneously. To enhance our test of each audit-firm characteristic, we include the main effects of industry expertise, tenure, and audit-firm size simultaneously as additional control variables in our hypothesis-testing models. The un-tabulated results support our three hypotheses after controlling for all audit-firm characteristics.

Table 8
The moderating effect of audit-firm size.

	Predicted sign	Full sample		Propensity score matching sample	
		(1)	(2)	(3)	(4)
Dependent variable:		*lnAUDIT_FEES*	*lnAUDIT_FEES*	*lnAUDIT_FEES*	*lnAUDIT_FEES*
breachvar:		*BREACH*	*NBREACH*	*BREACH*	*NBREACH*
breachvar	+	0.498***	0.497***	0.462***	0.462***
		(0.135)	(0.135)	(0.136)	(0.136)
BIG4	+	0.299***	0.299***	0.254***	0.254***
		(0.025)	(0.025)	(0.042)	(0.042)
*BIG4***breachvar*	(H3) -	−0.355**	−0.398***	−0.321**	−0.360***
		(0.144)	(0.139)	(0.144)	(0.139)
MTB	+	0.004***	0.004***	0.002	0.002
		(0.001)	(0.001)	(0.002)	(0.002)
lnAT	+	0.537***	0.537***	0.537***	0.537***
		(0.007)	(0.007)	(0.010)	(0.010)
DEBTR	+	0.166***	0.166***	0.185**	0.185**
		(0.052)	(0.052)	(0.074)	(0.074)
CRTR	+	0.725***	0.726***	0.923***	0.924***
		(0.051)	(0.050)	(0.077)	(0.077)
ROI	–	−0.267***	−0.267***	−0.256***	−0.256***
		(0.028)	(0.028)	(0.068)	(0.068)
QCKR	–	−0.034***	−0.034***	−0.033***	−0.033***
		(0.002)	(0.002)	(0.005)	(0.005)
LOSS	?	0.113***	0.113***	0.124***	0.124***
		(0.015)	(0.015)	(0.020)	(0.020)
SEG	+	0.054***	0.054***	0.058***	0.058***
		(0.005)	(0.005)	(0.006)	(0.006)
Intercept		9.541***	9.540***	9.309***	9.305***
		(0.127)	(0.127)	(0.301)	(0.298)
Year fixed effects		Included	Included	Included	Included
Industry fixed effects		Included	Included	Included	Included
Observations		22,467	22,467	12,708	12,708
Adjusted R-squared		0.838	0.838	0.813	0.813

Columns (1) and (2) present the results based on the full sample. Columns (3) and (4) present the results based on the propensity score matching sample. The propensity score matching sample consists of the observations of the treatment firms (firms which have breaches during the sample period) and the matched control firms (firms which have no breaches during the sample period). See the Appendix A for variable definitions. ***, **, and * represent significance levels at 1%, 5%, and 10%, respectively. In parentheses are the standard errors of coefficients, which are clustered by firms. All regressions include dummy variables to control for year fixed effects and industry fixed effects (one-digit SIC).

The second additional test is the sensitivity test of audit-firm tenure. In the main test of Hypothesis 2, we use the cutoff of 4 and 13 years of tenure. To examine whether the results are driven by the chosen cutoff, we re-run the regression using alternative tenure cutoffs. Using 8, 9, and 10 years as long tenure cutoffs and 3 and 5 years as short tenure cutoffs, the results are mostly similar, except for less significance in some regression results. The coefficient of *TENURE_long***breachvar* remains negative while that of *TENURE_short***breachvar* remains statistically insignificant.

