# Audit Firm Assessments of Cyber-Security Risk:

# Evidence from Audit Fees and SEC Comment Letters

**Pierangelo Rosati**[*]
Irish Institute of Digital Business
DCU Business School

**Fabian Gogolin**
Leeds University
Business School

**Theo Lynn**
Irish Institute of Digital Business
DCU Business School

## ABSTRACT

This study investigates the impact of cyber-security incidents on audit fees. Using a sample of 5,687 firms, we find that (i) breached firms are charged 12 percent higher audit fees, (ii) firms operating in the same industry of a breached firm are charged 5 percent higher fees. Finally, using a difference-in-difference regression on a propensity score matched sample, we provide evidence suggesting that auditors do not revise their audit risk assessment following a breach. Overall, these results suggest that the increase in audit fees in the year of a breach is only temporary, and that auditors include cyber-security risk in their audit risk assessment even before an incident occurs. Higher cyber-security risk is ultimately reflected in higher audit fees paid by auditees.

**Keywords:** Audit Risk; Audit Fees; Cyber Security; SEC Comment Letters.

[*] Corresponding author: Irish Institute of Digital Business, DCU Business School, Dublin City University, Collins Avenue, Glasnevin, Dublin 9, Ireland. Mail: pierangelo.rosati@dcu.ie.

Acknowledgment: The research work described in this paper was supported by the Irish Centre for Cloud Computing and Commerce, an Irish National Technology Centre funded by Enterprise Ireland and the Irish Industrial Development Authority. We thank Rashad Abdel-Khalik (editor), Jessen L. Hobson (associate editor), two anonymous reviewers, and Aaron Yoon (discussant) for their careful and constructive guidance during the review process, and the attendees of the 30th Illinois Symposium of The International Journal of Accounting for their feedback.

## 1. Introduction

In this paper, we address the question of how external auditors respond to risks emanating from cyber-security incidents. In order to formally test this, we adopt audit fees as a proxy for audit effort and audit risk. Specifically, this study investigates two related questions. First, we examine whether firms that experience cyber-security incidents are charged higher audit fees in the year of an incident. Second, we assess whether cyber-security incidents result in a more long-lasting shift in audit fees.

As firms increasingly rely on collected, processed and stored data, the potential for damage resulting from cyber-security incidents has risen dramatically. While the media reports damages caused by hacker attacks on a daily basis, they are not the only type of cyber-security incidents. Gordon, Loeb & Zhou (2011, p. 35) define cyber-security incidents (or security breaches) as any event that compromises the confidentiality, integrity or availability of an information asset. As such, cyber-security incidents may consist of different types of events such as malware, ransomware or denial-of-service attacks, card payment fraud, malicious insiders, or even human error[1]. Cyber-security incidents are often difficult to detect and estimating their potential impact, for example in terms of records lost or stolen and associated direct and indirect costs, is a complex process. An exemplar case is the series of data breaches disclosed by Yahoo Inc. in late 2016. Although the first data breach was disclosed on September 22, 2016, the breach itself occurred in late 2014 when a hacker gained access to the firm's network and stole the account information of at least 500 million users (Perlroth, 2016). Similarly, Yahoo Inc. disclosed a second data breach on December 14, 2016 although this hack originally occurred in August 2013 (Thielman, 2016). As part of this attack, three billion user accounts were compromised and it represents, so far, the biggest data breach in history

[1] Appendix B provides a list of different types of cyber-security incidents included in our study and exemplar case for each breach type.

(Perlroth, 2017). Whether or not the two attacks were linked is still an open question. In both cases, the information stolen included names, email addresses, telephone numbers, dates of birth, hashed passwords and, in some cases, encrypted or unencrypted security questions (Perlroth, 2016; Thielman, 2016). The fact that it took more than two years for a large technology company, such as Yahoo Inc., to detect and confirm the intrusions and to estimate the number of records stolen, provides an idea of how complex and arduous such processes can be.

The implications of cyber-security incidents at firm-and market-level are well documented (Spanos & Angelis, 2016; Rosati et al., 2017; Kamiya et al., 2018). However, cyber-security incidents also affect a number of external stakeholders (Hovav & Gray, 2014). External auditors, in particular, have a number of reasons to be particularly concerned about cyber-security incidents affecting their clients. First and foremost, when a cyber-security incident occurs, external auditors are responsible for evaluating the client's accounting for losses, claims and liabilities related to the incident, and for assessing the ultimate impact on the financial statements (CAQ, 2014). Firms that suffer cyber-security incidents find themselves facing numerous and unexpected direct and indirect costs. Direct costs include remediation costs, legal fees, fines, and lost transactions (Aral, Dellarocas, & Godes, 2013). For example, ChoicePoint was fined $10 million and had to pay another $5 million to compensate affected individuals (Federal Trade Commission - FTC, 2009). Similarly, Nasdaq and BATS suffered a 24-hour cyber-attack to their website which led to a 12-percent decline in US daily trading activity (Krudy, 2012; Savitz, 2012). Indirect costs include loss of present and future revenues as well as the deterioration of customer and partner trust (Aral, Dellarocas, & Godes, 2013; Cavusoglu, Mishra, & Raghunathan, 2004; Charette, Adams, & White, 1997; Dennis, Wixom, & Tegarden, 2015). Such costs are, by definition, difficult to estimate; therefore, they imply

some degree of discretion[2], which ultimately may increase the risk for the external auditor (Abbott, Parker & Peters, 2006).

Second, cyber-security incidents may also signal potential failures in relation to internal control over financial reporting (ICFR) (Lawrence, Minutti-Meza & Vyas, 2018). External auditors are legally responsible for detecting such deficiencies in internal controls. Given the increasing use of IT for financial reporting as well as for other business activities, and the increasing interconnected nature of modern business IT systems along the value chain, auditors are now practically required to extend their audits to other systems that could potentially be exploited for unauthorized access, irrespective of whether the system directly relates to financial reporting and accounting. In fact, operating and financial reporting activities tend to rely more and more on shared controls. As such, a weakness in one area might affect the other (Lawrence et al., 2018). In this context, it is not completely surprising that the Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 12 explicitly requires auditors to obtain an understanding of how their clients use information technology (IT) and the impact of IT on financial statements (PCAOB, 2013). More specifically, auditors are held accountable for testing and monitoring the access controls their auditees implement, and evaluating cyber-security threats in their audit risk model. The financial statement audit, and the audit of ICFR, include procedures with respect to a company's financial reporting systems and evaluating the risks of material misstatement resulting from unauthorized access to such systems (CAQ, 2014; Joe et al., 2015; PCAOB, 2010). Personal interviews with senior IT auditors in the Big 4 audit firms [3] provided further confirmation on this point. Cyber-security risk has become more and more important as part of the audit risk assessment; auditing IT systems not strictly related to

[2] For example, Home Depot, which was breached in 2014, reported "$252 million of pretax gross expenses due to the data breach, partially offset by $100 million of expected insurance proceeds" in its 10-Q (Coleman, 2015). Furthermore, they forecast that they would "incur additional legal and other professional services expenses associated with the data breach in future periods" (Coleman, 2015).
[3] One from Ernst&Young, KPMG and PricewaterhouseCoopers, and two from Deloitte.

financial reporting typically represents a source for additional audit evidence.

Third, external auditors are subject to growing pressure from regulators and standard setters in relation to cyber-security. The Centre for Audit Quality (CAQ), for example, has repeatedly highlighted the fact that auditors must pay particular attention to these types of incidents (CAQ, 2014; 2016), and that auditors can play a significant role in preventing and/or mitigating the effects of these incidents by providing additional assurance around the IT controls of their clients (CAQ, 2017). In a similar vein, the Security Exchange Commission (SEC) has increased its disclosure requirements in relation to cyber-security risk. Such risk must now be explicitly discussed in the financial statements (SEC, 2011; 2014; 2015; 2018). Finally, a recent report from the PCAOB has further reiterated that cyber-security represents an evolving risk for auditors that requires ongoing focus, and that risk remains even when a past incident has not affected ICFR, as it may highlight potential vulnerabilities (PCAOB, 2018).

Given the discussion above, it clearly emerges that cyber-security breaches, irrespective of their nature, have potential implications for auditors. We hypothesize that, when a cyber-security incident occurs, external auditors exert additional effort in order to assess the implications for a firm's financial reporting and consequently mitigate an increase in audit risk. As a result of the additional effort, we expect to observe an increase in audit fees (Pratt & Stice, 1994; Bell, Landsman, & Shackelford, 2001; Frino, Palumbo, & Rosati, 2017). However, auditors are also required to assess their clients' risk related to cyber-security irrespective of whether they have been affected by a breach already. Cyber-security risk should be included into clients' IT risk assessment and, as such, be part of the overall audit risk assessment (PCAOB, 2013). Hogan and Wilkins (2008) suggest that auditors increase their fees in the year before the disclosure of internal control weaknesses to reflect the additional effort required to gather additional audit evidence. As cyber-security incidents may signal for potential weaknesses in internal controls, we expect to see a similar pattern in the years prior to an

incident. As such, we further hypothesize that if auditors are able to properly assess the cyber-security risk of client firms, they should charge higher fees to riskier clients even before a breach occurs. In this instance, we expect to see no significant differences in audit fees for breached clients before and after an incident. In other words, we expect that any change in audit fees in the year of a breach should be temporary and likely due to additional costs related to remediation and investigation activities, and that audit fees revert to pre-incident levels when the incident is resolved.

Using a sample of 168 cyber-security incidents from 2005 to 2014, we find that external auditors charge, on average, 12 percent higher audit fees to breached firms in the year of an incident. We find evidence that incidents due to failures of internal controls, rather than external access control, result in a more significant increase in audit fees. We also find that the results cannot be explained by past breaches or the number of years passed since the last breach. In addition, we document the existence of a contagion effect within industries with auditors charging, on average, five percent higher audit fees to firms operating in the same industry as a breached firm.

Further, we find evidence that the effect of cyber-security incidents on audit fees is only temporary as audit fees revert to a pre-incident level a year after the incident. Using a propensity score matched sample and a difference-in-difference (DID) approach, we show that breached firms pay, on average, nine percent higher fees than non-breached firms both in the pre- and post-breach periods. These results suggest that auditors are able to identify, among firms with a similar cyber-risk profile, those firms which are more likely to be breached and include such higher risk in their audit fees.

In order to understand whether auditors rely only on their audit evidence when assessing cyber-security risk, or integrate them with other external information, we analyze a subsample of

firms that have received an SEC Comment Letter related to cyber-security. This reveals that auditors revise their audit fees upwards in the periods following the Comment Letter, and further suggests that auditors consider Comment Letters related to cyber-security as a signal of potential higher audit risk. Overall, our results indicate that auditors incorporate cyber-security risk as part of their audit risk assessment.

We include a number of robustness tests to ensure that our results are not driven by omitted or unobserved variables. First, we re-estimate our main analysis using abnormal audit fees as our independent variable (Blankley, Hurtt, & MacGregor, 2012; Choi, Kim, & Zang, 2010, Han et al., 2016). Second, we include a measure of IT control weaknesses in our regression specification as per Canada, Sutton and Randel Kuhn Jr (2009). Third, we take several measures to control for endogeneity. We re-run our main analysis using a propensity-score matched sample and adopt a Heckman (1979) two-stage regression approach. Finally, to further ensure the reliability of our DID analysis, we run the DID analysis using different time periods and on an entropy balanced matched sample. Our tests collectively confirm the robustness of our results and the positive association between cyber-security and audit fees.

In a work that most closely aligns to ours, Li, No, & Bortiz (2016) provide evidence suggesting that auditors increase their audit fees the year prior a cyber-attack and that such an increase is lower for firms that have experienced a cyber-attack in the past. Our study corroborates but also extend this work, differing in a number of important respects. Firstly, our study investigates the effect of not only malicious external attacks, but also the effect of different types of cyber-security incidents. In fact, while cyber-attacks attract most of the media attention, there is a larger variety of incidents that firms might have to deal with and that might signal for potential control deficiencies; some of them may potentially be more dangerous than external attacks. It may be easier for a malicious insider, for example, to steal confidential information than it is for an outsider. Secondly, our study provides a more comprehensive analysis of the changes in

audit fees around cyber-security incidents by looking at changes pre- and post-incidents, and by investigating whether a spill-over effect within industries emerges.

This study contributes to the auditing literature in at least three ways. First, this study extends the literature on audit risk. We provide evidence that external auditors explicitly account for cyber-security related risks and include them in to their risk assessment. Even though information technology is already regarded as a contributor to audit risk (PCAOB, 2010; COSO, 2013), empirical evidence is still limited and focuses on auditees' IT capabilities (Chen et al., 2014) and IT investments (Han et al., 2016), rather than cyber-security incidents. To our knowledge, this is one of the first studies to explicitly consider the relationship between cyber-security risk, audit risk, and fees charged for auditing services, and the first to investigate whether auditors include cyber-security risk in their audit risk assessment before the incidents occur.

Second, this study also contributes to the extensive literature on the effectiveness of audit risk assessment by providing empirical evidence that cyber-security risk is included in auditors' risk models. While previous studies on audit risk have typically focused on auditors' ability in assessing the risk of financial frauds (Hammersley, Johnstone, & Kadous, 2011; Boritz, Kochetova-Kozloski, & Robinson, 2014), this study is the first to investigate auditors' ability to effectively detect a new and significant risk factor, cyber-security risk, before an incident occurs.

Third, we provide novel evidence showing how external auditors use SEC Comment Letters as an external source of information and include them in their audit risk assessment. Despite the interest Comment Letters have stimulated in the research community, empirical studies directly relating SEC Comment Letters to audit risk are scarce (Gietzmann & Pettinicchio, 2014). While Gietzmann and Pettinicchio (2014) analyze the effect of Comment Letters on

audit risk from a general perspective, our study provides a unique contribution to this literature by investigating the effect of Comment Letters explicitly related to cyber-security on audit risk.

The rest of the paper is organized as follows. In Section 2, we discuss prior literature on audit fees and on the effects of cyber-security incidents, and present our hypothesis. In Section 3, we describe the data used in this study and outline the research methodology. Section 4 presents the results of the empirical analysis, while Section 5 describes our robustness tests. Finally, in Section 6, we discuss our results, research limitations, and considerations for future research.

## 2. Background and Hypothesis

Audit fees compensate auditors for auditing services and are typically determined by both the amount of work an auditor must perform (i.e. audit effort) and the audit risk (Pratt & Stice, 1994; Bell, Landsman & Shackelford, 2001; Frino, Palumbo, & Rosati, 2017). Audit risk, in particular, is a function of two factors: (i) the risk of material misstatement, which is the risk that the financial statements are materially misstated prior to the audit; and (ii) detection risk, which is the risk that the auditor will not detect individual or aggregated misstatements (Lobo & Zhao, 2013). The auditing literature suggests that auditors counteract an increase in the risk of material misstatement by increasing their audit effort to lower detection risk resulting in an increase in audit fees (Allen et al., 2006; Budescu, Peecher, & Solomon, 2012; Hogan & Wilkins, 2008).

There is a well-established research base on different determinants of audit risk and audit fees. Existing research suggests that audit fees depend on company size (Simunic, 1980; Koh & Tong, 2013; Gietzmann & Pettinicchio, 2014; Han et al., 2016), auditee complexity (Craswell, Francis, & Taylor, 1995; Choi et al., 2008; Hogan & Wilkins, 2008; Han et al., 2016), asset structure (Stice, 1991; Sundgren, 1998; Krishnan & Visvanathan 2009), financial condition (Stice, 1991; Craswell, Francis, & Taylor, 1995; Chang & Hwang, 2003; Desai, Hogan, &

Wilkins, 2006;), business risk (Bell, Landsman, & Shackelford, 2001; Koh & Tong, 2013), earnings quality (Becker et al., 1998; Bartov, Gul & Tsui, 2000; Bedard & Johnstone, 2004; Abbott et al., 2006; Dechow, Ge, & Schrand, 2010), corporate governance (Chen et al., 2014; Srinidhi, Yan, & Tayi, 2015), and regulatory environment (Jaggi & Low, 2011; Su & Wu, 2017). Furthermore, researchers have also considered the effect of external monitoring on audit risk. Empirical evidence suggests that additional external monitoring, as provided by short-term lenders or credit rating agencies, also lowers audit risk (Gul & Tsui, 1997; Gul & Goodwin, 2010).

More recently, following a growing interest from regulators, policy makers and standard setters, an emerging stream of research has focused on the link between information technology, audit risk and audit fees. Chen et al. (2014) posit that auditees' IT capabilities lead to strong internal controls and, therefore, to a decrease in auditors' risk and audit fees. Han et al. (2016) provide evidence of a positive relationship between auditees' IT investments, audit risk, and the probability of auditors' issuance of a going-concern opinion. While providing interesting insights with regard to the interplay between information technology and audit risk, the extant research does not specifically address the rising concerns with respect to cyber-security.

