Financial Statement Audits and Data Breaches

Lisa Yao Liu*

April 2023

Abstract: Financial statement audits for public companies require that auditors test the internal controls over the client's information systems that are material to the financial reporting process. Given the increasingly integrated nature of corporate data and control systems, a standard audit may therefore have a positive effect on firms' other information systems such as those that help prevent data breaches. In this paper, I provide evidence on whether and how auditors help prevent data breaches. I find that plausibly exogenous improvements in auditing reduce the likelihood of data breaches. I explore two mechanisms through which the effect occurs: auditors' provision of relevant information about financial data systems and increasing firms' ex ante incentives for internal controls. I find evidence consistent with both mechanisms. Collectively, this paper provides evidence that an improvement in accounting information systems can have a positive impact on non-accounting systems.

Keywords: Data breaches, auditing, internal control, digital automation, data technology.

JEL Classification: C81, C82, M15, M42, M48, O14

---

* Columbia Business School, Columbia University (yl4689@gsb.columbia.edu). This paper was previously titled "Do Auditors Help Prevent Data Breaches?." I greatly appreciate the guidance and support of my dissertation committee: Philip G. Berger, Hans Christensen (chair), Christian Leuz, Mark Maffett, and Mike Minnis. I thank Ionela Andreicovici, Ehsan Azarmsa, Thomas Bourveau, Matthias Breuer, Yiwei Dou, Raphael Duguay, Mihir Gandhi, Jon Glover, Luzi Hail, Katharina Hombach, Sudarshan Jayaraman, W. Robert Knechel, Kalin Kolev, Gemma Lee, Shirley Lu, Maximilian Muhn, Jordan Schoenfeld, Doug Skinner, Abbie Smith, Chad Syverson, Joanna Wu, Martin Wu, and participants at the 2019 AAA/Deloitte Foundation/J. Michael Cook Doctoral Consortium, the 2019 CMU Accounting Mini Conference emerging scholar session, the 2021 Global AI Finance Research Conference, the 2022 FARS Midyear Meeting, Columbia University, London Business School, London School of Economics, New York University, Northwestern University, NYCU International Finance Conference, Rochester University, Stanford University, the University of Chicago, the University of Pennsylvania, and the University of Toronto for helpful comments and suggestions. I thank Kamay Lafalaise (the attorney in the Office of the General Counsel from the Federal Trade Commission) for providing me with the FTC data information. I thank Martha Van Haitsma (the co-director of the University of Chicago Survey Lab) and Sona Margaryan (director of Strategic Initiatives at the University of Chicago) for their help with my survey design. I acknowledge research support from the Accounting Research Center at the University of Chicago Booth School of Business. I thank Daniel Chavez, Cagdas Okay, Georgios Tzortzis, Benjamin Levine, Chanho Moon, and Dhuv Baid for double-checking my data matching process. I gratefully acknowledge financial support from the University of Chicago Booth School of Business, the Deloitte Foundation, and the Bradley Fellowship awarded by the Stigler Center for the Study of the Economy and the State. This study was exempt from further review by the Institutional Review Board at the University of Chicago (IRB19-1066), under Federal Regulation (45 CFR 46.101(b)).

* I appreciate discussions with various industry professionals, including Mark Lavalle, audit partner at KPMG; Len Jui, board member of IAASB and partner at KPMG; Jodilia Vasanji, managing director at Deloitte & Touche LLP; Paulo Blanc, IT audit supervisor at ArcelorMittal; Rashesh Patel, principal examiner, IT risk and controls at FINRA; Vishal Dalal, consulting, internal audit, and SOX professional at Vonya Global; Rong Liu, IT audit, compliance, risk and internal control at Wolters Kluwer; Vincent Banks, CPA, CGMA, vice president internal audit at GreenSky®; Chris G Nicholson, FCA CPA, audit committee member; Dan Gaffney, MBA, CPA, CIA, CISA, internal audit and IT audit consultant; and many anonymous audit partners, internal auditors, external auditors, and legal counsels.

1. Introduction

Recent advancements in information technology (IT) allow companies to collect increasing amounts of data, leading to many business opportunities such as improving demand prediction and product design (e.g., Goldfarb and Tucker 2012; Farboodi et al. 2019). However, the big-data also raises concerns regarding data security and data breaches (e.g., Ashraf 2022; Schoenfeld 2022),[1] which can be costly for companies and harm other stakeholders (e.g., Duffie and Younger 2019; Liu and Strahilevitz 2022). In response to data security concerns, several regulators, including accounting regulators, are calling for increased scrutiny. For example, the SEC (2018) has required firms to implement internal accounting controls related to data breaches, and the PCAOB (2019) has encouraged auditors to devote more resources to defend against breaches. As most firms' financial statements derive from data stored in the cloud and other enterprise technology platforms, IT controls are within the scope of most financial statement audits.

In this paper, I provide evidence on whether and how external auditors can improve controls that prevent data breaches. As part of public audits, auditors are required to test the internal controls over the client's information systems that are material to the financial reporting process. While external auditors may not have a primary focus on preventing data breaches, their financial statement audits could still have spillover effects that help prevent such incidents, given that data systems are interconnected, and data centers usually store both financial and non-financial data.[2] As a result, standard financial statement audits may have a positive impact on firms' other information control systems, including those that prevent data breaches.

[1] Data breaches refer to external attacks, such as hacking and malware, and the internal mismanagement of sensitive information, such as improperly disposed of records, lost unencrypted laptops, and other accidental disclosures (Privacy Rights Clearinghouse 2017).

[2] In this paper, financial data are all information included in financial statements (e.g., revenue and payroll expense) and non-financial data are information not included in financial statements (e.g., consumer and employee personal information). For example, when financial data are breached, personal information (such as consumer names and addresses) is also compromised (Audit Analytics 2019).

Institutional insights from accounting firm partners and industry professionals interviewed suggest two mechanisms for auditors' roles in preventing data breaches: advice and monitoring.[3] First, external auditors can provide relevant and useful information for data protection by verifying financial data and detecting deficiencies in financial data systems. For example, as part of their auditing process, IT auditors test IT general controls, including examining whether there is unauthorized access to economic transaction data in order to prevent the manipulation of transactions. This information is also taken into account when assessing the risk of material misstatement (AICPA, SAS 108 - 110; Auditing Standards No. 5, No. 12 Appendix B; Li et al. 2012; Schroeder and Shepardson 2015).[4] Because data systems are interconnected and data centers usually hold both financial and non-financial data, this information could alert firms to potential weaknesses in their non-financial data systems. Second, external auditors can also increase the *incentives* for firms to adopt high-quality internal controls through *ex post monitoring*. These high-quality internal controls serve the entire organization, as they are applied to both financial and non-financial data protection.

To explore whether auditors help prevent data breaches, I start with descriptive evidence on the relation between the likelihood of data breaches and audit-quality measures (e.g., big auditors and the audit fee ratio). I find a negative association between the likelihood of data breaches and audit quality. While this preliminary evidence is consistent with my hypothesis, it is subject to endogeneity concerns because firms can choose their level of audit quality. For example,

[3] I conducted 36 interviews and created an anonymous survey for industry professionals to further obtain institutional insights and collect information on possible mechanisms. The interviewees include 11 accounting firm partners, five (non-partner) external auditors, nine internal auditors, one audit committee member, five corporate legal counsels/experts, and five regulators.

[4] IT auditors to assist the financial statement audit are a mandatory part of the auditing process. These auditors focus on IT application controls (which apply to business processing transactions like the processing of sales or cash receipts) and IT general controls (which apply to all aspects of the IT function, such as IT security, access controls, data backup, program changes, program development, change management, and computer operations). IT general controls need to be effective for auditors to rely on application controls.

large firms may have complex organizational structures and, hence, implement robust internal control systems, which may result in fewer data breaches. As these large firms are likely to engage big auditors, I could spuriously observe a negative association between big auditors and the likelihood of data breaches, even if audits do not reduce data breaches.

To alleviate endogeneity concerns, I use two more plausibly exogenous sources of variation in audit quality. The first source of variation is due to a regulatory change: the initiation of inspection fieldwork conducted by the Public Company Accounting Oversight Board (PCAOB). Prior research finds that PCAOB inspections improve the quality of internal control audits, facilitate auditors' learning, and improve audit quality (e.g., DeFond and Lennox 2017; Aobdia and Shroff 2017; Aobdia 2018; Gipper, Leuz, and Maffett 2019; Hanlon and Shroff 2022). Inspections assess the audit process (e.g., they test internal controls) (DeFond and Lennox 2017); one important aspect of these inspections is the assessment of auditors' tests of their clients' IT general controls (PCAOB 2010 and 2013).[5] The initial PCAOB inspections are staggered across different auditors over time. Using generalized difference-in-differences (DiD) analysis, I find that the clients of auditors that are inspected by the PCAOB are less likely to have data breaches as compared to the clients of other auditors that have not been inspected yet.

The second source of variation is auditors' learning from other clients regarding internal control testing or data breach information. If an auditor's client experiences a breach incident, the auditor could help transmit relevant information to raise awareness among other clients regarding the potential risks of data breaches. Asthana et al. (2021) find that data breaches can result in an

[5] PCAOB specifically requires that auditors have an "understanding of how the organization is dependent on or enabled by information technologies; and the manner in which information systems are used to record and maintain financial information" (PCAOB, QC Section 40, 2003). PCAOB (2013) Stuff Audit Practice Alert No. 11 lists information technology (IT) considerations (such as system-generated data and reports) as a significant, frequent auditing deficiency cited in PCAOB inspection reports.

auditor's reputation loss. As a result, auditors may enhance their auditing practices for their other clients and even invest in human capital related to breaches (Li et al. 2022). Different auditors will experience this "learning" at different times, creating staggered variation.[6] I examine the likelihood of future data breaches among the learning auditor's other clients and find a lower likelihood of data breaches among these other clients.

To further corroborate the impact of auditing on data breaches, I examine cross-sectional differences in the extent of integrated systems, audit and risk-technology committees, and internal control weaknesses. I expect that: (1) in more integrated data systems, information spillover from financial data systems to other systems is more likely; (2) firms' ex ante incentive for strengthening internal controls is stronger when auditors' ex post monitoring is likely more useful, which is proxied by firms with more audit and risk-technology committee members on the board and firms with strong internal control systems. Consistent with my expectations, I find that the reduction in the likelihood of data breaches is larger in firms with more integrated systems, a greater percentage of audit committee members on the board, and firms with stronger internal controls.

This paper makes several contributions. First, it adds to the literature on the effect of auditing services. Survey papers of the audit literature call for more research on the effects of audits and auditors' expertise beyond financial statement assurance (e.g., DeFond and Zhang, 2014). These questions have been hard to address due to the lack of data and the opaque nature of the auditing setting. To the best of my knowledge, I provide the first attempt at investigating whether financial statement audits affect firms' IT systems and data security. My paper shows that

[6] One potential concern is that an auditor's other clients could also learn about data breaches through local geographical network effects, instead of auditors' cross-client information transmission (e.g., Ashraf 2022). If it were the case, this client learning would also occur in the control group, and having the control group in the generalized DiD can help account for such client learning. To further mitigate this concern, I define an alternative treatment group as auditors' other clients in different states so that the learning is only through auditors instead of clients' learning. I continue to find robust results. I also find that auditors' learning takes (at least) two years to materialize (untabulated).

auditors add value beyond financial statement assurance (e.g., Minnis 2010; Shroff 2017).

Second, my paper adds to the literature on the benefit of improving internal controls. The literature studies how the improvement in internal controls can benefit internal managerial decisions, leading to more accurate management forecasts (Feng et al. 2009), increased investment efficiency (Cheng et al. 2013), and effective inventory management (Feng et al. 2015). I contribute to the literature by providing evidence on the role of the auditing process in disciplining control systems that can help prevent data breaches and by estimating the magnitude of this effect. Data breach risk is captured as part of the ESG rating (in the Social component – Customer Welfare, Product Safety, and Data Security (FitchRatings 2021)). With the rise of big data, a new type of agency friction between firms and *data providers* (e.g., consumers and employees) has emerged. That is, firms may commit to a robust data usage policy[7] ex ante when consumers and employees provide their personal data, but it may be difficult for firms to enforce the policy ex post (Jin 2018; Schoenfeld 2022). My findings show that the verification process can help reduce this new type of agency friction.

Finally, this paper relates to the burgeoning literature on data breaches, which focuses mainly on the consequences of breaches. Regarding the relation between data breaches and auditing, previous papers (e.g., Hoffman et al. 2018; Li et al. 2020; Rosati et al. 2022) mainly study auditors' *ex post* responses to breaches (e.g., increasing audit fees), which suggests that auditors do care about data breaches. Schoenfeld (2022) studies the benefits and costs of the SOC (system and organization controls) audit in evaluating cybersecurity risk. Li et al. (2022) shows that auditors respond to cybersecurity risks by investing more heavily in cybersecurity human capital. My paper complements the literature by exploring auditors' *ex ante* role in preventing breaches.