The third additional test is the sensitivity test of the PSM sample. Instead of the one-to-ten PSM sample, we use matched samples with different numbers of nearest neighbors (from nine to five). Thus, the size of the PSM sample becomes 11,655 (one-to-nine), 10,470 (one-to-eight), 9406 (one-to-seven), 8328 (one-to-six), and 7216 (one-to-five). The un-tabulated empirical results of the base model, i.e., Eq. (1), and the industry expertise model, i.e., Eq. (2), using different PSM samples are qualitatively similar to those using the one-to-ten PSM sample. For the variable of interest (*EXPERTISE***breachvar*), the coefficients remain significantly negative ($p < 0.05$) across different PSM samples. In the tenure test, i.e., Eq. (3), the main effects of *breachvar*, *TENURE_short,* and *TENURE_long* using different PSM samples are qualitatively similar to those using the one-to-ten PSM sample, while the coefficients of *TENURE_long***breachvar* become less significant ($p < 0.10$) or insignificant. In the audit-firm size test, i.e., Eq. (4), the results using different PSM samples are mostly similar to those using the one-to-ten PSM sample, albeit the insignificant coefficients of *BIG4***breachvar* in the one-to-six and one-to-five PSM samples.

5. Conclusions and discussion

This paper examines how audit-firm characteristics affect auditors' efforts to understand and assess clients' information security risks. In particular, we focus on the moderating effects of audit-firm industry expertise and tenure as well as audit-firm size on the association between reported information security breaches and the subsequent audit fees. Given the importance of IT in a firm's operating environment, information security risks may potentially have an impact on the confidentiality, integrity, and availability of a firm's information, which in turn relates to/affects the reliability of the financial reporting, operation and reputation of the firm,

Table 9
Endogenous model for the base model.

	Predicted sign	Full sample		Propensity score matching sample	
		First stage	Second stage	First stage	Second stage
Dependent variable:		*BREACH*	*lnAUDIT_FEES*	*BREACH*	*lnAUDIT_FEES*
Predicted_BREACH	+		0.104*		0.125*
			(0.057)		(0.065)
MTB		−0.000***	0.005***	−0.000	0.003
		(0.000)	(0.001)	(0.000)	(0.002)
lnAT		0.003***	0.574***	0.005***	0.558***
		(0.000)	(0.006)	(0.001)	(0.009)
DEBTR		−0.001	0.173***	−0.004	0.195***
		(0.002)	(0.052)	(0.004)	(0.074)
CRTR		0.001	0.767***	0.014***	0.939***
		(0.002)	(0.051)	(0.005)	(0.077)
ROI		−0.003*	−0.281***	−0.030**	−0.217***
		(−0.002)	(0.029)	(0.013)	(0.070)
QCKR		−0.000	−0.033***	−0.000	−0.033***
		(0.000)	(0.002)	(0.000)	(0.005)
LOSS		−0.001*	0.124***	−0.005**	0.124***
		(0.001)	(0.016)	(0.002)	(0.020)
SEG		0.001**	0.050***	0.001	0.057***
		(0.000)	(0.005)	(0.000)	(0.006)
IV_MTB		−0.009		−0.009	
		(0.006)		(0.010)	
IV_lnAT		0.175***		0.248***	
		(0.015)		(0.034)	
IV_DEBTR		−0.012		−0.157	
		(0.148)		(0.261)	
IV_CRTR		0.307**		0.667***	
		(0.138)		(0.244)	
IV_ROI		2.685***		2.720***	
		(0.283)		(0.614)	
IV_QCKR		−0.003		0.001	
		(0.016)		(0.022)	
IV_LOSS		0.183***		0.171*	
		(0.056)		(0.094)	
IV_SEG		0.004		0.011	
		(0.012)		(0.019)	
Intercept		−0.001	9.373***	−0.028	9.376***
		(0.010)	(0.265)	(0.015)	(0.283)
Year fixed effects		Included	Included	Included	Included
Industry fixed effects		Included	Included	Included	Included
Observations		22,467	22,467	12,708	12,708
Adjusted R-squared		0.888	0.832	0.715	0.810