The growing use of the Internet, cloud computing, and mobile devices have left firms vulnerable to cyber-security risks and contributed to a surge of cyber-security incidents (Romanosky, Hoffman, & Acquisti, 2014; Abbasi, Sarker, & Chiang, 2016). Cyber-security incidents can result in significant damage to breached firms in terms of remediation costs, fines, and reputation (Cavusoglu, Mishra, & Raghunathan, 2004; Gordon, Loeb, & Zhou, 2011; Rosati et al., 2017). Prior studies also show that cyber-security incidents can lead to a loss in market value up to five percent (Campbell et al., 2003; Garg, Curtis, & Halper, 2003), and that such an impact varies depending on the type of incidents, the industry a firm operates in, the

time period examined, and a firm's visibility (Gordon, Loeb & Zhou, 2011; Rosati et al., 2019).

However, while cyber-security incidents represent an obvious threat for breached firms, they also carry risks for external auditors (CAQ 2014; Joe et al. 2015). External auditors provide objective and independent assurance with respect to the quality of a firm's financial reporting and are responsible for auditing financial statements and internal controls over financial reporting (ICFR) (Christopher, Sarens, & Leung, 2009; Stefaniak, Houston, & Cornell, 2012; CAQ 2014; Kajüter, Klassmann, & Nienhaus, 2016; Frino, Palumbo, & Rosati, 2017). As such, they provide assurance to external stakeholders about the quality and reliability of the information reported in the financial statements of their clients.

Cyber-security incidents, irrespective of their nature, impact external auditors in at least three ways. First of all, auditors are required to evaluate the impact of such incidents on the financial statements (CAQ, 2014). This is not a trivial exercise as cyber-security incidents generate direct (and typically short-term) costs which are simple enough to quantify (e.g. fines, remediation costs, legal services, etc.), but also indirect (long-term) costs (e.g. loss of business opportunities, revenue and customer trust), the quantification of which are difficult to quantify objectively and involve a greater degree of discretion by management. As such, indirect costs typically result in higher audit risk (Abbott et al., 2006). Secondly, the use of information technology in financial reporting impacts external auditors. While IT serves as the foundation of more effective internal controls, it also increases the vulnerability of firms to IT-related risks, such as cyber-security risks (Masli et al., 2010; Li, Sun, & Ettredge, 2010; Haislip et al., 2016). Prior research has linked cyber-security incidents to potential internal control weaknesses (Chernobai, Jorion, & Yu, 2011; Benaroch, Chernobai, & Goldstein, 2012; Lawrence et al., 2018). Cyber-security risk can materialize in the form of so called "more-than-reporting" control weaknesses (Feng, McVay, & Skaife, 2014) (e.g. IT control weaknesses), or as "financial reporting-only" weaknesses (Hogan and Wilkins, 2008). As such, external

auditors must carefully evaluate and understand the strengths and weaknesses of firms' information technology and incorporate those in their risk assessment (PCAOB, 2013; Joe et al., 2015). Finally, auditors face growing pressure from standard setters to play a more active role in preventing and assessing the consequences of cyber-security incidents (CAQ, 2014; 2016; 2017; PCAOB, 2018). Similarly, the SEC has recently issued, after many years of debates, disclosure guidance that requires firms to discuss cyber-security risk in their financial statements (SEC, 2018).

Based on the above discussion, we posit that cyber-security incidents represent real concerns for external auditors. As such, the disclosure of a cyber-security incident increases the risk for the external auditor. This typically triggers an increase in audit effort, which ultimately translates in higher audit fees. Our first hypothesis is stated as follows:

**H1:** The disclosure of cyber-security incidents is associated with a contemporaneous increase in audit fee for the affected firm.

PCAOB Auditing Standard No. 8 states:

> "to form an appropriate basis for expressing an opinion on the financial statements, the auditor must plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement due to error or fraud. Reasonable assurance is obtained by reducing audit risk to an appropriately low level through applying due professional care, including obtaining sufficient appropriate audit evidence" (PCAOB, 2010).

This implies that auditors are expected to identify existing or potential risk factors and to adjust their audit risk assessment accordingly. With respect to cyber-security incidents, an incident may signal a weakness in IT controls, which would raise the risk of failure in the financial

reporting system and hence the audit risk (Hammersley, Myers, & Shakespeare, 2008; Klamm, Kobelsky, & Watson, 2012; Haislip et al., 2016). However, auditors should be able to accurately assess cyber-security risks and price those risks before a firm has been breached. Hence, if auditors properly assess the cyber-security risk of their auditees, audit fees should not increase after the occurrence of an incident. Our second hypothesis is stated as follows:

**H2:** Following a cyber-security incident, audit fees revert to pre-breach levels.

## 3. Sample Selection and Research Design

### *3.1 Sample Selection*

We begin the construction of our sample by identifying all firms in the Audit Analytics Audit Fees database from 2003 to 2015. From this sample, we eliminate (i) financial firms (SIC Codes 6000-6999) due the different nature of their financial statements[4], (ii) firms which are not in Compustat, (iii) firms with missing data, and (iv) firms with non-Big4 auditors[5]. The final sample includes 5,687 firms, corresponding to 40,771 firm-years.

To identify the cyber-security incidents, we use the Privacy Rights Clearinghouse[6] (PRC) database. This database reports detailed information about cyber-security incidents that affected US citizens and were subject to mandatory disclosure since 2005 as collected through either government agencies or verifiable media sources. Security Breach Notification Laws[7]

[4] Appendix C reports the frequency distribution of incidents in our original list of breaches across different industries. Even though financial firms account for approximately 33 percent of the events in our original dataset, the nature of their financial statement makes it hard to compare their financial ratios with the ones obtained by non-financial firms. Such ratios are typical control variables in audit fees models.

[5] Previous studies report that Big 4 auditors provide higher audit quality (Eshleman & Guo, 2014) and stricter controls (Krishnan, Rama, & Zhang, 2008; De Franco et al., 2011), and are able to charge higher fees to their clients (Choi et al., 2008) than non-Big4 auditors. As such, we include only firms audited by Big 4 auditors to ensure homogeneity in terms of audit quality (Blankley, Hurtt, & MacGregor, 2012). In our original list of cyber-security incidents, only 10 firms were audited by non-Big 4 auditors when the incident occurred. This may be interpreted as a further confirmation of the fact that Big 4 auditors have more resources and expertise in relation to cybersecurity than non-Big 4 and therefore can ensure higher audit quality.

[6] Privacy Rights Clearinghouse is a California based nonprofit corporation. The organization looks to, among other activities, identify trends in privacy protection and communicate its findings to advocates, policymakers, industry, media and consumers. Detailed information on data breaches is available at http://www.privacyrights.org/data-breach. Examples of studies that adopted this dataset include Garrison & Ncube (2011), Higgs et al. (2016), Rosati et al. (2017), and Rosati et al. (2019).

[7] The first SBNL was enacted in California in 2002. Since then forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted their own SNBLs (NCSL, 2017).

(SBNLs) require mandatory and timely notification of a security breach if personally identifiable information has been lost, or is likely to be acquired by an unauthorized person (Romanosky, Telang, & Acquisti, 2011). The timeliness of the disclosure is particularly important in order to limit possible harm (Romanosky, Hoffman, & Acquisti, 2014). It is worth noting that some security breaches may only be discovered after a significant amount of time[8], and that, in some instances, the exact time and duration of the intrusion may not be determined[9]. However, SBNLs' disclosure requirements allow researchers to consider the disclosure date of an incident as a close approximation of the discovery date (Rosati et al., 2017).

Unlike other types of corporate events (e.g. M&A, earnings announcement etc.), it is difficult to compile a fully exhaustive list of cyber-security breaches since "many organizations are not aware they have been breached or are not required to report it based on reporting laws" (PRC, 2017). However, the wide adoption of Security Breach Notification Laws (SNBLs) across different states, their increasing disclosure requirements, and the fact that PRC gathers information from multiple information sources, mitigate potential sampling biases in the database. This dataset includes 4,537 cyber-security incidents disclosed by firms, non-profit organizations, healthcare organizations and government agencies in the US from April 2005 to December 2014. To distinguish between different types of cyber-security incidents, we do not restrict our sample to hacker attacks[10] and include in our sample includes different types of cyber-security incidents (see Table 2 and Appendix B further details). The final sample consists of 168 breached firms and 5,519 non-breached firms. Table 1 provides a summary of the sample construction.

*Insert Table 1 here*

[8] The case of Yahoo Inc. reported in the introduction is a typical example.
[9] Facebook Inc., for example, reported that "the breach began sometime in 2012" when disclosing a six-million records security breach on 21 June 2013.
[10] Even though hacker attacks grab most of the media and public attention, they represent only part of the wide range of cyber-security incidents organizations may face (PwC, 2016).

*3.2 Research Design*

Following prior studies (e.g., Hogan & Wilkins, 2008; Han et al., 2016; Frino, Palumbo, & Rosati, 2017), we adopt audit fees as a proxy for audit risk. Audit fees are the compensation auditors require for their auditing services and depend on audit effort, litigation risk, and normal profits (Simunic, 1980; Choi et al., 2008). Given that the data are cross-sectional and time-series in nature, we calculate t-statistics using the robust cluster technique suggested by Petersen (2009) to reduce concerns about heteroscedasticity and autocorrelation.

To test the effect of cyber-security incidents on audit fees (H1), we adopt the following regression model:

$$\begin{aligned} LAF_{i,t} = \beta_0 + \beta_1 BREACH_{i,t} + \beta_2 LTA_{i,t} + \beta_3 LEV_{i,t} + \beta_4 CUR_{i,t} \\ + \beta_5 QUICK_{i,t} + \beta_6 ROA_{i,t} + \beta_7 DEBTEQ_{i,t} + \beta_8 YE_{i,t} \\ + \beta_9 BUSSEG_{i,t} + \beta_{10} FOREIGN_{i,t} + \beta_{11} ICWEAK_{i,t} \\ + \beta\ Industry\ Indicators + \beta\ Year\ Indicators + \varepsilon_{i,t} \end{aligned} \quad (1)$$

where:

| | | |
|---|---|---|
| *LAF* | = | natural logarithm of audit fees; |
| *BREACH* | = | 1 if a firm experiences a cyber-security incident in year *t*, 0 otherwise; |
| *LTA* | = | natural logarithm of end of year total assets; |
| *LEV* | = | current liabilities divided by total assets; |
| *CUR* | = | current assets divided by total assets; |
| *QUICK* | = | difference between current assets and inventory divided by current liabilities; |
| *ROA* | = | earnings before interest and taxes divided by total assets; |
| *DEBTEQ* | = | total debt divided by equity book value; |
| *YE* | = | 1 if a firm's fiscal year does not end on December 31, 0 otherwise; |
| *BUSSEG* | = | natural logarithm of the number of business segments in which a firm operates; |
| *FOREIGN* | = | foreign sales divided by total sales; |
| *ICWEAK* | = | 1 if a firm's internal controls were not found to be effective under Section 302 of the Sarbanes-Oxley Act of 2002, 0 otherwise; |
| *Year Indicators* | = | year indicators; |
| *Industry Indicators* | = | industry indicators based on two-digit SIC codes; |
| $\varepsilon$ | = | error term. |

Audit fees reflect the economic costs of auditors and are known to vary with size, complexity, riskiness, and other client-specific characteristics (Johnstone & Bedard, 2003; Gul & Goodwin, 2010). Consistent with prior studies (e.g. Gul & Goodwin, 2010; Hay & Knechel, 2010; Frino,

Palumbo, & Rosati, 2017), we include control variables for all these factors. Firm size (*LTA*) controls for audit effort, while the number of business segments (*BUSSEG*) and the proportion of foreign sales to total sales (*FOREIGN*) control for firms' complexity. In order to control for inherent audit risk, we include the quick ratio (*QUICK*) and the ratio of current assets to total assets (*CUR*). Other factors that typically affect audit risk are firms' profitability (*ROA*), leverage (*LEV*), debt-to-equity ratio (*DEBTEQ*), and internal control weaknesses (*ICWEAK*). Finally, we include control variables for off-peak fiscal year-end (*YE*).

Previous studies suggest that the impact of a cyber-security incident might depend on its cause (Cavusoglu, Mishra, & Raghunathan 2004; Gordon, Loeb, & Zhou, 2011). In order to address this potential concern, we include in our regression model an indicator variable for each type of incident as classified by PRC (Posey et al., 2017; Rosati et al., 2019). *CARD* is an indicator variable equal to 1 if a cyber-security incident was due to payment card fraud and 0 otherwise; *DISC* is an indicator variable equal to 1 if a cyber-security incident was due to unintended disclosure and 0 otherwise; *HACK* is an indicator variable equal to 1 if a cyber-security incident was due to a malicious outsider attack and 0 otherwise; *INSD* is an indicator variable equal to 1 if a cyber-security incident was due to malicious insider(s) and 0 otherwise; *PHYS* is an indicator variable equal to 1 if a cyber-security incident was due to unauthorized physical access and 0 otherwise; *PORT* is an indicator variable equal to 1 if a cyber-security incident was due to stolen or lost portable device(s) and 0 otherwise; *STAT* is an indicator variable equal to 1 if a cyber-security incident was due to stationary device(s) and 0 otherwise; and *UNKN* is an indicator variable equal to 1 if a cyber-security incident was due to an unknown cause and 0 otherwise.

Previous studies (e.g. Hribar, Kravet & Wilson, 2014) provide evidence supporting the idea that not only current, but also past and future events may be associated with changes in audit

fees. In order to test whether past or future cyber-security incidents have a significant effect on audit fees, we include the following two variables in the regression model: *BREACH_T-1*, an indicator variable equal to 1 if a firm reported a cyber-security incident in the past fiscal year and 0 otherwise; and *BREACH_T+1*, an indicator variable equal to 1 if a firm reported a cyber-security incident in the following fiscal year and 0 otherwise.

SBNLs require breached firms to disclose incidents in a timely manner. However, they do not provide specific cut-off times; also, incidents disclosure "may be delayed if necessary to avoid impeding a criminal investigation" (Winn, 2009, p. 1142). This means that incidents disclosed within a fiscal year might have been discovered in the previous fiscal year and not disclosed. This may be more likely for events disclosed early in the fiscal year. Similarly, auditors' investigation and remediation may span over multiple fiscal years particularly if the incident is disclosed towards the end of the fiscal year. In order to control for these potential effects, we sourced the date when each incident was disclosed as reported by PRC[11] and estimated the number of days to the next fiscal year end. We run the regression model presented above on the subsample of breached firms in the year of the breach only and include the variable *BREACH_TO_NEXT_FYEND*, which is equal to the natural logarithm of the number of days to between the disclosure date and the end date of the fiscal year as reported on Compustat. We also regress the same variable on audit fees of the previous and of the following fiscal year.

Prior incidents might also affect the impact of a cyber-security incident (Gatzlaff & McCullough, 2010; Rosati et al. 2017) with auditors potentially charging higher fees to firms which have been breached in the recent past. In order to establish whether past incidents matter, we run the regression model presented above on the subsample of breached firms and alternatively include in the model the following two variables: *PAST_BREACH*, an indicator

[11] In order to make sure that breaches did not become public in earlier dates, we checked on Lexis-Nexis whether any media outlet reported any incident within seven days before the announcement date as per Rosati et al. (2019).

variable equal to 1 if a firm was breached in the past and 0 otherwise; and $\Delta YR\_PAST\_BREACH$ which measures the number of years since the last recorded incident.

Finally, there might be a contagion effect within industries (Zafar, 2012; Kashmiri, Nicol, & Hsu, 2017) with auditors charging higher fees to non-breached firms operating in the same industry. In order to assess whether such a contagion effect exists, we add the following two variables to our regression model: *PEER_BREACH*, an indicator variable equal to 1 if a cyber-security incident occurred in the previous fiscal year[12] within a given industry and 0 otherwise; *N_PEER_BREACH*, which measures the number of cyber-security incidents that occurred within a given industry in the previous fiscal year.

The regression model presented in Equation (1) investigates whether auditors charge higher fees when a cyber-security incident occurs, but it does not reveal whether such an increase is due to (a) the incident (and therefore short-term); (b) an increase in cyber-security risk (and therefore long-term); or (c) a higher cyber-security risk embedded in the auditor's risk assessment in advance of the incident. In order to disentangle this issue, and to address our second hypothesis, we perform a difference-in-difference (DID) analysis[13] on a propensity-score matched sample for breached firms as outlined by Lechner (2011). DID estimation is a well-established methodology to estimate causal relationships and represents an effective way to circumvent many of the endogeneity problems that typically arise when making comparisons between heterogeneous individuals or organizations (Bertrand, Duflo, & Mullainathan, 2004). Further, when compared to standard fixed effects, DID has the advantage of allowing to pull together in a single regression many changes and years producing more precise and robust results (Duflo, 2002). We use a DID analysis to compare the average level of audit fees paid

[12] Anecdotal evidence suggest that audit fees are negotiated at the beginning of the fiscal year when the auditing plan is approved and that they are unlikely to change unless any extraordinary event occurs to the auditee.
[13] "The difference-in-difference technique is a powerful way of controlling for random causes of changes in the dependent variable over time, and for addressing heteroscedasticity and auto-correlation" (Knechel & Sharma 2012, p. 105).

by breached (i.e. treatment sample) and non-breached firms (i.e. control sample) in the pre- and post-breach periods. If the effect of cyber-security incidents is only temporary (i.e. short-term), the level of audit fees paid by breached firms should not change significantly after the breach. On the contrary, if a breach leads to a reassessment of the audit risk of the affected firm, it would result in higher audit fees for the breached firm after the incident.