[7] A robust data usage policy includes collecting, using, maintaining, protecting, and disclosing personal data.

2. Institutional background and conceptual development

In this section, I discuss how auditors' assurance can contribute to data protection. I outline the direct role of external auditors in financial data security, delineate two potential channels through which external auditors could help prevent data breaches, and present conditions under which heterogeneous effects occur.

2.1 The Role of Auditing in Financial Data Security

With many manual processes and documentation moving to the digital world, more financial numbers are automated by information systems, and much audit evidence is becoming computer-based (e.g., Efendi et al. 2006; Alves 2010; Brands and Smith 2016). Thus, auditors must understand and test these data controls before concluding that automated information is reliable.[8] Auditors have long been concerned with physical assets (e.g., inventory); faced with ever-growing digital technology, they now also need to care about intangible and digital assets (e.g., customer lists).

Auditing standard AS5 states that "the identification of risks and controls within IT is not a separate evaluation. Instead, it is *an integral part* [emphasis added] of the top-down approach" in an integrated audit, which combines a financial statement audit with an audit of internal controls. IT auditors assist financial statement auditors with verifying financial statement values. They focus on IT general controls and IT application controls. IT general controls relate to the overall integrity

[8] See https://www.cpapracticeadvisor.com/home/article/10263076/the-evolution-of-technology-for-the-accounting-profession. Information systems consist of the methods and records used to record, process, summarize, and report a company's transactions and to maintain accountability for the related accounts. In 1984, AICPA issued SAS No. 48 (*The Effects of Computer Processing on the Examination of Financial Statements*), because IT could impact the nature, timing, and extent of audit procedures (Yang and Guan 2004; Hoffman et al. 2018). See also Appendix 5 for concrete procedures for auditing IT controls. I provide additional institutional information and empirical evidence in Appendix 3 to demonstrate that auditors have the relevant skills to test data protection controls. If a client's IT systems are too complex and specialized, IT specialists are invited to assist in the auditing process (e.g., Bauer and Estep 2019). Overall, auditors must understand the design of the internal controls and must examine their strength in a financial statement audit.

of the system and apply to all aspects of IT functions, such as file security, access controls, data/program access changes, new system developments, current system changes, and computer operations. IT application controls apply to processing transactions, like sales or cash receipts, and test the performance of individual computer applications, such as accepting authorized input, correct processing, and generating the appropriate output.[9] IT general controls need to be effective so that auditors can rely on the IT application controls. Auditors then design and implement the scope of substantive test procedures based on the results of the internal control tests. If the system does not operate effectively, the need for substantive procedures will increase to reduce the detection risk.

When assessing the risk of material misstatement in financial statements, auditors are required to consider a company's IT systems and controls, including the IT risks stemming from unauthorized access (e.g., Auditing Standards No. 12 Appendix B; Center for Audit Quality 2016, 2017; Li et al. 2012; Schroeder and Shepardson 2015). The rationale is that if a firm's data access control is not robust, transactions are vulnerable to manipulation, and the reliability of the financial statements can be compromised. Data controls that aim to make numbers accurate and reliable can also help make the numbers secure.[10] This means that auditors are concerned not only with the final financial numbers but also with their generation and the data that underlie them.

2.2 How External Auditors Help with Non-Financial Data Protections

As the interview evidence in the paper indicates, information technology (IT) controls are well within the scope of most financial statement audits because many firms' financial statements

[9] Transaction processing entails the immediate processing of transactions and batch processing (e.g., periodically gathering information as a group from the computer). Access controls include those designed to protect the information from unauthorized access. Auditors could specifically test passwords and firewalls to prevent outside threats.

[10] Small firms (e.g., non-accelerated filers) have less stringent internal control testing by auditors (SOX 404b), but their scope for improvement is larger.

derive from data stored in the cloud and on other enterprise technology platforms. The anecdotes from interviews with industry professionals suggest that external auditors can help firms with general data protection in (at least) two ways: by providing relevant information about financial data systems and ex ante incentives for high-quality internal controls. The information spillover channel can work through the intertwined relation in firms' data systems and through interactions with firms' audit committees and with internal auditors.

Through the interconnectedness of firms' data systems, risks and deficiencies identified by external auditors in the financial data system may spill over to non-financial systems. Specifically, by conducting audits of financial control systems, auditors can provide relevant and useful information that alerts clients to possible weaknesses in the IT infrastructure, thus uncovering potential vulnerabilities in non-financial controls. In addition, auditors may not assess IT general controls in isolation but in combination with other data control systems, especially if those controls affect related accounts (PCAOB 2013). For example, in the analytical procedure, when auditors verify payroll expenses, they also test the HR systems to confirm the number of employees and their salaries. Even if companies outsource data services, external auditors will examine their clients' physical security and request an SOC report from the vendor, which helps ensure that vendors have data protection controls and that these controls map onto clients' control systems. Schoenfeld (2022) provides descriptive evidence on SOC audits in the era of big data.

The external auditor's engagement with the audit committee and internal auditors serves as a communication channel facilitating the relevant information transmission from financial to non-financial data systems. The Sarbanes-Oxley Act requires that audit committees oversee compliance, risk management, and internal controls for companies' financial reporting. Two salient examples are the reactions of proxy advisors ISS and Glass Lewis to the Target breaches

and to Facebook's use of data, respectively. At the annual shareholder meeting in 2014, ISS vetoed the election of all Target audit committee members because they failed to fulfill the responsibility of risk assessment. Glass Lewis and other institutional investors argued that Facebook's audit committee neglected to oversee the risk and compliance related to Facebook users' data. Several communication channels exist between audit committees and external auditors. An audit committee engages with the auditor throughout the entire audit—during planning, at interim reporting periods, and at year-end. Additionally, audit procedures should adapt to each company's unique IT environment and an auditor would discuss these changes with the audit committee and with management. Specifically, Auditing Standard No. 5 requires that auditors evaluate the severity of a control deficiency and communicate these deficiencies to the audit committee and to management in an integrated audit (Auditing Standards No. 13).

External auditors also interact with internal auditors, who monitor firms' quality and control systems. Specifically, internal auditors examine how firms operate and evaluate firms' internal controls; these controls include the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance with laws and regulations. External and internal auditors compare testing results and share information. When external auditors raise any concerns about weaknesses in firms' internal control over financial reporting, internal auditors could look for similar issues in other systems. Thus, the information channel can be operationalized through the interconnectedness of firms' data systems as well as through the interactions with firms' audit committees and with internal auditors.

The second channel through which auditors can help prevent data breaches is to strengthen firms' ex ante incentives for internal controls. Auditors could provide *ex ante incentives* for firms to adopt high-quality internal control systems and procedures through *ex post monitoring.* For

example, auditors could detect deficiencies in internal controls, assess the design of internal controls, and disclose the quality of internal controls to external parties. In turn, this *ex post monitoring* could raise awareness and foster better practices in data protection for the company overall. A firm's overall information and data-protection systems can be strengthened with high-quality internal controls in place (e.g., Hogan and Wilkins 2008; Feng et al. 2009; Feng et al. 2015; Altamuro and Beatty 2010; Barrios, Lisowsky, and Minnis 2019).

3. Data

My information on data breaches comes from the Privacy Rights Clearinghouse (PRC). The data are available from 2005 and include data breaches and the number of compromised records (as reported by government agencies or verifiable media sources).[11] Kamiya et al. (2021) select a random sample and verify PRC's data to double-check its accuracy. However, potential concerns, such as materiality thresholds for breach disclosures (e.g., Amir et al. 2018), may still exist and lead to the over- or under-estimation of treatment effects. For example, if breaches are immaterial in the later period without disclosure, I may overestimate the treatment effect. Although breaches are defined annually in the paper, if a breach is not detected within a year and more data breaches are detected over time, this would bias against my finding the treatment effect. Therefore, I perform several cross-checks to alleviate these concerns. First, the data are collected by a third-party nonprofit organization that is incentivized to search for and report data breaches to encourage public scrutiny and action. Second, I use a simple descriptive assessment to ensure that the smallest

[11] http://www.privacyrights.org/data-breach. See https://www.privacyrights.org/data-breach-FAQ for detailed data information. One federal government source is the Department of Health and Human Services Office for Civil Rights (https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf), which provides the most well-structured and up-to-date information available (Privacy Rights Clearinghouse 2019). I repeat the main analyses in the table while incorporating the Audit Analytics Data and find similar results (Amir et al. 2018; Haislip et al. 2019). Although Audit Analytics data are well-organized and do not require manual collection and checking, I choose not to use it as the main data source for two reasons: (1) Audit Analytics data start from 2011, which limits my identification strategies and variations. (2) Audit Analytics data include only cyberattacks, while the PRC dataset also includes non-cyberattack breaches, which closely relate to firms' internal controls.

firm sizes for breached and unbreached companies are similar. When I implement this restriction, only around 1.4% of observations are dropped, and the results have stronger statistical power. Third, I match firms on variables correlated with data breaches and find that my results still hold (untabulated). Finally, my descriptive results are robust to the FTC datasets (which I accessed by invoking the Freedom of Information Act (FOIA)). These datasets are comprised of customers' self-reports to the FTC about identity theft. It is difficult for companies to hide these cases: they are reported by data providers, who have incentives to report to the FTC promptly.[12]

Data breaches include hacking or malware by outsiders (as Figure 1 shows, this accounts for 25% of data breaches) and data mishandling by insiders (e.g., data digitally sent to the wrong party; intentional breach of information by someone with legitimate access; payment card fraud; physical loss of paper documents or a portable device; stationary computers lost, inappropriately accessed, discarded, or stolen). If a firm's information system is vulnerable to outsiders, it is also vulnerable to insiders. Thus both types of data breaches relate to the vulnerability of firms' information systems and internal controls.[13]

The PRC dataset is my primary data source. I manually match the data from PRC with public companies to get 1,214 observations with 524 unique firms. The simple descriptive statistics in Table 1 show that breached companies are relatively larger, are less likely to experience a loss,

[12] The observed data breaches are the joint probability of data breaches occurring and being detected, which is equal to the unconditional probability of a data breach occurring multiplied by the probability of detection, conditional on an occurrence. Therefore I examine a case when breaches are certain to be detected (i.e., the probability of being detected, conditional on an occurrence, is equal to one) to empirically assess concerns about detection and reporting biases.

[13] For example, as discussed by SQN Banking Systems in "Manipulated Data: The New Bank Hack," "[A]ccess control…helps to prevent and reduce *internal data manipulation*, it also reduces the number of avenues through which *hackers can gain entry to manipulate the data*." (See https://sqnbankingsystems.com/blog/manipulated-data-new-bank-hack/.) In the subsequent empirical analyses on the effect of auditing on the likelihood of data breaches, I split the sample into hacking and nonhacking cases. While I find a slightly larger reduction for nonhacking cases, its higher power (due to its larger sample size) may confound the interpretation that auditors play a bigger role in reducing nonhacking breaches.

and have higher asset intangibility (proportion of assets that are not PP&E) than the other companies.

My firm-level financial data are from Compustat. I collect data for all U.S. firms that are listed on the NYSE, Amex, and Nasdaq. Using firm names, I manually match firms in the PRC dataset to public firm databases (e.g., Compustat, CRSP, and SEC filings). I also use a variety of other platforms (e.g., Bloomberg) to ensure that organizations are listed during the sample period.[14] My auditor data are from Audit Analytics from 2004 to 2016. For each firm-year observation, I collect the firm's auditor, audit office, and audit fees. Audit-related fees are important because they include the information technology security review fees. For example, in the contract between EY and Equifax, "EY charged $4.3 million of that total for audit-related services including service auditor examinations, or SOC reports, provided to banks and other financial firm customers to prove First Data's controls over data security, availability, processing integrity, confidentiality, and privacy meet legal and regulatory requirements." I then merge financial data from the Compustat Annual file. I use SEC 10-K filings to extract firms' business addresses, accelerator status, and public float information. I use BoardEx data to compute the percentage of different committee members on a firm's board of directors. All continuous variables are trimmed at the 1% level.

4. The Effect of Auditing on Non-Financial Information Control Systems

4.1 Descriptive Evidence

I first estimate a regression model to examine potential firm characteristics that are related to data breaches. The goal of this analysis is two-fold. First, it provides descriptive evidence on

[14] I also check to see whether an organization's parent company is publicly listed. I compare the matching rate with that of prior literature and find similar matching rates for online hacks. Specifically, Kamiya et al. (2021) find 307 online attacks and 224 unique public firms. I find 304 online hacks and 211 unique public firms. In total, I find 1,214 data breaches and 524 unique firms.

whether auditing-related variables are associated with the likelihood of data breaches. Second, it helps determine what control variables should be included in the subsequent analyses. I estimate the following model at a firm-year level (suppressing time and firm subscripts):

$$Breach = \sum \beta_i Determinants_i + \sum \alpha Fixed\ Effects + \epsilon \quad (1)$$

Breach is an indicator variable equal to one if a firm experiences data breaches in a given year, and zero otherwise. I include auditing-related variables to assess whether the likelihood of data breaches is associated with firms' auditing-related resources. Auditing-related variables include the percentage of audit committee members (measured as the number of audit committee members divided by the total number of board members), internal control weakness, big auditors, and audit fee ratio (defined as audit fees divided by the sum of audit fees and non-audit fees, following Rajgopal et al. 2021). I also include firm performance (measured as a loss indicator), size (measured as the natural log of total assets), and asset intangibility (measured as the proportion of assets that are not PP&E) following prior literature (e.g., Kamiya et al. 2021).

