JOURNAL OF INFORMATION SYSTEMS
Vol. 33, No. 3
Fall 2019
pp. 227–265

American Accounting Association
DOI: 10.2308/isys-52379

Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches

Vernon J. Richardson
University of Arkansas

Rodney E. Smith
California State University, Long Beach

Marcia Weidenmier Watson
The University of North Carolina at Charlotte

ABSTRACT: In this paper, we examine the consequences of data breaches for a breached company. We find the economic consequences are, on average, very small for breached companies. On average, breaches result in less than −0.3 percent cumulative abnormal returns in the short window around the breach disclosure. Except for a few catastrophic breaches, the nominal difference in cumulative abnormal returns between breach companies and the matched companies disappears within days after the breach. We also test whether data breaches affect future accounting measures of performance, audit and other fees, and future Sarbanes-Oxley Section 404 reports of material internal control weaknesses, but find no differences between breach and matched companies. Our results address the question why companies are not spending more to reduce breaches. We conclude by providing a few explanations of why there appears to be an effect at the economy-wide level, but no noticeable effect on individual company performance.

Keywords: cybersecurity; breaches; financial impact.

Much Ado About Nothing

> Every minute, we are seeing about half a million attack attempts that are happening in cyber space.
> —Derek Manky, Fortinet global security strategist (CNBC 2015)

> There are only two types of companies: Those that have been hacked and those that don't know they have been hacked.
> —Chambers (2018)

I. INTRODUCTION

The above quotes encapsulate the current business environment where "the [a]ssumption of a breach is the new norm" (Hayden 2013) and data breaches are growing "larger in number and impact" (De Groot 2019). Potential impacts of a data breach include both tangible (direct) and intangible (indirect) costs to the breached company (Layton and Watters 2014). These potential costs include expenditures for legal counsel, class action settlements, state and federal regulation compliance, and restoring/improving computer systems, as well as loss of reputation, intellectual property, and productivity (Gwebu, Wang, and Xie 2014; Layton and Watters 2014; Morgan 2017a). In addition, data breaches expose real, underlying operational control risks in a company (Lawrence, Minutti-Meza, and Vyas 2018). Accordingly, cybersecurity is the top concern for both executives and accounting professionals (AICPA 2015; Protiviti 2016). Yet, companies are still not spending

Editor's note: Accepted by Tawei (David) Wang.

Submitted: April 2018
Accepted: November 2018
Published Online: February 2019

enough on cybersecurity to prevent data breaches (Morgan 2017b). With such a (potentially) high cost and level of concern about cybersecurity, why are companies not working harder (and investing more) to reduce the number of data breaches by investing in cybersecurity?

To gain insights on this question, this study examines four potential economic impacts of data breaches. We define a data breach as "a security violation in which sensitive, protected or confidential *data* is copied, transmitted, viewed, stolen or used by an unauthorized individual" (Privacy Rights Clearinghouse 2018; emphasis added).[1] We focus on four economic impacts based on a review of extant literature, which can be grouped into the following four main categories: stock market response, impact on accounting measures of performance, impact on audit and other fees, and impact on Sarbanes-Oxley Section 404 (SOX 404) internal control material weakness reporting.[2]

Our literature review shows that the stock market response to a data breach announcement is the most researched category, with 75 percent of the studies finding a negative response to a data breach. However, results appear to vary based on data source, time period, and type of estimation model used. The second-most researched category is the impact of a data breach on future performance. With respect to this category, extant literature has mixed findings with respect to the short-term and long-term positive or negative impact on different performance measures (e.g., sales, return on assets, earnings). The next two categories, audit fees and SOX 404, are just beginning to be researched. Audit fee studies generally find that audit fees increase after a breach due to increased risks requiring additional audit work (e.g., Smith, Higgs, and Pinsker 2019; Li, No, and Boritz 2016; Yen, Lim, Wang, and Han 2018). But, once again, research does not agree what type of data breach is driving the results. Finally, with respect to SOX 404, Westland (2018) reports that SOX 404 material weaknesses are very effective at identifying credit card breaches (100 percent) and somewhat effective at identifying insider breaches (33 percent). On the other hand, Lawrence et al. (2018) determine that SOX 404 reporting may miss operational controls problems, including data breaches, and is more likely to report them on a less, rather than more, timely basis.

While myriad studies examine these four economic consequences, only a few studies examine multiple (but not all) categories at the same time (e.g., Akey, Lewellen, and Liskovich 2018; Bianchi and Tosun 2018; Hilary, Segal, and Zhang 2016). Thus, gaining an understanding of the (complete) economic consequences to a breached company is difficult as each study generally focuses on one consequence using a variety of data sources, sample selection criteria, time periods, and estimation models. Accordingly, Kvochko and Pant (2015) state that the stock market will not react to a data breach because investors do not have enough information to measure the breach's impact. To gain a better understanding of the economic impacts of a data breach, we take a holistic approach examining all four economic consequences using the same data sources, sample selection criteria, and time period. This approach allows us to determine how each category affects breached companies, as well as the (likely) magnitude of any economic consequences.

Our study contributes to the growing literature surrounding cybersecurity. Specifically, our approach allows us to gain a deeper understanding of the totality of economic consequences, or lack thereof, of data breaches. Our study should help regulators, executives, investors, analysts, and auditors understand how a data breach can economically impact a company. For regulators, our study is timely as the PCAOB and SEC are prioritizing cybersecurity as major initiatives (Hammer and Zuckerman 2018; PCAOB 2017).[3] Our results should provide useful information for the companies as they begin to calculate the cost of cyber risk in monetary terms (i.e., Factor Analysis of Information Risk [FAIR]) (Evolver Inc. 2018). In addition, if we find that companies do not experience costly economic consequences after a breach, it may explain why executives do not spend money on cybersecurity ahead of time. Our results should help investors and analysts better understand the long-term financial impact of a data breach to make/guide investment decisions. Finally, auditors should find our results helpful as they determine how a data breach changes the company's risk and what changes to the audit plan are necessary to minimize audit risk.

We obtain our sample of data breaches from two sources. First, we use publicly available information from privacyrights.org, which documents data breaches that affect privacy rights, over the period 2005 to 2017. Second, we obtain data from Audit Analytics documenting data breaches over the period 2004 to 2018.[4] We augment the sample with archival data from CRSP, Compustat, Audit Analytics, and hand collection. After identifying 827 companies with data breaches over the period, we form matched samples to ensure we fully capture company characteristics consistent with those of the breach

[1] Data breaches are a subset of security breaches (i.e., breach without loss of data), which are, in turn, a subset of security incidents (i.e., breaches of security or loss of integrity) (European Parliament 2013). We also include 20 reported denial of service attacks, because those can have similar economic impacts.

[2] Appendix A presents a summary of this research grouped by the four categories.

[3] On February 7, 2018, the SEC's Office of Compliance Inspections and Examinations announced that the SEC is prioritizing cybersecurity (Hammer and Zuckerman 2018).

[4] The last data breach in the sample occurred on May 25, 2018.

companies. This allows us to assess any economic impact of data breaches using a sample that is many times larger than most extant research.

Our results show that the consequences of data breaches are on average very small for the breached companies. On average, breaches result in average returns of −0.03 percent and cumulative abnormal returns less than −0.274 percent in the short window around the breach disclosure. While, multivariate tests show that the breach companies' cumulative abnormal return is significantly different than matched companies' returns, the nominal difference in cumulative abnormal returns between breach companies and the matched companies disappears within days after the breach. Most of the difference between companies disclosing breaches and matched companies is driven by the rare catastrophic incidents. We also do not find a difference between breach and matched companies for (1) future performance, (i.e., total revenue, sales growth, return on sales, and return on assets), (2) audit and other fees, and (3) SOX 404 reports of material internal control weaknesses. Overall, we find no material economic impacts for a company after a data breach.

Our results do not suggest that breaches have no economic impact, but the effect seems to be at the economy-wide level rather than at the level of the individual company. A recent report by the Council of Economic Advisors (2018) estimates the cost of malicious cyber activity to the U.S. economy between $57 billion and $106 billion in 2016.[5] The report also notes that much of those costs reflect negative externalities imposed on other economic entities and private citizens rather than on the breach company. Moreover, with the average financial or commercial business identifying multiple attacks per month (Gogan 2017; Weisbaum 2018), breach victims may suffer from breach fatigue. Given that the source of the breach is typically unknown, these victims believe that their personal data are compromised and, rather than blaming the company that improperly disclosed the data, they simply change passwords, add two-factor authentication, and try to safeguard identities (Kan 2017).

We organize the remainder of the study as follows: In Section II, we review the data breach literature and develop our hypotheses; in Section III, we describe our sample, and the research design is described in Section IV; we discuss the results in Section V, and provide concluding comments in Section VI.

II. BACKGROUND AND HYPOTHESIS DEVELOPMENT

Data Breaches

In 2013, hackers stole 40 million credit cards and 70 million customers' personal data from Target Corporation after stealing the credentials of a refrigerator, heating, and air conditioning subcontractor (Krebs 2014).[6] Credit card issuers spent $200 million reissuing credit cards. Target was named in at least 90 lawsuits; the CIO, CISO, and CEO lost their jobs; and analysts estimate Target will spend billions to respond to the breach (Gonsalves 2014). In 2014, The Home Depot Inc. had 56 million credit card numbers and 53 million email addresses stolen after hackers obtained an outside vendor's system credentials (Winter 2014). Home Depot spent $109 million in responding to the breach. In 2017, Equifax, Inc. experienced a massive data breach with 148 million customers' personally identifiable information being stolen (Fung 2018) after failing to apply a needed security patch (Shepardson 2017). Hackers were able to stay in the system for months before the breach was detected at the end of July. Equifax's stock plunged 18.4 percent in the days following the public breach announcement (Nusca 2017), and it was named in over 240 class action lawsuits (Surane and Westbrook 2018).

These high-profile cyber breaches are just a few of the cyber incidents over the last decade. As these three cases show, the number of victims (i.e., customers and employees) affected is increasing over time. Companies also appear to suffer dire consequences after cyber incidents. Accordingly, preventing security threats is the top technology-related priority for American and Canadian professional accountants (AICPA 2015). Moreover, executives rank cybersecurity as their top operational concern (Protiviti 2016); unsurprising, given that cyberattacks will cost businesses an estimated $2.9 trillion globally by 2019 (Morgan 2016). It is also the crime that U.S. consumers worry about the most (Riffkin 2014).

With this level of concern about cybersecurity, why do the incidents continue to happen? One would think that given the outcomes for Target, Home Depot, and Equifax, which included firings, indictments, lawsuits, and massive costs to respond, companies would go to great lengths (and great expense) to prevent cyber incidents. However, cyber incidents continue to happen at an increasing rate—potentially because companies are not investing in cybersecurity (Morgan 2017b). This viewpoint was supported by Jason Spaltro, Sony Corporation's executive director of information security, who stated that "'it's a valid business decision to accept the risk of a security breach. I will not invest $10 million to avoid a possible $1 million loss" (Holmes 2007). Several popular press articles also support this viewpoint, claiming that the pervading belief by executives is

[5] These cost figures are likely underestimated as there is widespread belief that most data breaches go unnoticed (e.g., Friedlander 2014; Thompson 2017).

[6] Unless otherwise noted, the information in this paragraph is from privacyrights.org and Barnes (2018).

that "worrying about data breaches isn't worth it" (e.g., Sherman 2015). For example, after insurance and the tax deduction effect, Target spent $105 million responding to its breach, or less than 0.01 percent of its 2014 sales revenues (Dean 2015).

However, U.S. companies may be finally paying attention to the occurrence of data breaches as costs continue to rise. According to a recent Ponemon Institute (2017) survey, compliance failures and rushing to notify are among the top five reasons why the cost of a breach is rising in the U.S. The same survey found that the average cost of a data breach is $7.35 million in 2017 (or $225 per record), which is an increase of 5 percent from 2016. Moreover, some breaches are far more costly than others. For example, Equifax spent $114 million resolving its data breach in 2017 (or 13.6 percent of its 2017 revenues) (Zachs Equity Research 2018)—a number large enough to get the attention of most executives.

Are companies making good business decisions by not investing in cybersecurity? It depends on the total economic consequence of a breach. Therefore, to better understand the economic consequences of a breach, we examine four categories of potential consequences: the stock market response, the impact on accounting measures of performance, the impact on audit and other fees, and the impact on Sarbanes-Oxley Section 404 internal control material weakness reporting. A review of the literature reveals that most studies focus on the stock market reaction, followed by the impact on performance. More recently, research has studied audit fees and SOX 404. Appendix A presents a summary of extant literature grouped by category. We draw on this literature review in the subsequent sections.

Stock Market Reaction

We begin with stock market reaction, as this is the most researched topic in the extant literature. Anecdotal evidence suggests that there may be no stock market reaction to a data breach. Kvochko and Pant (2015) argue that shareholders have neither enough information about data breaches nor sufficient tools to measure their impact. The long and mid-term effects of lost intellectual property, disclosure of sensitive data, and loss of customer confidence may result in a loss of market share, but these effects are difficult to quantify. Therefore, shareholders only react to breach news when it has direct impact on business operations, such as litigation charges (i.e., in the case of Target) or results in immediate changes to a company's expected profitability. But, given that cost of an average data breach in the U.S. to a company is only a small percentage of a large companies' revenues or profits,[7] combined with mixed evidence about the impact of a breach on company's short-term and long-term performance,[8] an argument can be made that data breaches have little, if any, short-term impact on the company and therefore on the stock market reaction.

Even if there is a short-term scare and reaction on the stock market to a data breach, we would expect no long-term impact because there is generally a minimal impact on future performance. This is consistent with Warren Buffett's comment on Graham and Dodd's (1934) statement that in the short-run, the stock market is like a popularity contest, but in the long-run is a scale. With little change in the scale (i.e., minimal change in operating performance), there is likely to be minimal long-term effects. In support of these statements, our literature review, shown in Table 11, Panel A of Appendix A, reveals that 15 percent of the studies do not find a significant impact on the stock market, with another 10 percent finding a significant reaction only at 10 percent significance. For example, Hilary et al. (2016) find that the short-term and long-term stock market reaction to a breach is not different than a matched sample. Kannan, Rees, and Sridhar (2007) find that removing 9/11 events makes cumulative abnormal returns insignificant, raising the question of just how many results may be impacted by including this time period.

Extant research does provide evidence of a negative impact on stock market reaction. A literature review by Spanos and Angelis (2016) finds that 75.6 percent of security breach studies report a negative impact on stock prices. Similarly, 75 percent of our updated and expanded literature review (Appendix A, Table 11, Panel A) finds that breaches have significant negative reactions ($p < 0.05$)—63 percent with an overall reaction and 12 percent with a reaction in the subset of the data. For example, significant negative stock market reactions were only found for confidential information (Campbell, Gordon, Loeb, and Zhou 2003; Aytes, Byers, and Santhanakrishnan 2006), when the breach was announced in a major newspaper (Bolster, Pantalone, and Trahan 2010), for employee data (Tanimura and Wehrly 2015), or only when a third party identified the breach (Amir, Levi, and Livne 2018).

For studies documenting an overall negative reaction, short-term reactions for breaches vary from −0.23 percent to over 5 percent. For example, Goel and Shawky (2009) find that, on average, the announcement of a data breach had a negative impact of about 1 percent of the market value of the company. Long-term reactions vary from −3.0 to over −7 percent. For example, Morse, Raval, and Wingender (2011) find that abnormal negative returns persist over the next year and a half (−8.68 percent)

[7] The average cost of a breach is $7.35 million (Ponemon Institute 2017).

[8] As discussed in the "Impact on Accounting Measures of Performance" section, some studies report improved performance after a breach (e.g., Zafar, Ko, and Osei-Bryson 2012), while other report reduced performance after a breach, especially for specific types of breaches (e.g., Ko, Osei-Bryson, and Dorantes 2009; Kamiya, Kang, Kim, Milidonis, and Stulz 2018).

moderated by the source of the breach with the market more heavily punishing those compromises that could have been avoided with reasonable precautions by the breached company.

In addition, 17 percent of the studies report that the stock market reaction changes over time. Some studies find a decreased response (Gordon, Loeb, and Zhou 2011; Goel and Shawky 2014; Pirounias, Mermigas, and Patsakis 2014; Yayla and Hu 2011), while other studies report an increased response (Cavusoglu, Mishra, and Raghunathan 2004; Gatzlaff and McCullough 2010). In contrast, some studies do not find a change in response over time (Hilary et al. 2016; Johnson, Kang, and Lawson 2017). Similar mixed results exist for whether the financial industry is impacted more (Arcuri, Brogi, and Gandolfi 2017; Bose and Leung 2014) or not (Arcuri, Brogi, and Gandolfi 2014; Johnson et al. 2017).

Therefore, results seem to vary based on the sample, selection criteria, and method (Gordon et al. 2011). To test if there is a stock market reaction to a data breach for our sample of companies, we examine the following hypothesis stated in alternative form:

H1: On average, data breaches have a negative impact on short-term and long-term stock market returns.

Impact on Accounting Measures of Performance

The second-most researched area regarding data breaches is the impact on company performance as indicated by standard accounting measures. If the prevailing attitude of executives is "'I will not invest $10 million to avoid a possible $1 million loss" (Holmes 2007), then there are three relevant questions when considering the impact of a data breach on future performance: (1) Is the cost of preventing a data breach, on average, more expensive than just experiencing one? (2) Is the average cost of a data breach for the average company material? and (3) Does a breach tarnish the company's reputation and therefore affect future sales and profitability?

For researchers, directly investigating the first two questions on a wide scale is difficult due to a lack of data. For many companies, we suspect that preventing, addressing, and detecting data breaches is an accepted cost of business to which essentially all companies are subject. Companies that spend less preventing a data breach might have a slightly higher cost of remediating but, on average, there will not be a measurable increase in prevention costs following a data breach. With the average cost of a breach at $7.35 million in 2017 (Ponemon Institute 2017), it does not seem that there will be a material impact on overall performance on large companies.

Assessing the impact on reputation is also difficult. However, future financial statement data are observable. So, examining the performance of companies after the breach should provide insights into the breach's impact on performance. A company's profitability may decrease from lower sales due to reputational effects[9] or due to costs required to resolve the breach (Layton and Watters 2014).