To build the control sample we perform a one-to-one propensity-score matching between breached and non-breached firms within the same industry and with the same probability of being breached. The intuition behind a matched-pair design is that, by matching firms from the same time-periods, industries, and other characteristics, the potential problems associated with correlated omitted variables are mitigated (Gordon, Loeb, & Sohail, 2010).

We adopt a propensity score matching approach consistent with Lawrence, Minutti-Meza, and Zhang (2011). Specifically, we estimate a cyber-security prediction model, and obtain probability estimates of being affected by a cyber-security incident. We then perform a one-to-one match between non-breached (i.e. control sample) and breached firms (i.e. treatment sample) based on the predicted value within the same industry and fiscal year, with no replacement and with a maximum distance of three percent[14].

Following Higgs et al. (2016), we estimate the probability of being breached with the following logistic regression:

$$\begin{aligned} Prob(BREACH = 1) = {} & \beta_0 + \beta_1 LTA_{i,t} + \beta_2 R\&D_{i,t} + \beta_3 LEV_{i,t} + \beta_4 LOSS_{i,t} \\ & + \beta_5 RISK\_COMMITTEE_{i,t} + \beta_5 COMP\_COMMITTEE_{i,t} \\ & + \beta_5 TECH\_COMMITTEE_{i,t} + \varepsilon_{i,t} \end{aligned} \quad (2)$$

where:

*BREACH* = 1 if a firm experiences a cyber-security incident in year *t*, 0 otherwise;
*LTA* = natural logarithm of end of year total assets;
*R&D* = natural logarithm of research and development expenses;

[14] We also perform a more restrictive matching with a maximum distance of one percent and the results (not tabulated) are consistent.

| | | |
|---|---|---|
| *LEV* | = | current liabilities divided by total assets; |
| *LOSS* | = | 1 if a firm reported negative net income, 0 otherwise; |
| *RISK_COMMITTEE* | = | 1 if a firm discloses the presence of a board-level committee with the word 'Risk' in the title in the proxy statement released prior to the date of the breach, 0 otherwise; |
| *COMP_COMMITTEE* | = | 1 if a firm discloses the presence of a board-level committee with the word 'Compliance' in the title in the proxy statement released prior to the date of the breach, 0 otherwise; |
| *TECH_COMMITTEE* | = | 1 if a firm discloses the presence of a board-level committee with the word 'Technology' in the title in the proxy statement released prior to the date of the breach, 0 otherwise; |
| $\varepsilon$ | = | error term. |

We control for firms' size (*LTA*) since large firms are more attractive breach targets (Premuroso & Bhattacharya, 2007; Higgs et al., 2016), but are also expected to implement better security controls and to have more resources to be invested in cyber-security than small firms (Gatzlaff & McCullough, 2010; Hovav & Gray, 2014). We control for firms' profitability since less profitable firms are less attractive breach targets (Premuroso & Bhattacharya, 2007; Higgs et al., 2016). We also control for auditee's financial conditions (*LEV*) since healthier firms tend to have larger resources to dedicate to cyber-security (Srinidhi, Yan, & Tayi, 2015) and fewer internal control weaknesses (Doyle, Ge, & McVay, 2007). Finally, we control for the presence of risk, compliance or technology committees since the existence of such committees has been found to be positively related with the probability of being breached (Higgs et al., 2016). Our sample matching takes into account factors which have been found to be correlated with the probability of being breached and, potentially, with audit risk. When assessing the audit risk of their clients, auditors carry on more in-depth analysis which goes well beyond the characteristics here considered. Therefore, if auditors are able to really discern clients which have a higher risk of being affected by a cyber-security incident, a difference between the treatment and the control sample should still be visible.

For each pair of firms, we first compare the audit fees charged in the two years prior to the breach, to those charged in from the incident onwards (0;+2) (DID I). Therefore, the pre-breach

period includes the two fiscal years before the breach (i.e. *t-2* and *t-1*), while post-breach period includes the three fiscal years after the breach (i.e. *t*, *t+1* and *t+2*). If a significant difference exists between the pre- and post-event periods, we can establish whether cyber-security incidents led to a revision in audit risk, and hence in audit fees. Our treatment sample includes breached firms which did not experience any cyber-security incidents in the two years before or after the incident which represents the focus of our analysis. Our control sample includes firms whose probability of being breached is comparable to the matched firms in the treatment sample, and that were not breached during the whole period of our analysis. However, one may argue that the year of a cyber-security incident is likely to be significantly different from other fiscal years. As such, an exceptional increase in audit fees due to remediation costs in that fiscal year may drive the results in the post-incident period. Therefore, in order to provide an "apple-to-apple" comparison between pre- and post- periods, we also adopt an alternative specification of the DID model. In this alternative specification (DID II), we exclude the year in which the incidents occur in order to directly compare the fees paid by breach and non-breached firms in the pre- (i.e. *t-2* and *t-1*) and post-event periods (i.e. *t+1* and *t+2*).

Figure 1 provides a graphical representation of the timeline adopted in our analysis.

*Insert Figure 1 here*

To test whether auditors include cyber-security risk in their audit risk assessment regardless an incident's occurrence or not (H2), we adopt the following regression model:

$$\begin{aligned} LAF_{i,t} = {} & \beta_0 + \beta_1 TREATMENT_{i,t} + \beta_2 POST_{i,t} + \beta_3 TREATMENT_{i,t} \times POST_{i,t} \\ & + \beta_4 LTA_{i,t} + \beta_5 LEV_{i,t} + \beta_6 CUR_{i,t} + \beta_7 QUICK_{i,t} \\ & + \beta_8 ROA_{i,t} + \beta_9 DEBTEQ_{i,t} + \beta_{10} YE_{i,t} + \beta_{11} BUSSEG_{i,t} \\ & + \beta_{12} FOREIGN_{i,t} + \beta_{13} ICWEAK_{i,t} + \beta\ Industry\ Indicators \\ & + \beta\ Year\ Indicators + \varepsilon_{i,t} \end{aligned} \quad (3)$$

Where *TREATMENT* is an indicator variable equal to 1 if a firm belongs to the treatment sample (i.e. the firm has been breached during the period of analysis) and 0 otherwise; *POST*

is an indicator variable equal to 1 if year *t* is after a cyber-security incident and 0 otherwise; *TREATMENTxPOST* is our DID estimator, and all other variables are as defined above. If there is no difference between the treatment and the control sample before a cyber-security incident, the regression coefficient of *TREATMENT* would be non-significant; conversely, if a difference exists after a cyber-security incident, the regression coefficient of *TREATMENTxPOST* would be significant. Finally, following Kausar, Shroff, & White (2016) and Lamoreaux (2016), we also included industry and year fixed-effect to take into account the staggered nature of cyber security incidents.

## 4. Results and Discussion

### *4.1 Descriptive Statistics*

Table 2 reports the frequency distribution of cyber-security incidents by year (Panel A), firm (Panel B), and breach type (Panel C). The largest number of incidents in our sample (37) occurred in 2006. The frequency distribution of incidents over time also shows an increase in the number of incidents reported since 2009 which is consistent with recent trends (Verizon, 2017). According to the results reported in Panel B, almost 29 percent of the firms affected by cyber-security incidents in our sample were breached more than once, with an average time gap of 2.34 years between incidents. AT&T has the highest number of incidents (seven) in our sample with an average time gap of 1.29 year (≈ 15 months). Panel C shows that most of the incidents in our sample were due to portable devices (PORT), malicious outsiders (HACK), unintended disclosure (DISC) and malicious insiders (INSD).

*Insert Table 2 here*

Table 3 (Panel A) provides the descriptive statistics for the variables used in our analysis. The mean (median) value of audit fees is $2.197 ($2.182) million and 3.9 percent reported

ineffective internal controls.

Panel B in Table 3 presents the t-tests on differences between breached and non-breached firms. The results suggest that, on average, breached firms pay higher fees than non-breached firms, which is in line with our expectations. Interestingly, the results also show that breached firms tend to be larger than non-breached firms. This might be due to the fact that large firms tend to have higher visibility than smaller firms, therefore they tend to be more known and searched for by individuals, and malicious outsiders alike (Johnson, 2008). Further, large firms tend to have more resources to invest in cyber-security and are therefore more likely to detect anomalies or intrusions into their systems (Gatzlaff & McCullough, 2010)[15]. Moreover, breached firms tend to have higher leverage and debt-to-equity ratios than non-breached firms, further supporting evidence of a negative relationship between a firm's financial condition and cyber-security effectiveness (Srinidhi, Yan, & Tayi, 2015; Higgs et al., 2016). Furthermore, breached firms have, on average, a larger proportion of non-current assets and higher quick ratio, which translates into higher inherent risk (Han et al., 2016). Finally, breached firms tend to have lower organization complexity and the same level of internal control weaknesses. These results partly contradict Han et al. (2016), who show a positive association between IT (and organizational) complexity and audit risk, and Klamm and Watson (2009), who provide evidence of a positive association between IT control weaknesses and audit risk.

*Insert Table 3 here*

Table 4 reports the Pearson correlation coefficients among the variables used in our analysis. Consistent with our prediction, the correlation coefficient between *LAF* and *BREACH*, is positive and significant, further suggesting a positive relationship between cyber-security and audit fees. Furthermore, *BREACH* is positively and significantly correlated with auditees' size

[15] A recent report from Verizon highlights that one in ten data breaches went undetected in 2016 (Verizon, 2017).

(*LTA*), fiscal year-end (*YE*), and auditees' complexity (*BUSSEG*), while it is negatively correlated with the proportion of current assets to total assets (*CUR*). Interestingly, there is no significant correlation between internal control weaknesses (*ICWEAK*) and *BREACH*, while a positive correlation exists between internal control weaknesses and audit fees. The correlations between other variables are consistent with previous studies.

*Insert Table 4 here*

*4.2 Contemporaneous effect of cyber-security incidents*

Table 5 presents the results of the cross-sectional regression analysis testing the impact of cyber-security incidents on audit fees and, therefore, the relationship between cyber-security incidents and audit risk. The results in Panel A suggest that cyber-security incidents (*BREACH*) have a positive and significant effect on audit fees with auditors charging, all else equal, on average, 12 percent[16] higher audit fees (approx. $1.1 million) to breached firms in the year in which a cyber-security incident occurs. Such a result is consistent with our expectation (H1)[17]. The regression results also suggest that audit effort (*LTA*), auditee's complexity (*BUSSEG* and *FOREIGN*), audit risk (*LEV*, *CUR*, and *ROA*), and internal control weaknesses (*ICWEAK*) have positive and significant impacts on audit fees. Finally, the results reveal that auditees whose fiscal years do not end on December 31 (*YE*) tend to pay lower fees. Panel B reports the results of the analysis of the effect of different types of cyber-security incidents. *UNKN* and *BREACH* were excluded to avoid collinearity with the former representing the baseline. The results suggest that cyber-security incidents due to malicious insiders (*INSD*), unauthorized physical access (*PHYS*) or to stationary (*STAT*) or portable devices (*PORT*) lead to a significantly

[16] The dependent variable of our model is log-transformed therefore to estimate the marginal effect of *BREACHED* we need to apply the following transformation: 100x(exp(β)-1).
[17] As cyber-security incidents are not random (Higgs et al., 2016), we run the same OLS regression model on a propensity score matched sample based on the probability of an incident to occur (see Equation 2) to test the robustness of the results on the full sample. Results (not tabulated) are consistent.

stronger increase in audit fees than other types of breaches. Such results might be interpreted as evidence of auditors charging higher fees to firms that have been breached because of a failure in internal rather than external access controls. The results on the subsample of breached firms, reported in Panel C and D in Table 5 further support our conclusions.

*Insert Table 5 here*

Table 6 reports the results of our analysis on potential lag or lead effects of cyber-security incidents. Panel A presents the results on the full sample which suggest that the firms disclosing a breach in the past (*BREACH_T-1*) or following (*BREACH_T+1*) fiscal year tend to pay higher fees. Results are similar for the subsample of breached firms (Panel B) and are consistent with the notion that past and future incidents may also affect the level of audit fees (Hribar et al., 2014). These results may also suggest that auditors are aware of potential risks of future incidents and therefore they price their fees accordingly. An alternative explanation may also be that these lag and lead effects are due to delays in disclosing already-discovered incidents. The analysis presented in Table 7 tries to disentangle this issue by investigating whether the distance between the disclosure of a breach and the end of the fiscal year is related to audit fees paid by the affected firm in the same, past or following year. The Incidents disclosed very early (late) in a fiscal year might have been discovered (disclosed) in the previous (following) year. However, this does not seem to be the case as *BREACH_TO_NEXT_FYEND* is not significant in any of the three panels. Overall, the results in Table 6 and 7 seem to be consistent with the idea that auditors include cyber-security risk in their audit risk assessment regardless of the actual disclosure of a cyber-security incident. The DID regression model presented below provides more robust evidence in relation to this matter.

*Insert Table 6 here*

*Insert Table 7 here*

Table 8 reports the results of our analysis focused on the effect of past breaches on audit fees. The results support the conclusion that neither past breaches nor the number of years since the last breach have a significant effect on audit fees in the year of the new breach.

*Insert Table 8 here*

Table 9 reports the results on the potential contagion effect within industries. Results for the full sample are again reported is Panel A and B and those for the subsample of breached firms in Panel C and D. The results suggest that auditors charge, on average, five percent higher fees to firms operating within the same industry of a breached firm in the following fiscal year and that such an increase is positively related to the number of breaches occurred in the industry. However, we find no evidence that the effect of peer breaches extends for more than one year since the inclusion of second and third-order lags are not significant[18].

*Insert Table 9 here*

*4.3 Ex-post effect of cyber-security incidents*

Table 10 reports summary statistics for the propensity-score matched sample as well as for the two subsamples of breached (i.e. treatment) and non-breached firms (i.e. control)[19]. Even though some differences remain between the two subsamples in terms of audit fees, size, leverage, organizational complexity, and year-end, they are more contained than the ones reported in Table 3. It is worth noting that irrespective of the effect of the matching procedure, audit fees are higher for breached firms than for non-breached firms; further suggesting a positive relationship between cyber security risk and audit fees.

[18] The results (not tabulated) are available from the authors upon request.
[19] We also run a series of t-tests comparing the average values of each variable across the two groups and different years to check whether treatment and control samples remained comparable across the whole period of the DID analysis. The results (not tabulated) confirm that the same differences appear every year therefore suggesting that the two samples remained relatively stable over time.

*Insert Table 10 here*

Table 11 presents the results of our assessment of the *ex-post* effect of cyber-security incidents on audit fees. Panel A and B report the results of the DID analysis which considers the year in which a breach is disclosed as the first year of the post-incident period (DID I). Similarly, Panel C and D present the results of our alternative specification for the DID model (DID II) which excludes the year of the breach. The variables of interest in both cases are *TREATMENT* and *TREATMENTxPOST*. The coefficient of *TREATMENT* is positive and significant across all the panels. This provides further confirmation of a positive association between cyber-security risk and audit fees. The coefficient of *TREATMENTxPOST* (our DID estimator) is positive and statistically significant in Panels A and B suggesting that cyber-security incidents result in an *ex-post* increase in audit fees. However, such a result is not confirmed in Panels C and D where the coefficient of *TREATMENTxPOST* is not statistically significant. This suggests that the results in Panels A and B are likely driven by the year of the breach which, based on the evidence provided so far and on anecdotal evidence gathered from personal interviews with auditors, is arguably different from other fiscal years. Based on the results presented in Panels C and D, the difference between the audit fees paid by breached and non-breached firms does not change after the incident. Given the empirical evidence, we conclude that auditors not only include cyber-security risk in their audit risk model before a cyber-security incident occurs (therefore increasing their audit fees) but they also seem to be able to identify, amongst firms with similar cyber-security risk profiles, those that are more likely to be breached and charge them higher fees than their peers. We also conducted a series of Chow Tests on the series of audit fees paid by breached firms in each panel. The results of the different tests consistently suggest that there is no structural break in the series; this provides further confirmation that the significant effect of *TREATMENTxPOST* in Panels A and B is driven by the year of the breach.

*Insert Table 11 here*

DID testing relies on the assumption that, in the absence of a cyber security incident, the average change in audit fees for breached and non-breached would be the same over the analysis period. This assumption is formally called the "parallel trend" assumption. Figure 2 reports the plots of the average value of audit fees paid by breached and non-breached firms and the t-test on the average change in audit fees between the two subsamples from t-2 to t-1. The graph shows a similar trend between the two groups pre-event, which is also confirmed by the t-test. Finally, following Tang, Mo, & Chan (2017), we compared the distributions of the audit fees for the two subsamples using Kernel density. The Kernel density plots show similar distribution between the two groups in the pre-event period and different patterns in the post-event period. The Kolmogorov-Smirnov tests confirmed such findings.

*Insert Figure 2 here*

In order to validate our empirical results, we carried out personal interviews with five senior IT auditors from the Big 4 audit firms. The interviewees confirmed that cyber-security risk has become a major component of the audit risk assessment. The issue of cyber-security is attributed a significant amount of attention, including annual revisions of the existing audit plan regardless of the occurrence of a cyber-security incident. Further, it emerged from the interviews that Big 4 firms charge their clients higher audit fees in the year of a cyber-security incident in response to the higher audit effort required. However, in line with our findings, the interviewees described the effect as temporary - a result of a larger number of hours billed (i.e. audit effort) rather than an increase in the fees per hours (i.e. audit risk). Overall, the evidence that emerged from our interviews provide further validation of our findings.