Big firms may have the resources to establish strong internal control systems, thereby reducing the likelihood of data breaches. However, big firms are also more visible and are therefore more likely to be targeted by hackers. Their organizational structures are also so complex that insider disclosure and the physical loss of information are both more likely to occur, making it exponentially more costly to defend against data breaches. Thus, the effect of firm size on data breaches is unclear. Poor-performance firms may lack the necessary resources to strengthen internal controls, making them vulnerable to data breaches. The predictions for firm asset intangibility are also unclear. Because intangible assets are important, firms are likely to be aware of best practices for data protection and have many effective defense mechanisms in place. Additionally, external auditors may focus specifically on intangible assets. On the other hand,

firms with high asset intangibility will likely have more data (e.g., customer and employee information) and are thus more likely to have data breaches (e.g., Kamiya et al. 2021). While these observable characteristics may be related to other important determinants (e.g., size is likely to be correlated with the number of employees and asset intangibility may associate with customer list and information), I acknowledge that other important yet unobservable determinants could play a role but are not included in the determinant table. Data breaches are correlated with industry characteristics (as shown in Figure A1), so I include industry fixed effects to control for static industry differences in Column (1) of Table 2. In addition to industry fixed effects, in Column (2) of Table 2, I include year fixed effects to account for general trends in data protection technologies. I cluster standard errors by industry (two-digit) to account for cross-sectional correlation within industries.

I report descriptive statistics in Table 1. Breaches are not frequent events: around 1.2% of firm-year observations have data breaches. Specifically, around 77% of unique sample firms have no data breaches, 8% have one over the sample period, and 15% have more than one data breach (in an untabulated check). On average, around 74% of observations have big auditors, and around 29.5% of firms' net income is negative. In Table 2, I report the results of estimating Model (1), and find that the likelihood of data breaches is positively related to bad performance (e.g., a loss indicator), asset intangibility (i.e., the portion of assets coming from items other than PP&E), and visibility (e.g., size), and that data breaches are negatively associated with audit-related variables (e.g., the percentage of audit committee members, internal control strength, big auditors, and audit fee ratios) across two specifications (Column 1 has year fixed effects and Column 2 has year as well as industry fixed effects). These are all statistically significant determinants of data breaches at (at least) the 5% level, except for the indicator of risk/technology committees, which are

insignificant in both columns, and for the audit fee ratio variable, which is statistically significant at the 10% level in Column (1) but significant at the 5% level in Column (2). The evidence in this table suggests that firm characteristics and auditing resources are related to data breaches.

Table 3 presents descriptive results related to audit quality. To further explore the negative coefficient on Big Auditors, I examine firms' likelihood of data breaches in two cases: (1) when firms switch from big to non-big auditors and (2) when they switch from non-big to big auditors (defined as the Big Four). Big auditors proxy for higher audit quality and stronger auditor incentives stemming from reputation and litigation concerns (e.g., DeFond and Zhang 2014). Thus, we should expect a positive and significant relation with the likelihood of data breaches when firms switch from big to non-big auditors (shown in Column (2) of Table 3); conversely, we would see a negative and significant association with the likelihood of data breaches when firms switch from non-big to big auditors (shown in Column (1) of Table 3).

Based on the results in my determinant table, I use the following control variables (in this and the subsequent tables), non-auditing related but associated with the likelihood of data breaches, in order to gauge the importance of firm characteristics in explaining the variation in auditing services I exploit: firm size (measured as the natural log of total assets), firm performance (measured as a loss indicator), and asset intangibility (measured as the portion of assets coming from items other than PP&E). Because the variations I explore in the following tables are related to auditing services, including auditing-related variables would incur "bad control problems" to the extent that firms' auditing-related resources vary with the shocks I exploit (Angrist and Pischke 2009). For firm control variables, in Table 3, I find that size, bad performance, and asset intangibility are positively and statistically correlated with the likelihood of data breaches, which is consistent with the determinant table.

Although the analyses above provide consistent descriptive evidence on the association between auditing and the likelihood of data breaches, these correlations may be subject to endogeneity concerns. For instance, if firms switch from a big to non-big auditor because of financial constraints, it is likely that this constraint also affects firms' data protection technologies. Thus, in the next section, I exploit plausibly exogenous shocks in order to provide more compelling evidence.

4.2 The Effect of Auditing on Reducing the Likelihood of Data Breaches

To explore the effect of auditing on the likelihood of data breaches, I exploit two shocks to the supply of audit services that (I argue) do not affect the demand for audit services. These shocks are not perfect and are subject to limitations (which I discuss below), but they complement each other. My baseline regression, suppressing time and firm subscripts, is

$$Breach = \alpha_1 Shocks + \sum \alpha_i Fixed\ Effects + \gamma_i Controls_i + \epsilon \qquad (2)$$

Breach is an indicator variable equal to one if a firm experiences data breaches in a given year, and zero otherwise. *Shocks*, the variable of interest, is an indicator coded as one for the different shocks I describe below.[15] I include year fixed effects to control for changes in the data technology and policies over time. I include firm×auditor fixed effects to control for differences in data protection, audit services, and other time-invariant factors among firms and auditors in order to isolate the variation in the firm-auditor relationship over time, excluding the variation of changing auditors.[16] This specification mitigates the concern that firms concerned about data breaches

[15] I choose to run a linear probability model (LPM) for two reasons: (1) estimating a stringent fixed effects model for non-linear regressions (e.g., logit or probit) can be problematic due to the incidental parameter problems, but it is less of a concern for LPM. (2) I am interested in marginal effects, which are robust for LPM (Angrist and Pischke 2009; Wooldridge 2010).

[16] Across different shocks, my results are robust to the following fixed effect structures: (1) year, firm, and auditor fixed effects; (2) industry×year fixed effects that control for time-varying industry conditions; (3) state×year fixed effects that control for time-varying changes in economic conditions within a state (except for the shock of auditors learning from data breaches: the magnitude more than doubles (-0.018) but the statistical significance is smaller (t-

change to "better" auditors. Because these shocks are on the auditor side, I explore, within the firm-auditor relationship, how the shocks affect their clients' likelihood of data breaches. I cluster standard errors by auditor to account for cross-sectional correlation in firms with the same auditor. One concern with this level of clustering is that some clusters may be unbalanced due to differences in auditors' client portfolios (Conley et al. 2018). To mitigate this concern, I verify that my results are robust to clustering by firm, state, industry, or year.

The first shock is the PCAOB's first-time inspection fieldwork (e.g., DeFond and Lennox 2017; Aobdia and Shroff 2017; Gipper, Leuz, and Maffett 2019; Hanlon and Shroffs 2022; Krishnan, Krishnan, and Song 2014; Lamoreaux 2016). A PCAOB inspection provides public oversight of auditing and strengthens auditor attestation of firms' internal control systems (e.g., Gipper, Leuz, and Maffett 2019). Gipper, Leuz, and Maffett (2019) argue that the new regime leads to improvements in auditing because of larger penalties, stricter enforcement, and audit deficiencies identified by the PCAOB. An important aspect is assessing auditors' tests of their clients' IT general controls (PCAOB 2010 and 2013). DeFond and Lennox (2017) find that the PCAOB inspections improve the quality of internal control audits and that auditors conduct more rigorous tests and evaluations of clients' internal control weaknesses after these inspections.

The PCAOB first-time inspections, staggered across different auditors at different times, provide variation on the auditor supply side.[17] Using the variation in the audit quality of inspected

stats: -1.18)); (4) state×industry×year fixed effects that account for time-varying changes in states and industries in order to isolate the variation of treated auditors (in the shock of auditors learning from data breaches, the magnitude almost triples (-0.022) though the statistical power is lower (t-stats: -1.15)).

[17] One concern about the PCAOB test is endogenous timing. To institutionally verify that the PCAOB does not explicitly consider data breaches when selecting auditors, I spoke with several PCAOB regulators. However, it might be possible that the selection criteria could perfectly predict the risk of data breaches. To mitigate this concern, in addition to including firm×auditor fixed effects (and robust to industry×year fixed effects), I include firm control variables that are highly correlated with the likelihood of data breaches in order to gauge how the change in these controls affects the variable of interest; my results remain robust in this specification. This paper uses the first inspection as the beginning of the treated period. Continuing inspections should further increase audit quality (if the elasticity of improvement is not zero), strengthening my results.

auditors, I examine whether those auditors' clients are less likely to have data breaches. Specifically, I exploit the variation that the PCAOB completes the first-time inspection at different timing for different auditors, which allows me to use firms whose auditors have not yet been inspected by the PCAOB as the control group. The treatment group is comprised of the clients of auditors inspected for the first time. *PCAOB First-Time Inspection*, the variable of interest, is an indicator coded as one after PCAOB first-time inspection for firms audited by an inspected auditor, zero otherwise. Thus, I identify the effects based solely on differences in the timing of the inspections. The staggered introduction mitigates concerns about concurrent economic and regulatory changes.

Table 4 shows that firms audited by higher quality auditors (proxied by being inspected by the PCAOB) are 0.4 percentage points less likely to have data breaches (Column 1 of Table 4); this result is statistically significant at the 10% level. The magnitude of the coefficient translates into about a 20% reduction in the likelihood of data breaches (relative to the mean value). Results remain stable after including control variables (Column 2 of Table 4); firm×auditor fixed effects absorb much of the variation in adjusted R-squared so I examine and find that the within R-squared (excluding fixed effects) doubles (untabulated), which both suggest that (to the extent that the observable characteristics are representative of unobservables) an omitted variable bias is less of a concern (Altonji, Elder, and Taber 2005; Oster 2019). For the control variables, as in the determinant table, size, poor performance, and asset intangibility are positively and statistically correlated with the likelihood of data breaches.

There are some important limitations for the test of *PCAOB First-Time Inspection*. Because my breaches data start in 2005, I cannot fully use the PCAOB-inspection regime change. The variation is on the intensive margin, i.e., differences in the timing of the inspections, mainly from

small auditors. There are several advantages to analyzing small auditors. For example, it shows that the effect holds for a broad spectrum of audit quality (not just for big auditors); because the clients of small auditors are less likely to be targeted by hackers, their data breaches likely stem from the vulnerability in firms' information systems as opposed to targeted hacking. Lastly, small auditors (inspected later) may be less sophisticated than big auditors, which means that they may learn and improve more as a result of PCAOB inspections; prior literature does find that the inspections improve audit quality for small auditors (e.g., DeFond and Zhang 2014). While small auditors are a sensible analysis group, they could be a low power test. Two other potential concerns are that 1) that the number of treated firms is not balanced over years and 2) the sample size of firms and auditors in later years is small. To assess how these concerns affect my results, I analyze firms with small (non-Big Four) auditors with matched size, performance, and asset intangibility (untabulated), and find the economic magnitude remains stable.

To mitigate limitations in the test of *PCAOB First-Time Inspection*, I exploit a second shock on the quality of auditing services: auditors learning from their prior experiences (in the spirit of Murfin 2012). If an auditor's client has a data breach, the auditor may gain information and use it to inform other clients of potential vulnerabilities in their data control systems. Prior research shows that audit fees increase after data breaches, suggesting auditors are aware of these breaches (e.g., Haislip et al. 2019; Li et al. 2020). Li et al. (2022) demonstrates that increase investment in cybersecurity human resources after one client experiences data breaches.

I examine the likelihood of future data breaches among the learning auditor's other clients. The control group is firms whose auditors have not yet been treated, and the treatment group is *other* clients of an auditor who learns from incidents. That is, the treatment group does not include the firms that induce auditors' learning. *Auditors Learning From Data Breaches*, the variable of

interest, is an indicator coded as one after auditors learn from data breaches with their other clients, zero otherwise.

The specification of auditors' cross-client learning can help mitigate several empirical concerns. For instance, a client experienced data breaches may subsequently strengthen its data security controls, making it difficult to differentiate between auditors' learning and client self-learning. I therefore investigate the future incidence of data breaches among auditors' *other* clients. Furthermore, because the incidence of data breaches directly relates to the outcome variable, one concern is that other clients in the same state could be treated from information spillover or network effects (Ashraf 2022), instead of just through the same auditor.[18] If it were the case, this client learning would also occur in the control group, and having the control group in the generalized DiD can help account for such client learning.