We identified nine studies examining the impact of a breach on future operating performance shown in Table 12 of Appendix A.[10] Table 12, Panel A shows that 16 measures have been scrutinized to determine the impact of a breach on future company performance. Overall, these studies report some evidence of a negative impact on ten measures:

- future sales (Ko and Dorantes 2006; Kamiya et al. 2018; Lending, Minnick, and Schorno 2018),
- return on assets (ROA) (Ko and Dorantes 2006; Ko et al. 2009; Kamiya et al. 2018),
- return on sales (ROS) for large breached companies ($p < 0.10$) (Ko et al. 2009),
- return on equity (ROE) (Kamiya et al. 2018),
- dividends ($p < 0.10$) (Bianchi and Tosun 2018),
- research and development expenditures ($p < 0.10$) (Bianchi and Tosun 2018),
- cost of goods sold (Ko et al. 2009),
- nonrecurring expenditures (most likely to repair reputation) (Kamiya et al. 2018),
- cash flow volatility (Kamiya et al. 2018), and
- long-term debt (Kamiya et al. 2018).

However, these results are either based on one study, only significant at the 10 percent level, or not consistent across multiple studies (e.g., sales, ROA, ROS, earnings, research and development, and cost of goods sold). The "Summary" for Table 12 (Panel C) reports that only one of the variables found to be significant at the 5 percent level is examined by more than one study. Moreover, some studies report a significant increase in performance after a breach (e.g., Zafar et al. 2012; Ko and

[9] See Ko and Dorantes (2006) for a discussion of the impact of loss of reputation.

[10] We also found Layton and Watters (2014); however, they estimate specific breach costs for two companies and, therefore, we do not include their study in Appendix A, Table 12, Panel B.

Dorantes 2006). To better understand the impact of a breach on future performance, we examine the following alternative hypothesis regarding performance:

H2: After a data breach, future company performance is negatively affected.

Impact on Audit and Other Fees

Table 13 of Appendix A presents the literature review exploring data breaches and audit fees and other fees. Auditors may increase their audit fees due to breach risk for several reasons. First, breaches are a type of client business risk that may adversely impact company operations potentially due to litigation, loss of profitability, increased costs, and loss of customers. Some evidence has been found that risk measures (i.e., beta, long-term debt, analyst forecast dispersion) increase after a breach (Cardenas, Coronado, Nicholas-Donald, Parra, and Mahmood 2012; Gwebu et al. 2014; Kamiya et al. 2018), indicating that business risk may increase after a breach causing total audit hours and audit fees to increase (Bell, Landsman, and Shackelford 2001).

Second, breaches are "actual realizations of an operational control risk" (Lawrence et al. 2018, 140). Given that operational and financial reporting mechanisms are based on the same controls, it is likely that an operational control risk (i.e., breach) is an indicator of a potential financial reporting risk that may affect specific accounts and require disclosure under SOX Section 404 (Lawrence et al. 2018). Moreover, operational failures may indicate management's lack of attention to control and other governance mechanisms (Lawrence et al. 2018). Thus, breaches may impact audit fees because the auditor has potentially perceived that control risk has increased, which, in turn, may increase audit risk, and ultimately audit fees (R. Hoitash, U. Hoitash, and Bedard 2008).

Compared to the prior categories, this category is relatively new, with the first study in 2016. Specifically, Li et al. (2016) test whether external auditors respond to cyberattacks[11] by charging higher audit fees. They find a significant positive relationship between increases in audit fees and hacking cyber incidents, but not other types of incidents. They argue that more audit work is required to address the increased audit risk. Three subsequent studies also document positive associations between breaches and audit fees (at 8 percent for customer record breaches and 13.5 percent for confidentiality breaches) even before future breaches (Smith et al. 2019; Lawrence et al. 2018; Yen et al. 2018). These studies also report that external breaches (e.g., hacks, portable data thefts, or server thefts) appear to be driving the positive association between (customer record) breaches and audit fees, and that audit firm characteristics (i.e., Big 4, industry-specific expertise, and longer tenure) negatively moderate the association for confidentiality breaches (Smith et al. 2019; Yen et al. 2018). Thus, different studies find different types of breaches driving the results.

Despite these findings, two arguments counter an increase in audit fees around breaches. The first is that the risks auditors face around breaches may be mitigated by corporate governance mechanisms (e.g., large shareholders, technology committees on the board) as well as CIOs and CEOs and CFOs with IT expertise. Haislip, Pinsker, Richardson, and Thevenot (2018), for example, find that the presence of a technology committee, high-profile CIO, IT-expert CEO, or IT-expert CFO reduces the time to detect, as well as the time to report, a data breach. The presence of board-level risk committees and more active audit committees may also mitigate the audit fee increases (Smith et al. 2019).

A second counter argument is that since these audit risks have long been known, audit firms already price them into their annual audit fees and audit workload, such that any subsequent increase in fees following a data breach would not be material to the average company and auditors. In addition, audit fees have stagnated to the inflation rate (Lenihan 2018), and anecdotal evidence indicates that intense competition for new audit clients makes it difficult for auditors to increase audit fees. In support of this argument, Chichernea, Holder, Petkevich, and Robin (2018) find that even though breached companies have higher levels of (business) risk, they pay auditors more for nonaudit services than audit services. The authors even determine that there is "some evidence [that] audit fees are lower for breached companies" than for non-breached companies (Chichernea et al. 2018, 4). Similarly, Westland (2018) determines that lower audit fees are correlated with breaches.

Thus, the impact of a breach on audit fees (before and after the announcement) is not clear. But, one cannot discount the opportunity for auditors to opportunistically charge more following a data breach. However, it is clear that given Chichernea et al.'s (2018) results, it is important to examine not only audit fees, but also other fees. This reasoning leads to our third hypothesis regarding audit and other fees, which we state in the null and alternative forms as follows:

H3: On average, there will be an increase in audit fees and other fees around a data breach.

[11] Li et al. (2016) define a cyber incident as "cyber-attacks that are initiated by hackers to steal or destroy sensitive information in the cyber realm." Therefore, they do not examine data breaches that are not related to cybersecurity, such as a stolen laptop.

Impact on SOX 404 Material Weakness Reporting

Table 14 of Appendix A reports the literature review for the last economic consequence, the impact of a breach on SOX 404 internal control material weakness reporting. The "strength of internal controls may be a significant factor in the occurrence of a breach" (Westland 2018, 41). Specifically, weak information technology (IT) access and security controls may allow hackers to penetrate a company's systems resulting in the unauthorized acquisition, use, and/or disposition of (customer) data, which may constitute a weakness in internal controls over financial reporting (ICFR) according to Rule 13a-15(f) of the Exchange Act (Griggs and Donahue 2014).[12] In fact, during the first year of SOX 404 reporting, 14.7 percent of the companies reported logical access issues and 4.1 percent reported security issues (Klamm and Watson 2009) as material weaknesses in their 10-K reports, indicating that auditors/managers believed there was a reasonable possibility that a material misstatement of the financial statements could occur due to these IT control weaknesses.[13]

Moreover, if a company has "poor practices related to access controls or patch management . . . they may not be confined to one system because these general IT controls are not typically managed or controlled separately" (McKenna 2017).[14] This was the case for Equifax where hackers used a flaw in a public website to access consumer data in the company's main systems (McKenna 2017). Thus, some data breaches may affect financial reporting controls and accounts, and therefore weak IT controls should be recognized as SOX 404 material weaknesses. Accordingly, Lawrence et al. (2018) find that breaches, a type of operational control failure, are associated with the future restatements as well as future SOX 404 control weaknesses ($p < 0.10$) and SEC comment letters. There is also evidence that SOX 404 is most effective at identifying control problems when there are credit card breaches (100 percent) and insider breaches (33 percent), but not other types of breaches (Westland 2018).

However, there is also evidence that IT control failures that may lead to breaches are not being reported. From the PCAOB's (2017, 13) perspective, "it appears that these cybersecurity incidents have not been related to the risks of material misstatement of financial statements, including disclosures, or led to the identification of material weaknesses in ICFR." From the auditor perspective, not only do the "largest global audit firms . . . say that an assessment of cybersecurity risks is outside the scope of a financial statement and ICFR audit based on auditing standards" (McKenna 2018), but there is also systematic bias in auditor judgment when assessing IT controls (Wolfe, Mauldin, and Diaz 2009). Specifically, auditors assess the significance of IT control deviations lower than that of manual control deviations (Wolfe et al. 2009) because people relate socially to computers (unlike other inanimate objects) and therefore blame them (not the humans behind them) for failures.[15] As a result, companies may be held less accountable for computer failures than other failures, making it less likely that data breaches (and/or breach risk) are reported as SOX 404 material weaknesses.[16]

There is also some evidence that breach reporting and SOX 404 reporting are intertwined as companies with fewer (previous) material weaknesses are more likely to disclose breaches than companies with more prior material weaknesses, due to stronger corporate governance (Amir et al. 2018). Thus, it is unclear whether breaches are associated with prior or future SOX 404 material weaknesses. This reasoning leads to our fourth hypothesis regarding SOX 404 material weaknesses, which we state in alternative form as follows:

H4: On average, there will be an increase in reported SOX 404 material weaknesses around a data breach.

III. SAMPLE

Sample

To examine the consequences of data breaches, we first used privacyrights.org to identify 1,165 publicly disclosed data breaches occurring between 2005 and 2017. We also acquired data breach information from Audit Analytics that covers 458 data breaches and 44 denial of service attacks between 2004 and 2018. We combined data from the two datasets, removing duplicate incidents. We first eliminated private companies, such as government, not-for-profit, medical, or educational

[12] In addition to violating SOX 404, attorneys at Zuckerman Law also state that a company's "failure to accurately disclose cybersecurity issues" may violate the following laws: (1) SEC Rule 10b-5, codified at 17 C.F.R. 240.10b-5, which prohibits omission of a material fact; (2) SEC Regulation S-K, which requires a company to disclose risk factors and discuss the most significant factors that make an offering speculative or risky; and (3) Item 303 of Regulation S-K, 17 C.F.R. § 229.303, which requires a company to discuss its financial condition, changes in financial condition, and results of operations (Hammer and Zuckerman 2018). However, these potential violations are beyond the scope of this paper.

[13] SOX 404 defines a material weakness as "a deficiency, or combination of deficiencies, in internal control over financial reporting such that there is a reasonable possibility that a material misstatement of the registrant's annual or interim financial statements will not be prevented or detected on a timely basis" (SEC 2007). Large, accelerated filers must also have their auditors evaluate and report on internal controls.

[14] This statement was made by Dr. Rani Hoitash of Bentley University.

[15] See Kelton, Fleischmann, and Wallace (2008) and Wolfe et al. (2009) for a human-computer interaction literature review.

[16] This may also affect the stock market reaction to cyber incidents.

institutions. We then eliminated companies without Compustat information for the fiscal year immediately prior to the breach disclosure, as well as companies that did not have complete market return information in CRSP for 120 days before and 21 days after the breach disclosure date. The final sample consists of 827 breach disclosures for 417 companies and is many times larger than the sample in most extant studies.

The rest of the data were collected as follows. Compustat provided financial information. CRSP provided stock market information. Audit Analytics provided audit fee information. Searching the internet, we also hand collected a variety of information about the data breach including information lost, how the data were stolen, and dates for the beginning and ending of the data breach, awareness of the incident, and public disclosure of the incident.

Matching Process

Prior research uses a variety of methods to match breach companies against non-breach companies.[17] The purpose of matching is, of course, to compare the performance of those companies disclosing breaches against similar companies that do not disclose breaches. Recently, Kamiya et al. (2018) use propensity score matching based on company size, stock performance, stock return volatility, and an institutional blockholder indicator to examine the relationship between cyberattacks and CEO pay components. Lending et al. (2018) also used propensity score matching to examine links between data breaches, corporate governance, and social responsibility. Propensity score matching matches companies based on a set of covariates that predict receiving the treatment (e.g., Rosenbaum and Rubin 1983; Guo and Fraser 2015). While propensity score matching is widely used, Shipman, Swanquist, and Whited (2017) caution that the technique has several limitations. One limitation is that the design choices are not standardized, and minor changes in the covariates can result in different conclusions. We therefore not only use propensity score matching, but also use alternate matching schemes to further test the results.

We employ our propensity score matching procedure in this way. First, we form a propensity score-matched sample to correct for endogenous selection on observed variables (Rosenbaum and Rubin 1983; Guo and Fraser 2015). We employ the Stata *psmatch2* routine (Leuven and Sianesi 2003), which implements propensity score matching for pretreatment observable differences between a group of treated (Breach firms) and untreated firms. We use all available companies with Compustat data for the year immediately prior to each breach disclosure, as well as CRSP information during the pre- and post-event periods. Following Lending et al. (2018), we regress a Breach firm indicator on year, Fama-French industry classification (Fama and French 1997), return on assets, and log of total assets. Consistent with Guo and Fraser (2015), we use a caliper of 25 percent of the standard deviation of the propensity score, the conditional treatment probability, to assure appropriate matches. Lending et al. (2018) achieve propensity scores for each matched pair within 71 percent of each other. Our propensity scores for Matched firms are within 5 percent of each other.

Second, we match the breach companies against other companies based on three different schemes. We match on (1) year, industry, and total assets, (2) year, industry, and return on assets, and (3) year, industry, and market value. Using three additional sets of matched companies allows us to confirm results from the propensity score-matched sample. We find the results to be similar, so we only report results for the propensity score-matched and market value-matched samples.

Table 1 describes selected statistics for Breach firms, Propensity-Matched firms, and Market Value-Matched firms. It shows that the matching process provides closely matched sets of companies. There is no significant difference between Breach firms and Propensity-Matched firms for total assets and return on assets. Breach firms, however, have higher market values, future changes in ROA, ROS, and Sales Growth than Propensity-Matched firms. Breach firms report marginally higher audit fees than both Propensity-Matched and Market Value-Matched firms, and more Breach firms report internal control material weaknesses than Market Value-Matched firms.

Breach Incident Statistics

Prior research confirms that breaches occur more frequently in retailing, banks, and internet services companies. Panel A of Table 2 confirms that distribution in our sample.[18] There are substantially more breaches in industries 15 (Retail Stores), 16 (Banks, Insurance Companies, and Other Financials), and 17 (Other). Category 17 includes communication and business service companies. Panel B describes the number of breaches per year. The most breaches occurred in 2014 and the fewest occurred in 2005, but there are clearly more breaches per year since 2009 than before 2009.[19] As noted earlier, there are 827 breaches involving 417 companies. Panel C shows that 256 companies had only one breach, but other companies were involved

[17] As shown in Appendix A, there are also many studies that do not use matched samples.

[18] Since we match on industry and year, there are the same number of Matched firms in each industry and year as there are Breach firms.

[19] The increased number of breaches per year since 2009 may be due to increased state reporting requirements rather than any fundamental change in the number of breaches.

TABLE 1

Descriptive Statistics

	Breach Firms		Propensity-Matched Firms		Market Value-Matched Firms	
	Mean	n	Mean	n	Mean	n
Market Value	9.609[a]	827	9.286	827	9.460	827
Assets	9.955[b]	827	9.845	827	9.652	827
ROA	0.047	827	0.042	827	0.051	827
Future Change in ROA	0.000[a]	786	−0.008	779	−0.002	780
ROS	0.077[b]	827	0.077	827	0.087	827
Future Change in ROS	0.001[a]	784	−0.021	778	−0.011	778
Sales Growth	0.064[b]	827	0.071	824	0.100	824
Future Change in Sales Growth	0.055[a]	785	0.046	775	0.082	778
Forecast Error	−0.005	765	−0.005	737	−0.005	742
Future Forecast Error	−0.004	720	−0.006	691	−0.004	702
Audit Fees	15.628[a,b]	792	15.501	798	15.378	788
Future Change in Audit Fees	0.054	737	0.044	730	0.043	724
Other Fees	0.015	792	0.016	798	0.018	788
Future Change in Other Fees	0.000	738	0.002	730	0.002	724
ICMW	0.027[b]	827	0.029	827	0.015	827
Future ICMW	0.028	784	0.033	779	0.019	779

This table presents selected descriptive statistics for Breach firms and firms matched by year, industry, and (1) total assets, (2) past ROA (average for previous three years), and (3) market value.

Variables are defined in Appendix B.

[a] Breach firm measure is substantially different than Propensity-Matched firm measure ($p < 0.10$, one-tailed t-test).

[b] Breach firm measure is substantially different than Market Value-Matched firm measure ($p < 0.10$, one-tailed t-test).

in multiple breaches. In our tests, we examine whether the results differ between companies with only one breach and companies with multiple breaches. Consistent with prior research, there is, however, little difference (e.g., Johnson et al. 2017).

Panel D provides additional information about breach characteristics derived from the information available at privacyrights.org, Audit Analytics, and our hand-collected data. We use the breach categories from privacyrights.org: (1) credit card skimming or fraud involving debit and credit cards that is not accomplished via hacking (e.g., skimming devices at point-of-service terminals), (2) denial of service attacks, (3) unintended disclosures, such as publicly posting sensitive information or sending information to the wrong party via email, fax, or other means, (4) hacking by an outside party or infected by malware, (5) insider breaches (someone with legitimate access, such as an employee, contractor, or customer, intentionally breaches information), (6) physical loss of paper documents, (7) loss of portable devices, (8) loss of stationary devices, and (9) other. We use categories from Audit Analytics for the type of data lost: (1) financial, such as credit card or account information, (2) personal, such as user names, passwords, and email addresses, (3) other—includes loss of intellectual property, and (4) none/unknown. The dominant source of breaches is from hacking; 55 percent of the incidents involve hacking. 53 percent of the incidents involve loss of personal data, while 34 percent involve loss of financial data. Panel D also describes the number of SEC 8-K filings due to the data breaches as well as the number of class action lawsuits resulting from breaches. Companies filed SEC 8-K reports for 159 (19.2 percent) of the incidents, and 3.2 percent of incidents resulted in class action lawsuits.[20]

IV. RESEARCH DESIGN

Tests of Relationship between Breaches and Market Returns

We examine cumulative abnormal returns around the breach disclosure dates for both breach companies and matched companies. We select daily returns for six months prior to the disclosure (days −120 to −5) and various short-term (day −1 to day +3) and longer-term windows (one month, three months, and six months) following the disclosure. We follow standard

[20] Ostensibly, data breaches with 8-K reports or class action lawsuits should have greater impact, but we did not find that those factors affect our results after considering the risk level of the breach (see Table 7).