### *4.4 Additional Analysis: SEC Comment Letters*

The results reported in Table 11 suggest that audit firms include cyber-security risk in their audit risk model regardless of an incident's occurrence and, therefore, charge higher fees to

client firms with higher cyber-security risk. Auditing standards suggest that auditors also consider third party evidence in their audit risk assessment; this may prove particularly valuable when auditing complex systems or organizations with poor internal controls (Janvrin, 2008). Previous studies suggest that external evidence tends to be of higher quality than internal evidence (Gupta, 2005); however, auditors pay significant attention to the reliability, integrity and consistency of the source from which they gather such additional evidence (Gantz, 2013; Goodwin, 1999).

SEC Comment Letters represent an extremely valuable and reliable third-party assessment for a firm's stakeholders. As an independent research agency pointed out:

> "SEC Comment Letters, and their responses, are analytically rich. We consistently find them to be an important and helpful supplement to some of the more formal disclosure and communication mechanisms available to, and employed by, registrants. Like us, public companies know that SEC Comment Letters reveal areas of Staff concern about their accounting and/or disclosure practices. To the average securities analyst or investor, the SEC Staff is in the enviable position of being able to ask, and often secure the answers to questions that are frequently dodged, dismissed, or ignored by a registrant when asked by a non-regulator." (SEC Insight Inc. 30 September 2004)[20]

Following the Sarbanes-Oxley Act (SOX) of 2002, the Division of Corporation Finance at the SEC must review all issuers no less than once every three years. Comment Letters are the primary regulatory instrument by which the SEC can start the process of requesting additional information about underlying items in the financial statements, disclosure practices and internal controls (Gietzmann & Pettinicchio, 2014). Gietzmann and Pettinicchio (2014) demonstrate

[20] 'SEC insight', filed and recorded on the SEC site http://www.sec.gov/news/press/s72804/secinsight093004.pdf.

that auditors adjust audit fees upwards when an auditee receives a Comment Letter and such an increase persists over time.

SEC Comment Letters predominantly relate to annual and quarterly financial reports (Form 10-Ks, Form 10-Qs), to material news disclosures (Form 8-Ks), to proxy statements (e.g., DEF 14A), and to registration and prospectus filings (e.g., Form S-1s) (Dechow, Lawrence, & Ryans, 2015). Comment Letters may also cover different topics which Audit Analytics classifies according to a proprietary taxonomy[21]. While previous studies tend to focus on Comment Letters in general, it is still unclear whether specific topics mentioned in the letters have differential effects on audit fees (Gietzmann & Pettinicchio, 2014). For the purpose of our study, one topic is particularly relevant: "Data Protection and Security Breach". It is unclear whether Comment Letters related to cyber-security play an important role in the audit risk assessment of external auditors. This section aims to provide some preliminary evidence and explore, for the first time, Comment Letters in relation to cyber-security incidents.

It would also be interesting to investigate whether auditors penalize firms affected by a cyber-security incident after receiving a Comment Letter related to cyber-security. Unfortunately, our sample does not allow us to address this question adequately. Only one firm (AT&T) in our sample received a Comment Letter before being breached. In this specific case, AT&T received a Comment Letter in 2012 before being subsequently breached in 2014. However, AT&T was also breached several times before.

Table 12 reports the frequency distribution of the Comment Letters in our sample and shows that only seven letters were sent to breached firms with four of them sent to firms which had been hacked.

[21] Exemplar topics includes "Reliance on suppliers, customers, governments", "Conflicts of interest/related party issues", and "Legal exposures, reliance, claims etc.".

*Insert Table 12 here*

In order to explore the effect of Comment Letters related cyber-security on audit fees, we select all the Comment Letters covering cyber-security as classified by Audit Analytics and merge them with our full sample. We first run a regression model similar to the one presented in Equation (1) but focused on the year a Comment Letter was received. Then, in accordance with our main analysis, we used the propensity-score matched sample based on the probability of being breached (see Equation 2) to investigate whether the subsequent change in audit fees is temporary or more substantial and log-lasting. We run a regression model similar to the one presented in Equation (3) but centered around the year of the Comment Letter (-2;+2). Our treatment sample, therefore, includes the 69 firms that received a Comment Letter related to cyber-security. Our control sample includes firms whose probability of being breached is comparable to the matched firms in the treatment sample, and that did not receive a Comment Letter. None of the firms in our sample received more than one Comment Letter related to cyber-security, therefore reducing the risk of confounding effects. Furthermore, we also run our analysis on the subsample of non-breached firms to check for consistency of the results. Using this sample, we perform the same regression analysis presented above, but considering the year of Comment Letters (instead of the year of the incidents) as year of interest.

Table 13 presents the results of our analysis. In Panel A and C, we run a regression model similar to the one presented in Equation (1) in which we substitute *BREACH* with *CLETTER*. *CLETTER* is equal to 1 if a firm receives a Comment Letter related to cyber-security in year *t*, and 0 otherwise. We present the results based on the full sample in Panel A and the results on a subsample of non-breached firms in Panel C. The coefficient of *CLETTER* is positive and significant suggesting that firms that receive a Comment Letter related to cyber-security pay, on average, four percent higher fees than firms with a comparable probability of being breached. All other results are consistent with those presented in Table 5.

Panel B and D in Table 13 report the results of the DID analysis performed on our propensity-score matched sample based on the full sample (Panel B) and on the subsample of non-breached firms (Panel D). Similarly to our previous DID II analysis around cyber-security incidents, we exclude the year of the event to avoid potential bias in the results and to directly compare pre- and post-event audit fees[22]. *TREATMENT_CL* is an indicator variable equal to 1 if a firm belongs to the treatment sample (i.e. received a Comment Letter) and 0 otherwise. The coefficient of *TREATMENT_CL* is positive but not significant suggesting that there is no significant difference between treatment and control before the Comment Letters. The coefficient *TREATMENT_CLxPOST* instead is positive and significant suggesting that audit firms revise the audit risk assessment upward when an auditee receives a Comment Letter related to cyber-security, which results, all else equal, on average, in 7.57 percent higher audit fees (approx. $300,000 per year). All other results are consistent with the ones reported in Table 11. Overall, our results suggest that audit firms revise their audit risk assessment when an auditee receives a Comment Letter related to cyber-security. As such, auditors supplement their internal audit evidence with external evidence gathered from third party assessments.

*Insert Table 13 here*

## 5. Robustness Tests

In order to test whether our main findings are driven by our proxy for audit risk, correlated omitted variables, specific material weaknesses, or by the time lengths we adopted for our DID analysis, we perform a number of robustness tests.

### *5.1 Abnormal Audit Fees*

[22] We also run the analysis including the year in which a Comment Letter was received (DID I). Even though results are consistent, we report the results of the model excluding the year of Comment Letters as this provides more robust results. In fact, Gietzmann and Pettinicchio (2014, p. 57) demonstrate that "auditors adjust audit fees upwards in the period in which the [Comment Letter] is received".

Abnormal audit fees are defined as the difference between actual audit fees and the expected normal level of audit fees (Blankley, Hurtt, & MacGregor, 2012). Previous studies argue that abnormal audit fees better capture factors that are idiosyncratic to a specific auditor-client relationship (Choi, Kim, & Zang, 2010), and are found to be positively related to audit quality (Hribar et al., 2014) and audit risk (Blankley, Hurtt, & MacGregor, 2012; Han et al., 2016).

To test the robustness of our results, we perform all the analyses presented in the previous sections using abnormal audit fees as our proxy for audit fees. To estimate abnormal audit fees we adopted the model proposed by Blankley, Hurtt and MacGregor (2012). Our results (not tabulated) are consistent; therefore our conclusions are robust to different audit risk proxies.

*5.2 First Breach*

It might be possible that auditors have revised their audit risk assessment of an auditee due to past cyber-security incidents. In order to further address issues around a potential sampling bias, we have re-run the analysis including only the first incident for each firm. The results (not tabulated) are consistent with our main conclusion.

Furthermore, in light of the fact that our dataset starts in 2005, and that there is no assurance that the first observation for each firm in the dataset is actually the first incident affecting a specific firm, we also run our analysis on the subsample of incidents occurring after 2010. Being US listed firms subject to a mandatory rotation of audit partners every five years (SEC, 2003), this setting ensures that breached firms in the more recent subsample would have, at least, changed audit partners since a potential previous incident. Results (not tabulated) are consistent with the ones obtained on the full sample.

*5.3 IT Material Weaknesses*

Canada, Sutton and Randel Kuhn Jr (2009) analyze a sample of firms reporting internal control

weaknesses related to information technology (i.e. IT material weaknesses). Their results show that firms reporting IT control weaknesses pay higher audit fees than firms reporting other internal control weaknesses, and firms not reporting any internal control weaknesses.

Given that IT internal control weaknesses may increase cyber-security risk (Klamm & Watson, 2009; Cereola & Cereola, 2011), we test the robustness of our results by adding such a factor in the regression models presented in Equation (1) and Equation (3). We also run the regressions with and without the indicator variable for internal control weakness (*ICWEAK*) to avoid potential multicollinearity-related bias. In both cases the results (not tabulated) are consistent with those presented in the section above.

*5.4 Endogeneity*

It is possible that cyber-security incidents are not random and this would raise some endogeneity concerns. This might be the case for the analysis we performed on the full sample. Previous studies show that the DID technique is an effective way of controlling for random causes of changes in the dependent variable over time, and for addressing heteroscedasticity and auto-correlation (Knechel & Sharma, 2012), particularly when used together with propensity-score matching (Tucker, 2010). As such endogeneity should not affect our DID analysis.

We address this endogeneity concern in two ways. First, we re-run the analysis on our propensity-score matched sample. Second, we conduct a Heckman (1979) two-stage approach by including the inverse Mills ratio (*IMR*) from Equation (2) in to the main regression model. The results (not tabulated) are consistent with our main findings therefore suggesting that our analysis is not affected by endogeneity.

*5.5 DID Time Period*

We also consider whether the results of our DID analysis depend on its specification. To address such concerns, we first perform the DID analysis on a balanced panel covering a 5-year period centered on the incidents' year. Second, we perform the same analysis expanding the time period to three, four, and five years before and after the incidents' year to check whether our results depend on the time interval selected. Our results (not tabulated) are consistent.

*5.6 Entropy Balance Matching*

Although the use of propensity score matching has been widely used in the accounting literature and has many benefits compared to other matching techniques, it also has limitations (Shipman, Swanquist, & Whited, 2017; Gaver & Utke, 2019). Above all, a major limitation of propensity score matching is that it does not ensure similarity between matched firms (Gaver & Utke, 2019). Conscious of the limitations of propensity score matching, we adopted entropy balanced matching as presented by Hainmueller (2012) and implemented by Hainmueller & Xu (2013). The results of the analysis on the entropy balance matched sample (not tabulated) are consistent with the ones presented above.

## 6. Summary and Conclusion

In this paper, we address the question of whether external auditors recognize risks emanating from cyber-security incidents and how they respond to them. In order to formally test this, we adopt audit fees as a proxy for audit effort and audit risk. Specifically, this study investigates two related questions. First, we examine whether firms that experience cyber-security incidents are charged higher audit fees and second, whether auditors are aware of potential security issues before an incident occurs and as a result revise their risk assessment before or following a cyber-security incident. The results of our study suggest that cyber-security risk is positively associated with audit fees. This can be explained by the supposition that cyber-security

incidents, and the perceived vulnerability of a firm to such incidents, result in higher risk of material misstatement (i.e. audit risk). As a result, audit firms increase their effort to ensure the accuracy of their clients' financial reporting. This increase in audit risk and effort ultimately results in higher audit fees.

The empirical analysis suggests that auditors charge, on average, 12 percent higher audit fees to breached firms in the year when a cyber-security incident occurs. We also find evidence that incidents due to failures of internal rather than external access control result in higher audit fees, and that the results cannot be explained by past breaches or the number of years passed since the last breach. Finally, we document the existence of a contagion effect within industries with auditors charging, on average, five percent higher audit fees to firms operating in the same industry as a breached firm. However, the difference in audit fees is not limited to the year of the incidents. Breached firms pay significantly higher audit fees than firms with a similar cyber-risk profile irrespective of whether a cyber-security incident has occurred, and such a difference does not change after an incident. Our results suggest that the effect of cyber-security incidents on audit fees is only temporary (i.e. short-term) and that auditors incorporate cyber-security risk in their audit risk assessment regardless of whether a cyber-security incident has occurred and typically before an incident occurs. As a result, cyber-security incidents, on average, do not result in, *ceteris paribus*, an *ex-post* (i.e. long-term) increase in audit fees since cyber-security risk has been embedded in the audit risk assessment *ex-ante*. This implies that any change in audit fees when an incident occurs should be temporary and primarily due to additional remediation efforts undertaken during the audit.

Our results are of interest not only for researchers, who benefit from new insights on the determinants of audit risk and audit fees; but also for regulators and practitioners, who obtain empirical evidence on the effectiveness of auditing guidelines and risk assessment procedures respectively. The research provides interesting insights into the relationship between auditee

risk assessments and the audit firm business model as reflected in audit fees charged. The degree to which this is formalized and is reflective of the actual effort or audit risk represented by perceived vulnerabilities is worthy of further research. Furthermore, even though our study is based on US firms only, in this era of global trade, cyber-security represents a concern for firms worldwide. Mandatory disclosure requirements are being enacted in different legislations (see, for example, the recent General Data Protection Regulation in Europe and the Privacy Amendment (Notifiable Data Breaches) Act 2017 in Australia). As such, the results of this study may be of interest at a more international level.

This study is also subject to limitations which future research may address. First, as Higgs et al. (2016) point out, Privacy Rights Clearinghouse does not include the entire population of breaches. Security Breach Notification Laws generally require organizations to disclose cyber-security incidents that affect third parties' data, but differ across different states (Winn, 2009) creating potential asymmetries among firms operating in different states. Similarly, this study focusses on US publicly-traded firms and in the context of changes to the European data protection regime, an international study in this area may be fruitful.

Second, our results suggest that auditors incorporate cyber-security risk into their audit risk model. However, the data does not provide insights into how and to what extent this is done. Previous studies posit that expert consultation (Asare & Wright, 2004), auditor specialization (Low, 2004), or formalized instructions (Knapp & Knapp, 2001) result in better audit risk assessment. Experimental or interview-based studies might shed light on the tools and techniques (if any) that auditors adopt when considering client-specific cyber-security risk and the method for incorporating such risk into audit fees.

Third, our results suggest that auditors are able to correctly assess a client firms' risk profile and charge firms that have a higher probability of being breached higher fees. How auditors

are able to accurately assess cyber-risks is a question for future research. Internal data provided by auditors or experimental study designs may able to provide further insights in this respect.

Fourth, auditors' ability to assess the audit risk associated with their clients is expected to improve over time together with their knowledge of the auditee's systems and practices. This could be particularly relevant in relation to cyber-security as auditees' IT infrastructure can be quite complex and therefore it takes time to develop a deep understanding of how it works and potential vulnerabilities. Further studies may look in to the relationship between auditor tenure, cyber-security risk and audit quality.

Finally, future research may analyze how auditors perceive IT outsourcing or the use of cloud computing in relation to the auditing risk. Due to technological advancements, outsourcing information systems and the adoption of cloud computing has increased over the last decade (Han & Mithas, 2013; Rosati & Lynn, 2016). Both outsourcing and cloud computing represent a significant challenge for auditors, particularly because of an increase in potential material weaknesses (Klamm, Kobelsky, & Watson, 2012) or in the risk of failure in financial reporting due to the provider's errors (Anderson et al., 2014). Qualitative and quantitative research may provide useful insights on auditors' perception of these recent trends.

**References**


Abbasi, A., Sarker, S., & Chiang, R. H. (2016). Big Data Research in Information Systems: Toward an Inclusive Research Agenda. *Journal of the Association for Information Systems,* 17(2), 1-22.

Abbott, L. J., Parker, S., & Peters, G. F. (2006). Earnings management, litigation risk, and asymmetric audit fee responses. *Auditing: A Journal of Practice & Theory,* 25(1), 85-98.

Allen, R. D., Hermanson, D. R., Kozloski, T. M., & Ramsay. R. J. (2006). Auditor risk assessment: Insights from the academic literature. *Accounting Horizons,* 20(2), 157-177.

Anderson, S. W., Christ, M. H., Dekker, H. C., & Sedatole, K. (2014). The use of management controls to mitigate risk in strategic alliances: Field and survey evidence. *Journal of Management Accounting Research,* 26(1), 1-32.

Aral, S., Dellarocas, C., & Godes, D. (2013). Introduction to the special issue-social media and business transformation: A framework for research. *Information Systems Research* 24(1): 3-13.

Asare, S. K., & Wright, A. M. (2004). The effectiveness of alternative risk assessment and program planning tools in a fraud setting. *Contemporary Accounting Research,* 21(2), 325-352.