To further mitigate these concerns, I examine the change in the likelihood of data breaches for auditors' *other clients in other geographic areas* (i.e., other states), excluding other clients in the same state as the breached firms. In Table 5, Columns (1) and (2) (other clients [OC] in other geographic areas [OGA] with the same auditor) show that other clients of auditors with a data breach are 0.7 percentage points less likely to have data breaches. For ease of interpretation, I translate this number into around a 40% reduction in the likelihood of data breaches (relative to the mean value) in order to interpret the economic magnitude. Because other clients in a same state could be treated (by the same auditor and/or by the breached company due to network effects), I examine whether the effect is larger if we include other clients (of the same auditor) in the same state. In Column (3), I test and find that the effect is larger (the magnitude more than doubles) after

[18] However, auditors could have a greater information advantage (DeFond and Zhang 2014) than peers in the same geographic area because of firms' vague disclosure (Kopp et al. 2017; Kashyap and Wetherilt, 2019).

including other clients in the same geographic area. Thus, the effect varies predictably.[19] When adding controls, the within R-squared doubles (untabulated) but the coefficient remains stable in Column 2, suggesting an omitted variable is less of a concern (Oster 2019). For the control variables, as in the determinant table, size, poor performance, and asset intangibility are positively and statistically correlated with the likelihood of data breaches. I also find that auditors' learning takes (at least) two years to materialize (untabulated).

There are some important assumptions and limitations in the auditor learning test. First, it takes time for learning to materialize. Second, there is an underlying assumption that learning does not depreciate. For *auditors learning from data breaches*, while I define the treatment as auditors' other clients in other states to tighten the identification strategy, confounding shocks (e.g., time-varying economic conditions within states) might still affect my results.[20]

I use different shocks to provide robust and consistent results that alleviate the endogeneity concerns. These shocks mitigate the endogeneity problem to the extent that they are not endogenously driven by firm-specific conditions. One concern is that differential trends in firm characteristics during this period may relate to the likelihood of data breaches, even in the absence

[19] The difference between Column 2 and Column 3 is short of conventional levels of significance (p-value 0.149). There are two ways to interpret the increased economic magnitude in Column 3: First, other clients in the same geographic area could learn from breached firms; second, auditors' learning could be diffused more effectively when learning is local. To further exclude the possibility that industry risks are correlated with the estimates, I define the treatment as firms in distinct states and different industries (at SIC 1–digit, 2-digit, and 3-digit levels) and repeat the same analyses (untabulated). I find that results are similar but with slightly larger magnitudes.

[20] To assess the validity of the parallel-trends assumption, in untabulated tests, I check and find that treated and non-treated firms have similar patterns in the likelihood of data breaches before the shocks but that treated firms are less likely to experience the breaches afterward. One exception is the shock of PCAOB inspection, in which the treatment effect starts one period before the inspection ("t-1"). This downward trend indicates that some companies may already have data risks and thus the incentives to strengthen their internal controls when facing the improved audit quality stemming from the PCAOB inspections. I also examine how internal control weakness (ICW) changes with the shocks I exploit. Although conceptually sensible, the empirical proxies used to measure ICW may not be precise, as prior research has shown that firms may not always acknowledge their control weaknesses during misstatement periods (e.g., Rice and Weber 2011). Empirically, I do not find significant changes in the shocks of *PCAOB first-time inspections*, but find more ICW reports after *auditors' learning from data breaches*. That is, companies are more likely to report ICW after their auditors learn from data breaches, reinforcing the notion that data breaches are a form of internal control failure.

of auditor shocks. Although my identification allows for different firm characteristics within the same auditor, the key to my identification is exploring the shock on the supply side while holding the demand side fixed. To the degree that pre-determined underlying differences do not vary with the shocks I exploit (i.e., the shock does not affect both the supply and the demand side of audit service), it cannot explain my results.

4.4 Mechanism Testing for the Effect of Auditing on Mitigating Data Breaches

Documenting precise mechanisms is challenging, and requires detailed within-firm data. To overcome these data challenges, I collect information on mechanisms through interviews as well as surveys and test for these proposed mechanisms empirically.

4.4.1 Interview and Survey Evidence

To obtain institutional insights and collect information on mechanisms for auditors' role in data protection, I conduct one-on-one interviews with 36 industry professionals. I conduct 19 interviews by phone, 14 interviews in person, and three interviews over online messages; interviewees include 11 accounting firm partners, five (non-partners) external auditors, nine internal auditors, one audit committee member, five corporate legal counsels/experts, and five regulators. For in person and phone interviews, the average length was around 42 minutes.

More than 90% of interviewees care about data breaches for several different reasons. One reason is that data breaches are related to failures in internal controls and could be an indication for bigger problems. For example, when data breaches happen, auditors need to understand the root cause in order to assess whether clients have adequate controls in place. They would also examine whether the data breach is isolated or whether it is an indication of systemic problem in a firm's control environment, something which could incur financial consequences. They would check clients' IT control environment and discuss with the IT department more generally. For

instance, one audit partner said that IT directors participated in audit committee meetings. Another reason is public perception, which is indirectly related to auditors' reputational risks. Although auditing standards do not specifically prescribe auditors' role in detecting and preventing data breaches, the public holds a (somewhat) strong belief in this role for auditors. This perception could indirectly affect auditors' behavior. The last reason is that auditors care about business risk and entity-level controls and data breaches may impact firms' business risks. Securing assets, virtual and physical, is important and data are a significant client asset.

Two channels are summarized from the ample anecdotes provided by interviewees: information spillover and internal controls, which are discussed briefly in the paper. For information spillover, auditors can inform firms of relevant and useful information related to data protection. For example, audit partners said that auditors could raise awareness, provide relevant information about systems, and could nudge managers about relevant knowledge and practice. Even though auditors only test some controls, the issues raised could spread due to correlations between different controls and data systems. External and internal auditors could also share their findings about firms' control environment with each other. For instance, external auditors use internal auditors' work and share information with them.

Another important channel is internal controls. For example, IT auditors' tests on IT general controls would include system and process controls, including logical access controls, change controls, change management controls, computer operations, data transfer, and system and process controls. One auditing partner stated that companies build not just financial data but also the whole environment, including controls over data access, data migration, and system change. When companies implement internal controls, it is hard to implement in one part (financial related controls) but not the other (non-financial related controls). In the Appendix 2, I provide further

information on these interviews and survey responses.

4.4.2 Cross-Sectional Evidence

To provide archival evidence, I exploit cross-sectional differences in intertwined systems, audit committees, and internal control weaknesses. I illustrate two cross-sectional predictions: (1) in more integrated data systems, information spillover from financial data to other systems is more likely; (2) firms' ex ante incentive for strengthening internal controls is stronger when auditors' ex post monitoring are likely to be useful. I measure *More (Less) Integrated Syste*ms as an indicator coded as one if the firm uses Enterprise Resource Planning (ERP) and CAD/CAM integration softwares, and zero otherwise. I obtain information on the ERP and CAD/CAM from the Harte-Hanks Ci Technology database (CiDB).[21] ERP systems have a common database to support all applications and have an integrated system to automate business processes (e.g., Morris 2011; Lecic and Kupusinac 2013), and they include features and "built-in" controls to help firms comply with the internal control over financial reporting (Morris 2011). The proxy variable for firms' ex ante incentives for adopting high-quality internal controls is firms' audit committees and their internal control strength. Specifically, *With (Without) Pre Committees* is an indicator coded as one if the firm has committee members specializing in risk, security, and technology, or if the number of audit committee members is greater than or equal to the median value in 2004, and zero otherwise. *No (With) Internal Control Weakness* is an indicator coded as one if the firm has (does not have) internal control weaknesses, and zero otherwise. Firms with audit committees are likely more cooperative with external auditors and more receptive to auditors' ex post monitoring;

[21] Due to their extensive coverage and high quality, the data have been extensively used by researchers for assessing the technological software or hardware of firms (e.g., Bloom et al. 2014; Azarmsa et al. 2023). I keep the firms that can be matched with the CiDB dataset. One potential concern about integrated systems is that hackers may have access to more data if systems are integrated and centralized. However, this concern would bias against my result. In addition, this concern applies *after* the system is breached instead of impacting the *prevention* of breaches.

measuring firms' strong internal control environment is a way to validate firms' ex ante incentives for adopting high-quality internal controls.

In Panels A and B of Table 6, In line with the cross-sectional predictions, I find that the reductions in the likelihood of data breaches are more prominent, and the economic effects are significantly greater when firms have more integrated integrated systems, audit committees, or robust internal controls. In the more versus less integrated system partition, the difference is not statistically significant in *PCAOB First-time Inspection* and *Auditors Learning From Data Breaches* (p-value 0.281 and 0.132 respectively). In the with versus without pre committees partition, the difference is statistically significant in *Auditors Learning From Data Breaches* (p-value 0.000) but falls short of conventional levels of significance in *PCAOB First-time Inspection* (p-value 0.461). In the with versus without internal control weakness, the difference is statistically significant in *Auditors Learning From Data Breaches* (p-value 0.089) but also falls short of conventional levels of significance in *PCAOB First-time Inspection* (p-value 0.197). The coefficients of the control variables are similar to the other tables. Because the proxy variables I use for cross-sectional partitioning are noisy and subject to alternative interpretations, these results should be interpreted with caution. I acknowledge that these tests are imperfect and subject to endogeneity concerns, but they could provide descriptive evidence and the sample size is large.

5. Conclusion

Using plausibly exogenous improvements in auditing, I find evidence that auditing can help reduce the likelihood of data breaches. I explore two mechanisms through which this effect occurs, namely, providing relevant information about financial data systems and increasing firms' incentives for internal controls. The findings suggest that improvements in accounting information systems can have a positive impact on non-accounting systems.

However, there are several limitations and caveats to this study. First, the main threat to its identification is a potential violation of the parallel-trends assumption. Although I use different settings to alleviate concerns about omitted variables and contemporaneous changes, there may still be other confounding factors. Second, I do not observe within-firm internal control procedures for data protection, which are emphasized in the SEC's Section 21(a) investigative report. While I conduct interviews and surveys to obtain institutional information on mechanisms as well as provide empirical evidence, the unobservable nature of mechanisms is a caveat to the findings. Finally, this study does not intend to examine all the potential costs and benefits of auditing, nor does it claim that auditing is the best way to prevent data breaches.

References

Altamuro, J., and Beatty, A. (2010). How does internal control regulation affect financial reporting?. Journal of Accounting and Economics, 49(1-2), 58-74.

Altonji, J. G., Elder, T. E., and Taber, C. R. (2005). Selection on observed and unobserved variables: Assessing the effectiveness of Catholic schools. Journal of Political Economy, 113(1), 151-184.

American Institute of Certified Public Accountants (AICPA). (1984). The effects of computer processing on the audit of financial statements. Statement on Auditing Standards No. 48.

American Institute of Certified Public Accountants (AICPA). (2006). Planning and supervision. Statement of Auditing Standards No. 108.

American Institute of Certified Public Accountants (AICPA). (2006). Understanding the entity and its environment and assessing the risks of material misstatement. Statement of Auditing Standards No. 109.

American Institute of Certified Public Accountants (AICPA). (2006). Performing audit procedures in response to assessed risks and evaluating the audit evidence obtained. Statement of Auditing Standards No. 110.

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

Angrist, J. D., and Pischke, J. S.(2009). Mostly harmless econometrics: An empiricist's companion, 1st ed. Princeton, NJ: Princeton University Press.

Aobdia, D. (2018). The impact of the PCAOB individual engagement inspection process—Preliminary evidence. The Accounting Review, 93(4), 53-80.

Aobdia, D., and Shroff, N. (2017). Regulatory oversight and auditor market share. Journal of Accounting and Economics, 63(2-3), 262-287.

Asthana, S. C., Kalelkar, R., and Raman, K. K. (2021). Does client cyber-breach have reputational consequences for the local audit office?. Accounting Horizons, 35(4), 1-22.

Ashraf, M. (2022). The role of peer events in corporate governance: Evidence from data breaches. The Accounting Review, 97(2), 1-24.

Azarmsa, E., Liu, L. Y., and Noh, S. (2022). Through the Lens of Internal Information: How Does Internal Communication Technology Affect External Communication?.

Ball, R. (1980). Discussion of accounting for research and development costs: The impact on research and development expenditures. Journal of Accounting Research, 27-37.

Barrios, J. M., Lisowsky, P., and Minnis, M. (2019). Measurement matters: Financial reporting and productivity. University of Chicago and Boston University working paper, 1-48.

Bauer, T. D., and Estep, C., (2019). One team or two? Investigating relationship quality between auditors and IT specialists: Implications for audit team identity and the audit process. Contemporary Accounting Research, 36(4), 2142-2177.

Bloom, N., Eifert, B., Mahajan, A., McKenzie, D., and Roberts, J. (2013). Does management matter? Evidence from India. Quarterly Journal of Economics, 128(1), 1-51.

Bloom, N., Garicano, L., Sadun, R., and Van Reenen, J. (2014). The distinct effects of information technology and communication technology on firm organization. Management Science, 60(12), 2859-2885.

Burks, J. J. (2011). Are investors confused by restatements after Sarbanes-Oxley? The Accounting Review, 86(2), 507-539.

Center for Audit Quality. (2016). Understanding cybersecurity and the external audit.

Center for Audit Quality. (2017). The CPA's role in addressing cybersecurity risk.