TABLE 2
Breach Incident Statistics

Panel A: Breaches by Industry

Fama-French Industry Categories	Number of Breaches	Percent of Total
1. Food	13	1.57
2. Mining and Minerals	3	0.36
3. Oil and Petroleum Products	10	1.21
4. Clothing, Textiles, Apparel and Footwear	9	1.09
5. Consumer Durables	1	0.12
6. Chemicals	0	0.00
7. Drugs, Soap, Perfumes, Tobacco	13	1.57
8. Construction and Construction Materials	17	2.06
9. Steel Works, etc.	3	0.36
10. Fabricated Products	0	0.00
11. Machinery and Business Equipment	61	7.38
12. Automobiles	17	2.06
13. Transportation	31	3.75
14. Utilities	14	1.69
15. Retail Stores	130	15.72
16. Banks, Insurance Companies, and Other Financials	201	24.30
17. Other	304	36.76
Total	827	100

(continued on next page)

event study methodology using the Stata *eventstudy2* routine (Kaspereit 2015). That routine allows several options for factor models, such as the single factor market model and the four factor Fama-French model (Fama and French 1992, 1993, 1996), which also includes a momentum factor (e.g., Chan, Jegadeesh, and Lakonishok 1996) that we employ.[21] We accumulate abnormal daily returns over the various windows and compare cumulative abnormal returns for breach companies against matched companies. For the multivariate analysis, we use the following model:

$$CAR = a_0 + b_1 Breach\ Firm + \sum d_i Controls_i + e, \tag{1}$$

where *CAR* is cumulative abnormal returns calculated as described above for each company and breach disclosure. *Breach Firm* indicates Breach firms relative to either Propensity-Matched or Market Value-Matched firms for that breach disclosure.[22] Controls are (1) the standard deviation of returns, (2) the average share turnover (share volume divided by total shares outstanding), (3) market value, and (4) prior market returns. Controls are calculated from CRSP information over the six-month estimation period prior to the breach disclosure.

Tests of Relationship between Breaches and Future Measures of Accounting Performance

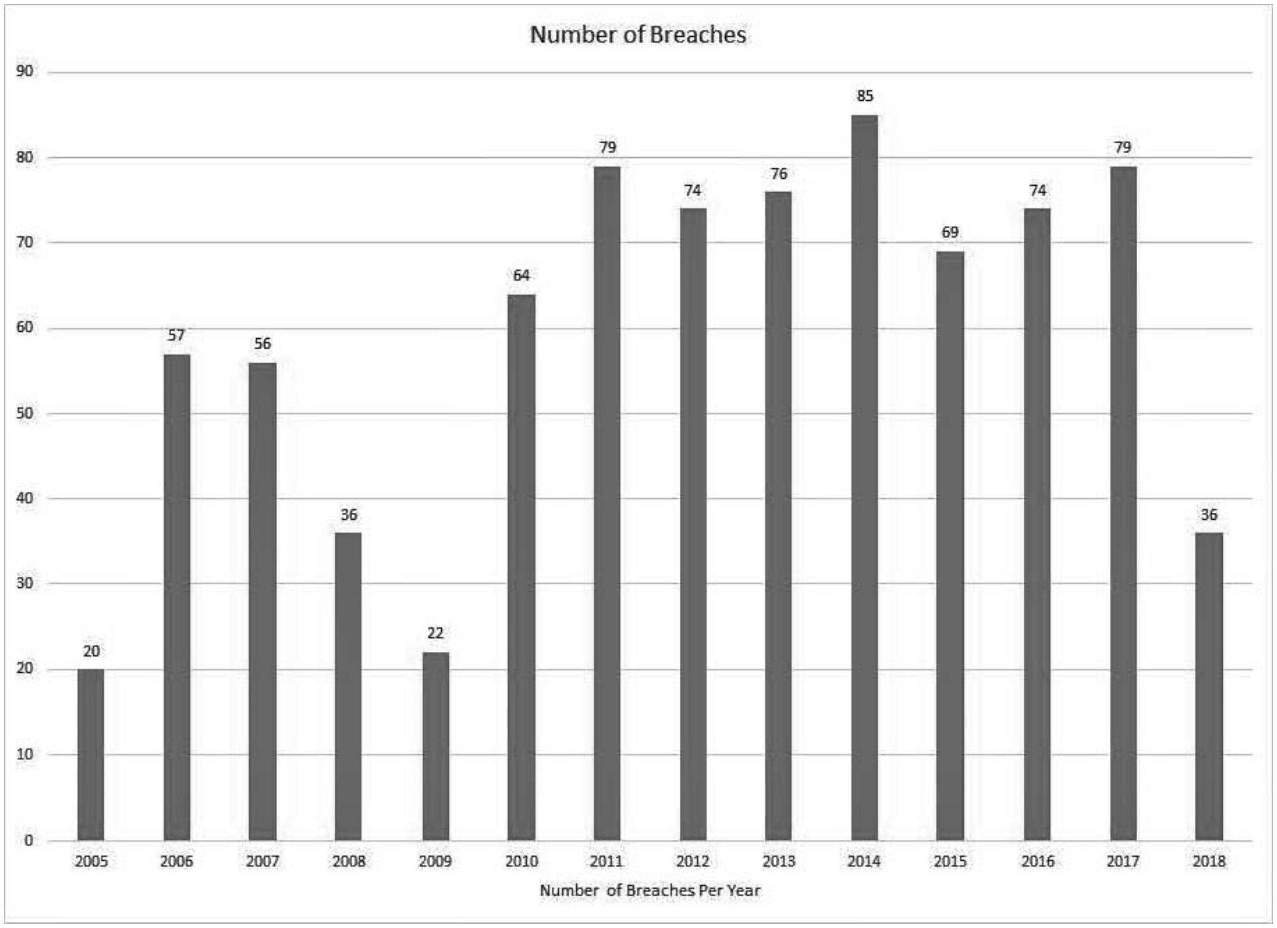
We examine the relationship between breach disclosures and future measures of accounting performance in two ways. First, for each company we include observations for three years prior to the breach disclosure (i.e., fiscal years t–2, t−1, and t) and three years following the breach disclosure (i.e., fiscal years t+1, t+2, and t+3). We test whether breach disclosures impact future total revenue, future sales revenue growth, future ROS (earnings before extraordinary items divided by total revenue), and future ROA (earnings before extraordinary items divided by total assets), controlling for prior values of those measures as well as industry performance. We employ a difference-in-differences design that interacts our *Breach Firm* dummy variable with a time-based dummy variable (*Post*) set to 1 for years after and 0 for the years before the disclosure. If the breach adversely affects future performance, the interaction term (*Post* × *Breach Firm*) will be significantly lower than corresponding

[21] Fama and French daily factors are available on WRDS or directly from Ken French's data library: http://mba.tuck.dartmouth.edu/pages/faculty/ken.french/data_library.html. We report results resulting from the four factor model, but results from a single factor market model are similar.

[22] We report multivariate results for Breach firms versus Propensity-Matched firms. The results are not sensitive to which Matched firms are included in the model.

TABLE 2 (continued)

Panel B: Breaches by Year



(continued on next page)

interaction terms for the Matched firms.

$$Future\ Performance = a_0 + b_1 Post + b_2 Breach\ Firm + b_3 Post \times Breach\ Firm + \sum d_i Controls_i + e, \quad (2)$$

where *Future Performance* is total revenue, sales growth, ROS, or ROA. Controls include prior performance (i.e., revenue, sales growth, ROS, or ROA, depending on the future performance examined), an indicator for mergers and acquisitions, capital expenditures, asset turns, leverage, total assets, and future changes in industry performance. These variables are defined in detail in Appendix B.

We also employ a broader sample, comparing Breach firm performance against all firms for which propensity scores were calculated. In this case, we use the propensity score as sampling weights. Guo and Fraser (2015) describe the general procedure for propensity score analysis to include (1) matching, (2) multivariate analysis using propensity scores as weights, and (3) analysis using stratification of propensity scores.[23] For each Breach firm, we include all available firm observations in the same Fama-French industry and year to estimate the following model.

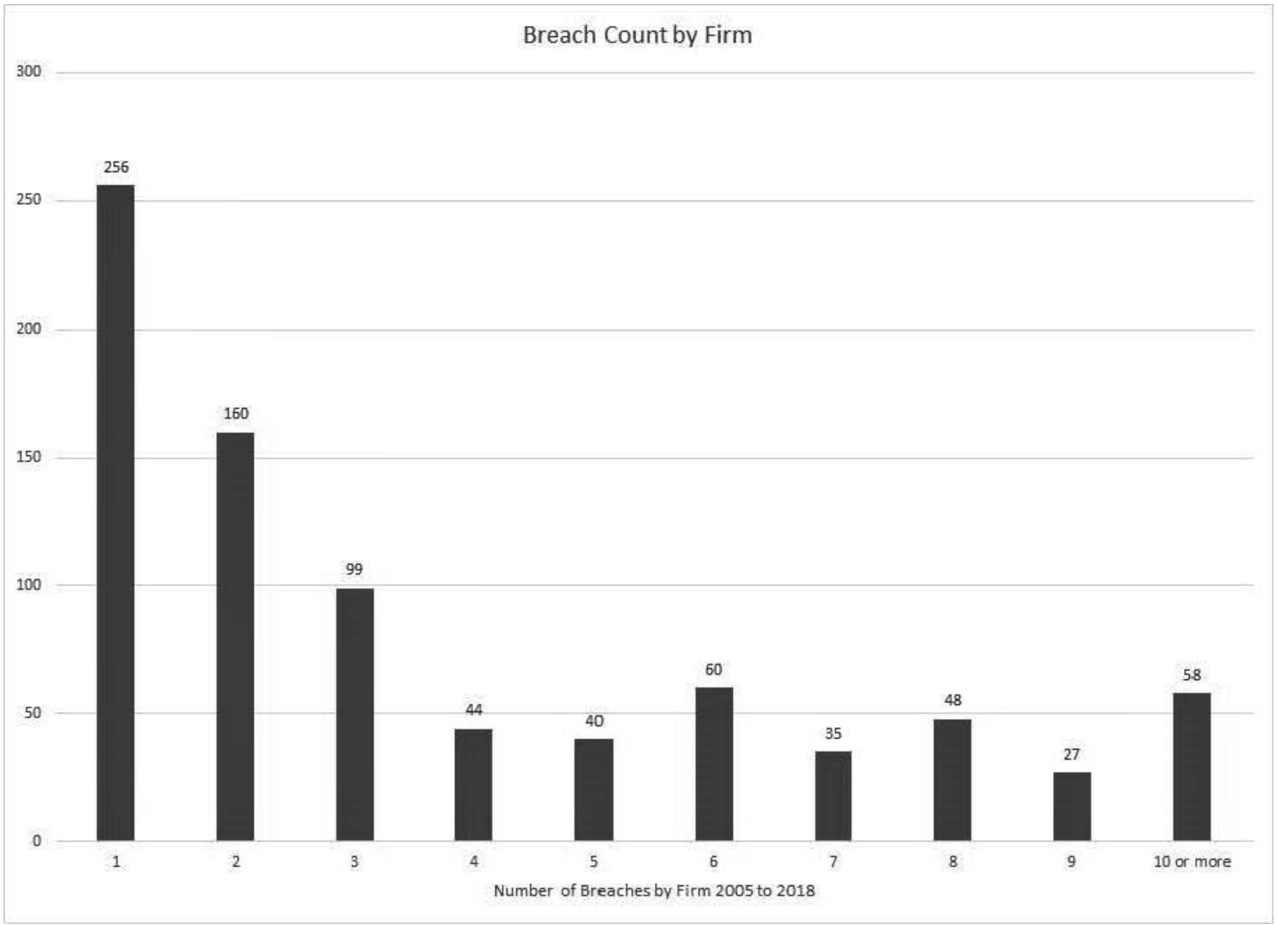
$$Future\ Performance = a_0 + b_1 Breach\ Firm + b_2 Pscore + \sum d_i Controls_i + e, \quad (3)$$

where future performance and controls are as defined for Equation (2).

[23] This research uses alternatives (1) and (2). We did not use propensity score stratification.

TABLE 2 (continued)

Panel C: Breaches by Firm

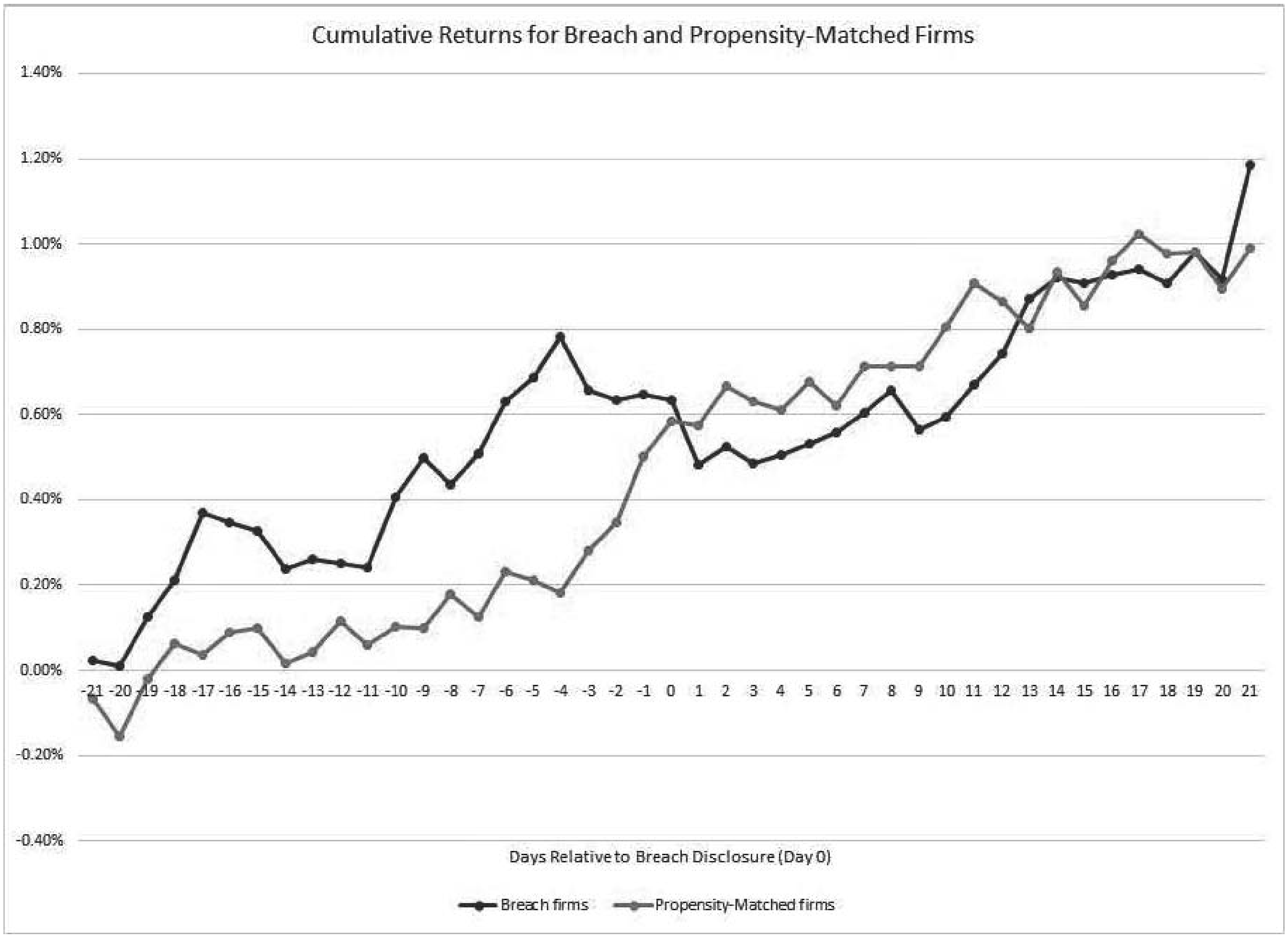


Panel D: Breach Characteristics

	Type of Data Lost					Reactions	
Breach Type	**Financial**	**Personal**	**Other**	**None/ Unknown**	**Total**	**Filed SEC 8-K**	**Class Action**
Credit Card Skimming	16	0	0	1	17	2	1
Denial of Service	0	0	0	20	20	0	0
Unintended Disclosure	29	50	1	1	81	0	3
Hack	158	226	57	11	452	151	13
Insider	41	35	9	2	87	1	3
Physical Loss	7	12	0	2	21	0	0
Portable Device Loss	15	98	1	2	116	3	4
Stationary Device Loss	1	13	0	0	14	0	0
Unknown	11	8	0	0	19	2	3
Total	278	442	68	39	827	159	27

This panel presents the number of breaches by type of breach and type of data lost. It also describes internal (Filed SEC 8-K) and external (class action litigation) reactions to the disclosure of the data breach. Breach types include credit card skimming, denial of service attacks aimed at websites, unintended disclosures, such as posting information on public bulletin board sites, hacks, insider malicious actions, physical loss of paper, and loss of portable and stationary devices. Types of data lost include financial, such as credit card or account information, personal, such as user names, passwords, and email addresses, and other includes loss of intellectual property. Filed SEC 8-K indicates that the firm filed an SEC 8-K referencing the breach. Class action indicates that the firm was involved in a class action lawsuit related to the loss of data.

FIGURE 1
Cumulative Returns around Breach Disclosures



Cumulative daily returns for Breach and Propensity-Matched firms over the period starting 21 days before and ending 21 days after breach disclosure.

Tests of Relationship between Breaches and Audit and Nonaudit Fees

We use similar approaches to examine the impact of breaches on future audit and other fees. Following the audit fee literature (e.g., Sharma, Tanyi, and Litt 2017), we regress audit and other fees on a variety of variables expected to affect those fees. Since our interest is in changes in fees, we include prior fees as dependent variables in the following model. Again, we focus on the interactions between the *Post* variable and the *Breach Firm* and *Matched Firm* indicators.

$$Future\ Fees = a_0 + b_1 Post + b_2 Breach\ Firm + b_3 Post \times Breach\ Firm + \sum d_i Controls_i + e, \quad (4)$$

or

$$Future\ Fees = a_0 + b_1 Breach\ Firm + b_2 Pscore + \sum d_i Controls_i + e, \quad (5)$$

where *Future Fees* are measured as the log of audit fees or other/miscellaneous fees from Audit Analytics. We include *Other/Miscellaneous Fees* to test whether nonaudit fees increase following the breach. We divided *Other Fees* by total fees to test whether the percent of other fees increase following the breach. Controls include (1) prior audit or other fees, (2) market value, (3) material weaknesses in internal controls indicator, (4) unqualified opinion indicator, (5) discontinued operations indicator, (6) extraordinary items indicator, (7) new shares issued indicator, (8) ratio of working capital to total assets, (9) Big 5 auditor

TABLE 3
Breach Impact on Market Returns

Panel A: Univariate Comparisons of Returns around Breach Disclosures

	Return Period Relative to Disclosure Date				
	[−120, 5]	**[−1, 3]**	**[−1, 21]**	**[−1, 63]**	**[−1, 126]**
Cumulative Daily Returns					
Breach Firms	4.595%[a]	−0.148%[a,b]	0.550%	1.004%	2.337%
Propensity-Matched Firms	1.390%	0.285%	0.646%	0.655%	1.218%
Market Value-Matched Firms	3.579%	0.176%	0.474%	0.826%	1.812%
Cumulative Excess Returns					
Breach Firms	−0.611%[a]	−0.313%[a,b]	−0.309%	−1.021%	−1.802%
Propensity-Matched Firms	−3.822%	0.118%	−0.209%	−1.357%	−2.914%
Market Value-Matched Firms	−1.637%	0.013%	−0.381%	−1.186%	−2.363%
Cumulative Abnormal Returns (CAR)					
Breach Firms		−0.274%[a,b,c]	−0.733%	−0.269%	−0.312%
Propensity-Matched Firms		0.380%	0.531%	−0.640%	0.285%
Market Value-Matched Firms		−0.036%	−0.452%	0.012%	0.173%
Standard Deviation of Returns					
Breach Firms	1.892%	1.653%	1.825%	1.908%	1.964%
Propensity-Matched Firms	1.947%	1.681%	1.852%	1.968%	2.016%
Market Value-Matched Firms	1.920%	1.736%	1.860%	1.934%	1.975%

This panel presents cumulative returns, excess returns (returns less equal-weighted market returns), residual returns (residual from Fama-French four-factor model), and the standard deviation of returns. Periods are prior six months [−120, 5], short window around disclosure [−1, 3], one month following disclosure [−1, 21], three months following disclosure [−1, 63], and six months following disclosure [−1, 126].