Bartov, E., Gul, F. A., & Tsui, J. S. (2000). Discretionary-accruals models and audit qualifications. *Journal of Accounting and Economics,* 30(3), 421-452.

Becker, C. L., DeFond, M. L., Jiambalvo, J., & Subramanyam, K. (1998). The effect of audit quality on earnings management. *Contemporary Accounting Research,* 15(1), 1-24.

Bedard, J. C., & Johnstone, K. M. (2004). Earnings manipulation risk, corporate governance risk, and auditors' planning and pricing decisions. *The Accounting Review,* 79(2), 277-304.

Bell, T. B., Landsman, W. R., & Shackelford, D. A. (2001). Auditors' perceived business risk and audit fees: Analysis and evidence. *Journal of Accounting Research,* 39(1), 35-43.

Benaroch, M., Chernobai, A., & Goldstein, J. (2012). An internal control perspective on the market value consequences of IT operational risk events. *International Journal of Accounting Information Systems* 13(4), 357-381.

Bertrand, M., Duflo, E., & Mullainathan, S. (2004). How much should we trust differences-in-differences estimates?. *The Quarterly Journal of Economics,* 119(1), 249-275.

Blankley, A. I., Hurtt, D. N., & MacGregor, J. E. (2012). Abnormal audit fees and restatements. *Auditing: A Journal of Practice & Theory,* 31(1), 79-96.

Boritz, J. E., Kochetova-Kozloski, N., & Robinson, L. (2014). Are fraud specialists relatively more effective than auditors at modifying audit programs in the presence of fraud risk? *The Accounting Review,* 90(3), 881-915.

Budescu, D. V., Peecher, M. E., & Solomon, I. (2012). The joint influence of the extent and nature of audit evidence, materiality thresholds, and misstatement type on achieved audit risk. *Auditing: A Journal of Practice & Theory,* 31(2), 19-41.

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

Canada, J., Sutton, S. G., & Randel Kuhn Jr, J. (2009). The pervasive nature of IT controls: An examination of material weaknesses in IT controls and audit fees. *International Journal of Accounting & Information Management,* 17(1): 106-119.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce,* 9(1), 70-104.

Center for Audit Quality - CAQ. (2014). *Cybersecurity and the External Audit*. (March 2014). Available at: http://www.thecaq.org/caq-alert-2014-03-cybersecurity-and-external-audit (last accessed September 28, 2016).

Center for Audit Quality - CAQ. (2016). *Understanding Cybersecurity and the External Audit*. (February 2016) Available at: https://www.thecaq.org/understanding-cybersecurity-and-external-audit (last accessed December 19, 2018)

Center for Audit Quality - CAQ. (2017). *The CPA's Role in Addressing Cybersecurity Risk*. (May 2017). Available at: https://www.thecaq.org/cpas-role-addressing-cybersecurity-risk (last accessed December 19, 2018).

Cereola, S. J., & Cereola, R. J. (2011). Breach of data at TJX: An instructional case used to study COSO and COBIT, with a focus on computer controls, data security, and privacy legislation. *Issues in Accounting Education,* 26(3), 521-545.

Chang, C. J., & Hwang, N.-C. (2003). The impact of retention incentives and client business risks on auditors' decisions involving aggressive reporting practices. *Auditing: A Journal of Practice & Theory,* 22(2), 207-218.

Charette, R.N., Adams, K.M., & White, M.B. (1997). Managing risk in software maintenance. *IEEE Software* 14(3): 43-50.

Chen, Y., Smith, A. L., Cao, J., & Xia, W. (2014). Information technology capability, internal control effectiveness, and audit fees and delays. *Journal of Information Systems,* 28(2),149-180.

Chernobai, A., Jorion, P., & Yu, F. (2011). The determinants of operational risk in US financial institutions. *Journal of Financial and Quantitative Analysis*, 46(6), 1683-1725.

Choi, J. H., Kim, J. B., Liu, X. & Simunic, D. A. (2008). Audit pricing, legal liability regimes, and big 4 premiums: Theory and cross‐country evidence. *Contemporary Accounting Research,* 25(1), 55-99.

Choi, J.-H., Kim, J.-B., & Zang, Y. (2010). Do abnormally high audit fees impair audit quality? *Auditing: A Journal of Practice & Theory,* 29(2), 115-140.

Christopher, J., Sarens, G., & Leung, P. (2009). A critical analysis of the independence of the internal audit function: evidence from Australia. *Accounting, Auditing & Accountability Journal,* 22(2), 200-220.

Coleman, D. (2015). *When is a Cybersecurity Incident Material?*. Audit Analytics. Available at: http://www.auditanalytics.com/blog/when-is-a-cybersecurity-incident-material/ (last accessed December 22, 2017).

Committee of Sponsoring Organizations of the Treadway Commission – COSO (2013). *Internal Control—Integrated Framework*. Durham, NC: AICPA.

Craswell, A. T., Francis, J. R., & Taylor, S. L. (1995). Auditor brand name reputations and industry specializations. *Journal of Accounting and Economics,* 20(3), 297-322.

Dechow, P., Ge, W., & Schrand, C. (2010). Understanding earnings quality: A review of the proxies, their determinants and their consequences. *Journal of Accounting and Economics,* 50(2), 344-401.

Dechow, P. M., Lawrence, A., & Ryans, J. P. (2015). SEC comment letters and insider sales. *The Accounting Review*, 91(2),, 401-439.

De Franco, G., Gavious, I., Jin, J. Y., & Richardson, G. D. (2011). Do private company targets that hire Big 4 auditors receive higher proceeds?. *Contemporary Accounting Research*, 28(1), 215-262.

Dennis, A., Wixom, B.H., & Tegarden, D. (2015). *Systems analysis and design: An object-oriented approach with UML*. John Wiley & Sons.

Desai, H., Hogan, C. E., & Wilkins, M. S. (2006). The reputational penalty for aggressive accounting: Earnings restatements and management turnover. *The Accounting Review,* 81(1), 83-112.

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

Duflo, E. (2002). *Empirical methods*. Handout of courses MIT 14 14.771/ Harvard 2390b. Available at: http://web.mit.edu/14.771/www/emp_handout.pdf (last accessed: July 26, 2017).

Eshleman, J.D., & Guo, P. (2014). Do Big 4 auditors provide higher audit quality after controlling for the endogenous choice of auditor?. *Auditing: A Journal of Practice & Theory,* 33(4), 197-219.

Frino, A., Palumbo, R., & Rosati, P. 2017. *Does Information Asymmetry Predict Audit Fees?*. Capital Markets Cooperative Research Center (CMCRC), and University of Chieti-Pescara.

Federal Trade Commission – FTC (2009). *Consumer Data Broker ChoicePoint Failed to Protect Consumers' Personal Data, Left Key Electronic Monitoring Tool Turned Off for Four Months*. (October 2009). Available at: https://www.ftc.gov/news-events/press-releases/2009/10/consumer-data-broker-choicepoint-failed-protect-consumers (last accessed September 28, 2016).

Feng, M., Li, C., McVay, S. E., & Skaife, H. (2014). Does ineffective internal control over financial reporting affect a firm's operations? Evidence from firms' inventory management. *The Accounting Review*, 90(2), 529-557.

Gantz, S. D. (2013). *The Basics of IT Audit: Purposes, Processes, and Practical Information*. Elsevier.

Garg, A., Curtis, J., & Halper, H. (2003). The financial impact of IT security breaches: what do investors think?. *Information Systems Security*, 12(1), 22-33.

Garrison, C. P., & Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management & Computer Security*, 19(4), 216-230.

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review,* 13(1), 61-83.

Gaver, J. J., & Utke, S. (2019). Audit Quality and Specialist Tenure. The Accounting Review, 94(3), 113-147.

Gietzmann, M. B., & Pettinicchio, A. K. (2014). External auditor reassessment of client business risk following the issuance of a comment letter by the SEC. *European Accounting Review,* 23(1), 57-85.

Goodwin, J. (1999). The effects of source integrity and consistency of evidence on auditors' judgments. *Auditing: A Journal of Practice & Theory* 18(2), 1-16.

Gordon, L. A., Loeb, M. P., Sohail, T., Tseng, C.-Y., & Zhou, L. (2008). Cybersecurity, capital allocations and management control systems. *European Accounting Review,* 17(2), 215-241.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, 34(3), 567-594.

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

Gul, F. A., & Tsui, J. S. L. (1997). A test of the free cash flow and debt monitoring hypotheses:: Evidence from audit pricing. *Journal of Accounting and Economics,* 24(2), 219-237.

Gul, F. A., & Goodwin, J. (2010). Short-term debt maturity structures, credit ratings, and the pricing of audit services. *The Accounting Review,* 85(3), 877-909.

Gupta, K. (2005). *Contemporary Auditing*. Tata McGraw-Hill.

Hainmueller, J. (2012). Entropy balancing for causal effects: A multivariate reweighting method to produce balanced samples in observational studies. Political Analysis 20(1), 25–46.

Hainmueller, J., & Xu, Y. (2013). Ebalance: A Stata package for entropy balancing. Journal of Statistical Software, 54 (7), 1–18.

Haislip, J. Z., Masli, A., Richardson, V. J., & Sanchez, J. M. (2016). Repairing Organizational Legitimacy Following Information Technology (IT) Material Weaknesses: Executive Turnover, IT Expertise, and IT System Upgrades. *Journal of Information Systems,* 30(1), 41-70.

Hammersley, J. S., Myers, L. A., & Shakespeare, C. (2008). Market reactions to the disclosure of internal control weaknesses and to the characteristics of those weaknesses under section 302 of the Sarbanes Oxley Act of 2002. *Review of Accounting Studies,* 13(1), 141-165.

Hammersley, J. S., Johnstone, K. M., & Kadous, K. (2011). How do audit seniors respond to heightened fraud risk? *Auditing: A Journal of Practice & Theory,* 30 (3), 81-101.

Han, K., & Mithas, S. (2013). Information Technology Outsourcing and Non-IT Operating Costs: An Empirical Investigation. *MIS Quarterly,* 37(1), 315-331.

Han, S., Rezaee, Z., Xue, L., & Zhang, J. H. (2016). The association between information technology investments and audit risk. *Journal of Information Systems,* 30(1), 93-116.

Hay, D., & Knechel, W. R. (2010). The effects of advertising and solicitation on audit fees. *Journal of Accounting and Public Policy* 29(1), 60-81.

Heckman, J. J. (1979). Sample selection bias as a specification error. *Econometrica*, 47, 153–162.

Higgs, J.L., Pinsker, R.E., Smith, T.J., & Young, G.R. (2016). The Relationship between Board-Level Technology Committees and Reported Security Breaches. *Journal of Information Systems,* 30(3), 79-98.

Hogan, C. E., & 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.

Hovav, A., & Gray, P. (2014). The ripple effect of an information security breach event: a stakeholder analysis. *Communications of the Association for Information Systems,* 34(50), 893-912.

Hribar, P., Kravet, T., & Wilson, R. (2014). A new measure of accounting quality. *Review of Accounting Studies*, 19(1), 506-538.

Jaggi, B., & Low, P.Y. (2011). Joint effect of investor protection and securities regulations on audit fees. *The International Journal of Accounting,* 46(3), 241-270.

Janvrin, D. (2008). To what extent does internal control effectiveness increase the value of internal evidence?. *Managerial Auditing Journal* 23(3), 262-282.

Joe, J. R., Janvrin, D. J., Barr-Pulliam, D., Mason, S., Pitman, M. K., Rezaee, Z., Sanderson, K.-A., & Wu, Y.-J. (2015). The Auditing Standards Committee of the Auditing Section of the American Accounting Association is Pleased to Provide Comments on PCAOB Staff Consultation Paper No. 2015-01, The Auditor's Use of the Work of Specialist s: Participating Committee Members. *Current Issues in Auditing,* 9(2), C18-C37.

Johnson, M. E. (2008). Information risk of inadvertent disclosure: An analysis of file-sharing risk in the financial supply chain. *Journal of Management Information Systems,* 25(2), 97-124.

Johnstone, K. M., & Bedard, J. C. (2003). Risk management in client acceptance decisions. *The Accounting Review,* 78(4), 1003-1025.

Kajüter, P., Klassmann, F., & Nienhaus, M. (2016). Do Reviews by External Auditors Improve the Information Content of Interim Financial Statements?. *The International Journal of Accounting,* 51(1), 23-50.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2018). What is the Impact of Successful Cyberattacks on Target Firms? (No. w24409). National Bureau of Economic Research.

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

Kausar, A., Shroff, N., & White, H. (2016). Real effects of the audit choice. *Journal of Accounting and Economics* 62(1), 157-181.

Klamm, B. K., & Watson, M. W. (2009). SOX 404 reported internal control weaknesses: A test of COSO framework components and information technology. *Journal of Information Systems,* 23(2), 1-23.

Klamm, B. K., Kobelsky, K. W., & Watson, M. W. (2012). Determinants of the persistence of internal control weaknesses. *Accounting Horizons,* 26(2), 307-333.

Knapp, C. A., & Knapp, M. C. (2001). The effects of experience and explicit fraud risk assessment in detecting fraud with analytical procedures. *Accounting, Organizations and Society,* 26(1), 25-37.

Knechel, W. R., & Sharma, D. S. (2012). Auditor-provided nonaudit services and audit effectiveness and efficiency: Evidence from pre-and post-SOX audit report lags. *Auditing: A Journal of Practice & Theory,* 31(4), 85-114.

Koh, K., & Tong, Y. H. (2013). The effects of clients' controversial activities on audit pricing. *Auditing: A Journal of Practice & Theory,* 32(2), 67-96.

Krishnan, J., Rama, D., & Zhang, Y. (2008). Costs to comply with SOX Section 404. *Auditing: A Journal of Practice & Theory*, 27(1), 169-186.

Krishnan, G., & Visvanathan, G. (2009). Do auditors price audit committee's expertise? The case of accounting versus nonaccounting financial experts. *Journal of Accounting, Auditing & Finance,* 24(1), 115-144.

Krudy, E. (2012). *Websites of exchanges Nasdaq, BATS hit in online attack*. (February 2012). Available at: http://www.reuters.com/article/us-nasdaq-attack-idUSTRE81D21720120214 (last eccessed Septmber 28, 2016): Reuters.

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), 313-337.

Lawrence, A., Minutti-Meza, M., & Zhang, P. (2011). Can Big 4 versus non-Big 4 differences in audit-quality proxies be attributed to client characteristics?. *The Accounting Review,* 86(1), 259-286.

Lawrence, A., Minutti-Meza, M., & Vyas, D. (2018). Is Operational Control Risk Informative of Financial Reporting Deficiencies?. Auditing: A Journal of Practice & Theory, 37(1), 139-165.

Lechner, M. (2011). The estimation of causal effects by difference-in-difference methods. *Foundations and Trends® in Econometrics,* 4(3), 165-224.

Li, H., No, W. G., & Boritz, E. (2016), Are External Auditors Concerned About Cyber Incidents? Evidence from Audit Fees. Available at SSRN: https://ssrn.com/abstract=2880928.

Li, C., Sun, L., & Ettredge, M. (2010). Financial executive qualifications, financial executive turnover, and adverse SOX 404 opinions. *Journal of Accounting and Economics,* 50(1), 93-110.

Lobo, G. J., & Zhao, Y. (2013). Relation between audit effort and financial report misstatements: Evidence from quarterly and annual restatements. *The Accounting Review,* 88(4), 1385-1412.

Low, K. Y. (2004). The effects of industry specialization on audit risk assessments and audit-planning decisions. *The Accounting Review,* 79(1), 201-219.

Masli, A., Peters, G. F., Richardson, V. J., & Sanchez, J. M. (2010). Examining the potential benefits of internal control monitoring technology. *The Accounting Review,* 85(3), 1001-1034.

National Conference of State Legislature (NCSL). 2017. *Security Breach Notification Laws*. Available at: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last accessed July 26, 2017).

Perlroth, N. (2016). *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*. The New York Times (September, 2016). Available at: https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html (last accessed July 27, 2017).

Perlroth, N. (2017). *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*. The New York Times (October, 2017). Available at:

https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html (last accessed December 22, 2017).

Petersen, M. A. (2009). Estimating standard errors in finance panel data sets: Comparing approaches. *Review of Financial Studies,* 22(1), 435-480.

Posey, C., Raja, U., Crossler, R. E., & Burns, A. J. (2017). Taking stock of organisations' protection of privacy: categorising and assessing threats to personally identifiable information in the USA. *European Journal of Information Systems*, 26(6), 585-604.

Public Company Accounting Oversight Board – PCAOB (2010). *Identifying and Assessing Risks of Material Misstatement*. AS No. 12: Public Company Accounting Oversight Board (PCAOB).

Public Company Accounting Oversight Board – PCAOB (2013). *Considerations for Audits of Internal Control over Financial Reporting*: Public Company Accounting Oversight Board (PCAOB).

Public Company Accounting Oversight Board – PCAOB (2018). *Standing Advisory Group Meeting – Panel Discussion – Cybersecurity*: Public Company Accounting Oversight Board (PCAOB).

Pratt, J., & Stice, J. D. (1994). The effects of client characteristics on auditor litigation risk judgments, required audit evidence, and recommended audit fees. *The Accounting Review*, 69(4), 639-656.