Chen, S., Sun, S. Y., and Wu, D. (2010). Client importance, institutional improvements, and audit quality in China: An office and individual auditor level analysis. The Accounting Review, 85(1), 127-158.

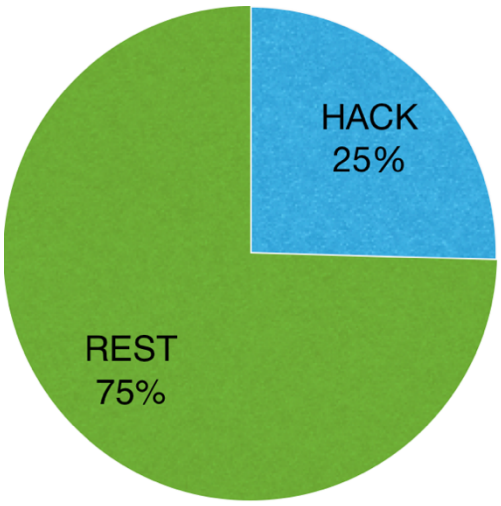
Cheng, M., Dhaliwal, D., and Zhang, Y. (2013). Does investment efficiency improve after the disclosure of material weaknesses in internal control over financial reporting?. Journal of accounting and

economics, 56(1), 1-18.
Conley, T., Gonçalves, S., and Hansen, C. (2018). Inference with dependent data in accounting and finance applications. Journal of Accounting Research, 56(4), 1139-1203.
DeFond, M. L., and Lennox, C. S. (2017). Do PCAOB inspections improve the quality of internal control audits?. Journal of Accounting Research, 55(3), 591-627.
DeFond, M., and Zhang, J. (2014). A review of archival auditing research. Journal of Accounting and Economics, 58(2-3), 275-326.
Duguay, R. (2022). The Effect of Financial Audits on Governance Practices: Evidence from the Nonprofit Sector. Available at SSRN 3273502.
Duffie, D., and Younger, J. (2019). Cyber Runs. Working paper, Stanford University.
Farboodi, M., Mihet, R., Philippon, T., and Veldkamp, L. (2019). Big data and firm dynamics. In AEA papers and proceedings (Vol. 109, pp. 38-42).
Feng, M., Li, C., and McVay, S. (2009). Internal control and management guidance. Journal of Accounting and Economics, 48(2-3), 190-209.
Feng, M., Li, C., McVay, S. E., and Skaife, H. (2015). Does ineffective internal control over financial reporting affect a firm's operations? Evidence from firms' inventory management. The Accounting Review, 90(2), 529-557.
Freyaldenhoven, S., Hansen, C., and Shapiro, J. M. (2019). Pre-event trends in the panel event-study design. American Economic Review, 109(9), 3307-38.
Furnham, A. (1986). Response bias, social desirability and dissimulation. Personality and Individual Differences, 7(3), 385-400.
Gipper, B., Leuz, C., and Maffett, M. (2019) Public audit oversight and reporting credibility: Evidence from the PCAOB inspection regime. Review of Financial Studies, forthcoming.
Goldfarb, A., and Tucker, C. (2012). Privacy and innovation. Innovation Policy and the Economy, 12(1), 65-90.
Haislip, J., Kolev, K., Pinsker, R., and Steffen, T. (2019). The economic cost of cybersecurity breaches: A broad-based analysis. In Workshop on the Economics of Information Security (WEIS) (pp. 1-37).
Haislip, J. Z., Peters, G. F., and Richardson, V. J. (2016). The effect of auditor IT expertise on internal controls. International Journal of Accounting Information Systems, 20, 1-15.
Hanlon, M., and Shroff, N. (2022). Insights into auditor public oversight boards: Whether, how, and why they "work". Journal of Accounting and Economics, 101497.
Hoffman, B. W., Sellers, R. D., and Skomra, J. (2018). The impact of client information technology capability on audit pricing. International Journal of Accounting Information Systems, 29, 59-75.
Hogan, C. E., and Wilkins, M. S. (2008). Evidence on the audit risk model: Do auditors increase audit fees in the presence of internal control deficiencies? Contemporary Accounting Research, 25(1), 219-242.
Hranaiova, J., and Byers, S. L. (2007). Changes in market responses to financial statement restatement announcements in the Sarbanes-Oxley era. Working Paper, SSRN 1319354.
Jin, G. Z. (2018). Artificial intelligence and consumer privacy. Working Paper, National Bureau of Economic Research.
Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., and Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics, 139(3), 719-749.
Kannan, K., Rees, J., and Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. International Journal of Electronic Commerce, 12(1), 69-91.
Kashyap, A. K., and Wetherilt, A. (2019, May). Some principles for regulating cyber risk. AEA Papers and Proceedings 109: 482-87.
Kopp, E., Kaffenberger, L., and Jenkinson, N. (2017). Cyber risk, Market failures, and financial stability. Working Paper, International Monetary Fund.
Krishnan, J., Krishnan, J., and Song, H. (2016). PCAOB international inspections and audit quality. The Accounting Review, 92(5), 143-166.
Lamoreaux, P. T. (2016). Does PCAOB inspection access improve audit quality? An examination of foreign

firms listed in the United States. Journal of Accounting and Economics, 61(2-3), 313-337.
Lawrence, A., Minutti-Meza, M., and Vyas, D. (2018). Is operational control risk informative of financial reporting deficiencies? Auditing: A Journal of Practice and Theory 37 (1): 139–165.
Lecic, D., and Kupusinac, A. (2013). The impact of ERP systems on business decision-making. TEM Journal, 2(4), 323.
Li, B., Li, Y., Pittman, J., and Wang, W. (2022). Auditors' Response to Cybersecurity Risk: Human Capital Investment and Cross-Client Influence. Available at SSRN 4192802.
Li, C., Peters, G. F., Richardson, V. J., and Weidenmier Watson, M. (2012). The consequences of information technology control weaknesses on management information systems: The case of Sarbanes-Oxley internal control reports. MIS Quarterly 36(1): 179-203.
Li, H., No, W. G., and Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. Auditing: A Journal of Practice & Theory, 39(1), 151-171.
Mansi, S. A., Maxwell, W. F., and Miller, D. P. (2004). Does auditor quality and tenure matter to investors? Evidence from the bond market. Journal of Accounting Research, 42(4), 755-793.
Minnis, M. (2011). The value of financial statement verification in debt financing: Evidence from private US firms. Journal of Accounting Research, 49(2), 457-506.
Morris, J. J. (2011). The impact of enterprise resource planning (ERP) systems on the effectiveness of internal controls over financial reporting. Journal of Information Systems, 25(1), 129-157.
Murfin, J. (2012). The supply-side determinants of loan contract strictness. Journal of Finance, 67(5), 1565-1601.
Oster, E. (2019). Unobservable selection and coefficient stability: Theory and evidence. Journal of Business & Economic Statistics, 37(2), 187-204.
Public Company Accounting Oversight Board (PCAOB). (2003). The personnel management element of a firm's system of quality control-competencies required by a practitioner-in-charge of an attest engagement. Quality Control Standards Section No. 40.
Public Company Accounting Oversight Board (PCAOB). (2006). An audit of internal control over financial reporting that is integrated with an audit of financial statements and related other proposals. Auditing Standard No. 5.
Public Company Accounting Oversight Board (PCAOB). (2007). An audit of internal control over reporting that is integrated with audit of financial statements and related independence rule and conforming amendments. Auditing Standard No. 5.
Public Company Accounting Oversight Board (PCAOB). (2010). Identifying and assessing risks of material misstatement. Auditing Standard No. 12. Appendix B – Consideration of Manual and Automated Systems and Controls.
Public Company Accounting Oversight Board (PCAOB). (2010). The auditor's responses to the risks of material misstatement. Auditing Standard No. 13.
Public Company Accounting Oversight Board (PCAOB). (2013). Staff Audit Practice Alert No. 11: Considerations for audits of internal control over financial reporting.
Public Company Accounting Oversight Board (PCAOB). (2019). Cybersecurity: Where we are; what more can be done? A call for auditors to lean in.
Rajgopal, S., Srinivasan, S., and Zheng, X. (2021). Measuring audit quality. Review of Accounting Studies, 26, 559-619.
Rice, S. C., and Weber, D. P. (2012). How effective is internal control reporting under SOX 404? Determinants of the (non-) disclosure of existing material weaknesses. Journal of Accounting Research, 50(3), 811-843.
Romanosky, S., Telang, R., and Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? Journal of Policy Analysis and Management, 30(2), 256-286.
Rosati, P., Gogolin, F., and Lynn, T. (2022). Cyber-security incidents and audit quality. European Accounting Review, 31(3), 701-728.
Schoenfeld, J. (2022). Cyber risk and voluntary Service Organization Control (SOC) Audits. Review of Accounting Studies, Forthcoming.

Schroeder, J. H., and Shepardson, M. L. (2015). Do SOX 404 control audits and management assessments improve overall internal control system quality? The Accounting Review, 91(5), 1513-1541.
Securities and Exchange Commission (SEC). (2018). Report of investigation pursuant to Section 21(a) of the Securities Exchange Act of 1934 regarding certain cyber-related frauds perpetrated against public companies and related internal accounting controls requirements.
Sherif, M., Taub, D., and Hovland, C. I. (1958). Assimilation and contrast effects of anchoring stimuli on judgments. Journal of Experimental Psychology, 55(2), 150.
Skinner, D. J., and Srinivasan, S. (2012). Audit quality and auditor reputation: Evidence from Japan. The Accounting Review, 87(5), 1737-1765.
Smith, T., J. L. Higgs, and R. Pinsker. (2019). Do auditors price breach risk in their audit fees? Journal of Information Systems, forthcoming.
Liu, L. Y., and Strahilevitz, L. (2022). Cash Substitution and Deferred Consumption as Data Breech Harms. University of Chicago Coase-Sandor Institute for Law & Economics Research Paper, (963).
Weber, J., Willenborg, M., and Zhang, J. (2008). Does auditor reputation matter? The case of KPMG Germany and ComROAD AG. Journal of Accounting Research, 46(4), 941-972.
Westermann, K. D., Cohen, J., and Trompeter, G. (2019). PCAOB inspections: Public accounting firms on "trial." Contemporary Accounting Research, 36(2), 694-731.
Wooldridge, J. 2010. Econometric analysis of cross section and panel data, 2nd ed. Cambridge, MA: MIT Press.
Yang, D. C., and Guan, L. (2004). The evolution of IT auditing and internal control standards in financial statement audits: The case of the United States. Managerial Auditing Journal, 19(4), 544-555.

Figure 1: Public Companies' Data Breaches by Type



Notes: This figure presents total data breaches by type. After manually matching the PRC dataset with public companies, there are 1,214 observations from 2005 to 2017. *HACK* (25%): Hacks by an outside party or infected by malware; *Rest* (75%): Data mishandled by insiders, including lost laptops without encryption, sensitive information posted publicly, etc.

Table 1: Descriptive Statistics

Variable	*N*	*Mean*	*Std. Dev.*	*Median*	*P10*	*P90*
Breached Public Firms (Firm-Year Level)						
Size	1,211	9.767	2.313	9.803	6.715	12.671
Loss	1,211	0.142	0.349	0.000	0.000	1.000
Asset Intangibility	1,211	0.834	0.191	0.917	0.541	0.993
Total Public Firms (Firm-Year Level)						
Size	55,827	6.577	2.203	6.552	3.709	9.461
Loss	55,827	0.295	0.456	0.000	0.000	1.000
Asset Intangibility	55,827	0.783	0.246	0.887	0.355	0.992
PCAOB First-Time Inspection	55,827	0.911	0.285	1.000	1.000	1.000
Auditors Learning From Restatements	55,827	0.735	0.441	1.000	0.000	1.000
Auditors Learning From Data Breaches	55,827	0.168	0.374	0.000	0.000	1.000
Determinants of Data Breaches (Firm-Year Level)						
Breach	55,827	0.012	0.111	0.000	0.000	0.000
% of Audit Committee Members	55,827	0.228	0.140	0.233	0.001	0.389
Risk/Technology Committee	55,827	0.032	0.177	0.000	0.000	0.000
Big Auditors	55,827	0.739	0.439	1.000	0.000	1.000
No Internal Control Weakness	55,827	0.688	0.463	1.000	0.000	1.000
Audit Fee Ratio	55,827	0.839	0.150	0.876	0.629	1.000
Public Firms and Firms Submit X-17A-5 Filings (Firm-Year Level)						
Big Auditors (Indicator)	111,028	0.577	0.494	1.000	0.000	1.000
Size	111,028	4.263	4.076	5.296	-1.997	8.892
Log (Liability)	111,028	3.331	4.667	4.370	-3.866	8.492
Log (Revenue)	111,028	3.954	3.604	4.508	-1.161	8.266
Treatment*Post	111,028	0.052	0.222	0.000	0.000	0.000
BLS (State-Occupation-Year Level)						
Log (Total Employment)	491,508	6.788	1.820	6.709	4.382	9.222
Log (Mean Annual Wage)	491,508	11.899	1.031	11.889	10.528	13.267

Notes: This table presents summary statistics for the firm-year and state-occupation-year level data sets used in the analysis. *Size* is the natural log of total assets. *Loss* is an indicator coded as one if the firm has a negative income, and zero otherwise. *Asset Intangibility* is defined as one minus the proportion of PPE in total assets. *Breach* is an indicator coded as one if the firm has a data breach in a given year, and zero otherwise. *% of Audit Committee Members* is the number of audit committee members divided by total number of board members. *Risk/Technology Committee* is an indicator coded as one if the firm has committee members specializing in risk, security, and technology, and zero otherwise. *Big Auditors* is an indicator coded as one if a firm hires a big auditor, and zero otherwise. Big auditors are defined as the Big Four. *No Internal Control Weakness* is an indicator coded as one for a firm with no internal control weakness, and zero otherwise. *Audit Fee Ratio* is measured as audit fees divided by the sum of audit fees and non-audit fees. *Log(Liability)* is the natural log of total liabilities. *Log(Revenue)* is the natural log of revenue. *Log(Employment)* is the natural log of employment at the state-occupation-year level. See Appendix A1 for further details on variable definitions.