[a] Breach firms' returns are significantly different than Propensity-Matched firms' returns ($p < 0.05$, one-tailed test).

[b] Breach firms' returns are significantly different than Market Value-Matched firms' returns ($p < 0.05$, one-tailed test).

[c] CAR for Breach firms (Patel's t-stat.= − 3.308, $p < 0.01$; Boehmer's t-stat. = −1.912, $p < 0.10$; Corrado and Zivney sign test = −0.987, $p < 0.324$; Generalized sign test = −1.301, $p < 0.193$).

Panel B: Multivariate Comparisons of Returns around Breach Disclosures

	Returns [−1, 3]	Returns [−1, 21]	CAR Fama-French Model [−1, 3]	CAR Fama-French Model [−1, 21]
Breach Firm	−0.005	−0.003	−0.006	−0.004
	(2.32)**	(0.67)	(2.56)**	(1.01)
SD Prior Returns	−0.550	−0.186	−0.531	−0.297
	(2.21)**	(0.52)	(2.29)**	(0.76)
Prior Share Turnover	0.002	−0.003	0.001	−0.001
	(1.12)	(0.83)	(0.71)	(0.42)
Prior Market Value	−0.000	0.002	−0.000	0.001
	(0.46)	(1.43)	(0.72)	(1.02)
Prior Returns	1.391	3.149	−0.649	−11.661
	(1.40)	(1.68)*	(0.64)	(6.01)***
Prior Market Returns	1.010	1.016	0.044	0.077
	(13.04)***	(15.80)***	(2.89)***	(1.35)
Constant	0.013	−0.023	0.017	−0.008
	(1.09)	(1.03)	(1.49)	(0.33)
Adjusted R^2	0.24	0.23	0.02	0.06
n	1,654	1,654	1,654	1,654

*, **, *** Denote $p < 0.1$, $p < 0.05$, and $p < 0.01$, respectively; clustered standard errors adjust for intrafirm correlation.

This panel presents a multivariate examination of a short window [−1, 3] and longer window [−1, 21] around breach disclosures for Breach and Propensity-Matched firms.

Variables are defined in Appendix B.

TABLE 4
Multivariate Tests of Data Breaches on Future Accounting Measures of Performance

	(1)	(2)	(3)	(4)	(5)	(6)
	Future Total Revenue	Future Sales Growth	Future ROS	Future ROA	Future Sales Growth	Future ROA
Breach Firm	0.007	0.001	0.006	0.005	0.015	0.007
	(1.03)	(0.21)	(2.34)**	(2.65)***	(1.70)*	(0.73)
Post	−0.026	−0.030	−0.007	−0.000		
	(3.31)***	(4.05)***	(2.25)**	(0.04)		
Post × *Breach Firm*	0.010	0.015	0.006	−0.002		
	(1.05)	(1.72)*	(1.66)*	(0.70)		
Prior Performance	0.986	0.082	0.619	0.595	0.030	1.763
	(388.90)***	(1.86)*	(23.27)***	(12.55)***	(2.06)**	(2.45)**
Pscore					−0.152	−0.867
					(3.43)***	(1.32)
Merger-Acquisition$_{it+1}$	0.117	0.118	−0.007	−0.009	0.172	−0.067
	(9.97)***	(10.31)***	(1.56)	(3.32)***	(27.23)***	(1.65)*
Capital Expenditures	0.686	0.493	0.009	0.083	0.443	−0.961
	(5.36)***	(4.62)***	(0.21)	(2.19)**	(9.70)***	(2.31)**
Asset Turns	0.004	0.003	0.001	−0.001	0.006	−0.002
	(3.25)***	(3.58)***	(3.98)***	(3.34)***	(12.73)***	(2.19)**
Leverage	−0.041	−0.016	0.002	0.013	0.031	−0.023
	(1.95)*	(0.91)	(0.20)	(1.43)	(2.78)***	(0.26)
Industry Performance$_{t+1}$	0.704	0.677	0.069	0.041	0.761	0.365
	(13.93)***	(13.86)***	(3.44)***	(2.81)***	(39.29)***	(4.42)***
Constant	0.083	−0.040	0.025	0.013	−0.074	0.111
	(3.60)***	(4.30)***	(6.89)***	(3.84)***	(16.34)***	(1.55)
Adjusted R^2	0.99	0.10	0.42	0.39	0.09	0.07
n	7,433	7,403	7,433	7,433	53,358	54,708

*, **, *** Denote $p < 0.1$, $p < 0.05$, and $p < 0.01$, respectively; clustered standard errors adjust for intrafirm correlation.
This table presents a multivariate examination of the impact of breaches on future financial performance controlling for past performance. Columns (1) to (4) use all available observations for Breach and Propensity-Matched firms for three years prior to the breach disclosure and three years following the breach disclosure. Columns (5) and (6) use all available observations with *Pscore* values. *Prior Performance* corresponds to the future performance variable, i.e., *Revenue, Sales Growth, ROS,* and *ROA*. Year and industry controls are omitted since propensity matching includes industry and year and models include industry performance. Future values are in year *t*+1, other values are in year *t* unless designated by subscript.
Variables are defined in Appendix B.

indicator, (10) ratio of accounts receivable plus inventories to total assets, (11) book-to-market ratio, (12) number of geographic segments, and (13) number of business segments. Prior audit research (e.g., Sharma et al. 2017; Hay and Knechel 2010; Ghosh and Pawlewicz 2009) suggests that those variables affect audit fees. Including prior fees also controls for other firm characteristics omitted from the model. Equation (4) applies to the matched data for three years before and after each breach. Equation (5) applies to the broader set of firms with propensity scores.

Tests of Relationship between Breaches and Material Internal Control Weaknesses

We again use similar approaches to test for the relationship between breaches and material weaknesses in internal control. We use a dummy variable to indicate whether a company reported a material internal control weakness in any year. We control for a variety of company performance and information uncertainty variables noted in prior research. Following Ashbaugh-Skaife, Collins, Kinney, and LaFond (2009) and Doyle, Ge, and McVay (2007), we assume that the market, and its intermediaries, form opinions on internal control quality prior to the SOX 404 reports based on observable company characteristics. Based on that argument, Ashbaugh-Skaife et al. (2009) develop a list of control variables capturing company performance, variation in that performance, and other factors that affect company risk. We employ similar controls in the following multivariate logit model.

TABLE 5

Multivariate Tests of Data Breaches on Audit and Other Fees

	(1) **Future Audit Fees**	**(2)** **Future Audit Fees**	**(3)** **Future Other Fees**	**(4)** **Future Other Fees**	**(5)** **Future Audit Fees**	**(6)** **Future Other Fees**
Post	0.006	0.011	−0.000	−0.001	0.008	−0.002
	(0.78)	(0.91)	(0.20)	(0.74)	(0.68)	(0.74)
Breach Firm	−0.024	−0.004	0.001	−0.002		
	(3.14)***	(0.28)	(0.76)	(1.00)		
Post × Breach Firm	0.010	0.009	−0.002	0.001		
	(0.89)	(0.49)	(1.12)	(0.39)		
Audit Fees$_{it}$	0.911	0.924	0.002	0.001	0.832	−0.003
	(103.81)***	(81.13)***	(1.79)*	(0.66)	(210.12)***	(5.38)***
Other Fees$_{it}$			0.595	0.653		0.376
			(13.06)***	(11.24)***		(22.59)***
Pscore					0.443	0.047
					(6.19)***	(3.69)***
Market Value	0.052	0.044	−0.000	−0.000	0.077	0.001
	(9.52)***	(6.40)***	(0.37)	(0.02)	(37.87)***	(2.13)**
ICMW$_{it+1}$	0.161	0.070	−0.003	0.001	0.178	−0.000
	(4.05)***	(1.00)	(1.20)	(0.21)	(19.27)***	(0.08)
Unqual Opinion	−0.075	0.024	0.009	0.013	−0.131	−0.007
	(1.84)*	(0.38)	(1.47)	(2.13)**	(0.82)	(0.61)
Disc Ops	−0.018	−0.023	−0.001	−0.001	0.008	−0.001
	(1.95)*	(2.03)**	(0.55)	(0.57)	(1.76)*	(0.95)
Xtra Items	0.110	−0.025	−0.006	−0.006	0.026	−0.001
	(3.96)***	(0.57)	(2.05)**	(3.12)***	(1.47)	(0.45)
Shares Issued	−0.013	−0.007	0.002	0.001	0.017	0.001
	(1.90)*	(0.78)	(1.59)	(0.87)	(4.79)***	(1.78)*
Current Assets	−0.071	−0.112	−0.004	−0.010	−0.055	−0.003
	(2.65)***	(3.19)***	(0.96)	(1.69)*	(6.90)***	(2.12)**
Big4	0.014	−0.024	−0.003	−0.004	0.071	−0.001
	(0.87)	(0.81)	(1.10)	(0.98)	(13.74)***	(1.62)
AR/Inventories	0.051	0.054	−0.000	0.002	0.132	−0.002
	(2.56)**	(1.94)*	(0.03)	(0.36)	(12.19)***	(1.12)
Merger-Acquisition	0.139	0.140	0.002	0.001	0.177	0.004
	(7.97)***	(5.97)***	(1.04)	(0.52)	(27.11)***	(4.20)***
Industry Sales Growth$_{t+1}$	0.184	0.079	−0.004	0.002	0.186	0.002
	(2.98)***	(1.00)	(0.57)	(0.22)	(12.06)***	(0.70)
Book-to-Market Ratio	0.023	0.003	0.000	0.001	0.001	−0.001
	(1.82)*	(0.18)	(0.63)	(0.77)	(0.54)	(2.22)**
Geo Segments	0.002	0.002	−0.000	0.000	0.007	0.000
	(0.99)	(1.08)	(0.46)	(0.04)	(10.30)***	(2.91)***
Constant	0.980	0.797	−0.024	−0.013	1.854	0.047
	(10.59)***	(5.56)***	(2.02)**	(0.98)	(11.35)***	(3.74)***
Adjusted R^2	0.96	0.97	0.39	0.41	0.94	0.17
n	6,911	2,740	6,911	2,741	40,866	40,866

*, **, *** Denote $p < 0.1$, $p < 0.05$, and $p < 0.01$, respectively; clustered standard errors adjust for intrafirm correlation.

This table presents a multivariate examination of the impact of breaches on future audit and other (nonaudit) miscellaneous fees controlling for past fees. Columns (1) to (4) use all available observations for Breach and Propensity-Matched firms for three years prior to the breach disclosure and three years following the breach disclosure. Columns (5) and (6) use all available observations with *Pscore* values. Year and industry controls are omitted since propensity matching includes industry and year and models include industry performance.

Variables are defined in Appendix B.

TABLE 6
Relationship between Data Breaches on ICMW

Panel A: Relationship between Internal Control Material Weaknesses and Breach Disclosures

	Any ICMW	Non-IT ICMW	IT ICMW	No ICMW
Year of Disclosure				
Breach Firms	22	20	2	805
Propensity-Matched Firms	25	20	5	802
Market Value-Matched Firms	12[a]	10[a]	2	815
During Three Years before Breach Disclosure				
Breach Firms	56	48	8	2,406
Propensity-Matched Firms	57	46	11	2,415
Market Value-Matched Firms	44	38	6	2,419
During Three Years after Breach Disclosure				
Breach Firms	48	45	3	2,073
Propensity-Matched Firms	56	47	9	1,995
Market Value-Matched Firms	33	30	3	2,045

This panel presents the number of internal control material weaknesses reported during the same year as a breach disclosure, during the previous three years, and during the following three years for Breach and Matched firms. IT ICMW indicates that the firm reported ICMWs with information systems as a causal factor; Non-IT ICMW indicates any other ICMW.

[a] Market Value-Matched firms have significantly fewer ICMWs than either Breach firms or Propensity-Matched firms ($p < 0.05$, one-tailed test).

(continued on next page)

$$Future\ ICMW = a_0 + b_1 Post + b_2 Breach\ Firm + b_3 Post \times Breach\ Firm + \sum d_i Controls_i + e, \tag{6}$$

or

$$Future\ ICMW = a_0 + b_1 Breach\ Firm + b_2 Pscore + \sum d_i Controls_i + e, \tag{7}$$

where *Future ICMW* equals 1 if the company reported one or more material weaknesses, and 0 otherwise. We control for prior (internal control material weakness) ICMW as well as (1) market value, (2) ROA, (3) debt to market value ratio, (4) operating cash flow, (5) loss, (6) number of geographic segments, (7) analyst following, (8) standard deviation of prior returns, (9) litigious industry, and (10) expected loss (analyst forecasted EPS less than 0). Equation (6) applies to the matched data for three years before and after each breach. Equation (7) applies to the broader set of firms with propensity scores.

Econometric Considerations

Since we use panel data for some analyses and companies may appear more than once, we adjust for intrafirm correlation using clustered standard errors (Petersen 2009). Petersen (2009) compared alternative approaches for dealing with serial correlation in panel datasets and concluded, in the presence of unobserved firm effects, clustered standard errors are unbiased and produce correctly sized confidence intervals while controlling for those unobserved effects. We therefore present results estimated using OLS (or logit) with clustered standard errors adjusted for intrafirm correlation.

V. RESULTS

Breaches and Market Returns

Figure 1 shows cumulative returns for Breach and Propensity-Matched firms for 21 days before and after breach disclosures. Prior to the disclosure, Breach firms enjoy higher returns. Returns decrease around the disclosure and the Matched firms temporarily show marginally higher returns. By the 12th day following the disclosure, cumulative returns are equal and remain equal for the rest of the selected period. Thus, it appears that the market reacts negatively to the disclosure, but the effects are short-lived.

TABLE 6 (continued)

Panel B: Multivariate Logit Tests of Data Breaches on ICMW

	Future ICMW			
	(1)	(2)	(3)	(4)
Breach Firm	0.263	0.169	0.106	0.086
	(1.08)	(0.79)	(0.41)	(0.32)
Post	0.040	−0.145		
	(0.18)	(0.63)		
Post × Breach Firm	−0.364	−0.357		
	(1.06)	(0.97)		
$ICMW_{it}$		3.094		2.449
		(10.34)***		(39.75)***
Pscore			−2.311	−2.085
			(1.52)	(1.52)
Market Value	−0.371	−0.299	−0.195	−0.168
	(5.61)***	(4.55)***	(8.16)***	(8.02)***
ROA	1.137	0.274	0.090	0.143
	(0.89)	(0.20)	(0.49)	(0.93)
Debt-to-Market Ratio	0.079	0.047	−0.027	−0.015
	(1.11)	(0.67)	(1.17)	(0.69)
Operating Cash Flow	−0.822	0.068	0.263	0.081
	(0.63)	(0.05)	(1.41)	(0.51)
Loss	0.217	0.089	0.266	0.110
	(0.70)	(0.32)	(3.55)***	(1.48)
Geo Segments	0.123	0.066	0.054	0.044
	(2.02)**	(1.81)*	(5.90)***	(5.56)***
Analyst Following	−0.022	−0.017	−0.024	−0.018
	(1.41)	(1.22)	(3.52)***	(2.91)***
Litigious Industry	−0.179	−0.097	−0.057	−0.037
	(0.65)	(0.42)	(0.77)	(0.61)
$Expected\ Loss_{it+1}$	0.112	0.123	0.201	0.161
	(0.33)	(0.38)	(2.62)***	(2.15)**
Constant	−0.708	−1.480	−1.688	−2.195
	(1.39)	(2.85)***	(11.39)***	(16.85)***
Pseudo R^2	0.10	0.22	0.04	0.14
n	7,384	7,384	39,940	39,940

*, **, *** Denote $p < 0.1$, $p < 0.05$, and $p < 0.01$, respectively; clustered standard errors adjust for intrafirm correlation.
This panel presents a logit analysis of the likelihood of an ICMW. This panel presents a multivariate logit examination of the impact of breaches on future reported material internal control weaknesses (year *t*+1). The sample uses all available observations for Breach and Matched firms for three years prior to the breach disclosure and three years following the breach disclosure. Year and industry controls are omitted, since we control for mean industry performance and we use industry and year to determine Propensity-Matched firms. All values are in year *t* except *Expected Loss,* which equals 1 if analysts' expected earnings are less than 0, and 0 otherwise.
Variables are defined in Appendix B.