Premuroso, R. F., & Bhattacharya, S. (2007). Is there a relationship between firm performance, corporate governance, and a firm's decision to form a technology committee?. *Corporate Governance: An International Review*, 15(6), 1260–1276.

PricewaterhouseCoopers - Pwc (2016). *2015 Information Security Breaches Survey – Technical Report*. Available at: http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf (last accessed September 28, 2016).

Privacy Rights Clearinghouse – PRC (2017). Chronology of Data Breaches: FAQ. Available at: https://www.privacyrights.org/chronology-data-breaches-faq (last accessed July 25, 2019).

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies,* 11(1), 74-104.

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft?. *Journal of Policy Analysis and Management*, 30(2), 256-286.

Rosati, P., Deeney, P., Cummins, M., Van der Werff, L., & Lynn, T. 2019. Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Research in International Business and Finance*, 47, 458-469.

Rosati, P., Deeney, P., Gogolin, F., Cummins, M., Van der Werff, L., & Lynn, T. 2017. The Effect of Data Breach Announcements Beyond The Stock Price: Empirical Evidence on Market Activity. *International Review of Financial Analysis*, 49, 146-154.

Rosati, P., & Lynn, T. (2016). AIS: Challenges to Technology Implementation. In: *AIS Companion*, edited by: Quinn, M., & Strauss, E. Routledge (forthcoming).

Savitz, E. (2012). *Nasdaq Web Site Shut Down By Denial Of Service Attacks*. (February 2012). Available at: http://www.forbes.com/sites/ericsavitz/2012/02/14/nasdaq-web-site-shut-down-by-denial-of-service-attacks/#443bc483bfb4 (last accessed September 28, 2016): Forbes.

Securities and Exchanges Commission – SEC (2003). *Strengthening the Commission's Requirements Regarding Auditor Independence* (March 2003). Available at: https://www.sec.gov/rules/final/33-8183.htm (last accessed July 27, 2017).

Securities and Exchanges Commission – SEC (2011). *CF Disclosure Guidance: Topic No. 2*. (October 2011). Available at: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (last accessed December 19, 2018).

Securities and Exchanges Commission – SEC (2014). *SEC to Hold Cybersecurity Roundtable*. (February 2014). Available at: https://www.sec.gov/News/PressRelease/Detail/PressRelease/1370540793626. (last accessed September 28, 2016).

Securities and Exchanges Commission – SEC (2015). *OCIE's 2015 Cybersecurity Examination Initiative*: Securities and Exchanges Commission (SEC).

Securities and Exchanges Commission – SEC (2018). *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*. (February 2018) Available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf (last accessed December 19, 2018).

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

Simunic, D. A. (1980). The pricing of audit services: Theory and evidence. *Journal of Accounting Research,* 18(1), 161-190.

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. Computers & Security, 58, 216-229.

Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems,* 75, 49-62.

Stefaniak, C. M., Houston, R. W., & Cornell, R. M. (2012). The effects of employer and client identification on internal and external auditors' evaluations of internal control deficiencies. *Auditing: A Journal of Practice & Theory,* 31(1), 39-56.

Stice, J. D. (1991). Using financial and market information to identify pre-engagement factors associated with lawsuits against auditors. *The Accounting Review,* 66(3), 516-533.

Su, X., & Wu, X. (2017). Public Disclosure of Audit Fees and Bargaining Power between the Client and Auditor: Evidence from China. *The International Journal of Accounting,* forthcoming.

Sundgren, S. (1998). Auditor choices and auditor reporting practices: evidence from Finnish small firms. *European Accounting Review,* 7(3), 441-465.

Tang, T., Mo, P. L. L., & Chan, K. H. (2017). Tax collector or tax avoider? An investigation of intergovernmental agency conflicts. *The Accounting Review* 92(2), 247-270.

Thielman, S. (2016). *Yahoo hack: 1bn accounts compromised by biggest data breach in history.* The Guardian (December, 2016). Available at: https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached (last accessed July 27, 2017).

Tucker, J. W. (2010). Selection Bias and Econometric Remedies in Accounting and Finance Research. *Journal of Accounting Literature*. Available at SSRN: https://ssrn.com/abstract=1756911.

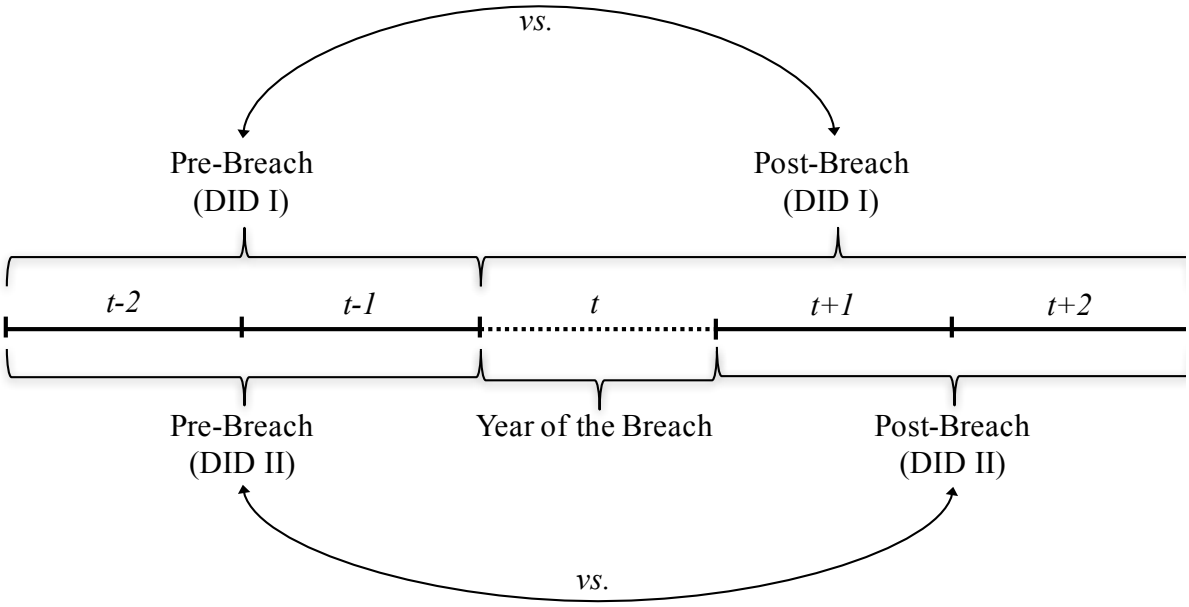
Verizon (2017). *2017 Data Breach Investigations Report*. Available at: http://www.verizonenterprise.com/verizon-insights-lab/dbir/ (last accessed July 27, 2017).

Winn, J. K. (2009). Are "Better" Security Breach Notification Laws Possible?. *Berkeley Technology Law Journal*, 24(3), 1133-1165.

Zafar, H. (2012). Financial Impact of Information Security Breaches on Breached Firms and their Non-Breached. *Journal of Computer Security*, 11(3), 431-448.

**FIGURE 1**

**Timeline of the DID analysis**




This figure provides a graphical representation of the timeline adopted in our DID analysis where *t* is the year in which a cyber security incident occurs. Note: the year of cyber-security incidents (*t*) is not included in the DID II analysis.

**TABLE 1**

**Sample Composition**

| | Firms | Firm-years |
|---|---|---|
| Audit Analytics audit fees file (2003-2015) | 21,074 | 132,676 |
| Less: | | |
| Financial Companies | (1,613) | (9,535) |
| Non-Compustat | (8,495) | (57,443) |
| Missing Data | (2,790) | (10,166) |
| Non-Big4 Auditors | (2,489) | (14,761) |
| Final sample | 5,687 | 40,771 |
| Breached | 168 | |
| Non-breached | 5,519 | |

This table summarizes the sampling process. Number of firms and firm-years deleted at each step in parenthesis.

**TABLE 2**

**Frequency Distribution of Cyber-Security Incidents by Year and Type**

**Panel A: Cyber-security incidents by year**

| Year | No. of breaches | Percentage |
|---|---|---|
| 2005 | 16 | 6.45 |
| 2006 | 37 | 14.92 |
| 2007 | 25 | 10.08 |
| 2008 | 19 | 7.66 |
| 2009 | 18 | 7.26 |
| 2010 | 21 | 8.47 |
| 2011 | 31 | 12.50 |
| 2012 | 30 | 12.10 |
| 2013 | 32 | 12.90 |
| 2014 | 19 | 7.66 |
| Total | 248 | 100 |

**Panel B: Cyber-security incidents by firm**

| No. of breaches | No. of firms | Percentage | Avg. Time Between Breaches (Year) |
|---|---|---|---|
| 1 | 120 | 71.43 | |
| 2 | 31 | 18.45 | 2.77 |
| 3 | 8 | 4.76 | 2.62 |
| 4 | 5 | 2.98 | 2.52 |
| 5 | 3 | 1.79 | 1.42 |
| 7 | 1 | 0.60 | 1.29 |
| Total | 168 | 100 | 2.34 |

**Panel C: Cyber-security incidents by Type**

| Type | No. of breaches | Percentage | No. of firms | Percentage |
|---|---|---|---|---|
| CARD | 7 | 2.82 | 7 | 4.17 |
| DISC | 37 | 14.92 | 31 | 18.45 |
| HACK | 65 | 26.21 | 55 | 32.74 |
| INSD | 35 | 14.11 | 26 | 15.48 |
| PHYS | 14 | 5.65 | 11 | 6.55 |
| PORT | 79 | 31.85 | 69 | 41.07 |
| STAT | 8 | 3.23 | 8 | 4.76 |
| UNKN | 3 | 1.21 | 3 | 1.79 |
| Total | 248 | 100 | | |

This table reports the frequency distribution of cyber-security incidents by year (Panel A), firms (Panel B) and breach type (Panel C). Appendix B reports the definitions of different breach types.

**TABLE 3**

**Descriptive Statistics and Tests of Differences**

**Panel A: Descriptive Statistics**

| Variable | Mean | Q1 | Median | Q3 | Std. Dev. |
|---|---|---|---|---|---|
| LAF | 14.603 | 13.856 | 14.596 | 15.373 | 1.279 |
| LTA | 13.751 | 12.336 | 13.729 | 15.156 | 2.128 |
| LEV | 0.245 | 0.118 | 0.189 | 0.291 | 1.010 |
| CUR | 0.439 | 0.204 | 0.424 | 0.649 | 0.273 |
| QUICK | 2.766 | 0.912 | 1.415 | 2.489 | 2.225 |
| ROA | 0.025 | -0.028 | 0.031 | 0.073 | 0.624 |
| DEBTEQ | 0.273 | 0.000 | 0.256 | 0.811 | 2.624 |
| BUSSEG | 0.614 | 0.000 | 0.000 | 1.099 | 0.747 |
| FOREIGN | 0.436 | 0.000 | 0.037 | 0.411 | 6.643 |
| YE | 0.252 | | | | |
| ICWEAK | 0.039 | | | | |
| BREACH | 0.006 | | | | |
| PAST_BREACH | 0.003 | | | | |
| CARD | 0.001 | | | | |
| DISC | 0.001 | | | | |
| HACK | 0.002 | | | | |
| INSD | 0.001 | | | | |
| PHYS | 0.001 | | | | |
| PORT | 0.002 | | | | |
| STAT | 0.001 | | | | |
| UNKN | 0.000 | | | | |

**Panel B: T-Test of Differences**

| Variable | Breached | Non-Breached | Diff. | t-statistic | p-value |
|---|---|---|---|---|---|
| LAF | 16.182 | 14.593 | 1.589 | 19.617 | 0.000*** |
| LTA | 16.525 | 13.734 | 2.791 | 20.793 | 0.000*** |
| LEV | 0.274 | 0.246 | 0.028 | 0.419 | 0.675 |
| CUR | 0.354 | 0.439 | -0.085 | -4.885 | 0.000*** |
| QUICK | 1.329 | 2.774 | -1.445 | -1.283 | 0.199 |
| ROA | 0.049 | 0.025 | 0.245 | 0.083 | 0.934 |
| DEBTEQ | 0.476 | 0.272 | 0.203 | 0.034 | 0.973 |
| BUSSEG | 0.754 | 0.613 | 0.142 | 2.988 | 0.003*** |
| FOREIGN | 0.244 | 0.436 | -0.192 | 0.182 | 0.855 |
| YE | 0.369 | 0.251 | 0.118 | 4.288 | 0.000*** |
| ICWEAK | 0.044 | 0.039 | 0.005 | 0.441 | 0.659 |

This table reports the descriptive statistics of the variables adopted in the empirical analysis (Panel A) and t-test on the differences between breached and non-breached firms (Panel B). All variables are defined in Appendix A. ***, **, * denote significance at 1, 5 and 10 percent levels, respectively.

**TABLE 4**

**Pearson Correlation Coefficients between Variables**

| Variable | LAF | | BREACH | | LTA | | LEV | | CUR | | QUICK | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| LAF | 1.000 | | | | | | | | | | | |
| BREACH | 0.097 | *** | 1.000 | | | | | | | | | |
| LTA | 0.793 | *** | 0.102 | *** | 1.000 | | | | | | | |
| LEV | -0.037 | *** | 0.002 | | -0.094 | *** | 1.000 | | | | | |
| CUR | -0.255 | *** | -0.024 | *** | -0.509 | *** | 0.071 | *** | 1.000 | | | |
| QUICK | -0.106 | *** | -0.007 | | -0.103 | *** | -0.018 | *** | 0.109 | *** | 1.000 | |
| ROA | -0.009 | * | 0.000 | | 0.032 | *** | -0.076 | *** | -0.021 | *** | 0.005 | |
| DEBTEQ | 0.004 | | 0.000 | | 0.006 | | 0.000 | | -0.006 | | -0.001 | |
| YE | -0.018 | *** | 0.021 | *** | -0.032 | *** | 0.011 | ** | 0.121 | *** | -0.003 | |
| BUSSEG | 0.304 | *** | 0.015 | *** | 0.270 | *** | 0.003 | | -0.140 | *** | -0.043 | *** |
| FOREIGN | -0.001 | | -0.001 | | -0.010 | ** | 0.000 | | 0.010 | ** | 0.001 | |
| ICWEAK | 0.055 | *** | 0.002 | | 0.015 | *** | 0.006 | | 0.020 | *** | -0.003 | |

This table reports the Pearson correlation coefficients among the main variables adopted in the empirical analysis. All variables are defined in Appendix A. ***, **, * denote significance at 1, 5 and 10 percent levels, respectively.

**Table 4 - Continued**

**Pearson Correlation Coefficients between Variables**

| Variable | ROA | DEBTEQ | YE | BUSSEG | FOREIGN | ICWEAK |
|---|---|---|---|---|---|---|
| LAF | | | | | | |
| BREACH | | | | | | |
| LTA | | | | | | |
| LEV | | | | | | |
| CUR | | | | | | |
| QUICK | | | | | | |
| ROA | 1.000 | | | | | |
| DEBTEQ | 0.002 | 1.000 | | | | |
| YE | -0.003 | 0.003 | 1.000 | | | |
| BUSSEG | 0.001 | 0.005 | -0.011 ** | 1.000 | | |
| FOREIGN | -0.001 | 0.000 | -0.005 | 0.001 | 1.000 | |
| ICWEAK | 0.002 | -0.010 * | 0.021 *** | 0.018 *** | -0.001 | 1.000 |

This table reports the Pearson correlation coefficients among variables adopted in the empirical analysis. All variables are defined in Appendix A. ***, **, * denote significance at 1, 5 and 10 percent levels, respectively.