Table 2: Determinants of Data Breaches

Dependent Variable: Breach	*(1)*	*(2)*
% of Audit Committee Members	-0.025***	-0.025***
	(-3.33)	(-3.19)
Risk/Technology Committee	-0.002	-0.002
	(-0.34)	(-0.37)
Loss	0.003**	0.003**
	(2.09)	(2.07)
Asset Intangibility	0.023***	0.022***
	(5.02)	(4.94)
Size	0.011***	0.011***
	(6.35)	(6.38)
No Internal Control Weakness	-0.006***	-0.008***
	(-3.85)	(-4.53)
Big Auditors	-0.008**	-0.006**
	(-2.61)	(-2.40)
Audit Fee Ratio	-0.009*	-0.012**
	(-1.82)	(-2.25)
Fixed Effects:		
Industry (2-Digit)	Yes	Yes
Year	No	Yes
Observations (Firm-Year)	55,827	55,827
Adjusted R-squared	0.040	0.042
Cluster	Industry	Industry

Notes: This table presents the determinants of data breaches. *Breach* is an indicator coded as one if a firm has a data breach in a given year, and zero otherwise. *% of Audit Committee Members* is the number of audit committee members divided by total number of board members. *Risk/Technology Committee* is an indicator coded as one if the firm has committee members specializing in risk, security, and technology, and zero otherwise. *Asset Intangibility* is defined as one minus the proportion of PPE in total assets. *Loss* is an indicator coded as one if the firm has a negative income, and zero otherwise. *No Internal Control Weakness* is an indicator coded as one for a firm with no internal control weakness, and zero otherwise. *Big Auditors* is an indicator coded as one if a firm hires a big auditor, and zero otherwise. Big auditors are defined as the Big Four. *Size* is measured as the natural log of total assets. *Audit Fee Ratio* is measured as audit fees divided by the sum of audit fees and non-audit fees. See Appendix A1 for further details on variable definitions. I include industry (two-digit) fixed effects in Column (1). I include industry (two-digit) and year fixed effects in Column (2). I cluster standard errors by industry (two digit) and report t-statistics in parentheses. *, **, and *** indicate statistical significance (two-sided) at the 10%, 5%, and 1% levels, respectively.

Table 3: Descriptive Evidence of Auditing on Data Breaches

Dependent Variable: Breach	*(1)*	*(2)*
Auditor Change (Non-Big → Big)	-0.009**	
	(-2.55)	
Auditor Change (Big → Non-Big)		0.002
		(1.24)
Size	0.004***	0.004***
	(2.84)	(2.81)
Loss	0.003***	0.003***
	(2.72)	(2.70)
Asset Intangibility	0.014*	0.014*
	(1.75)	(1.78)
Fixed Effects		
Firm	Yes	Yes
Auditor	Yes	Yes
Year	Yes	Yes
Observations (Firm-Year)	55,827	55,827
Adjusted R-squared	0.123	0.123
Cluster	Industry	Industry

Notes: This table presents descriptive evidence on the relationship between auditing and data breaches. *Breach* is an indicator coded as one if a firm has a data breach in a given year, and zero otherwise. *Auditor Change (Non-Big → Big)* is an indicator coded as one after a firm changes from a non-big to a big auditor, and zero otherwise. *Auditor Change (Big → Non-Big)* is an indicator coded as one after a firm changes from a big auditor to a non-big auditor, and zero otherwise. *Breach* is an indicator coded as one if a firm has a data breach in a given year, and zero otherwise. *Firm Controls* include *Size, Loss,* and *Asset Intangibility*. *Size* is the natural log of total assets. *Loss* is an indicator coded as one if a firm has a negative income, and zero otherwise. *Asset Intangibility* is defined as one minus the proportion of PPE in total assets. See Appendix A1 for further details on variable definitions. I include firm and year fixed effects. I cluster standard errors by industry (two digit) and report t-statistics in parentheses. *, **, and *** indicate statistical significance (two-sided) at the 10%, 5%, and 1% levels, respectively.

Table 4: Effect of Auditing on Data Breaches with PCAOB

Dependent Variable: Breach	*(1)*	*(2)*
PCAOB First-Time Inspection	-0.004*	-0.004*
	(-1.93)	(-1.93)
Size		0.003***
		(6.53)
Loss		0.003**
		(2.49)
Asset Intangibility		0.013**
		(2.58)
Fixed Effects		
Firm×Auditor	Yes	Yes
Year	Yes	Yes
Firm Controls	No	Yes
Observations (Firm-Year)	55,827	55,827
Adjusted R-squared	0.105	0.105
Cluster	Auditor	Auditor

Notes: This table reports results on the effect of overseeing accounting information systems on data breaches, using the shock of PCAOB first-time inspection. *Breach* is an indicator coded as one if a firm has a data breach in a given year, and zero otherwise. *PCAOB First-Time Inspection*, the variable of interest, is an indicator coded as one after PCAOB first-time inspection for firms audited by an inspected auditor, zero otherwise. *Firm Controls* include *Size, Loss,* and *Asset Intangibility*. *Size* is the natural log of total assets. *Loss* is an indicator coded as one if the firm has a negative income, and zero otherwise. *Asset Intangibility* is defined as one minus the proportion of PPE in total assets. See Appendix A1 for further details on variable definitions. I include firm×auditor and year fixed effects. I cluster standard errors by auditor and report t-statistics in parentheses. Variations in identification strategy are illustrated in Appendix 1. *, **, and *** indicate statistical significance (two-sided) at the 10%, 5%, and 1% levels, respectively.

Table 5: Effect of Auditing on Data Breaches with Auditor Learning

Dependent Variable: Breach	*OC in OGA* *(1)*	*OC in OGA* *(2)*	*OC* *(3)*
Auditors Learning From Data Breaches	-0.007***	-0.007***	-0.015*
	(-3.09)	(-3.16)	(-1.76)
Size		0.003***	0.003***
		(6.38)	(5.99)
Loss		0.003**	0.003**
		(2.48)	(2.48)
Asset Intangibility		0.013**	0.013**
		(2.56)	(2.51)
Fixed Effects			
Firm×Auditor	Yes	Yes	Yes
Year	Yes	Yes	Yes
Firm Controls	No	Yes	Yes
Observations (Firm-Year)	55,827	55,827	55,827
Adjusted R-squared	0.105	0.105	0.105
Cluster	Auditor	Auditor	Auditor

Notes: This table reports results on the effect of auditing on data breaches with the shock of auditor "learning from data breaches." *Breach* is an indicator coded as one if a firm has a data breach in a given year, and zero otherwise. *Auditors Learning From Data Breaches*, the variable of interest, is an indicator coded as one after auditors learn from data breaches with their other clients, zero otherwise. *OC in OGA,* in Columns (1) — (2), defines treatment firms as other clients (*OC*) in other geographic areas (*OGA*) with the same auditor. *OC,* in Column (3), defines treatment firms as other clients (*OC*) with the same auditor. *Firm Controls* include *Size, Loss,* and *Asset Intangibility*. *Size* is the natural log of total assets. *Loss* is an indicator coded as one if the firm has a negative income, and zero otherwise. *Asset Intangibility* is defined as one minus the proportion of PPE in total assets. See Appendix A1 for further details on variable definitions. I include firm×auditor and year fixed effects. I cluster standard errors by auditor and report t-statistics in parentheses. Variations in the identification strategy are illustrated in Appendix 1. *, **, and *** indicate statistical significance (two-sided) at the 10%, 5%, and 1% levels, respectively.

Table 6: Cross-Sectional Analyses on the Effect of Auditing

Panel A: PCAOB First-Time Inspection

	Integrated Systems		*Pre Committees*		*Internal Control Weakness*	
Dependent Variable: Breach	*More*	*Less*	*With*	*Without*	*No*	*With*
	(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*
PCAOB First-Time Inspection	-0.005*	0.001	-0.006*	-0.003	-0.005*	-0.001
	(-1.65)	(0.88)	(-1.87)	(-1.63)	(-1.64)	(-0.16)
Difference (p-value)	0.281		0.461		0.197	
Size	0.008***	0.002	0.005***	0.006**	0.005***	0.001
	(6.71)	(1.18)	(3.16)	(2.53)	(4.91)	(1.06)
Loss	0.004***	0.002	0.002	0.004	0.003	0.002
	(3.36)	(1.26)	(1.10)	(1.59)	(1.48)	(1.59)
Asset Intangibility	0.008	0.004	0.022***	0.008	0.018**	0.001
	(0.84)	(0.71)	(3.81)	(0.77)	(2.31)	(0.38)
Fixed Effects						
Firm×Auditor	Yes	Yes	Yes	Yes	Yes	Yes
Year	Yes	Yes	Yes	Yes	Yes	Yes
Firm Controls	Yes	Yes	Yes	Yes	Yes	Yes
Observations (Firm-Year)	21,990	14,961	22,522	11,943	37,651	15,345
Adjusted R-squared	0.126	0.021	0.135	0.120	0.124	0.127
Cluster	Auditor	Auditor	Auditor	Auditor	Auditor	Auditor

Panel B: Auditors Learning From Data Breaches

	Integrated Systems		*Pre Committees*		*Internal Control Weakness*	
Dependent Variable: Breach	*More*	*Less*	*High*	*Low*	*No*	*With*
	(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*
Auditor Learning From Data Breaches	-0.009***	-0.004	-0.010***	0.003	-0.008***	-0.004**
	(-2.89)	(-1.38)	(-4.93)	(0.87)	(-2.88)	(-2.04)
Difference (p-value)	0.132		0.000		0.089	
Size	0.008***	0.002	0.005***	0.006**	0.005***	0.001
	(6.72)	(1.18)	(3.15)	(2.54)	(5.04)	(1.08)
Loss	0.004***	0.002	0.002	0.004	0.003	0.002
	(3.32)	(1.26)	(1.07)	(1.59)	(1.48)	(1.57)
Asset Intangibility	0.007	0.004	0.021***	0.008	0.018**	0.001
	(0.81)	(0.70)	(3.82)	(0.79)	(2.24)	(0.38)
Fixed Effects						
Firm×Auditor	Yes	Yes	Yes	Yes	Yes	Yes
Year	Yes	Yes	Yes	Yes	Yes	Yes
Firm Controls	Yes	Yes	Yes	Yes	Yes	Yes
Observations (Firm-Year)	21,990	14,961	22,522	11,943	37,651	15,345
Adjusted R-squared	0.126	0.021	0.135	0.120	0.124	0.127
Cluster	Auditor	Auditor	Auditor	Auditor	Auditor	Auditor

Table 6 Continued

Notes: This table reports cross-sectional results on the effect of auditing on data breaches. Panel A reports the results using the PCAOB shock. Panel B reports results using "auditors learning from data breaches." *More (Less) Integrated Syste*ms is an indicator coded as one if the firm uses Enterprise Resource Planning (ERP) and CAD/CAM integration softwares, and zero otherwise. *With (Without) Pre Committees* is an indicator coded as one if the firm has committee members specializing in risk, security, and technology, or if the number of audit committee members is greater than or equal to the median value in 2004, and zero otherwise. *No (With) Internal Control Weakness* is an indicator coded as one if the firm does not have (has) internal control weaknesses, and zero otherwise. The dependent variable, *Breach*, is an indicator coded as one if the firm has a data breach in a given year, and zero otherwise. *Firm Controls* include *Size, Loss,* and *Asset Intangibility*. *Size* is the natural log of total assets. *Loss* is an indicator coded as one if the firm has a negative income, and zero otherwise. *Asset Intangibility* is defined as one minus the proportion of PPE in total assets. See Appendix A1 for further details on variable definitions. I include firm×auditor and year fixed effects. I cluster standard errors by auditor and report t-statistics in parentheses. *, **, and *** indicate statistical significance (two-sided) at the 10%, 5%, and 1% levels, respectively.