The results are based on two-stage least squares with generated instrumental variables as suggested by Lewbel (2012). *IV_vars* are the instrumental variables generated by the product of mean-centered *var* and the residuals from the auxiliary regression, which regresses *BREACH* on all control variables (*vars*). Columns (1) and (2) present the results based on the full sample, and Columns (3) and (4) present the results based on the propensity score matching sample. The propensity score matching sample consists of the observations of the treatment firms (firms which have breaches during the sample period) and the matched control firms (firms which have no breaches during the sample period). See the Appendix A for variable definitions. ***, **, and * represent significance levels at 1%, 5%, and 10%, respectively. In parentheses are the standard errors of coefficients, which are clustered by firms. All regressions include dummy variables to control for year fixed effects and industry fixed effects (one-digit SIC).

and even continuity of the firm. In this study, we bring the audit-firm characteristics to the context of information security by arguing that audit-firm industry expertise, tenure, and size help auditors comprehend emerging and common issues regarding information security within the industry and become equipped with client-specific knowledge. Our findings suggest that these three audit-firm characteristics negatively moderate the positive association between information security breaches and audit fees. We believe that our findings not only enrich the existing literature related to both auditing and information security in academics but also provide implications in practice. As several parties, such as the SEC, PCAOB, and AICPA, have raised concerns about the potential threats of information security vulnerabilities to business operations and financial reporting quality, our results highlight the importance for auditors to be equipped with knowledge about information security risks. Our results also provide implications to these professional associations that a more detailed guidance for auditors to examine and detect information security vulnerabilities is urgently needed in correspondence with the escalating information security issues.

We acknowledge several limitations and suggest several avenues for future research. First, as discussed in Section 3, we consider only publicly available confidentiality-type incidents. Examining additional types of information security breaches (when publicly available) might be a fruitful future research endeavor. Second, our empirical study does not capture the processes of how auditors evaluate clients' information security risks or assess clients' information security management policies. For future research avenues, first, it would be interesting to examine whether external audits may improve the effectiveness of a firm's information security risk management. Second, future research may examine auditor retention after breaches, as auditors may choose to leave instead of charging higher fees, to avoid high audit risk resulting from the change in a client's information security risk.

Appendix A. Variable definitions

Variable	Definition	Data source
Dependent variable:		
lnAUDIT_FEES	Natural log of total fees of year $t + 1$ to perform the audit or review in accordance with GAAS	*Audit Analytics*
Major independent variables:		
BREACH	1 if one or more information security breach incidents are reported in year t, and 0 otherwise	*DataLossDB*
NBREACH	Number of reported information security breach incidents in year t	*DataLossDB*
EXPERTISE	1 if the audit firm has the largest or more than 10% of market share in the industry in which the client operates, and 0 otherwise. The market share of an industry is measured by total assets	*Audit Analytics*
TENURE_short (long)	1 if the incumbent audit firm has audited the client for 4 years or fewer (13 years or more), and 0 otherwise	*Audit Analytics*
BIG4	1 if the client is audited by one of the Big 4 audit firms, and 0 otherwise	*Audit Analytics*
Control variables		
MTB	Market to book ratio, which is the market value over book value of common equity at the end of year t	*Compustat*
lnAT	Natural log of total assets at the end of year t	*Compustat*
DEBTR	Debt ratio, which is the long-term debt over total assets at the end of year t	*Compustat*
CRTR	Current ratio, which is the current assets over total assets at the end of year t	*Compustat*
ROI	Return on investment, which is the earnings before interest expenses and taxes over total assets of year t	*Compustat*
QCKR	Quick ratio, which is current assets (minus inventories) over current liabilities at the end of year t	*Compustat*
LOSS	1 if there is a net loss in any of the past three years, and 0 otherwise	*Compustat*
SEG	Number of business segments or operating segments (if business segments are not reported) in year t	*Compustat*

References

Acquisti, A., Friedman, A., Telang, R., 2006. Is there a cost to privacy breaches? An event study. The Fifth Workshop on the Econom. Inform. Security (WEIS). Robinson College, University of Cambridge, London.

AICPA, 2006. Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatements. AICPA, New York, NY.