**TABLE 5**

**Regression Results: Effect of Cyber-Security Incidents on Audit Fees**

| | Panel A: Full Sample | | Panel B: Full Sample | | Panel C: Breached Firms | | Panel D: Breached Firms | |
|---|---|---|---|---|---|---|---|---|
| **Variable** | **Coeff.** | **p-value** | **Coeff.** | **p-value** | **Coeff.** | **p-value** | **Coeff.** | **p-value** |
| INTERCEPT | 9.947 | 0.000 *** | 9.947 | 0.000 *** | 7.579 | 0.000 *** | 7.114 | 0.000 *** |
| BREACH | 0.113 | 0.002 *** | | | 0.103 | 0.004 *** | | |
| CARD | | | -0.037 | 0.840 | | | -0.064 | 0.524 |
| DISC | | | 0.015 | 0.864 | | | 0.006 | 0.892 |
| HACK | | | -0.053 | 0.466 | | | -0.010 | 0.766 |
| INSD | | | 0.175 | 0.033 ** | | | 0.154 | 0.028 ** |
| PHYS | | | 0.298 | 0.017 ** | | | 0.235 | 0.094 * |
| PORT | | | 0.228 | 0.000 *** | | | 0.227 | 0.032 ** |
| STAT | | | 0.363 | 0.011 ** | | | 0.267 | 0.004 *** |
| LTA | 0.530 | 0.000 *** | 0.530 | 0.000 *** | 0.442 | 0.000 *** | 0.455 | 0.000 *** |
| LEV | 0.033 | 0.073 * | 0.033 | 0.072 * | 0.015 | 0.040 ** | 0.015 | 0.040 ** |
| CUR | 0.499 | 0.000 *** | 0.499 | 0.000 *** | 0.042 | 0.000 *** | 0.042 | 0.000 *** |
| QUICK | -0.001 | 0.128 | -0.001 | 0.128 | 0.001 | 0.056 * | 0.001 | 0.056 * |
| ROA | 0.004 | 0.004 *** | 0.004 | 0.004 ** | 0.002 | 0.079 * | 0.002 | 0.079 * |
| DEBTEQ | 0.000 | 0.573 | 0.000 | 0.573 | 0.000 | 0.228 | 0.000 | 0.228 |
| YE | -0.066 | 0.000 *** | -0.066 | 0.000 *** | -0.025 | 0.098 * | -0.025 | 0.098 * |
| BUSSEG | 0.116 | 0.000 *** | 0.116 | 0.000 *** | 0.157 | 0.017 ** | 0.157 | 0.017 ** |
| FOREIGN | 0.000 | 0.063 * | 0.000 | 0.063 * | 0.001 | 0.062 * | 0.001 | 0.062 * |
| ICWEAK | 0.447 | 0.000 *** | 0.447 | 0.000 *** | 0.307 | 0.000 *** | 0.307 | 0.000 *** |
| Industry fixed-effect | Yes | | Yes | | Yes | | Yes | |
| Year fixed-effect | Yes | | Yes | | Yes | | Yes | |
| F-statistic | 35.03 | | 75.31 | | 39.44 | | 27.41 | |
| p-value | 0.000 | | 0.000 | | 0.000 | | 0.000 | |
| R-squared | 0.72 | | 0.72 | | 0.85 | | 0.85 | |
| N | 40,771 | | 40,771 | | 1,590 | | 1,590 | |

This table presents the results of the regression analysis for the model presented in Equation (1). The dependent variable is the natural logarithm of audit fees (LAF) for all the regressions. All other variables are defined in Appendix A. ***, **, * denote significance at 1, 5 and 10 percent levels, respectively.

**TABLE 6**

**Regression Results: Lagged and Lead Effect of Cyber-Security Incidents on Audit Fees**

| | Panel A: Full Sample | | Panel B: Breached Firms | |
|---|---|---|---|---|
| **Variable** | **Coeff.** | **p-value** | **Coeff.** | **p-value** |
| INTERCEPT | 9.331 | 0.000 *** | 7.332 | 0.000 *** |
| BREACH_T-1 | 0.062 | 0.069 * | 0.090 | 0.006 *** |
| BREACH | 0.121 | 0.001 *** | 0.104 | 0.003 *** |
| BREACH_T+1 | 0.103 | 0.028 ** | 0.082 | 0.056 * |
| LTA | 0.513 | 0.000 *** | 0.523 | 0.000 *** |
| LEV | 0.352 | 0.000 *** | 0.336 | 0.001 *** |
| CUR | 0.486 | 0.000 *** | 0.440 | 0.000 *** |
| QUICK | -0.025 | 0.164 | -0.001 | 0.194 |
| ROA | 0.006 | 0.002 *** | 0.005 | 0.000 *** |
| DEBTEQ | 0.000 | 0.753 | 0.000 | 0.242 |
| YE | -0.019 | 0.051 * | -0.034 | 0.000 *** |
| BUSSEG | 0.099 | 0.000 *** | 0.107 | 0.000 *** |
| FOREIGN | 0.001 | 0.034 ** | 0.001 | 0.000 *** |
| ICWEAK | 0.436 | 0.014 ** | 0.372 | 0.038 ** |
| Industry fixed-effect | Yes | | Yes | |
| Year fixed-effect | Yes | | Yes | |
| F-statistic | 32.07 | | 40.47 | |
| p-value | 0.000 | | 0.000 | |
| R-squared | 0.73 | | 0.74 | |
| N | 40,771 | | 1,590 | |

This table presents the results of the regression analysis for the model presented in Equation (1). The dependent variable is the natural logarithm of audit fees (LAF) for all the regressions. All other variables are defined in Appendix A. ***, **, * denote significance at 1, 5 and 10 percent levels, respectively.

**TABLE 7**

**Regression Results: Effect of Time of Disclosure on Audit Fees**

| | Panel A: Year *t-1* | | Panel B: Year *t* | | Panel C: Year *t+1* | |
|---|---|---|---|---|---|---|
| **Variable** | **Coeff.** | **p-value** | **Coeff.** | **p-value** | **Coeff.** | **p-value** |
| INTERCEPT | 7.415 | 0.000 *** | 8.563 | 0.000 *** | 7.904 | 0.000 *** |
| BREACH_TO_NEXT_FYEND | -0.055 | 0.406 | -0.079 | 0.226 | -0.072 | 0.242 |
| LTA | 0.490 | 0.000 *** | 0.405 | 0.000 *** | 0.397 | 0.000 *** |
| LEV | 0.208 | 0.081 * | 0.282 | 0.072 * | 0.079 | 0.042 ** |
| CUR | 0.412 | 0.000 *** | 0.342 | 0.001 *** | 0.324 | 0.005 *** |
| QUICK | 0.105 | 0.251 | 0.127 | 0.233 | 0.123 | 0.383 |
| ROA | 0.009 | 0.073 * | 0.005 | 0.068 * | 0.008 | 0.096 * |
| DEBTEQ | 0.004 | 0.838 | 0.001 | 0.652 | 0.007 | 0.632 |
| YE | -0.051 | 0.042 ** | -0.067 | 0.021 ** | -0.052 | 0.023 ** |
| BUSSEG | 0.131 | 0.058 * | 0.124 | 0.002 *** | 0.189 | 0.000 *** |
| FOREIGN | 0.009 | 0.095 * | 0.011 | 0.058 * | 0.006 | 0.016 ** |
| ICWEAK | 0.419 | 0.007 *** | 0.420 | 0.012 ** | 0.375 | 0.000 *** |
| Industry fixed-effect | | Yes | | Yes | | Yes |
| Year fixed-effect | | Yes | | Yes | | Yes |
| F-statistic | | 24.67 | | 23.26 | | 26.15 |
| p-value | | 0.000 | | 0.000 | | 0.000 |
| R-squared | | 0.86 | | 0.86 | | 0.88 |
| N | | 248 | | 248 | | 248 |

This table presents the results of the regression analysis for the model presented in Equation (1). The dependent variable is the natural logarithm of audit fees (LAF) for all the regressions. BREACH_TO_NEXT_FYEND is equal to the natural logarithm of the number of days between the date when an incident became public and the end date of the fiscal year in which the incident was disclosed. All other variables are defined in Appendix A. ***, **, * denote significance at 1, 5 and 10 percent levels, respectively.

**TABLE 8**
**Regression Results: Effect of Past Cyber-Security Incidents on Audit Fees**

| | Panel A | | Panel B | |
|---|---|---|---|---|
| **Variable** | **Coeff.** | **p-value** | **Coeff.** | **p-value** |
| INTERCEPT | 7.244 | 0.000 *** | 7.827 | 0.000 *** |
| PAST_BREACH | 0.003 | 0.952 | | |
| ΔYR_PAST_BREACH | | | -0.033 | 0.396 |
| LTA | 0.437 | 0.000 *** | 0.327 | 0.000 *** |
| LEV | 0.024 | 0.022 ** | 0.098 | 0.092 * |
| CUR | 0.460 | 0.000 *** | 0.377 | 0.007 *** |
| QUICK | 0.001 | 0.056 * | 0.001 | 0.038 ** |
| ROA | 0.003 | 0.078 * | 0.007 | 0.023 ** |
| DEBTEQ | 0.000 | 0.228 | 0.000 | 0.264 |
| YE | -0.025 | 0.097 * | -0.022 | 0.091 * |
| BUSSEG | 0.157 | 0.017 ** | 0.197 | 0.007 *** |
| FOREIGN | 0.002 | 0.057 * | 0.001 | 0.012 ** |
| ICWEAK | 0.302 | 0.001 *** | 0.316 | 0.075 * |
| Industry fixed-effect | Yes | | Yes | |
| Year fixed-effect | Yes | | Yes | |
| F-statistic | 33.95 | | 13.38 | |
| p-value | 0.000 | | 0.000 | |
| R-squared | 0.85 | | 0.87 | |
| N | 1,590 | | 1,590 | |

This table presents the results of the regression analysis for the model presented in Equation (1). The dependent variable is the natural logarithm of audit fees (LAF) for all the regressions. PAST_BREACH is an indicator variable equal to 1 if a firm was previously affected by a cyber-security incident(s), 0 otherwise. ΔYR_PAST_BREACH is equal to the number of fiscal years since the disclosure of the disclosure of previous breach (if any). All other variables are defined in Appendix A. ***, **, * denote significance at 1, 5 and 10 percent levels, respectively.

**TABLE 9**

**Regression Results: Effect of Peer Cyber-Security Incidents on Audit Fees**

| | Panel A: Full Sample | | Panel B: Full Sample | | Panel C: Breached Firms | | Panel D: Breached Firms | |
|---|---|---|---|---|---|---|---|---|
| **Variable** | **Coeff.** | **p-value** | **Coeff.** | **p-value** | **Coeff.** | **p-value** | **Coeff.** | **p-value** |
| INTERCEPT | 9.257 | 0.000 *** | 9.247 | 0.000 *** | 7.116 | 0.000 *** | 7.101 | 0.000 *** |
| PEER_BREACH | 0.111 | 0.000 *** | | | 0.058 | 0.043 ** | | |
| N_PEER_BREACH | | | 0.032 | 0.000 *** | | | 0.038 | 0.000 *** |
| LTA | 0.518 | 0.000 *** | 0.530 | 0.000 *** | 0.534 | 0.000 *** | 0.534 | 0.000 *** |
| LEV | 0. 031 | 0.081 * | 0.033 | 0.072 * | 0.049 | 0.009 *** | 0.047 | 0.019 ** |
| CUR | 0.499 | 0.000 *** | 0.499 | 0.000 *** | 0.045 | 0.001 *** | 0.052 | 0.000 *** |
| QUICK | -0.002 | 0.114 | -0.001 | 0.128 | 0.004 | 0.048 ** | 0.002 | 0.051 * |
| ROA | 0.003 | 0.012 ** | 0.004 | 0.004 ** | 0.001 | 0.053 * | 0.001 | 0.042 ** |
| DEBTEQ | 0.000 | 0.551 | 0.000 | 0.573 | 0.000 | 0.123 | 0.000 | 0.118 |
| YE | -0.064 | 0.000 *** | -0.066 | 0.000 *** | -0.021 | 0.053 * | -0.020 | 0.058 * |
| BUSSEG | 0.115 | 0.000 *** | 0.116 | 0.000 *** | 0.142 | 0.000 *** | 0.142 | 0.000 *** |
| FOREIGN | 0.000 | 0.076 * | 0.000 | 0.063 * | 0.002 | 0.043 ** | 0.002 | 0.048 ** |
| ICWEAK | 0.454 | 0.000 *** | 0.447 | 0.000 *** | 0.234 | 0.000 *** | 0.235 | 0.000 *** |
| Industry fixed-effect | Yes | | Yes | | Yes | | Yes | |
| Year fixed-effect | Yes | | Yes | | Yes | | Yes | |
| F-statistic | 34.45 | | 75.31 | | 38.61 | | 33.19 | |
| p-value | 0.000 | | 0.000 | | 0.000 | | 0.000 | |
| R-squared | 0.78 | | 0.72 | | 0.79 | | 0.80 | |
| N | 35,575 | | 35,575 | | 1,590 | | 1,590 | |

This table presents the results of the regression analysis for the model presented in Equation (1) for the full sample (Panel A) and for the subsample of breached firms (Panel B). The dependent variable is the natural logarithm of audit fees (LAF) for all the regressions. PEER_BREACH is an indicator variable which is equal to 1 if a cyber-security incident occurred within the same industry in the previous fiscal year, 0 otherwise. N_PEER_BREACH is the number of cyber-security incidents occurred within the same industry in the previous fiscal year. All other variables are defined in Appendix A. ***, **, * denote significance at 1, 5 and 10 percent levels, respectively.

**TABLE 10**

**Descriptive statistics and Test on Differences on Matched Sample**

| Variable | Overall | Breached | Non-Breached | Diff. | t-statistic | p-value | |
|---|---|---|---|---|---|---|---|
| LAF | 15.727 | 15.994 | 15.689 | 0.304 | 6.01 | 0.000 | *** |
| LTA | 8.783 | 9.010 | 8.549 | 0.462 | 4.87 | 0.000 | *** |
| LEV | 2.340 | 0.267 | 0.197 | 0.070 | 9.10 | 0.000 | *** |
| CUR | 0.380 | 0.382 | 0.378 | 0.004 | 1.55 | 0.261 | |
| QUICK | 1.487 | 1.450 | 1.523 | -0.073 | -1.10 | 0.386 | |
| ROA | 0.034 | 0.041 | 0.028 | 0.012 | 1.44 | 0.149 | |
| DEBTEQ | 0.574 | 0.513 | 0.573 | -0.080 | -0.85 | 0.397 | |
| BUSSEG | 0.734 | 0.704 | 0.764 | -0.060 | -1.85 | 0.176 | |
| FOREIGN | 0.261 | 0.235 | 0.287 | -0.052 | -2.22 | 0.026 | ** |
| YE | 0.320 | 0.367 | 0.273 | 0.092 | 3.46 | 0.001 | *** |
| ICWEAK | 0.027 | 0.032 | 0.023 | 0.009 | 0.96 | 0.339 | |
| N(Firm-years) | 856 | 428 | 428 | | | | |
| Firms | 214 | 107 | 107 | | | | |

This table presents the descriptive statistics of the variables adopted in the empirical analysis for the propensity-score matched sample.
All the variables are defined in Appendix A. ***, **, * denote significance at 1, 5 and 10 percent levels, respectively.

**TABLE 11**

**Regression Results: Cyber-Security Incidents and Audit Fees - DID Analysis**

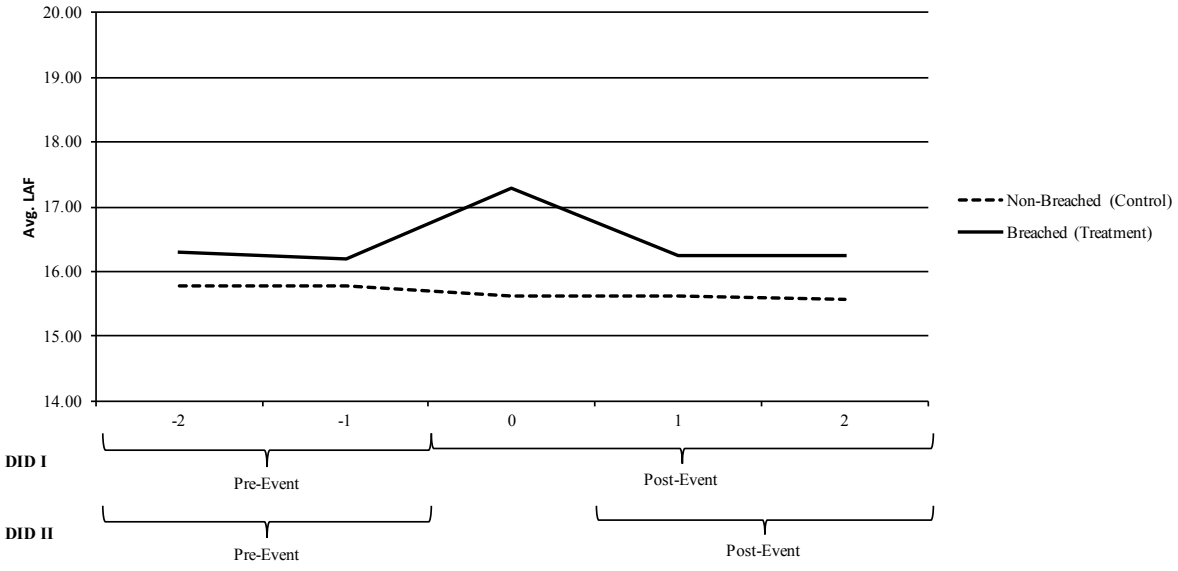
| | DID I | | | | DID II | | | |
|---|---|---|---|---|---|---|---|---|
| | Panel A: Matched Sample | | Panel B: Matched Sample (First Breach) | | Panel C: Matched Sample | | Panel D: Matched Sample (First Breach) | |
| **Variable** | **Coeff.** | **p-value** | **Coeff.** | **p-value** | **Coeff.** | **p-value** | **Coeff.** | **p-value** |
| INTERCEPT | 10.326 | 0.000 *** | 10.166 | 0.000 *** | 10.384 | 0.000 *** | 10.392 | 0.000 *** |
| TREATMENT | 0.313 | 0.002 *** | 0.330 | 0.007 *** | 0.308 | 0.002 *** | 0.351 | 0.003 *** |
| POST | 0.024 | 0.453 | 0.036 | 0.315 | 0.018 | 0.605 | 0.019 | 0.568 |
| TREATMENTxPOST | 0.241 | 0.026 ** | 0.213 | 0.029 ** | -0.201 | 0.265 | -0.522 | 0.213 |
| LTA | 0.546 | 0.000 ** | 0.560 | 0.000 ** | 0.537 | 0.000 *** | 0.538 | 0.000 *** |
| LEV | 0.065 | 0.003 *** | 0.054 | 0.004 *** | 0.056 | 0.024 ** | 0.054 | 0.032 ** |
| CUR | 0.038 | 0.024 ** | 0.044 | 0.014 ** | 0.041 | 0.032 ** | 0.041 | 0.031 ** |
| QUICK | 0.003 | 0.049 ** | 0.002 | 0.041 ** | 0.001 | 0.062 * | 0.001 | 0.055 ** |
| ROA | 0.003 | 0.004 *** | 0.004 | 0.000 *** | 0.002 | 0.014 * | 0.002 | 0.014 ** |
| DEBTEQ | 0.000 | 0.601 | 0.000 | 0.542 | 0.000 | 0.331 | 0.000 | 0.330 |
| YE | -0.026 | 0.473 | -0.025 | 0.568 | -0.027 | 0.506 | -0.029 | 0.471 |
| BUSSEG | 0.106 | 0.000 *** | 0.162 | 0.000 *** | 0.112 | 0.000 *** | 0.116 | 0.000 *** |
| FOREIGN | 0.004 | 0.000 *** | 0.002 | 0.000 *** | 0.003 | 0.028 ** | 0.003 | 0.023 ** |
| ICWEAK | 0.045 | 0.693 | 0.002 | 0.689 | 0.085 | 0.430 | 0.079 | 0.488 |
| Industry fixed-effect | Yes | | Yes | | Yes | | Yes | |
| Year fixed-effect | Yes | | Yes | | Yes | | Yes | |
| F-statistic | 29.16 | | 16.61 | | 31.04 | | 13.38 | |
| p-value | 0.000 | | 0.000 | | 0.000 | | 0.000 | |
| R-squared | 0.82 | | 0.82 | | 0.81 | | 0.81 | |
| N | 1,070 | | 1,020 | | 856 | | 816 | |

This table presents the results of the difference-in-difference (DID) on the propensity-score matched sample – Equation (3). The dependent variable is the natural logarithm of audit fees (LAF). Panels A and B present the results of DID I while Panels C and D present the results of DID II (see Figure 1). TREATMENT is an indicator variable which is equal to 1 if a firm belongs to our treatment sample (i.e. if it was breached), 0 otherwise. POST is an indicator variable which is equal to 1 in the post-breach event, 0 otherwise. TREATMENTxPOST is the DID estimator. All other variables are defined in Appendix A. ***, **, * denote significance at 1, 5 and 10 percent levels, respectively.

Chow Tests for structural breaks on breached firms audit fees: p-value=0.264 (Panel A); p-value=0.135 (Panel B);-p-value=0.186 (Panel C); p-value=0.158 (Panel D).

**FIGURE 2**

**Audit Fees Distribution by Time and Propensity-Score Matched Subsamples**




T-test on average change in audit fees between treatment and control:
(-2;-1): t-statistics = 0.646; p-value = 0.516
(-1;0): t-statistics = 21.19; p-value = 0.000***
(0;+1): t-statistics = 18.37; p-value = 0.000***
(+1;+2): t-statistics = 0.548; p-value = 0.639

This figure reports the distribution of audit fess by time and propensity-score matched subsamples, and t-tests on the difference in the average change in audit fees between breached and non-breached firms across different time periods. ***, **, * denote significance at 1, 5 and 10 percent levels, respectively.
Note: the year of cyber-security incidents (i.e. 0) is reported to graphically show the trend of the average value of the audit fees around the breach announcement. However, it is not included in the DID analysis (Table 10) whose objective is to directly compare the pre- and post-event periods.

**TABLE 12**

**Frequency Distribution by SEC Comment Letters by Incident Type**

| Type | No. of Letter | Percentage | No. of firms | Percentage |
|---|---|---|---|---|
| Non-Breached | 62 | 89.86 | 62 | 89.86 |
| CARD | 1 | 1.45 | 1 | 1.45 |
| DISC | 1 | 1.45 | 1 | 1.45 |
| HACK | 4 | 5.80 | 4 | 5.80 |
| INSD | 1 | 1.45 | 1 | 1.45 |
| Breached | 7 | 10.14 | 7 | 10.14 |
| Total | 69 | 100.00 | 69 | 100.00 |

Average Time Gap Between Incidents and Comment Letters: 1 Year

This table summarizes the frequency of SEC Comment Letters related to cyber-security by incident type and the time gap between incidents and Comment Letters.

**TABLE 13**
**Regression Results: Effect of SEC Comment Letters on Audit Fees**

| | Panel A: Full Sample | | | | Panel B: Non-Breached Firms | | | |
|---|---|---|---|---|---|---|---|---|
| **Regression Type** | **OLS** | | **DID** | | **OLS** | | **DID** | |
| **Variable** | **Coeff.** | **p-value** | **Coeff.** | **p-value** | **Coeff.** | **p-value** | **Coeff.** | **p-value** |
| INTERCEPT | 9.948 | 0.000 *** | 9.546 | 0.000 *** | 9.948 | 0.000 *** | 9.547 | 0.000 *** |
| CLETTER | 0.043 | 0.013 ** | | | 0.043 | 0.011 ** | | |
| TREATMENT_CL | | | 0.045 | 0.132 | | | 0.045 | 0.131 |
| POST | | | 0.025 | 0.011 ** | | | 0.025 | 0.011 ** |
| TREATMENT_CLxPOST | | | 0.073 | 0.018 ** | | | 0.073 | 0.018 ** |
| LTA | 0.530 | 0.000 *** | 0.423 | 0.000 *** | 0.530 | 0.000 *** | 0.423 | 0.000 *** |
| LEV | 0. 033 | 0.073 * | 0.025 | 0.023 ** | 0. 033 | 0.073 * | 0.025 | 0.025 ** |
| CUR | 0.499 | 0.000 *** | 0.564 | 0.000 *** | 0.499 | 0.000 *** | 0.563 | 0.000 *** |
| QUICK | -0.001 | 0.127 | -0.001 | 0.058 * | -0.001 | 0.127 | -0.001 | 0.058 * |
| ROA | 0.004 | 0.004 *** | 0.006 | 0.029 ** | 0.004 | 0.004 *** | 0.006 | 0.030 ** |
| DEBTEQ | 0.000 | 0.574 | 0.001 | 0.821 | 0.000 | 0.574 | 0.002 | 0.821 |
| YE | -0.066 | 0.000 *** | -0.043 | 0.000 *** | -0.066 | 0.000 *** | -0.043 | 0.000 *** |
| BUSSEG | 0.116 | 0.000 *** | 0.117 | 0.073 * | 0.116 | 0.000 *** | 0.117 | 0.073 * |
| FOREIGN | 0.000 | 0.062 * | 0.000 | 0.066 * | 0.000 | 0.062 * | 0.001 | 0.061 * |
| ICWEAK | 0.449 | 0.000 *** | 0.489 | 0.037 ** | 0.449 | 0.000 *** | 0.489 | 0.037 ** |
| Industry fixed-effect | Yes | | Yes | | Yes | | Yes | |
| Year fixed-effect | Yes | | Yes | | Yes | | Yes | |
| F-statistic | 39.47 | | 36.95 | | 39.47 | | 36.95 | |
| p-value | 0.000 | | 0.000 | | 0.000 | | 0.000 | |
| R-squared | 0.71 | | 0.73 | | 0.71 | | 0.73 | |
| N | 40,771 | | 552 | | 40,687 | | 496 | |

This table presents the results of the regression analysis for the model presented in Equations (1) and (3). The dependent variable is the natural logarithm of audit fees (LAF) for all the regressions. TREATMENT_CL is an indicator variable which is equal to 1 if a firm belongs to our treatment sample (i.e. if it received a SEC Comment Letter), 0 otherwise. POST is an indicator variable which is equal to 1 in the post-letter event (i.e. *t+1* and *t+2*), 0 otherwise. TREATMENT_CLxPOST is the DID estimator. All other variables are defined in Appendix A. ***, **, * denote significance at 1, 5 and 10 percent levels, respectively. The year of SEC Comment Letter is not included when running the DID regression since the objective is to directly compare the pre- and post-letter periods.

**Appendix A**

**This table provides the definition of the variables included in the analysis and the respective data sources.**

| Variable | Source | Definition |
|---|---|---|
| LAF | Audit Analytics - Audit Fees | Natural logarithm of audit fees. |
| LTA | Compustat | Natural logarithm of end of year total assets. |
| LEV | Compustat | Current liabilities divided by total assets. |
| CUR | Compustat | Current assets divided by total assets. |
| QUICK | Compustat | Difference between current assets and inventory divided by current liabilities. |
| ROA | Compustat | Earnings before interest and taxes divided by total assets. |
| DEBTEQ | Compustat | Total debt divided by equity book value. |
| BUSSEG | Compustat | Natural logarithm of number of business segments. |
| FOREIGN | Compustat | Foreign sales divided by total sales. |
| R&D | Compustat | Natural logarithm of research and development expenses. |
| ABAFEES | | Abnormal Audit Fees. |
| IMR | | Inverse Mills Ratio. |
| YE | Compustat | 1 if a firm's fiscal year does not end on December 31, 0 otherwise. |
| ICWEAK | Compustat | 1 if a firm's disclosure controls were not found to be effective under Section 302 of the Sarbanes-Oxley Act of 2002, 0 otherwise |
| RISK_COMMITTEE | Audit Analytics Officer Director Changes | 1 if a firm discloses the presence of a board-level committee with the word 'Risk' in the title in the proxy statement released prior to the date of the breach, 0 otherwise. |
| COMP_COMMITTEE | Audit Analytics Officer Director Changes | 1 if a firm discloses the presence of a board-level committee with the word 'Compliance' in the title in the proxy statement released prior to the date of the breach, 0 otherwise. |
| TECH_COMMITTEE | Audit Analytics Officer Director Changes | 1 if a firm discloses the presence of a board-level committee with the word 'Technology' in the title in the proxy statement released prior to the date of the breach, 0 otherwise. |
| BREACH | Privacy Rights Clearinghouse | 1 if a firm has a cyber-security incident in year *t*, 0 otherwise. |
| TREATMENT | | 1 if a firm belongs to the treatment sample (i.e. breached) used in the DID analysis for the effect of cyber-security incidents on audit fees, 0 otherwise. |
| CARD | Privacy Rights Clearinghouse | 1 if a cyber-security security incident was due to payment cards, 0 otherwise. |
| DISC | Privacy Rights Clearinghouse | 1 if a cyber-security security incident was due to unintended information disclosure, 0 otherwise. |
| HACK | Privacy Rights Clearinghouse | 1 if a cyber-security security incident was due to a malicious outsider attack, 0 otherwise. |

**Appendix A (continued)**
**This table provides the definition of the variables included in the analysis and the respective data sources.**

| Variable | Source | Definition |
|---|---|---|
| INSD | Privacy Rights Clearinghouse | 1 if a cyber-security security incident was due to a malicious insider, 0 otherwise. |
| PHYS | Privacy Rights Clearinghouse | 1 if a cyber-security security incident was due to unauthorized physical access, 0 otherwise.. |
| PORT | Privacy Rights Clearinghouse | 1 if a cyber-security security incident was due to lost or missing portable device(s), 0 otherwise. |
| STAT | Privacy Rights Clearinghouse | 1 if a cyber-security security incident was due to stationary device(s), 0 otherwise. |
| PAST_BREACH | Privacy Rights Clearinghouse | 1 if a firm was previously affected by a cyber-security incident(s), 0 otherwise. |
| ΔYR_PAST_BREACH | Privacy Rights Clearinghouse | Number of years since the last cyber-security incident. |
| PEER_BREACH | Privacy Rights Clearinghouse | 1 if a cyber-security incident occurred within the same industry of a firm in the previous fiscal year, 0 otherwise. |
| N_PEER_BREACH | Privacy Rights Clearinghouse | Number of cyber-security incidents occurred within the same industry of a firm in the previous fiscal year, 0 otherwise. |
| BREACH__T-1 | Privacy Rights Clearinghouse | 1 if a firm disclosed a cyber-security incident(s) in the previous fiscal year, 0 otherwise. |
| BREACH_T+1 | Privacy Rights Clearinghouse | 1 if a firm disclosed a cyber-security incident(s) in the following fiscal year, 0 otherwise. |
| BREACH_TO_NXT_FYEND | Privacy Rights Clearinghouse<br>Compustat | Natural logarithm of the number of days between the date when a cyber-security incident became public and the end date of the fiscal year in which the incident was disclosed. |
| CLETTER | Audit Analytics<br>SEC Comment Letters | 1 if when an firm receives a Comment Letter, 0 otherwise. |
| TREATMENT_CL | | 1 if a firm belongs to the treatment sample (i.e. breached) used in the DID analysis for the effect of SEC Comment Letter related to cyber-security on audit fees, 0 otherwise. |
| POST | | 1 if a fiscal-year is after a cyber-security incident (Table 10) or after a SEC Comment Letter related to cyber-security (Table 12), 0 otherwise. |

**Appendix B**

**This table provides the definition and exemplar cases of different types of cyber security incidents as classified and reported by Privacy Rights Clearinghouse.**

| Type | Definition | Example |
|---|---|---|
| CARD | Payment card fraud. | Company: Barnes & Nobles Inc.<br>Disclosure Date: October 24, 2012.<br>Records Breached: Unknown.<br>Brief Description: PIN pad devices used to process credit and debit card information in 63 stores in nine states stores were compromised. |
| DISC | Unintended information disclosure. | Company: Choice Hotels Internationals Inc.<br>Disclosure Date: April 26, 2012.<br>Records Breached: Unknown.<br>Brief Description: An unknown number of customers had their personal information entered into the wrong field in a database. The information should have been encrypted but was not because of the error. |
| HACK | Malicious outsider attack. | Company: LinkedIn.com.<br>Disclosure Date: June 6, 2012.<br>Records Breached: 167,000,000.<br>Brief Description: A file containing 6,458,020 encrypted passwords was posted online by a group of hackers. It is unclear what other types of information were taken from Linkedin users. |
| INSD | Malicious insider. | Company: Expedia Corporate Travel.<br>Disclosure Date: November 15, 2006.<br>Records Breached: Unknown.<br>Brief Description: A former call center employee somehow gained access to credit card numbers and may have misused the information. The former employee attempted to make unauthorized charges at least twice. |
| PHYS | Physical loss. | Company Name: Denny's Corp.<br>Disclosure Date: September 30, 2013.<br>Records Breached: 200.<br>Brief Description: Job applications from a Denny's in Phoenix were found in a dumpster behind the Denny's. The paperwork dated back to August of 2012. The information included addresses, Social Security numbers, and other information normally found on job applications. |
| PORT | A lost, discarded or stolen portable device. | Company: Forrester Research<br>Disclosure Date: December 5, 2007.<br>Records Breached: Unknown.<br>Brief Description: Thieves stole a laptop from the home of a Forrester Research employee, potentially exposing the names, addresses and Social Security numbers of an undisclosed number of current and former employees and directors. |
| STAT | Stationary device. | Company: Oracle Corporation.<br>Disclosure Date: November 11, 2007.<br>Records Breached: 132.<br>Brief Description: A computer that contained employee and contractor information was misplaced during a move. Employees and contractors of Lodestar may have had their names, Social Security numbers, addresses, earning information and expense information exposed. |

**Appendix C**

**Frequency Distribution of Cyber-Security Incidents by Industry**

| SIC Code | No. of breaches | Percentage |
|---|---|---|
| 13 | 1 | 0.27% |
| 15 | 2 | 0.54% |
| 16 | 1 | 0.27% |
| 17 | 2 | 0.54% |
| 20 | 5 | 1.35% |
| 23 | 2 | 0.54% |
| 27 | 2 | 0.54% |
| 28 | 9 | 2.43% |
| 29 | 3 | 0.81% |
| 30 | 1 | 0.27% |
| 33 | 1 | 0.27% |
| 35 | 12 | 3.23% |
| 36 | 16 | 4.31% |
| 37 | 14 | 3.77% |
| 38 | 7 | 1.89% |
| 40 | 2 | 0.54% |
| 45 | 5 | 1.35% |
| 47 | 1 | 0.27% |
| 48 | 24 | 6.47% |
| 49 | 9 | 2.43% |
| 50 | 4 | 1.08% |
| 51 | 1 | 0.27% |
| 52 | 5 | 1.35% |
| 53 | 12 | 3.23% |
| 54 | 2 | 0.54% |
| 55 | 6 | 1.62% |
| 56 | 9 | 2.43% |
| 57 | 2 | 0.54% |
| 58 | 14 | 3.77% |
| 59 | 18 | 4.85% |
| 60 | 53 | 14.29% |
| 61 | 22 | 5.93% |
| 62 | 16 | 4.31% |
| 63 | 21 | 5.66% |
| 64 | 4 | 1.08% |
| 65 | 1 | 0.27% |
| 67 | 6 | 1.62% |
| 70 | 2 | 0.54% |
| 72 | 4 | 1.08% |
| 73 | 40 | 10.78% |
| 78 | 4 | 1.08% |
| 87 | 1 | 0.27% |
| 99 | 5 | 1.35% |
| Total | 371 | 100.00% |

This table reports the frequency distribution of cyber-security incidents by Industry. Note: only non-financial firms were included in our final sample.