Table 3 examines market returns prior to and following the breach disclosures for Breach and Matched firms. First, Panel A provides univariate comparisons of returns for Breach and Matched firms over various windows before and after breach disclosures. Prior to breach disclosures, Breach firms have higher cumulative returns than both Propensity-Matched and Market Value-Matched firms. The short window [−1, 3] results suggest that Breach firms experience significant, but not substantial losses. Breach firms have lower cumulative returns in the short window around the disclosure than both Propensity-Matched and Market Value-Matched firms. Over the five days around the breach disclosure, the average cumulative return is –0.148 percent for Breach firms, or less than 0.03 percent per day. Cumulative abnormal returns (CAR) values for Breach firms are significantly negative using both Patell's (1976) t-statistic ($p < 0.\ 01$) and Boehmer's (Boehmer, Musumeci, and Poulsen 1991) t-statistic assuming event-induced variance ($p < 0.10$). However, the Corrado and Zivney (1992) and generalized sign tests are not significant. This suggests that although the mean CAR is negative, many firms do not suffer losses around the breach disclosure. In the short window, however, Breach firms do have significantly lower returns than Matched firms. In

TABLE 7
Data Breach Severity

Panel A: Relationship between Abnormal Returns and Breach Severity

	Breach Level Severity					
	Breach Level Scores					
	Minimal 1–2.9	Moderate 3–4.9	Critical 5–6.9	Severe 7–8.9	Catastrophic 9–10	Total
Number of Breaches	485	98	154	77	13	827
CAR [−1, 3]	−0.216%	−0.249%	−0.013%	−0.657%	−5.844%[a]	−0.312%
CAR [−1, 21]	−0.259%	0.508%	−0.211%	−0.473%	−6.298%[a]	−0.274%
CAR [−1, 63]	−0.976%	−0.055%	−0.041%	−0.512%	−6.479%[a]	−0.733%
BHAR [−1, 126]	−0.747%	−3.488%	1.487%	4.996%	−10.352%[a]	−0.269%
Percentage Filing SEC 8-K	16.91%	11.22%	13.64%	41.56%	100.00%	19.23%
Percentage in Litigation	1.65%	0.00%	3.90%	9.09%	46.15%	3.26%
Average Reported Cost ($000s)	$33,900	$7,433	$25,200	$37,300	$155,000	$57,100
Number of Firms Disclosing Cost	23	3	2	7	9	44

This panel examines the impact of data breaches according to the severity of the breach level. Breach-level information is obtained from https://breachlevelindex.com/data-breach-risk-assessment-calculator, a website that provides comprehensive information about data breaches worldwide. We used their breach-level calculator to assess the breach level for all data breaches in our sample based on information that firms disclosed.

[a] Incidents in the catastrophic level result in significantly lower cumulative abnormal or buy-and-hold returns than for firms in the minimal level ($p < 0.05$, one-tailed t-tests).

Panel B: Relationship between Cumulative Abnormal Returns and Reported Breach Cost

Breach Costs Reported	Average Cost/ Revenue	n	CAR [−1, 3]	CAR [−1, 21]	CAR [−1, 63]	BHAR [−1, 126]
No Cost Reported (n = 783)	0.00%	783	−0.11%	−0.01%	−0.29%	0.03%
Low Cost Reported (n = 22)	0.18%	22	−1.75%	−2.51%	−1.98%	5.36%
High Cost Reported (n = 22)	2.50%	22	−5.93%	−7.30%	−15.50%	−16.71%
Total	1.34%	827	−0.31%	−0.27%	−0.73%	−0.27%

(continued on next page)

longer windows of one, three, or six months, there is no difference between Breach and Matched firms' cumulative returns. For the six-month window [−1, 126], we measure buy-and-hold returns consistent with Lyon, Barber, and Tsai (1999). Of note, Breach firms' standard deviation of returns is lower than Asset-Matched and Past-ROA-Matched firms and almost identical to Market Value-Matched firms across all periods. This suggests that Breach firms are lower risk than Matched firms before and after the breach disclosures.

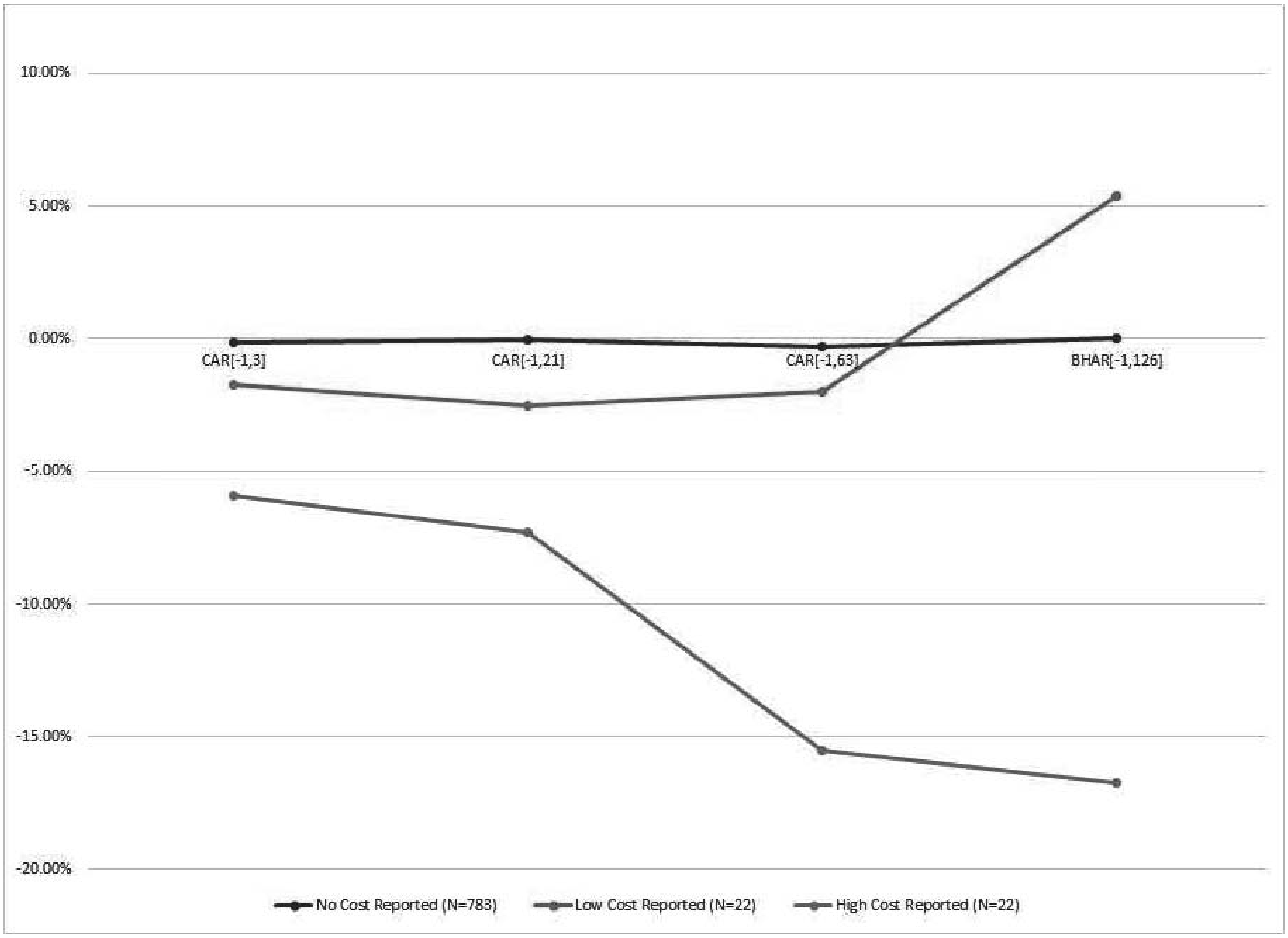
Panel B presents a multivariate comparison of returns in the five-day and one-month windows around breach disclosures. The results are consistent with the univariate results in Panel A. Breach firms have lower returns in the five-day window around the disclosure, but after controlling for prior return standard deviation, share turnover, market values, and prior returns, there is no significant difference in cumulative residual or excess returns in the one-month window.

Breaches and Future Accounting Measures of Performance

Table 4 examines the impact of breaches on future accounting measures of performance, i.e., future revenue, future sales growth, future ROS, and future ROA. In the first four columns, the interaction term *Post × Breach Firm* indicates differences in the coefficients for Breach and Matched firms as described in Equation (2). To the extent that breaches affect future performance, the coefficient should be negative; however, Breach firms do not have lower future total revenue (after controlling for prior revenue), sales growth, ROS, or ROA than Matched firms. In columns (5) and (6), we use all available observations with propensity scores per Equation (3). For brevity, we only show results for future sales growth and ROA, but in all cases, the coefficient on *Breach Firm* is positive. Thus, there is no evidence that future accounting measures of performance are affected by data breaches in this sample.

TABLE 7 (continued)

Panel C: Cumulative Abnormal Returns following Data Breaches Categorized by Cost Reported



In untabulated tests, we also restricted the regressions in columns (1) to (4) to the year before and year after the breach disclosure, rather than three years before and after. Those results are similar. Relationships between control variables and future performance are consistent with expectations. Mergers and acquisitions tend to increase revenue, but reduce ROS. Companies with higher asset turns have higher future sales growth and ROS, but lower ROA. Industry averages are also positively related to future performance. Thus, like many extant studies we do not find an impact on future performance. The one main difference in our results is that we do not find a change in ROS, while Ko and Dorantes (2006) and Ko et al. (2009) do. However, the difference is mostly likely due to their earlier sample windows (1997–2004) and small sample sizes.

Breaches and Audit and Other Fees

Table 5 shows results for the multivariate analysis of the impact of breaches on audit and other fees. In columns (1) and (3), the models include all available observations for the three years before and after breach disclosures. In columns (2) and (4), the models only include the years immediately before and after the breach disclosure. Columns (5) and (6) include all available observations with propensity scores rather than just Propensity-Matched firms. Theory suggests that data breaches may indicate an increase in business and control risk that requires additional audit work or generates other miscellaneous work. However, results show no significant difference in future audit or other fees between Breach and Matched firms post-disclosure. Since the

TABLE 8

Changes in Analysts Information around Breach Disclosure

Variable	Mean Values of Analyst Information Month Before	Month After	n
Breach Firms			
EPS Estimate	3.008	3.028	736
Standard Deviation	0.150	0.144	696
Analyst Following	17.367	17.431	736
Propensity-Matched Firms			
EPS Estimate	3.150	2.664	680
Standard Deviation	0.151	0.150	613
Analyst Following	14.031	14.031	680
Market Value-Matched Firms			
EPS Estimate	3.449	3.444	680
Standard Deviation	0.162	0.157	619
Analyst Following	15.076	15.021	680

This table presents a summary of analyst estimates, standard deviation of estimates, and number of analysts following the firm in the month before and month after the breach disclosures; none of the changes are significantly different from 0 at standard levels of significance.

model controls for prior fees, some of the control variables no longer affect future fees, but in general the relationship between the control variables and future fees is consistent with expectations. In untabulated tests, we examine whether the type of breach (e.g., hacking) or the type of information lost (e.g., financial data) affect future audit and other fees. We find little difference among types of breaches or information losses. Thus, unlike most of the research in Table 13 of Appendix A, we do not find an impact on audit fees and other fees even for specific types of breaches (Smith et al. 2019). Our sample is much larger than the extant literature study, so sample selection criteria could be driving prior results.

Breaches and Control Weaknesses

Table 6 examines relationships between breaches and SOX 404 material internal control weaknesses. Panel A presents univariate information about reports of material weaknesses before and after data breaches. This panel suggests that there is little relationship. Twenty-two Breach firms report internal control weaknesses in the year of the breach, but 25 Propensity-Matched firms also report ICMW. Breach firms only report internal control weaknesses in about 2 percent of the firm years prior to the breach disclosure and after the disclosure, consistent with rates for Propensity-Matched firms.

Panel B presents results of multivariate logit tests of the likelihood of reporting material internal control weaknesses following data breaches. In columns (1) and (2), we contrast with Propensity-Matched firms per Equation (6). In columns (3) and (4), we use the entire available population with propensity scores per Equation (7). In columns (2) and (4), we control for prior ICMW. These results confirm that Breach firms do not experience greater future rates of material weaknesses than Matched firms, which is not surprising given that relatively few of the companies in our sample report material weaknesses. Thus, our results are counter to the three extant studies on SOX 404 and data breaches. The main difference between our study and those studies is that we have a much bigger sample than the extant literature, indicating that sample selection criteria may be driving some results.

TABLE 9

Summary of Hypotheses

	Hypothesis	Result
H1	On average, data breaches have a negative impact on short-term and long-term stock market returns.	Not supported.
H2	After a data breach, future company performance is negatively affected.	Not supported.
H3	On average, there will be an increase in audit fees and other fees around a data breach.	Not supported.
H4	On average, there will be an increase in reported SOX 404 material weaknesses around a data breach.	Not supported.

TABLE 10

Summary of Breach Consequences

Panel A: Percent of Companies with a Particular Negative Consequence

	Main Economic Consequences			
	Negative CAR [−1, 21]	Reduced Performance (Future ROA)	Increased Audit Fees	SOX 404 Material Weakness
Breach Firms	51.70%	48.00%	68.00%	2.81%
Propensity-Matched	50.07%	48.50%	68.93%	3.34%
Market Value-Matched	50.91%	47.33%	68.67%	1.93%

This panel shows the percentage of Breach and Matched firms reporting negative performance after a data breach. Negative performance is defined as a CAR [−1, 21] less than 0, a future change in ROA less than 0, a future change in audit fees less than 0, or a future ICMW. There is no significant difference between percentages for Breach and Matched firms for any of the economic consequences.

Panel B: Percent of Companies with "X" Number of Negative Consequences

	0	1	2	3	4
Breach Firms	10.04%	34.06%	38.67%	16.82%	0.41%
Propensity-Matched	10.96%	30.96%	41.64%	15.62%	0.82%
Market Value-Matched	11.19%	33.43%	40.06%	14.50%	0.83%

This panel shows the percentage of Breach and Matched firms reporting 0, 1, 2, 3, or 4 incidents of negative performance after a data breach. Negative performance is defined as a CAR [−1, 21] less than 0, a future change in ROA less than 0, a future change in audit fees less than 0, or a future ICMW.

Additional Tests

Clearly, some data breaches are catastrophic. Equifax, for example, lost approximately 36 percent of its market value following its major 2017 breach. Many of the studies listed in Appendix A examine particular types of data breaches as well as the types of information lost. For the additional analysis, we use a breach-level risk calculator available at https://breachlevelindex.com/data-breach-risk-assessment-calculator. The website https://breachlevelindex.com/ compiles information about data breaches worldwide. Since 2013, Gemalto, an international data security company that sponsors the website, identified and published information about 8,590 data breaches, which was then used to evaluate associated risk. Gemalto's risk calculator generates risk levels from 1 to 10 based on the number of records exposed, the type of attack, and the type of information lost. Based on the calculated risk level, they also provide severity categories that range from Minimal (1 to 2.9), Moderate (3 to 4.9), Critical (5 to 6.9), Severe (7 to 8.9), and Catastrophic (9 to 10).

Panel A of Table 7 examines the impact of breach disclosures based on those severity categories. Although only 13 of the 827 breaches in our sample are in the Catastrophic category, those incidents clearly have more adverse impacts. The average buy-and-hold return for the six months following a Catastrophic breach is greater than 10 percent, over 14 times that of the Minimal-level breaches. As the severity level increases, companies are more likely to report the breach in an SEC 8-K filing and be involved in litigation. In our sample, 44 firms reported cost figures related to responding to a breach. Those cost figures are substantially higher for Catastrophic breaches.

We attempted various analyses to examine the impact of risk level and breach severity on accounting measures of performance, audit fees, and ICMW, but we found few differences in the multivariate analyses, probably due to the relatively few Catastrophic breaches. We conclude that, on average, there is little impact from a data breach except in those rare situations involving massive data exposures.

We also consider the possibility that investors use a rational expectations model to react to the breach disclosure. We examine whether the reported costs are related to CAR values in Panel B. We formed two groups based on reported breach costs and contrasted CAR values with firms that did not report costs. There is clearly a strong relationship. The Breach firms that did not report breach costs experienced CARs over the five-day, one-month, and three-month periods, and BHARs over the six-month period that are not significantly different from 0. However, all the firms that reported costs had negative CARs over those periods, and firms reporting high costs (as a percent of revenue) suffered substantial losses. The chart associated with Panel B provides a summary of those relationships. This again indicates that many of the reported negative results of data breaches are driven by those costly catastrophic breaches.

Our final test examines whether analysts adjusted their forecasts around breach disclosures. Table 8 shows little evidence that forecasts were changed. The average forecast earnings per share (EPS) increased and the standard deviation of estimates decreased for Breach firms but not for Propensity-Matched or Market Value-Matched firms. The number of analysts following Breach firms marginally increased. Therefore, we do not find a major impact on analysts' forecasts.

Summary of Results and Contributions

Overall, the results suggest very few consequences to data breaches. Market returns for breach companies are nominally lower, but not significantly different than the matched companies. There is no discernible impact on performance, measured as future revenue, sales growth, return on sales, or return on assets. Also, there is no discernible impact on audit fees or other fees, and companies that report data breaches are not more likely to report SOX 404 material internal control weaknesses. In untabulated tests, we also examine whether results differ for companies with multiple breaches, companies that filed SEC 8-K reports, companies with greater numbers of records exposed, or companies that faced class action lawsuits or federal and state fines due to the breach. In all cases, the difference in results is not material. The only major impact that we identify is that as the severity level of a breach increases, companies are more likely to report the breach in an SEC 8-K filing and be involved in litigation, and for catastrophic breaches, the average buy-and-hold return is greater than 10 percent.

Unlike extant research, we use one consistent sample to study the economic consequences that may impact a company after a breach over a longer period of time (2005–2018) than any prior study. Our sample is many times larger than that used by most extant studies. Unlike the majority of prior literature, we do not find that most companies experience major consequences after a breach.

Table 9 shows that none of the hypothesis are supported. Moreover, Panels A and B of Table 10 show that most companies experience no unexpected consequences at all. Panel A of Table 10 compares the percentage of Breach firms suffering negative economic consequences to both Propensity-Matched and Market Value-Matched firms. For Panel A, we define negative consequences as a CAR $[-1, 21]$ less than 0, a future change in ROA less than 0, a future change in audit fees less than 0, or a future ICMW. In Panel B, we examine the percent of Breach or Matched firms that suffer multiple negative consequences. Again, there is little difference among Breach and Matched firms. Therefore, our results explain the dichotomy between (most) extant breach research and actual reality. Based on extant literature, it would seem that companies would attempt to limit breaches because breaches are associated with bad economic consequences. Our results show that is not true. By stepping back and taking a wholistic approach, our research better captures the realities of the real business world.

VI. CONCLUSION

As we asked earlier, why are companies not working harder (and investing more) to reduce the number of data breaches by investing in cybersecurity? The answer seems to be that there are few, if any, significant consequences to the average company that experiences a data breach. If there is not a significant impact on operations, why would companies invest to prevent data breaches? While the rate of data breaches is increasing, many breaches are not detected or disclosed. The cost of data breaches spills over from the initial targets to individuals and economically linked companies. As companies do not account for these negative externalities, companies underinvest in cybersecurity. Companies are unlikely to change their investment patterns unless the cost of breaches increases dramatically or regulatory bodies enforce change.