Armstrong, C.S., Jagolinzer, A.D., Larcker, D.F., 2010. Chief executive officer equity incentives and accounting irregularities. J. Account. Res. 48 (2), 225–271.

Balsam, S., Krishnan, J., Yang, J.S., 2003. Auditor industry specialization and earnings quality. AUDITING: J. Pract. Theory 22 (2), 71–97.

Basel Committee on Banking Supervision (BCBS), 2001. Operational Risk: Supporting Document to the New Basel Capital Accord (accessed 2017/05/01). http://www.bis.org/publ/bcbsca07.pdf.

Beatty, R.P., 1993. The economic determinants of auditor compensation in the initial public offerings market. J. Account. Res. 31 (2), 294–302.

Bell, T.B., Knechel, W.R., Payne, J.L., Willingham, J.J., 1998. An empirical investigation of the relationship between the computerization of accounting systems and the incidence and size of audit differences. AUDITING: J. Pract. Theory 17 (1), 13–38.

Boritz, E., Hayes, L., Lim, J.H., 2012. A content analysis of auditors' reports on IT internal control weaknesses: the comparative advantages of an automated approach to control weakness identification. Int. J. Account. Inform. Syst. 14 (2), 138–163.

Campbell, K., Gordon, L.A., Loeb, M.P., Zhou, L., 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. J. Comput. Secur. 11 (3), 431–448.

Center for Audit Quality (CAQ), 2014. Cybersecurity and the external audit (accessed 2017/05/08). http://thecaq.org/caq-alert-2014-03-cybersecurity-and-external-audit.

Carcello, J.V., Nagy, A.L., 2004a. Audit firm tenure and fraudulent financial reporting. AUDITING: J. Pract. Theory 23 (2), 55–69.

Carcello, J.V., Nagy, A.L., 2004b. Client size, auditor specialization and fraudulent financial reporting. Manage. Audit. J. 19 (5), 651–668.

Cavusoglu, H., Mishra, B., Raghunathan, S., 2004. The effect of internet security breach announcements on market value of breached firms and internet security developers. Int. J. Electr. Commer. 9 (1), 69–105.

Compliance Week, 2017. Companies Will Soon Have New Way to Gut Check Cyber Risk (accessed 2017/05/08). https://www.complianceweek.com/blogs/accounting-auditing-update/companies-will-soon-have-new-way-to-gut-check-cyber-risk-.WPy-29LDE2w.

Curtis, M.B., Jenkins, J.G., Bedard, J.C., Deis, D.R., 2009. Auditors' training and proficiency in information systems: a research synthesis. J. Info. Syst. 23 (1), 79–96.

Davis, L.R., Soo, B.S., Trompeter, G.M., 2009. Auditor tenure and the ability to meet or beat earnings forecasts. Contemp. Account. Res. 26 (2), 517–548.

DeFond, M., Zhang, J., 2014. A review of archival auditing research. J. Account. Econ. 58 (2–3), 275–326.

Dinev, T., Hu, Q., 2007. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. J. Assoc. Inf. Syst. 8 (7), 386–408.

Dopuch, N., Simunic, D., 1982. Competition in auditing: an assessment. In: Symposium on Auditing Research IV. University of Illinois, Urbana, pp. 401–450.

Dunn, K., Mayhew, B., 2004. Audit firm industry specialization and client disclosure quality. Rev. Account. Stud. 9 (1), 35–58.

Ettredge, M.L., Richardson, V.J., 2003. Information transfer among internet firms: the case of hacker attacks. J. Info. Syst. 17 (2), 71–82.

Fafatas, S.A., Sun, K.J., 2010. The relationship between auditor size and audit fees: further evidence from Big 4 market shares in emerging economies. Res. Account. Emerg. Econ. 10, 57–85.

Financial Executives Research Foundation (FERF), 2016. Mitigating Increases in Audit Fees (accessed 2017/05/08). http://www.financialexecutives.org/ferf/download/2016Final/2016-001.pdf.

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

Finkelstein, S., Hambrick, D.C., 1990. Top-management-team tenure and organizational outcomes: the moderating role of managerial discretion. Adm. Sci. Q. 35 (3), 484–503.

Francis, J.R., 1984. The effect of audit firm size on audit prices. J. Account. Econ. 6 (2), 133–151.

Francis, J.R., Simon, D.T., 1987. A test of audit pricing in the small-client segment of the U. S. audit market. Account. Rev. 62 (1), 145–157.

Francis, J.R., Stokes, D.J., 1986. Audit prices, product differentiation, and scale economies: further evidence from the Australian market. J. Account. Res. 24 (2), 383–393.

Gal-Or, E., Ghose, A., 2005. The economic incentives for sharing security information. Inf. Syst. Res. 16 (2), 186–208.

Garg, A., Curtis, J., Halper, H., 2003. Quantifying the financial impact of IT security breaches. Inf. Manage. Comput. Secur. 11 (2), 74–83.

Geiger, M.A., Raghunandan, K., 2002. Auditor tenure and audit reporting failures. AUDITING: J. Pract. Theory 21 (1), 67–78.

Ghosh, A., Doocheol, M., 2005. Auditor tenure and perceptions of audit quality. Account. Rev. 80 (2), 585–612.

Gordon, L.A., Loeb, M.P., 2002a. The economics of information security investment. ACM Trans. Inf. Syst. Secur. 5 (4), 438–457.

Gordon, L.A., Loeb, M.P., 2002b. Return on information security investments: myths vs. realities. Strateg. Finan. 84 (5), 26–31.

Gordon, L.A., Loeb, M.P., 2006. Budgeting process for information security expenditures. Commun. ACM 49 (1), 121–125.

Gordon, L.A., Loeb, M.P., 2010. Market value of voluntary disclosures concerning information security. MIS Q. 34 (3), 567–594.

Gordon, L.A., Loeb, M.P., Lucyshyn, W., 2003. Sharing information on computer systems security: an economic analysis. J. Account. Publ. Policy 22 (6), 461–485.

Gordon, L.A., Loeb, M.P., Lucyshyn, W., Sohail, T., 2006. The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. J. Account. Publ. Policy 25 (5), 503–530.

Gordon, L.A., Loeb, M.P., Sohail, T., Tseng, C.-Y., Zhou, L., 2008. Cybersecurity, capital allocations and management control systems. Eur. Account. Rev. 17 (2), 215–241.

Gordon, L.A., Loeb, M.P., Zhou, L., 2011. The impact of information security breaches: has there been a downward shift in costs? J. Comput. Secur. 19 (1), 33–56.

Greene, W., 2000. Econometric Analysis, fourth ed. Wiley, Hoboken, NJ.

Hay, D.C., Knechel, W.R., Wong, N., 2006. Audit fees: a meta-analysis of the effect of supply and demand attributes. Contemp. Account. Res. 23 (1), 141–191.

Herring, R.J., 2002. The Basel 2 approach to bank operational risk: regulation on the wrong track. J. Risk Finan. 4 (1), 42–45.

Higgs, J.L., Pinsker, R., Smith, T.J., 2017. Do auditors price breach risk in their audit fees? Working paper. Florida Atlantic University and University of South Florida. < http://aaahq.org/Meetings/2017/Accounting-Information-Systems/Program > .

Hovav, A., D'Arcy, J., 2003. The impact of Denial-of-Service attack announcements on the market value of firms. Risk Manage. Insur. Rev. 6 (2), 97–121.

Hsu, C., Lee, J.-N., Straub, D.W., 2012. Institutional influences on information systems security innovations. Inf. Syst. Res. 23 (3-part-2), 918–939.

Hsu, C., Wang, T., 2014a. Composition of the top management team and information security breaches. In: Cruz-Cunha, M.M., Portela, I.M. (Eds.), Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance. IGI Global, Hershey, PA.

Hsu, C., Wang, T., 2014b. Exploring the association between board structure and information security breaches. Asia Pac. J. Inf. Syst. 24 (4), 531–557.

Hsu, C., Wang, T., Lu, A., 2016. The Impact of ISO 27001 Certification on Firm Performance. Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS), Kauai, Hawaii.

Hu, Q., Dinev, T., Hart, P., Cooke, D., 2012. Managing employee compliance with information security policies: the critical role of top management and organizational culture. Decis. Sci. 43 (4), 615–660.

IBM, 2016. 2016 Cost of Data Breach Study: Global Study (accessed 2017/05/12). https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN.

Ireland, J.C., Lennox, C.S., 2002. The large audit firm fee premium: a case of selectivity bias? J. Account. Audit. Finance 17 (1), 73–91.

Johnson, E., Khurana, I.K., Reynolds, J.K., 2002. Audit-firm tenure and the quality of financial reports. Contemp. Account. Res. 19 (4), 637–660.

Johnston, A., Hale, R., 2009. Improved security through information security governance. Commun. ACM 52 (1), 126–129.

Kannan, K., Rees, J., Sridhar, S., 2007. Market reactions to information security breach announcements: an empirical study. Int. J. Electr. Commer. 12 (1), 69–91.

Krishnan, G., 2003. Does Big 6 auditor industry expertise constrain earnings management? Account. Horizons 17, 1–16.

Krishnan, J., 1994. Auditor switching and conservatism. Account. Rev. 69 (1), 200–215.

Krishnan, J., Krishnan, J., 1997. Litigation risk and auditor resignations. Account. Rev. 72 (4), 539–560.

Kwon, J., Rees, J., Wang, T., 2013. The association between top management involvement and compensation and information security breaches. J. Info. Syst. 27 (1), 219–236.

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

Lewbel, A., 2012. Using heteroscedasticity to identify and estimate mismeasured and endogenous regressor models. J. Bus. Econ. Stat. 30 (1), 67–80.

Li, C., Peters, G.F., Richardson, V.J., Watson, M., 2012. The consequences of information technology weaknesses on management information systems: the case of Sarbanes Oxley Internal Control Reports. MIS Quarterly 36 (1), 179–204.

Li, D., 2010. Does auditor tenure affect accounting conservatism? Further evidence. J. Account. Publ. Policy 29 (3), 226–241.

Li, H., No, W.G., Boritz, E., 2017. Are external auditors concerned about cyber incidents? Evidence from audit fees. Working paper, Rutgers, the State University of New Jersey, and University of Waterloo. SSRN: < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2880928 > .

Lim, C.-Y., Tan, H.-T., 2010. Does auditor tenure improve audit quality? Moderating effects of industry specialization and fee dependence. Contemp. Account. Res. 27 (3), 923–957.

Messier, W.F., Eilifsen, A., Austen, L.A., 2004. Auditor detected misstatements and the effect of information technology. Int. J. Audit. 8 (3), 223–235.

Ming, K., Rosenbaum, P.R., 2000. Substantial gains in bias reduction from matching with a variable number of controls. Biometrics 56 (1), 118–124.

Myers, J.N., Myers, L.A., Omer, T.C., 2003. Exploring the term of the auditor-client relationship and the quality of earnings: a case for mandatory auditor rotation? Account. Rev. 78 (3), 779–799.

Neal, T.L., Riley Jr., R.R., 2004. Auditor industry specialist research design. AUDITING: J. Pract. Theory 23 (2), 169–177.

Nolan, R., McFarlan, F., 2005. Information technology & the boards of directors. Harvard Bus. Rev. 83 (10), 96–106.

O'Keefe, T.B., Simunic, D.A., Stein, M.T., 1994. The production of audit services: evidence from a major public accounting firm. J. Account. Res. 32 (2), 241–261.

Palmrose, Z.-V., 1986. Audit fees and auditor size: further evidence. J. Account. Res. 24 (1), 97–110.