Appendix:

1. Variable Definitions
2. Further Summary of Interviews and Surveys
3. Validation of Underlying Empirical Assumptions
4. Public Companies' Data Breaches by SIC Industry (2-digit)
5. Number of Data Breaches by Year
6. Effective Dates of State Security Breach Notification Laws
7. Examples of Firms' Disclosure and Practitioners' Discussions

Appendix 1:
Table A1 : Variable Definitions

Breach	An indicator coded as one if the firm has a data breach in a given year, and zero otherwise.
% of Audit Committee Members	The number of audit committee members divided by the total number of board members.
Risk/Technology Committee	An indicator coded as one if the firm has committee members specializing in risk, security, and technology, and zero otherwise.
Asset Intangibility	One minus the proportion of PPE in total assets.
Loss	An indicator coded as one if the firm has a negative income, and zero otherwise.
No Internal Control Weakness	An indicator coded as one for a firm with no internal control weakness, and zero otherwise.
Big Auditors	An indicator coded as one if a firm hires a big auditor, and zero otherwise. Big auditors are defined as the Big Four.
Audit Fee Ratio	Audit fees divided by the sum of audit fees and non-audit fees for a given firm-year.
Auditor Change (Non-Big → Big)	An indicator coded as one after the firm changes from non-big to big auditors, and zero otherwise.
Auditor Change (Big → Non-Big)	An indicator coded as one after the firm changes from big to non-big auditors, and zero otherwise.
PCAOB First-Time Inspection	An indicator coded as one after PCAOB first-time inspection for firms audited by an inspected auditor, zero otherwise.
Auditors Learning From Data Breaches	An indicator coded as one after auditors learn from data breaches with their other clients, zero otherwise. The initial period for auditors' learning from data breaches is 2005.
Size	The natural log of total assets.
More (Less) Integrated Systems	An indicator coded as one if the firm uses Enterprise Resource Planning (ERP) and CAD/CAM integration softwares, and zero otherwise.
With (Without) Pre Committees	An indicator coded as one if the firm has committee members specializing in risk, security, and technology, or if the number of audit committee members is greater than or equal to the median value in 2004, and zero otherwise, and zero otherwise.
No (With) Internal Control Weakness	An indicator coded as one if the firm does not have (has) internal control weaknesses, and zero otherwise.
Treatment	An indicator coded as one if a company submits X-17A-5 filings, and zero otherwise.
Post	An indicator coded as one if the year is after 2013, and zero otherwise.
Log(Employment)	The natural log of employment for an occupation in a given state and year.
DBState	An indicator coded as one if the state passes state security breach notification laws, and zero otherwise.
Auditor	An indicator coded as one if accountants and auditor occupations, and zero otherwise.

Appendix 2: Further Summary of Interviews and Surveys

I conducted one-on-one interviews with 36 industry professionals to obtain institutional insights and to collect information on mechanisms beyond empirical analyses. I conducted 19 interviews by phone, 14 interviews in person, and three interviews via online messages; the interviewees included 11 accounting firm partners, five (non-partner) external auditors, nine internal auditors, one audit committee member, five corporate legal counsels/experts, and five regulators. In-person and phone interviews were around 42 minutes on average. I did not make any audio recordings for privacy reasons but took notes in all interviews. This section summarizes the mechanisms suggested by the interviews and survey findings.

To keep from leading my interviewees, I usually started by asking about the relationship between external auditors and data breaches. Their responses helped provide rich mechanisms and anecdotes about how auditors could potentially help protect their clients' data. These interviews also provide helpful discussions on how the regulation and their prior experiences improve their audit quality.

All interviewees believe that while it is not an external auditor's main job to detect data breaches, however, the interviewees care about data breaches and provide anecdotes on how their work could potentially affect their clients' data protection procedures. Two channels can be summarized from the ample anecdotes provided in the interviews: information spillovers and internal control, as discussed in the paper.

Auditing partners also talked about the application of knowledge learned from previous incidents, such as changing questions and procedures, and adjusting thought processes. When assessing risks for their other clients, auditors also raise skepticism and awareness, although they try to make sure engagement processes are consistent. Because external auditors reflect on why these incidents happen, they are able to take knowledge and experience to other firms. For example, they use their professional skillsets, look for commonalities, and ask deeper questions in order to discover patterns.

Although interviews provide evidence unobservable in data, they may suffer from some biases (e.g., the social desirability bias (Furnham 1986) or the anchoring bias (Sherif et al. 1958)), especially when the interactions are in person. To mitigate these concerns, I also conducted anonymous surveys. In order to maximize the unbiasedness and informativeness of the survey responses, I used a neutral tone, asked professional consultants to help design the survey, and pre-tested it with some academics and practitioners. I currently have 20 survey responses, which can be summarized as follows. Seventy-seven percent of auditors think accounting information and IT systems are intertwined. Ninety percent of auditors think IT audit and internal control tests can help protect firms' financial reporting data. Seventy-seven percent of auditors believe IT audit and internal control tests can also help protect firms' non-financial data (e.g., employee information,

consumer information, and any other non-financial data). Eighty-seven percent of auditors indicate that financial and non-financial data are stored in the same data repository. Eighty-five percent of auditors reveal that IT general controls operate in combination with other data control systems. I also asked an open question about how auditors could help protect their clients' data; most of their answers mention internal control reviews. For example, they discussed attack and penetration tests, access management controls, change management controls, and IT control. One survey participant also noted that it depends on whether the data protection is an element of enterprise risk assessment.

Appendix 3: Validation of Underlying Empirical Assumptions

An assumption maintained throughout this paper is that auditors have the relevant skills to test data protection controls. To further validate this assumption, I provide additional institutional information and empirical evidence below.

Auditors learn relevant skills through their education and certification. Many professional accounting programs (e.g., graduate-level programs) have courses on data analytics, and AICPA has consistently issued guidance on auditing IT controls. The Statement on Standards for Attestation Engagements (SSAE) No. 16 and No. 18 (AT-C 105 and 205 Examinations) provide detailed guidance on SOC 1 (internal control over financial reporting) and SOC 2 (non-financial data protection) audits. Both SOC 1 and SOC2 audits evaluate internal controls, policies, and procedures. The SOC 1 audit reports user entities' internal control over financial reporting, while the SOC 2 audit examines firms' non-financial data control policies and procedures to help them achieve five "trust services principles" (security, availability, processing integrity, confidentiality, and privacy). SOC 1 and SOC 2 audits are not mutually exclusive, as the same vendor could process and store both non-financial (e.g., user information) and financial information (e.g., user-related transactions that affect firms' financial reporting). Schoenfeld (2022) provides further descriptive evidence on SOC audits. Big auditing firms are also equipped with resources such as personnel, training, and experience. In the payment card industry, auditors conduct a PCI Compliance Audit to ensure that customers' data are protected.

Next, I explore two regulatory shocks outside of my paper's setting to help me identify how audit services change with the rising cost of data breaches. The first regulatory shock is the "Regulation S-ID: Identity Theft Red Flags Rule" jointly issued by the SEC and the Commodity Futures Trading Commission (CFTC) in 2013. On April 19, 2013, the two agencies published their joint final rules and guidelines and included a compliance date of November 20, 2013. The Red Flags Rule requires financial institutions to implement a robust written program that can identify, detect, prevent, and mitigate identity theft. The rules help firms comply with the SEC's enforcement authority. Companies covered by this rule include most registered brokers, dealers, and investment companies, as well as some registered investment advisers.[22] Because firms' incentives to mitigate the identity theft of consumers are stronger after Regulation S-ID, the higher likelihood that firms hire high-quality auditors in the post-Regulation S-ID period (relative to the control group) suggests that auditors play a role in detecting consumer information theft. Because big auditors have the incentive and capabilities to reduce potential business risks in order to maintain their reputation and reduce legal liabilities (e.g., DeFond and Zhang 2014), and because this variable is available in both the treatment and control group, I examine the change in the likelihood of hiring big auditors between the treatment and control group after Regulation S-ID. My baseline

[22] See https://www.sec.gov/rules/final/2013/34-69359.pdf.

regression, suppressing time and firm subscripts, is

$$Big\ Auditors = \alpha_1 Treatment \times Post + \sum \alpha_i Fixed\ Effects + \gamma_i Controls + \epsilon \quad (1)$$

The dependent variable, *Big Auditors*, is an indicator variable equal to one if a firm hires a big auditor, and zero otherwise. Companies that submit X-17A-5 filings to the SEC are subject to Regulation S-ID and are the treatment group (*Treatment*). Companies that submit 10K (but not X-17A-5) filings are the control group. The year after the 2013 compliance date is the post-period (*Post*). I include firm fixed effects to account for time-invariant firm differences in auditor hiring and include year fixed effects to flexibly account for changes over time in firms' auditor hiring that are common to both the treatment and control groups. In Column 1 of Table A2 Panel A, the treatment group is 2% more likely than the control group to hire big auditors in the post Regulation S-ID period. From the descriptive statistics in Table 1, we see that a typical treatment firm is much smaller than the typical control firm (e.g., the mean and median of the combined treatment and control are smaller than the mean and median of the control alone), which suggests that there are differences in the underlying firm characteristics of the treatment and control groups. To assess how these differences affect my estimates, I include control variables in Column 2. I include *Size*, *Log (Liability)*, and *Log (Revenue)*, which are all reported by both the treatment and control firms (firms submitting X-17A-5 filings report only a limited set of financial numbers). These control variables play an economic role in firms' decision to hire big auditors (e.g., Mansi et al. 2004; Chen et al. 2010), and including them in my specification helps me gauge how they affect the variable of interest (Altonji et al. 2005; Oster 2019). After I include the control variables in Column 2, the effect holds with a slightly larger magnitude (2.7%). For the control variables, larger firms and firms with higher revenue are more likely to hire big auditors. Liability is statistically insignificant in the regression; this could be due to collinearity among control variables.

The second regulatory shock is the "State Security Breach Notification Laws," which have a staggered implementation across states.[23] The law requires companies to notify their consumers in a timely manner if their personal information was breached. Romanosky et al. (2011) argue that by increasing the costs of breaches, data breach disclosure laws could incentivize firms to strengthen their data protection. I explore the staggered implementation of this law and examine the subsequent change in auditor employment (relative to other occupations) in order to further corroborate the role of auditors in firms' data protection. My baseline regression, suppressing time, state, and occupation subscripts, is

[23] See Appendix 4 for the effective dates of the state security breach notification laws. Although consumer residency determines notification requirements, firms in states with data breach notification laws are aware of such incidents and are motivated to strengthen their data protection to avoid the potential costs of notification. This is consistent with the findings in Romanosky et al. (2011).

$$Log(Employment) = \alpha_1 DBState * Auditor + \alpha_2 DBState + \sum \alpha_i Fixed\ Effects + Controls + \epsilon \quad (2)$$

The dependent variable, *Log(Employment)*, is the natural log of employment at the state-occupation-year level. *DBState* is an indicator variable equal to one for states that pass breach notification laws, and zero otherwise. *Auditor* is an indicator variable equal to one if the occupation is auditors, and zero otherwise. I use a different fixed effects structure than those in previous regressions because I also have different observation units (at the state, year, and occupation levels). The fixed effects structure also varies depending on the specification. In Column (1), I include state fixed effects to account for static state differences in occupation and include year fixed effects to control for changes in occupation over time that are common across states. I also include occupation fixed effects to control for time-invariant occupation characteristics. In Column (2), in addition to year fixed effects, I include state×occupation fixed effects to control for average state-level differences in occupation. In Column (3), in addition to occupation fixed effects, I include state×year fixed effects to control for the time-varying economic changes in states that could differentially affect my outcome variables across treatment and control states. In Column (4), I include state×year and state×occupation fixed effects to control for time-varying economic changes in states and for average state-level differences in occupation employment, respectively.[24] Across these four specifications (shown in Table A2 Panel B), I find consistent results that auditor employment increases (relative to other occupations) from 8% (Columns 3 and 4) to 10% (Columns 1 and 2) in states that passed data breach notification laws. Although the evidence is indirect, it suggests that auditors have a role in mitigating the risk of data breaches. Note that state security notification laws affect firms that internalize the benefits of audit services and auditors that supply audit services, so the results should be interpreted as an estimate of how state laws influence the equilibrium outcomes of auditor employment.

In this analysis, the key identifying assumption is that the timing of the regulatory shock is not correlated with other factors that led to a change in auditor supply. One potential concern is that a string of high-profile data breaches led to the regulatory shock, thereby affecting the audit market (Ball 1980). However, this interpretation reinforces auditors' role in mitigating the risk of data breaches, which is consistent with my findings. Additionally, after the passage of Regulation S-ID, data breach scandals would have a similar effect on the control group. Moreover, Romanosky et al. (2011) conduct empirical analyses and find no systematic evidence for endogenous timing when states pass breach notification laws.