One potential way to help enforce that companies be accountable for data breaches is to require breaches to be reported in an 8-K filing. This should help bring the breaches to the attention of regulators and investors. A second way is to expand SOX 404 requirements. Data breaches are the result of the lack of operational controls, specifically those over a company's IT systems. SOX 404 requires listed companies to annually evaluate and report on their IT and non-IT controls over *financial reporting*. Cyberattacks, however, can enter companies not only from financial reporting systems, but also from operating systems, which are not included in SOX 404 inspections/reports. In addition, breaches may be an indicator of material weaknesses in controls across the company, which may be missed or reported later than sooner (Lawrence et al. 2018). Therefore, breaches should be reported as a material weakness even if they have no significant impact on the stock market, future performance, audit/other fees, or analyst forecasts.

Countries, like China, require the evaluation of not only financial reporting controls, but also controls over company operations and operating systems. Should the U.S. expand SOX to cover all reporting systems making auditors/managers annually evaluate operational controls as well as financial controls? If such an expanded regulatory system were put in place, breaches (and *a priori* breach risk) should be captured by SOX 404 disclosures. Future research in such a regulatory regime could determine how effective SOX 404 is at capturing these IT weaknesses. Specifically, if an expanded SOX 404 report included an IT-related material weakness *prior to* the cybersecurity breach, then SOX is effective at helping companies, regulators, and investors identify potential IT problems before they happen. If an expanded SOX 404 report never reports or includes an IT-related material weakness until *after* a cybersecurity breach, then SOX is inadequately capturing the risk of cybersecurity breaches. A broadened SOX 404 should help encourage companies to take cybersecurity seriously and better protect the private information of its customers and employees.

REFERENCES

Acquisti, A., A. Friedman, and R. Telang. 2006. *Is There a Cost of Privacy Breaches? An Event Study*. Proceedings of the 3rd International Conference on Information Systems, Milwaukee, WI.

Akey, P., S. Lewellen, and I. Liskovich. 2018. *Hacking corporate reputations*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3143740

American Institute of Certified Public Accountants (AICPA). 2015. *Security regains place as top technology priority for CPAs, North American survey finds*. Available at: https://www.aicpa.org/press/pressreleases/2015/pages/security-regains-place-as-top-technology-priority-for-cpas-north-american-survey-finds.aspx

Amir, E., S. Levi, and T. Livne. 2018. *Do firms underreport information on cyber-attacks? Evidence from capital markets*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3136193

Andoh-Baidoo, F. K., K. Amoako-Gyampah, and K.-M. Osei-Bryson. 2010. How internet security breaches harm market value. *IEEE Security and Privacy* 8 (1): 36–42. https://doi.org/10.1109/MSP.2010.37

Arcuri, M. C., M. Brogi, and G. Gandolfi. 2014. *The Effect of Information Security Breaches on Stock Returns: Is the Cyber Crime a Threat to Firms?* Proceedings of the European Financial Management Meeting, Rome, Italy.

Arcuri, M. C., M. Brogi, and G. Gandolfi. 2017. *How Does Cyber Crime Affect Firms? The Effect of Information Security Breaches on Stock Returns*. Proceedings of the First Italian Conference on Cybersecurity, 175–193, Venice, Italy.

Ashbaugh-Skaife, H., D. W. Collins, W. R. Kinney, Jr., and R. LaFond. 2009. The effect of SOX internal control deficiencies on firm risk and cost of equity. *Journal of Accounting Research* 47 (1): 1–43. https://doi.org/10.1111/j.1475-679X.2008.00315.x

Aytes, K., S. Byers, and M. Santhanakrishnan. 2006. *The economic impact of information security breaches: Firm value and intra-industry effects*. Available at: https://pdfs.semanticscholar.org/7711/71bbe69e54b8229bee8c5bb1d7b12fdadc12.pdf

Barnes, S. 2018. *Those that have been hacked and those that will be hacked*. Available at: https://byronvaleadvisors.com/there-are-only-two-types-of-companies-those-that-have-been-hacked-and-those-that-will-be-hacked/

Bell, T. B., W. R. Landsman, and D. A. Shackelford. 2001. Auditor's perceived business risk and audit fees: Analysis and evidence. *Journal of Accounting Research* 39 (1): 35–43. https://doi.org/10.1111/1475-679X.00002

Bianchi, D., and O. Tosun. 2018. *Cyber-attacks and stock market activity*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3190454

Boehmer, E., J. Musumeci, and A. B. Poulsen. 1991. Event-study methodology under conditions of event-induced variance. *Journal of Financial Economics* 30 (2): 253–272. https://doi.org/10.1016/0304-405X(91)90032-F

Bolster, P., C. Pantalone, and E. Trahan. 2010. Security breaches and firm value. *Journal of Business Valuation and Economic Loss Analysis* 5 (1): 1–11. https://doi.org/10.2202/1932-9156.1081

Bose, I., and A. C. M. Leung. 2014. Do phishing alerts impact global corporations? A firm value analysis. *Decision Support Systems* 64: 67–78. https://doi.org/10.1016/j.dss.2014.04.006

Campbell, K., L. A. Gordon, M. P. Loeb, and L. Zhou. 2003. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security* 11 (3): 431–448. https://doi.org/10.3233/JCS-2003-11308

Cardenas, J., A. S. Coronado, A. Nicholas-Donald, F. Parra, and M. A. Mahmood. 2012. *The Economic Impact of Security Breaches on Publicly Traded Corporations: An Empirical Investigation*. Proceedings of the Eighteenth Americas Conference on Information Systems, Seattle, WA.

Cavusoglu, H., B. Mishra, and S. Raghunathan. 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. https://doi.org/10.1080/10864415.2004.11044320

Chambers, J. T. 2018. *There are two types of companies: Those that have been hacked, and those who don't know they have been hacked*. Available at: https://www.brainyquote.com/quotes/john_t_chambers_821369

Chan, L. K. C., N. Jegadeesh, and J. Lakonishok. 1996. Momentum strategies. *The Journal of Finance* 51 (5): 1681–1713. https://doi.org/10.1111/j.1540-6261.1996.tb05222.x

Chen, J. V., H. C. Li, D. C. Yen, and K. V. Bata. 2012. Did consulting firms gain when their clients were breached? *Computers in Human Behavior* 28 (2): 456–464. https://doi.org/10.1016/j.chb.2011.10.017

Chen, X., I. Bose, A. C. M. Leung, and C. Guo. 2011. Assessing the severity of phishing attacks: A hybrid data mining approach. *Decision Support Systems* 50 (4): 662–672. https://doi.org/10.1016/j.dss.2010.08.020

Chichernea, D., A. Holder, A. Petkevich, and A. Robin. 2018. *Better audits, better cybersecurity?* Working paper, University of Denver, The University of Toledo, and Rochester Institute of Technology.

CNBC. 2015. *Biggest cybersecurity threats in 2016*. Available at: http://www.cnbc.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html

Corrado, C. J., and T. L. Zivney. 1992. The specification and power of the sign test in event study hypothesis tests using daily stock returns. *Journal of Financial and Quantitative Analysis* 27 (3): 465–478. https://doi.org/10.2307/2331331

Council of Economic Advisors. 2018. *The cost of malicious cyber activity to the U.S. economy*. Available at: https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

Dean, B. 2015. *Why companies have little incentive to invest in cybersecurity*. Available at: http://theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570

De Groot, J. 2019. *The history of data breaches*. Available at: https://digitalguardian.com/blog/history-data-breaches

Doyle, J., W. Ge, and S. McVay. 2007. Determinants of weaknesses in internal control over financial reporting. *Journal of Accounting & Economics* 44 (1/2): 193–223. https://doi.org/10.1016/j.jacceco.2006.10.003

Ettredge, M. L., and V. J. Richardson. 2003. Information transfer among internet firms: The case of hacker attacks. *Journal of Information Systems* 17 (2): 71–82. https://doi.org/10.2308/jis.2003.17.2.71

European Parliament. 2013. *Data and security breaches and cyber-security strategies in the EU and its international counterparts*. Available at: http://www.europarl.europa.eu/RegData/etudes/note/join/2013/507476/IPOL-ITRE_NT(2013)507476_EN.pdf

Evolver Inc. 2018. *Whitepaper (updated): Reflections on the SECs cybersecurity guidance: The rise of the investor in the discussion*. Available at: https://evolverinc.com/sec-cyber-security-risk-disclosure/

Fama, E. F., and K. R. French. 1992. The cross-section of expected stock returns. *The Journal of Finance* 47 (2): 427–465. https://doi.org/10.1111/j.1540-6261.1992.tb04398.x

Fama, E. F., and K. R. French. 1993. Common risk factors in the returns on stocks and bonds. *Journal of Financial Economics* 33 (1): 3–56. https://doi.org/10.1016/0304-405X(93)90023-5

Fama, E. F., and K. R. French. 1996. Multifactor explanations of asset pricing anomalies. *The Journal of Finance* 51 (1): 55–84. https://doi.org/10.1111/j.1540-6261.1996.tb05202.x

Fama, E. F., and K. R. French. 1997. Industry costs of equity. *Journal of Financial Economics* 43 (2): 153–193. https://doi.org/10.1016/S0304-405X(96)00896-3

Friedlander, G. 2014. *Why 85% of data breaches are undetected*. Available at: https://www.observeit.com/blog/why-85-percent-data-breaches-undetected/

Fung, B. 2018. *Equifax's massive 2017 data breach keeps getting worse*. Available at: https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/?noredirect=on&utm_term=.36a8868c885d

Garg, A., J. Curtis, and H. Halper. 2003a. Quantifying the financial impact of IT security breaches. *Information Management & Computer Security* 11 (2): 74–83. https://doi.org/10.1108/09685220310468646

Garg, A., J. Curtis, and H. Halper. 2003b. The real cost of being hacked. *Journal of Corporate Accounting & Finance* 14 (5): 49–52. https://doi.org/10.1002/jcaf.10183

Gatzlaff, K. M., and K. A. McCullough. 2010. The effect of data breaches on shareholder wealth. *Risk Management & Insurance Review* 13 (1): 61–83. https://doi.org/10.1111/j.1540-6296.2010.01178.x

Ghosh, A., and R. Pawlewicz. 2009. The impact of regulation on auditor fees: Evidence from the Sarbanes-Oxley Act. *Auditing: A Journal of Practice & Theory* 28 (2): 171–197. https://doi.org/10.2308/aud.2009.28.2.171

Goel, S., and H. A. Shawky. 2009. Estimating the market impact of security breach announcements on firm values. *Information & Management* 46 (7): 404–410. https://doi.org/10.1016/j.im.2009.06.005

Goel, S., and H. A. Shawky. 2014. The impact of federal and state notification laws on security breach announcements. *Communications of the Association for Information Systems* 34: 37–50. https://doi.org/10.17705/1CAIS.03403

Gogan, M. 2017. *Insider threats as the main security threat in 2017*. Available at: https://www.tripwire.com/state-of-security/security-data-protection/insider-threats-main-security-threat-2017/

Gonsalves, J. 2014. *Target top security officer reporting to CIO seen as a mistake*. Available at: https://www.csoonline.com/article/2363210/data-protection/target-top-security-officer-reporting-to-cio-seen-as-a-mistake.html

Gordon, L. A., M. P. Loeb, and L. Zhou. 2011. The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security* 19 (1): 33–56. https://doi.org/10.3233/JCS-2009-0398

Graham, B., and D. L. Dodd. 1934. *Security Analysis: Principles and Technique*. New York, NY: McGraw-Hill.

Griggs, L. L., and S. M. Donahue. 2014. *Financial reporting and the law: Cybersecurity breaches may be the result of weaknesses in internal controls*. Available at: https://www.morganlewis.com/blogs/financialreporting/2014/03/cybersecurity-breaches-may-be-the-result-of-weaknesses-in-internal-controls

Guo, S., and M. W. Fraser. 2015. *Propensity Score Analysis; Statistical Methods and Applications*. Thousand Oaks, CA: Sage Publications Inc.

Gwebu, K. L., J. Wang, and W. Xie. 2014. *Understanding the Cost Associated with Data Breaches*. Proceedings of the Pacific Asia Conference on Information Systems.

Haislip, J., R. Pinsker, V. J. Richardson, and M. Thevenot. 2018. *For whom the breach tolls: Effects of IT governance on timeliness of data security breach detection*. Working paper, Texas Tech University, Florida Atlantic University, and University of Arkansas.

Hammer, D., and J. Zuckerman. 2018. *Protections and rewards for cybersecurity whistleblowers*. Available at: https://www.zuckermanlaw.com/protections-and-rewards-for-cybersecurity-whistleblowers/

Hay, D. C., and W. R. Knechel. 2010. The effects of advertising and solicitation on audit fees. *Journal of Accounting and Public Policy* 29 (1): 60–81. https://doi.org/10.1016/j.jaccpubpol.2009.10.001

Hayden, E. 2013. *Data breach protection requires new barriers*. Available at: https://searchsecurity.techtarget.com/feature/Data-breach-protection-requires-new-barriers

Hilary, G., B. Segal, and M. H. Zhang. 2016. *Cyber-risk disclosure: Who cares?* Working paper, Georgetown University, Fordham University, and Hebrew University.

Hinz, O., M. Nofer, D. Schiereck, and J. Trillig. 2015. The influence of data theft of the share prices and systematic risk of consumer electronics companies. *Information & Management* 52 (3): 337–347. https://doi.org/10.1016/j.im.2014.12.006

Hoitash, R., U. Hoitash, and J. C. Bedard. 2008. Internal control quality and auditing pricing under the Sarbanes-Oxley Act. *Auditing: A Journal of Practice & Theory* 27 (1): 105–126. https://doi.org/10.2308/aud.2008.27.1.105

Holmes, A. 2007. *Your guide to good-enough compliance*. Available at: https://www.cio.com/article/2439324/risk-management/your-guide-to-good-enough-compliance.html?page=2

Hovav, A., and J. D'Arcy. 2003. The impact of denial-of-service attack announcements on the market value of firms. *Risk Management & Insurance Review* 6 (2): 97–121. https://doi.org/10.1046/J.1098-1616.2003.026.x

Hovav, A., and J. D'Arcy. 2004. The impact of virus attack announcements on the market value of firms. *Information Systems Security* 13 (3): 32–40. https://doi.org/10.1201/1086/44530.13.3.20040701/83067.5

Ishiguro, M., H. Tanaka, K. Matsuura, and I. Murase. 2006. *The effect of information security incidents on corporate values in the Japanese stock market*. Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.212.4556

Johnson, M. S., M. J. Kang, and T. Lawson. 2017. *Stock price reaction to data breaches*. Available at: http://jofi.aof-mbaa.org/66910-jfi-1.4148543/t-001-1.4148551/f-001-1.4148552/a-007-1.4148566

Kamiya, S., J. Kang, J. Kim, A. Milidonis, and R. Stulz. 2018. *What is the impact of successful cyberattacks on target firms?* Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3143314

Kan, M. 2017. *Here's how much your identity goes for on the dark web*. Available at: https://www.pcmag.com/news/357382/heres-how-much-your-identity-goes-for-on-the-dark-web

Kannan, K., J. Rees, and S. Sridhar. 2007. Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce* 12 (1): 69–91. https://doi.org/10.2753/JEC1086-4415120103

Kaspereit, T. 2015. *EVENTSTUDY2: A program to perform event studies with complex test statistics in Stata*. Available at: https://ideas.repec.org/c/boc/bocode/s458086.html

Kelton, K., K. R. Fleischmann, and W. A. Wallace. 2008. Trust in digital information. *Journal of the American Society for Information Science and Technology* 59 (3): 363–374. https://doi.org/10.1002/asi.20722

Klamm, B. K., and M. W. Watson. 2009. SOX 404 reported internal control weaknesses: A test of COSO framework components and information technology. *Journal of Information Systems* 23 (2): 1–23. https://doi.org/10.2308/jis.2009.23.2.1

Ko, M., and C. Dorantes. 2006. The impact of information security breaches on financial performance of the breached firms: An empirical investigation. *Journal of Information Technology Management* 17 (2): 13–22.

Ko, M., K.-M. Osei-Bryson, and C. Dorantes. 2009. Investigating the impact of publicly announced information security breaches on three performance indicators of the breached firms. *Information Resources Management Journal* 22 (2): 1–21. https://doi.org/10.4018/irmj.2009040101

Krebs, B. 2014. *Target hackers broke in via HVAC company*. Available at: https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Kvochko, E., and R. Pant. 2015. *Why data breaches don't hurt stock prices*. Available at: https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices

Lawrence, A., M. Minutti-Meza, and D. Vyas. 2018. Is operational control risk informative of undetected financial reporting deficiencies? *Auditing: A Journal of Practice & Theory* 37 (1): 139–165. https://doi.org/10.2308/ajpt-51784

Layton, R., and P. A. Watters. 2014. A methodology for estimating the tangible cost of data breaches. *Journal of Information Security and Applications* 19 (6): 321–330. https://doi.org/10.1016/j.jisa.2014.10.012

Lending, C., K. Minnick, and P. J. Schorno. 2018. *Corporate governance, social responsibility, and data breaches*. Working paper, Western Washington University, Bentley University, and Ally Financial.

Lenihan, R. 2018. *Consulting practices draw regulatory scrutiny as their growth accelerates*. Available at: https://warrington.ufl.edu/centers/icraa/docs/Accounting_and_Auditing.pdf (last accessed on April 3, 2018).

Leung, A., and I. Bose. 2008. *Indirect financial loss of phishing to global markets*. Available at: https://aisel.aisnet.org/icis2008/5

Leuven, E., and B. Sianesi. 2003. *PSMATCH2: Stata module to perform full Mahalanobis and propensity score matching, common support graphing, and covariate imbalance testing*. Available at: https://www.researchgate.net/publication/4794420_PSMATCH2_Stata_Module_to_Perform_Full_Mahalanobis_and_Propensity_Score_Matching_Common_Support_Graphing_and_Covariate_Imbalance_Testing

Li, H., W. G. No, and J. E. Boritz. 2016. *Are external auditors concerned about cyber incidents? Evidence from audit fees*. Working paper, Rutgers University and University of Waterloo.

Lyon, J. D., B. M. Barber, and C. L. Tsai. 1999. Improved methods for tests of long-run abnormal stock returns. *The Journal of Finance* 54 (1): 165–201. https://doi.org/10.1111/0022-1082.00101

Malhotra, A., and C. K. Malhotra. 2011. Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research* 14 (1): 44–59. https://doi.org/10.1177/1094670510383409

Mann, C. L. 2015. Information lost: Will the "paradise" that promises, to both consumer and firm, be "lost" on account of data breaches? The epic is playing out. In *Economic Analysis of the Digital Economy*. Chicago, IL: University of Chicago Press.

Martin, K. D., A. Borah, and R. W. Palmatier. 2017. Data privacy: Effects on customer and firm performance. *Journal of Marketing* 81 (1): 36–58. https://doi.org/10.1509/jm.15.0497

McKenna, F. 2017. *Equifax auditors are on the hook for data security risk controls*. Available at: https://www.marketwatch.com/story/equifax-auditors-are-on-the-hook-for-data-security-risk-controls-2017-10-02

McKenna, F. 2018. *SEC issues updated cybersecurity risk guidance bust some say not nearly enough*. Available at: https://www.marketwatch.com/story/sec-issues-updated-cybersecurity-risk-guidance-but-some-say-not-nearly-enough-2018-02-21

Modi, S., M. Wiles, and S. Mishra. 2015. Shareholder value implications of service failures in triads: The case of customer information security breaches. *Journal of Operations Management* 35 (1): 21–39. https://doi.org/10.1016/j.jom.2014.10.003

Moore, T., R. Clayton, and R. Anderson. 2009. The economics of online crime. *The Journal of Economic Perspectives* 23 (3): 3–20. https://doi.org/10.1257/jep.23.3.3

Morgan, S. 2016. *Cyber crime costs projected to reach $2 trillion by 2019*. Available at: https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#789dae3d3a91

Morgan, S. 2017a. *Cybercrime to $6 trillion by 2021*. Available at: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Morgan, S. 2017b. *2018 cybersecurity market report*. Available at: https://cybersecurityventures.com/cybersecurity-market-report/ (last accessed August 17, 2018).

Morse, E.A., V. Raval, and J. R. Wingender, Jr. 2011. Market price effects of data security breaches. *Information Security Journal: A Global Perspective* 20 (6): 263–273.

Nicholas-Donald, A., J. F. Matus, S. Ryu, and A. M. Mahmood. 2011. *The economic effect of privacy breach announcements on stocks: A comprehensive empirical investigation*. Available at: https://aisel.aisnet.org/amcis2011_submissions/341

Nusca, A. 2017. *Equifax has plunged 18.4% since it revealed massive breach*. Available at: https://fortune.com/2017/09/11/equifax-stock-cybersecurity-breach/

Patel, N. 2010. *The effect of IT hack announcements on the market value of publicly traded corporations*. Available at: https://sites.duke.edu/djepapers/files/2016/10/Patel_DJE.pdf

Patell, J. 1976. Corporate forecasts of earnings per share and stock price behavior: Empirical test. *Journal of Accounting Research* 14 (2): 246–276.

Petersen, M. 2009. Estimating standard errors in finance panel data sets: Comparing approaches. *Review of Financial Studies* 22 (1): 435–480. https://doi.org/10.1093/rfs/hhn053

Pirounias, S., D. Mermigas, and C. Patsakis. 2014. The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study. *Journal of Information Security Applications* 19 (4/5): 257–271. https://doi.org/10.1016/j.jisa.2014.07.001

Ponemon Institute. 2017. *2017 cost of cyber crime study: Global*. Available at: https://www.ibm.com/downloads/cas/ZYKLN2E3

Privacy Rights Clearinghouse. 2018. *What to do when you receive a data breach notice*. Available at: https://www.privacyrights.org/consumer-guides/what-do-when-you-receive-data-breach-notice

Protiviti. 2016. *Executive perspectives on top risks for 2016*. Available at: https://erm.ncsu.edu/az/erm/i/chan/library/NC-State-Protiviti-Survey-Top-Risks-2016.pdf

Public Company Accounting Oversight Board (PCAOB). 2017. *PCAOB publishes staff inspection brief previewing 2016 inspection findings*. Available at: https://pcaobus.org/News/Releases/Pages/staff-inspection-brief-2016-preview-11-9-17.aspx

Riffkin, R. 2014. *Hacking tops list of crimes Americans worry about most*. Available at: https://news.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx

Rosati, P., M. Cummins, P. Deeney, F. Gogolin, L. van der Werff, and T. Lynn. 2017. The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis* 49 (January): 146–154. https://doi.org/10.1016/j.irfa.2017.01.001

Rosenbaum, P. R., and D. B. Rubin. 1983. The central role of the propensity score in observational studies for causal effects. *Biometrica* 70 (1): 41–55. https://doi.org/10.1093/biomet/70.1.41

Schatz, D., and R. Bashroush. 2016. The impact of repeated data breach events on organisations' market value. *Information and Computer Security* 24 (1): 73–92. https://doi.org/10.1108/ICS-03-2014-0020

Securities and Exchange Commission (SEC). 2007. *Definition of the term significant deficiency. SEC 17 CFR Parts 210 and 240*. Available at: https://www.sec.gov/rules/final/2007/33-8829.pdf

Sharma, D. S., P. N. Tanyi, and B. A. Litt. 2017. Costs of mandatory periodic audit partner rotation: Evidence from audit fees and audit timeliness. *Auditing: A Journal of Practice & Theory* 36 (1): 129–149. https://doi.org/10.2308/ajpt-51515

Shepardson, D. 2017. *Equifax failed to patch security vulnerability in March: Former CEO*. Available at: https://www.reuters.com/article/us-equifax-breach/equifax-failed-to-patch-security-vulnerability-in-march-former-ceo-idUSKCN1C71VY

Sherman, E. 2015. *The reason companies don't fix cybersecurity*. Available at: https://www.cbsnews.com/news/the-reason-companies-dont-fix-cybersecurity/

Shipman, J. E., Q. T. Swanquist, and R. L. Whited. 2017. Propensity score matching in accounting research. *The Accounting Review* 92 (1): 213–244. https://doi.org/10.2308/accr-51449

Smith, T. J., J. L. Higgs, and R. Pinsker. 2019. Do auditors price breach risk in their audit fees? *Journal of Information Systems*. https://doi.org/10.2308/isys-52241

Spanos, G., and L. Angelis. 2016. The impact of information security events to the stock market: A systematic literature review. *Computers & Security* 58: 216–229. https://doi.org/10.1016/j.cose.2015.12.006

Surane, J., and J. Westbrook. 2018. *Equifax CIO put "2 and 2 together" then sold stock, SEC says*. Available at: https://www.bloomberg.com/news/articles/2018-03-14/sec-says-former-equifax-executive-engaged-in-insider-trading

Tanimura, J. K., and E. W. Wehrly. 2015. The market value and reputational effects from lost confidential information. *International Journal of Financial Management* 5 (4): 8–35. https://doi.org/10.21863/ijfm/2015.5.4.020

Telang, R., and S. Wattal. 2007. An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering* 33 (8): 544–557. https://doi.org/10.1109/TSE.2007.70712

Thompson, M. 2017. *You had an ongoing data breach for months. How could you not know?* Available at: https://www.business.com/articles/data-security-breach-why-they-go-unnoticed/ (last accessed on July 19, 2018).

Wang, T., J. R. Ulmer, and K. Kannan. 2013. The textual contents of media reports of information security breaches and profitable short-term investment opportunities. *Journal of Organizational Computing and Electronic Commerce* 23 (3): 200–223. https://doi.org/10.1080/10919392.2013.807712

Weisbaum, H. 2018. *Data breaches happening at record pace, report finds*. Available at: https://www.nbcnews.com/business/consumer/data-breaches-happening-record-pace-report-finds-n785881

Westland, J. C. 2018. *The information content of Sarbanes-Oxley in predicting security breaches*. Working paper, University of Illinois at Chicago.

Winter, M. 2014. *Home Depot hackers used vendor log-on to steal data, e-mails*. Available at: https://www.usatoday.com/story/money/business/2014/11/06/home-depot-hackers-stolen-data/18613167/

Wolfe, C. J., E. G. Mauldin, and M. C. Diaz. 2009. Concede or deny: Do management persuasion tactics affect auditor evaluation of internal control deviations? *The Accounting Review* 84 (6): 2013–2037. https://doi.org/10.2308/accr.2009.84.6.2013

Yayla, A. A., and Q. Hu. 2011. The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology* 26 (1): 60–77. https://doi.org/10.1057/jit.2010.4

Yen, J-C., J-H. Lim, T. Wang, and C. Han. 2018. The impact of audit firms' characteristics on audit fees following information security breaches. *Journal of Accounting and Public Policy* 37 (6): 489–507. https://doi.org/10.1016/j.jaccpubpol.2018.10.002

Zachs Equity Research. 2018. *Equifax (EFX) earnings and revenues beat estimates in Q4*. Available at: https://www.nasdaq.com/article/equifax-efx-earnings-and-revenues-beat-estimates-in-q4-cm929239

Zafar, H., M. S. Ko, and K.-M. Osei-Bryson. 2012. Financial impact of information security breaches on breached firms and their non-breached competitors. *Information Resources Management Journal* 25 (1): 21–37. https://doi.org/10.4018/irmj.2012010102

APPENDIX A

Security Event Literature Review

Table 11
Stock Market Reaction

Panel A: Literature Review

Authors and Year	Breach Sample	Period	Match	Event Window	Model	Significant Results for Breach Companies	Conclusions
DB							
Acquisti, Friedman, and Telang 2006	79	1999–2006		[0, +1] [0, +2] [0, +5] [0, +10] Graph: [−5, +10]	1	[0, 0]: −0.4% [+1, +1]: −0.58%	Short negative CAR to privacy breach on announcement day.
Bolster et al. 2010	114	2000–2007		[−1, 0] [−1, +1] [+1, +30]	1	Big News Outlets: [−1, 0]: −0.56% [−1, +1]: −0.46%*	Negative CAR only when announced in major newspaper right around the announcement. Breach-specific and company-specific factors do not have an impact.
Gatzlaff and McCullough 2010	77	2004–2006		[0, +1] [0, +180]	1	−0.84%	Overall effect is negative CAR. Loss is greater when company is not forthcoming about details of breach. Higher market-to-book companies have greater losses. Company size and subsidiary status mitigate losses. Losses greater in more recent periods.
Patel 2010	34	2001–2009	Yes	[0, +3] [0, +8] [0, +30]	1	ns	Overall, insignificant CAR for hacked companies.
A. Malhotra and C. Malhotra 2011	93	2000–2007		[−1, +1] [+2, +30]	1, 4	[−1, +1]: −0.82% [+2, +30]: 1.47%	Negative CAR associated with loss of customer information in the long run and short run. Larger companies (number of employees) have more negative CAR, and more negative CAR from larger breaches.
Morse et al. 2011	306	2000–2010		[0, 0] [0, +1] [0, +5] [0, +10] [+1, +220] [+1, +240] [+1, +440] [+1, +480]	1	[0, 0]: −0.30% [0, +1]: −0.28% [+1, +220]: −4.8% [+1, +240]: −4.02% [+1, +440]: −6.74% [+1, +480]: −8.68%	Negative CAR following the announcement of a breach, which persists over several years. Source of data breach moderates the price effect; market punishes avoidable breaches.
Nicholas-Donald, Matus, Ryu, and Mahmood 2011	29	2000–2010		[−1, +1]	1	−1.5%	Privacy breaches have a negative, short-term effect on CAR, increase beta, and increase trading volume around the announcement.

(continued on next page)

TABLE 11 (continued)

Authors and Year	Breach Sample	Period	Match	Event Window	Model	Significant Results for Breach Companies	Conclusions
Goel and Shawky 2014	201	2001–2008		[−1, +1] Graph: [−30, +30]	4	Before Laws: −1% After Laws: −0.5%	Negative impacts of security breach announcements on stock prices have been reduced significantly after the enactment of federal and state security breach notification laws.
Pirounias et al. 2014	105	2008–2012		[−1, 0] [−1, +1] [0, 0] [0, +1]	1, 3	[−1, 0]: −0.39%* [0, 0]: −0.33%*	Fama-French three-factor model has negative CARs ($p < 0.10$). CAPM does not. Technology companies impacted more than nontechnology companies. Effect seems to have decreased over time.
Hinz, Nofer, Schiereck, and Trillig 2015	6 (6), 62 Competitors	2011–2012		[−3, −1] [0, +1] [0, +2] [0, +3] [0, +4] [0, +5] [0, +20]	1	[0, 0]: −1.16% [0, +1]: −1.82% [0, +2]: −4.06% Competitors: [0, +3]: −0.90%	Breached companies and similar companies have negative CAR (i.e., information transfer); systematic risk does not change.
Modi, Wiles, and Mishra 2015	146	2005–2010	Yes	[−2, 2] [0, +60] [0, +180] [0, +365] [0, +730]	4	[−1, +1]: 1.17%	Breaches by the front-end service provider lead to greater shareholder losses than by the buyer company. Some evidence that employee productivity (not leverage) at the buyer company moderates the impact.
Tanimura and Wehrly 2015	152	2000–2007		[0, 1]	1	Overall: −0.23% Laptop: −0.37% No Third Party: −0.27% Employee: −0.55%	Negative CAR after a data breach for specific types. Drop in market value mirrors direct costs indicating no reputational loss after breach. However, reputational loss for employee (not customer) data breach.
Hilary, Segal, and Zhang 2016	213 (168)	2005–2014	Yes	[−1, +1] [0, +180] [0, +365]	3, 4	ns	Small significant short-term (−0.5%) (not long-term) reaction to breach announcement but not significantly different from matched sample. More impact for more severe breaches and for high book-to-market companies. No impact for inclusion in annual report, company size, or time trend.
Martin, Borah, and Palmatier 2017	293 (199) Rivals: 299 (176)	Not Spec.	Yes	[0, 0] [−1, 0] [0, +1] [−1, +1]	1	[−1, 0]: −0.29%; Rivals: [−1, 0]: −0.17%	An actual data breach reduces the company's stock value by −0.29% and its closest rival's by −0.17%.
Schatz and Bashroush 2016	50 (25)	2005–2013		[−2, +2]	1	First Event: −2.38*	Weak evidence of negative reaction to first breach, but not the second.

(continued on next page)

TABLE 11 (continued)

Authors and Year	Breach Sample	Period	Match	Event Window	Model	Significant Results for Breach Companies	Conclusions
Johnson et al. 2017	467 (261)	2005–2014		[−1, +1]	1	−0.37%	Publicly traded companies lost, on average, 0.37% of their equity after a breach. Payment card frauds have the highest loss (−3%). Larger companies are more likely to experience subsequent breaches. Companies are not penalized more for repeated breaches. Reaction does not change over time (2005–2009 versus 2010–2014). No greater impact on retail or financial companies.
Akey et al. 2018	287	1999–2006	Yes	[−1, +3] [−1, +5] [−1, +10] [−1, +30] [−1, +60]	3	[−1, +3]: −0.83% [0, +30]: −2.57%	Companies with greater pre-event corporate social responsibility (CSR) exhibit less negative CAR. There is a long-term impact of a data breach on market-to-book ratios and Tobin's Q (−10 to −20%) up to four years after the incident. Breached companies invest in CSR to repair reputations. Smaller and lower market-to-book ratio companies are more likely to have a breach.
Bianchi and Tosun 2018	41	2004–2016	Yes (PM)	[−1, +1] [−2, +2] [−3, +3] [−3, +1] [−2, +1] [−1, +2] [−1, +3]	4, 5	−1.4% Average Daily Basis	CAR is negative the day after the (first time) breach announcement, while trading volume and bid-ask spreads increase. Short-term market activity is driven by selling pressure.
Kamiya et al. 2018	188 (144)	2005–2017	Yes (PM)	[−1, +1]	3, 4	Overall: −0.84% Driven by Financial: −1.09%	Cyberattacks occur at larger, more visible companies, with more intangible assets, and that are less financially constrained. Corporate governance has no impact on the likelihood of cyberattack, but companies with risk management are less likely to be attacked. Impact adverse when consumer financial information lost, but otherwise little impact. Where consumer financial information is lost, negative stock market reaction.
Lending et al. 2018	271	2004–2012	Yes (PM)	[−1, +1] [0, +365] [0, +730]		[−1, +1]: −1.3% [0, +365]: −3.5% Large Breach: [0, +365]: −7.1%	Companies with better corporate governance (i.e., smaller and more financial experts) and social responsibility (i.e., product or environmental safety) are less likely to be breached. Significant negative one-year buy-and-hold abnormal returns for companies (−3.5%).

(continued on next page)

TABLE 11 (continued)

Authors and Year	Breach Sample	Period	Match	Event Window	Model	Significant Results for Breach Companies	Conclusions
SB							
Campbell et al. 2003	43 (38)	1995–2000		[−1, +1]	1	CI: −5.46%	Only negative CAR for confidential (company or customer) information. Nature of breach impacts CAR.
Garg, Curtis, and Halper 2003a	22	1999–2001		[0, +2]		[0, 0]: −2.7% [0, +2]: −4.5%	Negative CAR to security breach (biggest for loss of credit card information). Positive CAR for security companies.
Garg, Curtis, and Halper 2003b	22	1999–2001		[0, +2]		[0, 0]: −2.7% [0, +2]: −4.5%	Negative CAR to security breach. Positive CAR for security companies (+10%). Negative CAR for insurance carriers (−2%).
Cavusoglu et al. 2004	66	1996–2001		[0, +1]	1	−2.1%	Nature of breach does not affect CAR. Small companies impacted more with increasing impact over time. Internet-only companies affected more. Positive information transfer to internet security companies (+1.36%).
Hovav and D'Arcy 2004	186	1988–2002		[−1, 0] [−1, +1] [−1, +5] [−1, +10] [−1, +25]		ns	In general, market does not penalize companies for virus attacks.
Aytes, Byers, and Santhanakrishnan 2006	67	1995–2005		[−2, +2]	1	−1.85% for CI	Positive CAR for competitors of breached company, larger for nonconfidential information (+0.70%, +0.88%). Breached company only has significantly negative CAR when breach involves confidential information (CI).
Ishiguro, Tanaka, Matsuura, and Murase 2006	70	2002–2005		[−1, +38]	1	−0.0189*	Japanese stock market responds slower than the U.S. stock market (ten days versus one day) to security incident announcements. Companies with more highly valued intangible assets are affected more.
Kannan et al. 2007	72	1997–2003	Yes	[−1, +2] [−1, +7] [−1, +29]	1	ns	CAR nonsignificant after eliminating 9/11 confounding events; CAR more negative during dot.com in the short term (−1.05%) but removing 9/11 events makes CAR insignificant.
Goel and Shawky 2009	168	2004–2005		[−5, +5]	1, 3	[−4, +2]: −1%	Average CAR of 1% during the days surrounding the event.
Andoh-Baidoo, Amoako-Gyampah, and Osei-Bryson 2010	41	1997–2003		[−1, +1]	1	−3.8%	Company characteristics (internet, time period) and attack characteristics are predictors of CAR. Breaches after February 2000 viewed more negatively (beginning of DOS attacks).

(continued on next page)

TABLE 11 (continued)

Authors and Year	Breach Sample	Period	Match	Event Window	Model	Significant Results for Breach Companies	Conclusions
Gordon et al. 2011	121 (85)	1995–2007		[−1, +1]	1, 3	Overall: −0.0136 Before 9/11: −0.024 After 9/11: ns Availability Breaches: 0.0295 before 9/11 and −0.0197 Overall	Decrease in the impact of security breaches on stock prices over time (9/11/2001 split); impact of information security breaches on CAR is significant; attacks associated with breaches of availability have most negative CAR. Fama-French three-factor model reveals results that CAPM does not.
Yayla and Hu 2011	123	1994–2000 2001–2006		[−1, +1] [−1, +5] [−1, +10]	1	[−1, +1]: −0.0092* [−1, +5]: −0.0161 [−1, +10]: −0.0152* E-commerce: [−1, +1]: −0.0451	Pure e-commerce firms experienced higher negative market reactions than traditional bricks-and-mortar firms. Denial of service attacks have higher negative impact than other types. Loss is significant for breaches before 2000 and not significant for breaches after 2001. Smaller companies hit more than larger companies in early period.
Cardenas et al. 2012	39	2002–2008		[−1, +1]	1	ns	No significant CAR, but increase in beta, increased in trading volume after cyberattack.
Wang, Ulmer, and Kannan 2013	89	1997–2008		[−1, +1]	1, 3	−0.15%*	Breach announcements containing specific information often lead to a negative CAR, with small trading volume reactions.
Arcuri et al. 2014	128 (81); Financial: 34 (17)	1995–2012		[−10, +10] [−5, +5] [−3, +3] [−1, +1] [−20, +20]	1	−0.003 to −0.029	Overall negative CAR for cybercrimes, but not negative for the financial sector. Industry matters in impact.
Arcuri et al. 2017	226 (110); Financial: 67 (34)	1995–2015		[−20, +20] [−20, −1] [−10, +10] [−10, −1] [−5, −1] [−5, +5] [−3, −1] [−3, +3] [0, +10] [0, +5] [0, +3] [0, +20]	1	−1.361% to −3.820%	Overall negative CAR for cybercrimes. More negative CAR (and earlier) for financial sector. Nonconfidential breaches have more impact.
Amir et al. 2018	276 (156)	2010–2015		[−1, +3] [−1, +30] Graph: [−1, +60]		Not Disclose: [−1, +3]: −1.47%, [−1, +60]: −3.56%	Companies withhold information about severe breaches, but report mild breaches. Significant negative CAR only for nondisclosing companies when a third party identifies the breach.

(continued on next page)

TABLE 11 (continued)

Authors and Year	Breach Sample	Period	Match	Event Window	Model	Significant Results for Breach Companies	Conclusions
DOS ONLY							
Ettredge and Richardson 2003	Four Attacked Companies, 275 Non-Attacked Companies	2000		[+1, +3]	1	Breached Companies: −2.67% to −4.42%	Find information transfer within industries attacked and internet industries not attacked (i.e., negative CAR). CAR more negative for larger companies. Internet security providers experience positive information transfer.
Hovav and D'Arcy 2003	23	1998–2002		[−1, 0] [−1, +1] [−1, +5] [−1, +10] [−1, +25]	1	ns	The market does not generally penalize companies for such attacks.
PHISHING							
Leung and Bose 2008	2,994	Before 2008		[−2, +2]	1	Overall: −5.1% Large: −6.1% Small: −4.5%	Phishing has a significantly negative CAR for companies regardless of their size. Place of incorporation, type of ownership, industry, and year affect impact.
Bose and Leung 2014	1,942	2003–2007		[−1,−1] [0, 0] [1, 1] [−1, 0] [0, 1] [−1, 1]	1, 3	[1, 1]: −0.03 [0, 1]: −0.05% [−1, 1]: −0.05%	Phishing has a significantly negative CAR and negative impact on volume. Bigger impact during 2006–2007 and for financial holding companies.

* Indicates results significant at $p < 0.10$.

Year indicates year of study. Match indicates if the study used a matched or propensity (PM) sample. Model indicates which model was used to generate returns: 1 stands for market model; 3, 4, and 5 stand for the Fama-French three-, four-, and five-factor model, respectively. CAR stands for cumulative abnormal return; overall significant CAR is given unless a subset is specified. CI stands for confidential information. ns stands for nonsignificant results. The following studies are not included because they are editorial, a literature review, or do not report the impact on the breached companies' CAR: Chen, Bose, Leung, and Guo (2011); Chen, Li, Yen, and Bata (2012), Hovav and D'Arcy (2004); Kvochko and Pant (2015); Mann (2015); Moore, Clayton, and Anderson (2009); Rosati et al. (2017); Spanos and Angelis (2016); and Telang and Wattal (2007).

Panel B: Summary for Panel A

								For Negative CAR at $p < 0.05$		
Type of Breach	n	Matched Samples	Propensity Matched Samples	1 Factor Model	Multiple Factor Model	Insignificant CAR	Negative CAR at 10%	Negative CAR Only for Subset	Overall Negative CAR	Changes Over Time
Data Breach (DB)	20	5	3	12	8	2	2	2	14	3
Security Breach (SB)	17	1	0	12	2	3	2	3	9	2
Denial of Service Only (DOS ONLY)	2	0	0	2	0	1	0	0	1	0
PHISHING ONLY	2	0	0	2	1	0	0	0	2	2
Total	41	6	3	28	11	6	4	5	26	7
Percent of Total		15%	7%	68%	27%	15%	10%	12%	63%	17%

Not all studies identify the model used, and some studies use more than one model.

TABLE 12

Future Performance Impact

Panel A: Literature Review

Authors	Year	Cat	Breach Sample Size	Time Period	Matched Sample	Sales	ROA	ROE	ROS	P/E	Div	EBITDA, Earn	R&D	Inv	CGS	SGA	Oper Exp	Non-Recur Exp	Cash Flow Vol	Acq	LT Debt
Ko and Dorantes	2006	DB	19	1997–2001	Yes	M	M		M			ns			ns		ns				
Ko, Osei-Bryson, and Dorantes	2009	SB	69	1997–2004	Yes		D*; Avail: D*; IT Int & Lg: D		Lg: D						IT Int: I						
Zafar, Ko, and Osei-Bryson	2012	SB	119	1997–2007	Yes		I for WD & DC									D					
Gwebu, Wang, and Xie	2014	SB	174	Unknown								ns									
Hilary, Segal, and Zhang	2016	DB	213 (168)	2005–2014	Yes		Ns														
Akey, Lewellen, and Liskovich	2018	DB	287	1999–2006	Yes	ns						D* /ns[a]						I			
Bianchi and Tosun	2018	DB	41	2004–2016	Yes (PM)	ns	Ns			ns	D*		D*	ns							
Kamiya, Kang, Kim, Milidonis, and Stulz	2018	DB	188 (144)	2005–2017	Yes (PM)	D* (D* for Lg)	ns (D* for Lg)	ns (D* for Lg)					ns	ns					I	ns	I
Lending, Minnick, and Schorno	2018	DB	271	2004–2012	Yes (PM)	-															

Panel B: Summary for Table 12

Breach Type	n	Matched Sample	Propensity Matched Sample
Data Breach	6	3	3
Security Breach	3	2	0
Total	9	5	3

Panel C: Articles Significance Frequency Analysis

Breach Type	Total	Sales	ROA	ROE	ROS	P/E	Div	EBITDA, Earn	R&D	Inv	CGS	SGA	Oper Exp	Non Recur Exp	Cash Flow Vol	Acq	LT Debt
DB																	
ns/Mixed	15	3	3	0	1	1	0	1	1	2	1	0	1	0	0	1	0
At 10%	4	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0
At 5%	7	0	1	1	1	0	0	0	0	0	1	0	0	1	1	0	1
SB																	
ns/Mixed	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
At 10%	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
At 5%	3	0	2	0	0	0	0	0	0	0	0	1	0	0	0	0	0
Total	30	4	6	1	2	1	1	3	2	2	2	1	1	1	1	1	1

* Indicates significance at $p < 0.10$.

Cat indicates category with DB = data breach (lost records), and SB = security breach. Sample size indicates the number of breaches (unique companies). If a propensity matched sample was used, PM is indicated in the Matched Sample column. Div stand for dividends. Inv stands for investment or capital expenditures. For the performance measures, * indicates significance at $p < 0.10$, ns indicates not significant, "D" indicates a decrease in the performance with significance of at least $p < 0.05$, "I" indicates an increase in the performance measure. Avail stands for Availability breach. IT Int stands for IT intensity. Lg stands for large company. WD stands for website defacement. DC stands for data corruption.

[a] Akey et al. (2018) find EBITDA to decrease one year after a breach ($p < 0.10$), but not four years after the breach.

TABLE 13

Audit and Nonaudit Fee Impact

Authors and Year	Cat	Breach Sample Size	Time Period	Matched Sample	Findings
Li, No, and Boritz 2016	SB	140 Nonfinancial Companies/ Events That Were Hacked	2005–2015		A significant positive relationship between increases in audit fees and hacking cyber incidents (not other incidents). Increases in audit fees are smaller for companies with prior cyber risk disclosure, implying that auditors price material cyber risk prior to the cyberattacks. In addition, companies with repeated cyber incidents or cyber incidents that involve intellectual property experience the larger increases in audit fees. Larger companies are breached more.
Chichernea, Holder, Petkevich, and Robin 2018	DB	43 Companies	2005–2015	Yes	Breached companies are younger, have higher growth and risk, and have longer tenure auditors (who presumably spend less time on the audit) who are paid more for nonaudit services, compared to control companies. Some evidence that audit fees are lower for breached companies. Audit fees moderate the relation between innovation attributes and subsequent data breaches.
Higgs et al. 2018	DB	203 Customer Breaches	2005–2014	Yes (PM)	Customer record breaches are associated with an 8 percent increase in fees. External breaches (e.g., hacks, portable data thefts, or server thefts) drive the results. The presence of board-level risk committees and more active audit committees may mitigate the audit fee increases.
Lawrence et al. 2018	SB	381 Firm-years	2005–2012	Yes (PM)	Audit fees are positively related to operational control risks (measured by data breaches).
Westland 2018	DB	213 Companies	2005–2015		Lower audit fees are associated with more breaches.
Yen et al. 2018	DB	248 Confidentiality Breaches for 164 Companies	2004–2013	Yes (PM)	Audit fees are 13.5 percent higher after a confidentiality security incident (and increase by 9.1 percent on average per breach), but are negatively moderated by audit firm characteristics, including Big 4, industry-specific expertise, and longer tenure.

Cat indicates category with DB = data breach (lost records), and SB = security breach. If a propensity matched sample was used, PM is indicated in the Matched Sample column.

TABLE 14

Sarbanes-Oxley Section 404 Material Weakness Reporting

Authors and Year	Cat	Breach Sample Size	Time Period	Matched Sample	Findings
Amir et al. 2018	SB	276 (156)	2010–2015		Companies with fewer (previous) MWs are more likely to disclose breaches.
Lawrence et al. 2018	SB	381 Firm-years	2005–2012	Yes (PM)	Operational control risks (measured by data breaches) are related to the future financial reporting control weaknesses ($p < 0.10$), restatements, SEC comment letters, and audit fees, even after controlling for current contemporaneous SOX 404 material weaknesses. Companies with high operational risk are 1.33 times more likely to have an accounting restatement and 1.39 times more likely to receive an SEC comment letter in the concurrent or following year. Companies with data breaches are 1.55 times more likely to report SOX 404 material weaknesses in the future. Audit fees are positively related to operational control risks. Findings suggest that SOX reporting may miss financial reporting problems or report them later rather than sooner.
Westland 2018	DB	213 Companies	2005–2015		SOX 404 adverse decisions on effectiveness of controls occurred in 100 percent of credit card data breaches, and 33 percent of insider breaches. SOX disclosure is poor at identifying control weaknesses from unintended disclosures, physical losses, hacking, malware, stationary devices, and unexplained disclosures. Hazard and occupancy models show SOX 404 more than three times as informative as SOX 302. Company size is not related to breaches.

Cat indicates category with DB = data breach (lost records); and SB = security breach. If a propensity matched sample was used, PM is indicated in the Matched Sample column. MW stands for material weakness. SOX stands for Sarbanes-Oxley Act.

APPENDIX B

Variable Definitions

General

Breach Firm = 1 if firm disclosed a breach, 0 otherwise.
Propensity-Matched Firm = 1 if firm matched to *Breach Firm* by propensity score based on industry, year, total assets, and return on assets, 0 otherwise.
Market Value-Matched Firm = 1 if firm matched to *Breach Firm* by year, industry, and market value (Compustat PRCC_F ∗ CSHO), 0 otherwise.
Post × *Breach Firm* = interaction term indicating relationships post-breach disclosure for *Breach Firm*.

Table 1 Variables

Market Value = market value (Compustat PRCC_F ∗ CSHO ($mm)), log transformed.
Assets = total assets (Compustat at ($mm)), log transformed.
ROA = (return on assets) earnings before extraordinary items (Compustat IB) divided by total assets (Compustat AT).
ROS = (return on sales) earnings before extraordinary items (Compustat IB) divided by total revenue (Compustat REVT).
Sales Growth = revenue in year t divided by revenue in year $t-1$, log transformed.
Forecast Error = analyst mean EPS forecast (I/B/E/S) for year $t+1$, scaled by price at the beginning of the year.

Audit Fees = log of audit fees (Audit Analytics).
Other Fees = miscellaneous nonaudit fees (Audit Analytics) divided by total fees (Audit Analytics).
ICMW = reported material weakness in internal control (Audit Analytics).
Future = values in year *t*+1 (following the data breach).

Table 3 Variables

Cumulative Daily Returns = sum of the log of daily returns (+1) over the designated return period.
Cumulative Excess Returns = sum of the log of daily returns less the equal-weighted market return (+1) over the designated return period.
Cumulative Abnormal Returns (CAR) = sum of the abnormal returns in the various event windows from Fama-French four-factor models for each firm over the estimation period [−120, −5], where the Fama-French and momentum factors are log transformed.
Standard Deviation of Returns = standard deviation of daily returns over the designated return period.
SD Prior Returns = standard deviation of daily returns over the estimation window [−120, −5] prior to the breach disclosure.
Prior Share Turnover = average firm daily volume divided by the number of shares outstanding, log transformed, over the estimation window prior to the breach disclosure.
Prior Market Value = average firm market value over the estimation window prior to the breach disclosure.
Prior Returns = average firm returns over the estimation window prior to the breach disclosure.
Prior Market Returns = average market return over the estimation window prior to the breach disclosure.

Table 4 Variables

Post = 1 if after the breach disclosure, 0 if before.
Total Revenue = total revenue (Compustat REVT ($mm)), log transformed.
Sales Growth = revenue in year *t* divided by revenue in year *t*–1, log transformed.
Merger-Acquisition = 1 if an acquisition affected earnings, 0 otherwise.
Capital Expenditures = capital expenditures (Compustat CAPX) divided by total assets.
Asset Turns = total assets (Compustat AT) divided by total revenue (Compustat REVT).
Leverage = long-term debt (Compustat DLTT) divided by total assets (Compustat AT).
Pscore = the propensity score from a probit model of the likelihood of a breach conditioned on industry, year, total assets, and return on assets.
Industry Sales Growth = average sales growth for the year and industry (Fama-French industry categories).
ROS = earnings before extraordinary items (Compustat IB) divided by total revenue (Compustat REVT).
Industry Performance = average change in *Sales Growth*/*ROS*/*ROA* for the year and industry (Fama-French industry categories).
Assets-to-Equity Ratio = total assets (Compustat AT) divided by common equity (Compustat CEQ).
Prior Performance = firm performance in year *t* for *Revenue, Sales Growth, ROS,* or *ROA* as appropriate.

Table 5 Variables

Audit Fees = log of audit fees (Audit Analytics).
Post = 1 if after the breach disclosure, 0 if before.
Other Fees = miscellaneous nonaudit fees (Audit Analytics) divided by total fees (Audit Analytics).
Market Value = market value (Compustat PRCC_F ∗ CSHO ($mm)), log transformed.
Pscore = the propensity score from a probit model of the likelihood of a breach conditioned on industry, year, total assets, and return on assets.
ICMW = reported material weakness in internal control (Audit Analytics).
Unqual Opinion = 1 if firm received an unqualified audit opinion, 0 otherwise.
Disc Ops = 1 if firm reported discontinued operations, 0 otherwise.
Xtra Items = 1 if firm reported extraordinary items (Compustat XI), 0 otherwise.
Shares Issued = 1 if firm issued common shares during the year, 0 otherwise.
Current Assets = working capital (current assets (Compustat ACT) minus current liabilities (Compustat LCT)) divided by total assets (Compustat AT).

Big4 = 1 if auditor was a Big 4 firm, 0 otherwise (Audit Analytics).
AR/Inventories = accounts receivable (Compustat ARC) plus total inventories (Compustat INVT) divided by total assets (Compustat AT).
Merger-Acquisition = 1 if an acquisition affected earnings, 0 otherwise.
Industry Sales Growth = average sales growth for the year and industry (Fama-French industry categories).
Book-to-Market Ratio = common equity (Compustat CEQ) divided by *Market Value* (Compustat PRCC_F ∗ CSHO).
Geo Segments = number of geographic segments (Compustat).

Table 6 Variables

ICMW = reported material weakness in internal control (Audit Analytics).
Market Value = market value (Compustat PRCC_F ∗ CSHO ($mm)), log transformed.
Pscore = the propensity score from a probit model of the likelihood of a breach conditioned on industry, year, total assets, and return on assets.
ROA = earnings before extraordinary items (Compustat IB) divided by total assets (Compustat AT).
Debt-to-Market Ratio = long-term debt (Compustat DLTT) divided by *Market Value* (Compustat PRCC_F ∗ CSHO).
Operating Cash Flow = operating cash flow (Compustat OANCF) divided by total assets (Compustat AT).
Loss = 1 if ROA $<$ 0, 0 otherwise.
Geo Segments = number of geographic segments (Compustat).
Analyst Following = I/B/E/S number of estimates.
Litigious Industry = 1 if the firm is in a litigious industry (SIC codes 2833–2836, 3570–3577, 3600–3674, 5200–5961, and 7370), 0 otherwise.
Expected Loss = 1 if the mean analyst EPS estimate (I/B/E/S) is less than 0, 0 otherwise.

All continuous variables except log transformed variables are winsorized 1 percent at each end of the distribution. Subscripts indicating firm and year are suppressed unless indicating future values, e.g., *it*+1. *Future* indicates values in year *t*+1.