Public Company Accounting Oversight Board (PCAOB), 2015. Emerging issues that could affect Audits, Auditors or the PCAOB (accessed 2017/05/12). https://pcaobus.org/News/Events/Documents/11-12-2015-SAG-Meeting/Emerging-Issues-SAG-meeting-Nov-2015.pdf.

PricewaterhouseCoopers, 2002. Mandatory Rotation of Audit Firms: Will It Improve Audit Quality? PricewaterhouseCoopers LLP, New York, NY.

Rosenbaum, P.R., Rubin, D.B., 1983. The central role of the propensity score in observational studies for causal effects. Biometrika 70 (1), 41–55.

Securities and Exchange Commission (SEC), 2011. CF disclosure guidance: Topic No. 2 Cybersecurity (accessed 2017/05/12). https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

Sen, R., Borle, S., 2015. Estimating the contextual risk of data breach: an empirical approach. J. of Mgmt. Info. Sys. 32 (2), 314–341.

Simon, D.T., Francis, J.R., 1988. The effects of auditor change on audit fees: tests of price cutting and price recovery. Account. Rev. 63 (2), 255–269.

Simsek, Z., 2007. CEO tenure and organizational performance: an intervening model. Strateg. Manage. J. 28 (6), 653–662.

Simunic, D.A., 1980. The pricing of audit services: theory and evidence. J. Account. Res. 18 (1), 161–190.

Simunic, D.A., Stein, M.T., 1996. Impact of litigation risk on audit pricing: a review of the economics and the evidence. AUDITING: J. Pract. Theory 15, 119.

Stanley, J.D., DeZoort, F.T., 2007. Audit firm tenure and financial restatements: an analysis of industry specialization and fee effects. J. Account. Publ. Policy 26, 131–159.

Sullivan, R.J., 2010. The changing nature of U.S. card payment fraud: Issues for industry and public policy. Workshop on the Economics of Information Security. Harvard University, Cambridge, MA.

Tucker, G., 2001. IT and the audit. J. Account. 192 (3), 41–43.

United States House of Representatives, 1985. Hearings before the subcommittee on oversight and investigations and the committee on energy and commerce. 99th Congress. First Session, February 20 and March 6.

Verizon, 2017. 2017 Data Breach Investigations Report (accessed 2017/05/12). http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_execsummary_en_xg.pdf.

Vermeer, T.E., Raghunandan, K., Forgione, D.A., 2009. Audit fees at U.S. non-profit organizations. AUDITING: J. Pract. Theory 28 (2), 289–303.

Wang, T., Hsu, C., 2010a. The composition of the top management team and the effectiveness of information security management. Americas Conference on Information Systems, Lima, Peru.

Wang, T., Hsu, C., 2010b. The impact of board structure on information security breaches. Pacific Asia Conference on Information Systems (PACIS), Taipei, Taiwan.

Wang, T., Hsu, C., 2013. Board composition and operational risk events of financial institutions. J. Bank. Finan. 37 (6), 2042–2051.

Wang, T., Kannan, K.N., Ulmer, J.R., 2013a. The association between the disclosure and the realization of information security risk factors. Inf. Syst. Res. 24 (2), 201–218.

Wang, T., Rees, J., Karthik, K., 2013b. The textual contents of media reports of information security breaches and profitable short-term investment opportunities. J. Organ. Comput. Electr. Commer. 23 (3), 200–223.

Wolk, C.M., Michelson, S.E., Wootton, C.W., 2001. Auditor concentration and market shares in the US: 1988–1999 a descriptive note. Br. Account. Rev. 33 (2), 157–174.

Wootton, C.W., Tonge, S.D., Wolk, C.M., 1994. Pre and post Big 8 mergers: comparison of auditor concentration. Account. Horizons 8 (3), 58–74.

Zajac, E.J., Westphal, J.D., 1996. Who shall succeed? How CEO/Board preferences and power affect the choice of new CEOs. Acad. Manage. J. 39 (1), 64–90.