In Table A2 Panels A and B, I exploit two regulatory shocks and find an increase in audit services

[24] Including occupation×year fixed effects leaves insufficient variation to estimate reliable treatment effects because it excludes a large number of treatment and control observations.

when the cost of data breaches rises. One interpretation is that firms' awareness of auditing's potential role in preventing data breaches increases with the cost of data breaches. Firms are also more likely to internalize the benefit of external auditors when they are willing to increase data protection and when the deficiencies discovered in audited data systems are more likely to transfer to other data systems (financial data are the majority in Regulation S-ID). Due to data limitations, however, my results are subject to other interpretations. Because I do not have much granular information about firms' demand for audit services (e.g., audit fees or specific audit services) other than the classification of big auditors in the setting of Regulation S-ID, I cannot rule out the possibility that the choice to hire a big auditor may serve other purposes. In the setting of the State Security Breach Notification Laws, I have auditor occupation data at the state-year level but do not have a detailed breakdown by type (i.e., internal auditors, government auditors, and other specialized auditors). These other auditors have responsibilities and skillsets directly related to data breaches (e.g., internal auditors are responsible for monitoring firms' data breaches). It is possible that my results capture this variation. If these alternative interpretations do not perfectly explain my results, however, these two analyses help further validate the assumption that auditors have the relevant skillset.

Table A2: Changes in Audit Services When the Cost of Data Breaches Increases

Panel A: Regulation S-ID

Dependent Variable: Big Auditors	*(1)*	*(2)*
Treatment*Post	0.020***	0.027***
	(4.95)	(6.40)
Size		0.023***
		(9.56)
Log (Liability)		-0.004
		(-0.67)
Log (Revenue)		0.003**
		(2.01)
Fixed Effects		
Firm	Yes	Yes
Year	Yes	Yes
Firm Controls	No	Yes
Observations (Firm-Year)	111,028	111,028
Adjusted R-squared	0.856	0.857
Cluster	Firm	Firm

Panel B: State Security Breach Notification Laws

Dependent Variable: Log(Employment)	*(1)*	*(2)*	*(3)*	*(4)*
DBState*Auditor	0.105***	0.098***	0.084***	0.076***
	(3.51)	(5.00)	(2.86)	(4.41)
DBState	-0.006	-0.005		
	(-0.20)	(-0.15)		
Fixed Effects				
State	Yes	No	No	No
Year	Yes	Yes	No	No
Occupation	Yes	No	Yes	No
State×Year	No	No	Yes	Yes
State×Occupation	No	Yes	No	Yes
Observations (State-Occupation-Year)	491,508	489,879	491,508	491,508
Adjusted R-squared	0.835	0.931	0.839	0.935
Cluster	State	State	State	State

Notes: This table reports results on the auditor's role using two data-protection regulatory settings. Panel A reports results in the setting of "Regulation S-ID: Identity Theft Red Flags Rule." Panel B reports results in the setting of "State Security Breach Notification Laws." *Big Auditors* is an indicator coded as one if the firm hires a big auditor (Big Four), and zero otherwise. *Treatment* is an indicator coded as one if companies submit X-17A-5 filings, and zero otherwise. *Post* is an indicator coded as one if the year is after 2013, and zero otherwise. *Log(Employment)* is the natural log of employment at the state-occupation-year level. *DBState* is an indicator coded as one if the state passes the state security breach notification laws, and zero otherwise. *Auditor* is an indicator coded as one for accountant and auditor occupations, and zero otherwise. *Firm Controls* includes *Size*, *Log(Liability)*, and *Log(Revenue)*, which are reported by both the treatment and control firms. *Size* is the natural log of total assets. *Log(Liability)* is the natural log of total liabilities. *Log(Revenue)* is the natural log of revenue. I cluster standard errors by firm in Panel A and by state in Panel B. I report t-statistics in parentheses. *, **, and *** indicate statistical significance (two-sided) at the 10%, 5%, and 1% levels, respectively.

Appendix 4: Effective Dates of State Security Breach Notification Laws

Table A3: Effective Date of State Security Breach Notification Law

State	*Effective Date*	*Statute*
Alabama	1-Jun-18	Ala. Code § 8-38-1 et seq
Alaska	1-Jul-09	Alaska Stat. § 45.48.010 et seq
Arizona	31-Dec-06	Ariz. Rev. Stat. § 18-551 et seq
Arkansas	12-Aug-05	Ark. Code § 4-110-101 et seq
California	1-Jul-03	Cal. Civ. Code § 1798.80 et seq; Cal. Health & Safety Code § 1280.15
Colorado	1-Sep-06	Colo. Rev. Stat. § 6-1-716
Connecticut	1-Jan-06	Conn. Gen. Stat. § 36a-701b
Delaware	28-Jun-05	Del. Code Ann. tit. 6 § 12B-101 et seq
District of Columbia	1-Jul-07	D.C. Code § 28-3851 et seq
Florida	1-Jul-14	Fla. Stat. § 501.171
Georgia	5-May-05	Ga. Code § 10-1-910 et seq
Hawaii	1-Jan-07	Haw. Rev. Stat. § 487N-1 et seq
Idaho	1-Jul-06	Idaho Code § 28-51-104 et seq
Illinois	27-Jun-06	815 Ill. Comp. Stat. 530/5 et seq
Indiana	1-Jul-06	Ind. Code § 24-4.9-1-1 et seq
Iowa	1-Jul-08	Iowa Code § 715C.1 et seq
Kansas	1-Jan-07	Kan. Stat. § 50-7a01 et seq
Kentucky	15-Jul-14	Ky. Rev. Stat. § 365.732
Louisiana	1-Jan-06	La. Rev. Stat. § 51:3071 et seq; La. Admin. Code tit. 16, § 701
Maine	31-Jan-06	10 Me. Rev. Stat. § 1346 et seq
Maryland	1-Jan-08	Md. Code Com. Law § 14-3501 et seq
Massachusetts	31-Oct-07	Mass. Gen. Laws 93H § 1 et seq
Michigan	2-Jul-07	Mich. Comp. Laws §§ 445.63, .72
Minnesota	1-Jan-06	Minn. Stat. § 325E.61
Mississippi	1-Jul-11	Miss. Code § 75-24-29
Missouri	28-Aug-09	Mo. Rev. Stat. § 407.1500
Montana	1-Mar-06	Mont. Code §§ 30-14-1701 - 1702, 1704
Nebraska	14-Jul-06	Neb. Rev. Stat. § 87-801 et seq
Nevada	1-Jan-06	Nev. Rev. Stat. 603A.010 et seq
New Hampshire	1-Jan-07	N.H. Rev. Stat. §§ 359-C:19 - C:21; N.H. Rev. Stat. § 332-I:5
New Jersey	1-Jan-06	N.J. Stat. §§ 56:8-161, 163, 165 - 166
New Mexico	16-Jun-17	N.M. Stat. §§ 57-12C-1 - 57-12C-12
New York	7-Dec-05	N.Y. Gen. Bus. Law § 899-aa
North Carolina	1-Dec-05	N.C. Gen. Stat. §§ 75-61, 75-65
North Dakota	1-Jun-05	N.D. Cent. Code §§ 51-30-01 - 07
Ohio	17-Feb-06	Ohio Rev. Code §§ 1349.19 - 192
Oklahoma	1-Nov-08	Ok. Stat., Tit. 24, §§ 161 - 166
Oregon	1-Oct-07	Or. Rev. Stat. §§ 646A.600 - 646A.628
Pennsylvania	20-Jun-06	73 Pa. Stat. § 2301 et seq
Rhode Island	1-Mar-06	R.I. Gen. Laws §§ 11-49.3-1 - 11-49.3-6
South Carolina	1-Jul-09	S.C. Code Ann. § 39-1-90
South Dakota	1-Jul-18	SDCL §§ 22-40-19 - 22-40-26
Tennessee	1-Jul-05	Tenn. Code Ann. §§ 47-18-2105-2107
Texas	1-Apr-09	Tex. Bus. & Com. Code §§ 521.002, 521.053, 521.151-152
Utah	1-Jan-07	Utah Code §§ 13-44-101 et seq
Vermont	1-Jan-07	9 V.S.A. §§ 2430, 2435
Virginia	1-Jul-08	Va. Code § 18.2-186.6; Va. Code § 32.1-127.1:05; Va. Code § 58.1-341.2
Washington	24-Jul-05	Wash. Rev. Code § 19.255.010 et seq
West Virginia	6-Jun-08	W.V. Code § 46A-2A-101 et seq
Wisconsin	31-Mar-06	Wis. Stat. § 134.98
Wyoming	1-Jul-07	Wyo. Stat. §§ 40-12-501, 40-12-502

Appendix 5: Examples of Firms' Disclosure and Practitioners' Discussions

a. Target 2013 10K Disclosure

The Data Breach we experienced involved the theft of certain payment card and guest information through unauthorized access to our network. Our investigation of the matter is ongoing, and it is possible that we will identify additional information that was accessed or stolen, which could materially worsen the losses and reputational damage we have experienced. For example, when the intrusion was initially identified, we thought the information stolen was limited to payment card information, but later discovered that other guest information was also stolen.

b. *Assure Professional* Discussion on the Relationship between Audit and Target Data Breach (April 29, 2014)

The massive data breach that Target incurred this winter was a textbook example of why audits are so important, especially when it comes to financial data.

c. The SEC's Cease-and-Desist Order on Yahoo! for Failing to Disclose Data Breaches

2. Despite its knowledge of the 2014 data breach, Yahoo did not disclose the data breach in its public filings for nearly two years. To the contrary, Yahoo's risk factor disclosures in its annual and quarterly reports from 2014 through 2016 were materially misleading in that they claimed the company only faced the risk of potential future data breaches that might expose the company to loss of its users' personal information stored in its information systems, as well as potential future litigation, remediation, increased costs for security measures, loss of revenue, damage to its reputation, and liability, without disclosing that a massive data breach had in fact already occurred. Yahoo management's discussion and analysis of financial condition and results of operations ("MD&A") in those reports was also misleading to the extent it omitted known trends or uncertainties with regard to liquidity or net revenue presented by the 2014 data breach.

d. Examples of Discussions from Practitioners and the Media

FIRM MGMT

How Accountants Can Help Clients Avoid Data Breaches

CHRIS NOVAK, GLOBAL DIRECTOR, RISK TEAM WITH VERIZON ENTERPRISE SOLUTIONS ON APR 14, 2017

Ia INTERNAL AUDITOR

What Can Auditors Do About Data Breaches?

In the wake of the Target incident, internal auditors should provide assurance that basic security measures are in place in their organization's commerce system.

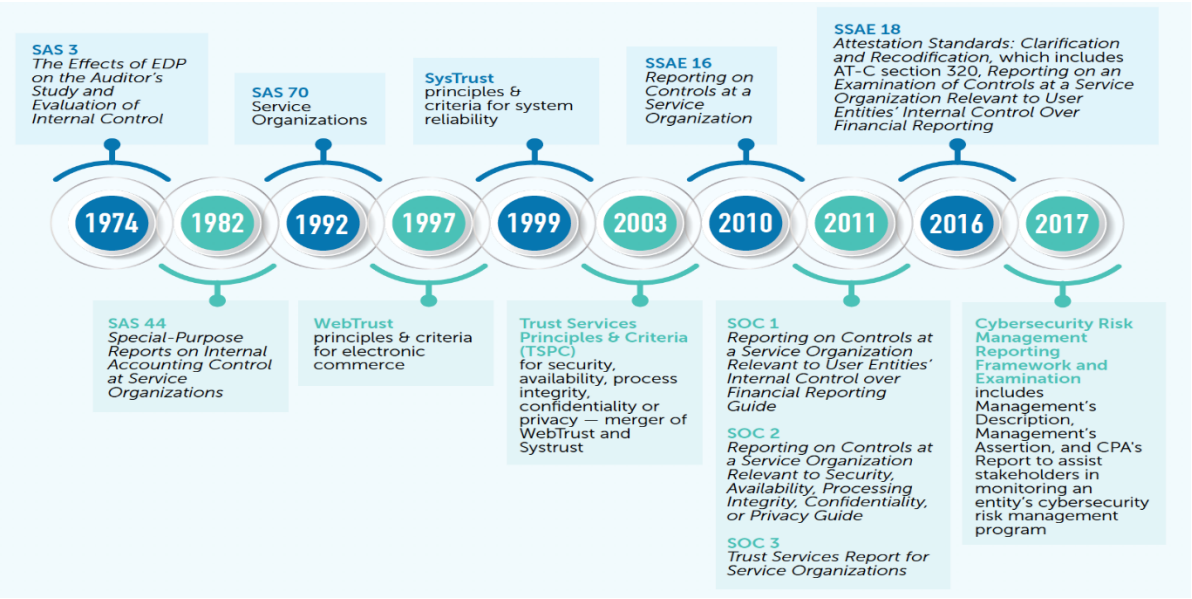
MarketWatch

Equifax auditors are on the hook for data security risk controls

By Francine McKenna
Published: Oct 3, 2017 9:50 a.m. ET

Before an auditor reviews numbers, it must make sure that execs set the right "tone at the top" on controls, including of IT systems

Auditing IT Controls *(Source: AICPA and Center for Audit Quality):*



One Example of Auditing Procedures on IT Controls: