THE ACCOUNTING REVIEW
Vol. 97, No. 2
March 2022
pp. 1–24

American Accounting Association
DOI: 10.2308/TAR-2019-1033

The Role of Peer Events in Corporate Governance: Evidence from Data Breaches

Musaib Ashraf
Michigan State University

ABSTRACT: Economic theory suggests that negative peer events can result in market-wide spillovers that help unaffected firms take real actions to enhance corporate governance. Motivated by the SEC's concern about cybersecurity, I study the role of peer events in corporate governance using the setting of data breaches. While controlling for firm-specific time-*varying* unobservable characteristics, I find that *peer* data breaches are associated with a reduction in future internal control material weaknesses for *non*-breached firms. The association is robust to a changes analysis and varies cross-sectionally with breach, firm, and board characteristics. Inferences remain consistent when studying IT-related material weaknesses only. Finally, non-breached firms are more likely to have a cybersecurity expert on the top management team after a peer breach. My findings have important implications for mandatory disclosure regulation in general and, in particular, suggest that regulators can help reduce market-wide exposure to cyber risk by facilitating disclosure of cyber incidents.

Data Availability: All data used in the study are publicly available.

JEL Classifications: G34; M15.

Keywords: peer events; corporate governance; internal controls; information technology; cybersecurity; information spillover; data breaches.

I. INTRODUCTION

Firms in the same industry share similar operational environments, and economic theory suggests that negative peer events can result in market-wide spillovers that induce unaffected firms to take real actions to enhance corporate governance (e.g., Leuz and Wysocki 2016)—or a "deterrent" role of peer events. Given that market-wide improvements in governance can be economically meaningful even when individual firm-level effects are small, understanding governance-related spillovers is of first-order importance. Studying these spillovers also has critical implications for mandatory disclosure regulation: if the disclosure of negative peer events has a deterrent effect for unaffected firms, then that provides important "economic justification of disclosure and reporting mandates" (Leuz and Wysocki 2016, 554). To that end, I examine the role of peer events in corporate governance using the setting of data breaches. Specifically, I study whether data breach incidents at peer firms induce non-breached firms (i.e., firms that do *not* experience a breach) to take real actions to enhance corporate governance, as proxied by internal control material weaknesses (U. Hoitash, R. Hoitash, and Bedard 2009).

I focus on the peer data breaches setting because, in addition to enabling me to study an important economic question, cybersecurity is a significant risk for firms. Cyber risks "pose grave threats to investors [and] our capital markets" (Securities and Exchange Commission [SEC] 2018a, 1) and are one of the top concerns for investors (PricewaterhouseCoopers [PwC] 2018). Despite the importance of cyber risk, the governance implications for the risk are not yet fully understood (Rajgopal and Srinivasan 2016) and there is some concern that, with the growing inevitability of being breached, firms may focus on managing the consequences after they are breached rather than proactively managing cyber risk (e.g., Sonnemaker 2019). Given that the exposure to cyber risk is correlated between firms in an industry (e.g., Ettredge and Richardson 2003; IBM

I thank Elaine G. Mauldin (editor), two anonymous referees, Ken Bills, Chris Hogan, John Jiang, Alon Kalay, Ranjani Krishnan, and Isabel Wang for their helpful feedback. I also thank my dissertation committee—Jayanthi Sunder (chair), Rick Mergenthaler, Paul Michas, and Shyam Sunder—for their invaluable guidance. I am grateful to the Eli Broad College of Business at Michigan State University and the School of Accountancy and Eller College of Management at The University of Arizona for funding that enabled this study. Any errors are my own.

Musaib Ashraf, Michigan State University, Broad College of Business, Department of Accounting and Information Systems, East Lansing, MI, USA.

Editor's note: Accepted by Elaine G. Mauldin, under the Senior Editorship of Mary E. Barth.

Submitted: November 2019
Accepted: February 2021
Published Online: April 2021

2017), peer data breaches are plausibly exogenous indicators of non-breached firms' exposure to cyber risk (conditional on empirically mitigating the "reflection problem" that is common to peer effect studies).[1] Consequently, the peer breaches setting offers a unique opportunity to evaluate whether firms do indeed take real actions to mitigate exposure to cyber risk.[2]

The peer data breaches setting is further attractive because I can observe both peer data breaches and internal control material weaknesses *within* a firm-year.[3] Within-firm-year variation enables me to analyze the effect of peer events on unaffected firms' corporate governance while controlling for time-*invariant* and time-*varying* unobservable characteristics that are *specific to the firm,* through the use of firm-year fixed effects (i.e., fixed effects for every firm-year rather than separate fixed effects for every firm and for every year) (Gormley and Matsa 2014). Although my identification strategy does not completely eliminate endogeneity concerns, it significantly mitigates them, especially concerns about the reflection problem.[4]

To analyze the impact of peer data breaches on the internal controls of non-breached firms, I use data from the Privacy Rights Clearinghouse (PRC). The PRC is a non-profit organization that has tracked data breaches since 2005. I use the PRC's data to calculate my test variable $PEER\_BREACH_{t-1}$ (a binary indicator for whether firm *i*'s industry peers exhibit a data breach in quarter $t-1$), and I restrict my sample exclusively to non-breached firms in order to study governance spillovers.

In my main analysis, I find that $PEER\_BREACH_{t-1}$ is significantly *negatively* associated with *MATERIAL_WEAKNESS* (a binary indicator for whether firm *i* exhibits an internal control material weakness in quarter *t*). The result is consistent in a levels analysis with firm-year fixed effects, as well as in a changes analysis. The result is also robust to restricting my test variable to breaches at industry leaders only (Brown, Tian, and Tucker 2018).

I reinforce my main finding with four cross-sectional tests. First, the effect is stronger (i.e., statistically more negative) when the peer breach is a stronger signal of cyber risk, as proxied by the breached firm's catastrophic stock price reaction to the breach and whether the peer breach is a "hack" by an outside party. Second, the effect is stronger when a non-breached firm has existing governance problems, as proxied by an existing material weakness or receiving a going concern opinion. Third, the effect is stronger for firms that possess complementary corporate governance mechanisms, as proxied by a more independent board and having an information security expert on the board. Finally, the external auditor does *not* appear to drive the effect.

Taken together, these results suggest that peer events play a crucial role in strengthening the corporate governance at unaffected firms. On average, a peer breach is associated with a 6.6 percent reduction in the incidence rate of material weaknesses for non-breached firms. The effect is economically stronger depending on breach, firm, and board characteristics: effect size ranges up to 40.9 percent in cross-sectional analyses.

One potential concern with the inferences drawn from my main analysis is whether internal controls have indeed improved or whether managers withhold the reporting of material weaknesses in fear of being targeted in a cyberattack. To address this concern, I employ a falsification test that reinforces my inferences. I also partition material weaknesses into IT-related and not-IT-related and find that the negative relation holds for *both* types of material weaknesses, albeit the latter is economically weaker.

Finally, to ensure that my findings are robust to different measures of cyber risk-related governance, I study the association between $PEER\_BREACH_{t-1}$ and *CYBER_EXPERT* (a binary indicator for whether firm *i* has a cybersecurity expert on the top management team in quarter *t*), an alternative measure of enhanced governance. I find that $PEER\_BREACH_{t-1}$ is significantly *positively* associated with *CYBER_EXPERT*. This result supports my inferences that non-breached firms enhance governance over cyber risk after a peer breach.

Overall, my study makes several important contributions. I provide empirical evidence that negative peer events generate information spillovers that help unaffected firms take real actions to enhance corporate governance. Given that modern capital markets depend on strong corporate governance (Armstrong, Guay, and Weber 2010), understanding the role of peer events in shaping market-wide governance is of critical importance (Leuz and Wysocki 2016). Yet, while extant literature has

[1] The reflection problem is a concern that an industry-driven factor (aside from cyber risk) may be simultaneously correlated with my test and dependent variables, even if the event itself is exogenous to the focal firm (Leary and Roberts 2014; Leuz and Wysocki 2016).

[2] For example, according to Walmart's Chief Information Officer, they "learned several big lessons from Target's massive 2013 data breach" and "began in-house testing of its networks following the Target attack" (Viebeck 2015). Similarly, in a conference call after Equifax's 2017 breach, TransUnion's CEO noted that "the moment we heard the [Equifax breach] news ... we immediately conducted a thorough global review of our systems" (SeekingAlpha 2017).

[3] I study internal controls that management must assess every *quarter* under Sarbanes-Oxley (SOX) 302 rather than an *annual* assessment of internal controls under SOX 404. While, by definition, SOX 302 is "disclosure controls and procedures" and SOX 404 is "internal controls over financial reporting," extant literature argues that in practice, the two types of internal controls are related, aside from timing differences and the fact that auditors must opine on the effectiveness of internal controls under SOX 404 (Doyle, Ge, and McVay 2007; Ashbaugh-Skaife, Collins, Kinney, and LaFond 2009; Costello and Wittenberg-Moerman 2011; Dhaliwal, Hogan, Trezevant, and Wilkins 2011).

[4] To be a threat to inferences, any correlated omitted variable (including ones at the industry level) would need to be firm-year-specific and simultaneously correlated with my dependent and test variables *within* each firm-year (Gormley and Matsa 2014), because firm-year fixed effects account for *between-firm-year* unobservable heterogeneity (which also naturally controls for between-firm, between-industry, between-industry-year, and between-year variation).

extensively studied capital markets implications of peer events (e.g., Gleason, Jenkins, and Johnson 2008), whether firms enhance corporate governance after a negative peer event (i.e., a deterrent effect) is an open question. In particular, peer events are diverse and complex, and spillover effects may vary greatly depending on the event. For example, while it may be relatively easy for a firm to increase risk factor disclosures in response to a peer's SEC comment letter (Brown et al. 2018), it is unclear whether firms make broad and costly changes to corporate governance, such as strengthening internal controls and enhancing the top management team, in response to negative peer events. In fact, Kedia, Koh, and Rajgopal (2015) suggest that firms *begin* earnings management after a peer firm discloses a restatement, contrary to the notion of a deterrent effect that leads to improvements in governance.[5]

My findings are further distinct from existing literature because the takeaways for stakeholders are vastly different when a deterrent effect arises through market mechanisms, such as public disclosure that a firm incurred a breach, compared to a deterrent effect that requires enforcement by a regulator, such as an SEC comment letter (Brown et al. 2018). Likewise, firms responding to an enforcement action at a peer does not imply that firms will also respond to other types of negative peer events. My evidence is particularly important considering that the collective magnitude of a market-wide improvement in governance can be economically meaningful.

Next, my analyses have implications for disclosure regulation. As my evidence suggests, disclosures of negative peer events drive beneficial market-wide governance externalities. The existence of these positive spillovers strengthens the economic justification for mandatory disclosure and facilitates a better calibration of the costs and benefits of disclosure regulation (Leuz and Wysocki 2016). If the social value of market-wide externalities outweighs private disclosure costs for affected firms, then the market is "better off" with regulation that mandates affected firms to make costly disclosures. My inferences are notably relevant in the cybersecurity setting, as regulators grapple with how best to mitigate the growing cyber risks faced by firms (e.g., SEC 2018a). My evidence suggests that one way regulators can help reduce market-wide exposure to cyber risk is by facilitating firms' disclosures of cyber incidents.

Finally, my findings expand our understanding of the corporate governance implications of cyber risk in general and peer data breaches in particular. Rajgopal and Srinivasan (2016) question whether boards take cyber risks seriously, and prior evidence is unclear (Lawrence, Minutti-Meza, and Vyas 2018; Richardson, Smith, and Watson 2019). Using peer breaches as a proxy of non-breached firms' exposure to cyber risk, my study suggests that boards *do* take cyber risk seriously and take steps to mitigate exposure to the risk (as proxied by enhanced internal controls and top management team). These findings also speak to the concern that firms may view data breaches as inevitable and opt to manage the consequences after being breached rather than take steps to proactively prevent breaches (e.g., Gordon, Loeb, Lucyshyn, and Zhou 2015; Sonnemaker 2019; Frolov 2019). Given that cyber incidents are a growing economy-wide risk, my study offers timely and relevant evidence that should be of interest to academics and non-academics alike.

II. INTERNAL CONTROLS, RELATED LITERATURE, AND HYPOTHESIS DEVELOPMENT

Internal Controls as Proxy of Corporate Governance

In this study, I focus on internal controls as my main proxy of corporate governance because, conceptually, material weaknesses are a strong signal of governance quality. Corporate governance is a set of mechanisms that "help align the actions and choices of managers with the interests of shareholders" (Armstrong et al. 2010, 181). This includes mechanisms that prevent the misuse of capital, as well as mechanisms that ensure timely and accurate financial reports, since accounting information is the primary means by which investors monitor the use of their capital (Sloan 2001; Beyer, Cohen, Lys, and Walther 2010). Within the just-discussed framework, material weaknesses are a strong indicator of governance quality because internal controls help not only prevent misappropriation of assets, but are also critical to generating the timely and accurate financial reports that investors depend on (Dechow, Ge, and Schrand 2010; Rice and Weber 2012). It should come as no surprise, then, that effective internal controls facilitate one of the primary goals of corporate governance: mitigating the agency problems that arise from separation of ownership and control (e.g., Hoitash et al. 2009; R. Hoitash, U. Hoitash, and Johnstone 2012; Cheng, Dhaliwal, and Zhang 2013).

[5] Kedia et al. (2015) posit that managers begin earnings management because managers perceive the expected costs of managing earnings to be low. Given that restatements are associated with information quality rather than impacting cashflows (e.g., Gleason et al. 2008), one plausible explanation why my inferences differ from the findings of Kedia et al. (2015) is the difference between a restatement and a data breach. Cybersecurity also impacts information risk (Ashraf, Michas, and Russomanno 2020), but data breaches can additionally have real negative impacts on a firm's cashflows (Kamiya et al. 2021). For example, Srinivasan, Paine, and Goyal (2019) report that Target incurred a 6.6 percent decrease in sales after its 2014 data breach. Thus, relative to a peer restatement, a peer breach provides firms with stronger, multifaceted incentives to enhance corporate governance and avoid experiencing a breach themselves.

Further, there is a strong conceptual link between cybersecurity and internal controls. Both cybersecurity and internal controls significantly rely on related information technology (IT) platforms (Lawrence et al. 2018; Richardson et al. 2019; Ashraf et al. 2020). Both cybersecurity and internal controls are also sensitive to "human vulnerabilities"—or the idea that failures in cybersecurity or internal controls may be a result of human error (Public Company Accounting Oversight Board [PCAOB] 2007; IBM 2014; SEC 2018b). The SEC (2018b, 2) supports the perspective that cybersecurity and internal controls are intertwined, noting that "having sufficient internal accounting controls plays an important role in an issuer's risk management approach to cyber-related threats" and counseling public firms to "consider cyber threats when implementing internal accounting controls" since investors rely on firms to address cyber threats with these controls (SEC 2018c, 1). Consistent with this notion, Deloitte (2015, 23) argues that "the pervasiveness of cyber issues increasingly affects financial information concerns and internal controls." Given the strong conceptual links between cybersecurity and internal controls and between internal controls and governance quality, using internal control material weaknesses as a proxy of corporate governance is appropriate for my setting.

Peer Effects Related Literature

Extant literature on peer effects in accounting and finance can generally be categorized into two groups: work that studies capital markets implications, and other work that studies real effects.[6] Focusing on the latter, real effects studies generally analyze either a "contagion" effect or a "deterrent" effect. A contagion effect is when a firm behaves similar to its peers. A deterrent effect is when a peer event generates information spillovers that induce unaffected firms to take steps that help the firms avoid, rather than copy, the actions of their peers.

Ample evidence supports the existence of contagion effects. For example, Chiu, Teoh, and Tian (2013) and Omer, Shelley, and Tice (2020) suggest that board interlocks serve as a conduit for the transmission of organizational practices among firms; Beatty, Liao, and Yu (2013) argue that firms make suboptimal investments when peers' earnings are overstated because a firm's investment policy is relative to its peers; Leary and Roberts (2014) show that corporate financial policy is set by firms in response to their peers' financial policies; and Kedia et al. (2015) provide evidence that the average firm *begins* earnings management after a peer firm announces a restatement.[7]

At the same time, extant evidence on deterrent effects is sparse in general, and whether negative peer events induce unaffected firms to make broad and costly improvements to corporate governance is an open question in particular. For example, Brown et al. (2018) find that firms enhance their risk factor disclosures when peer firms receive an SEC comment letter about risk factors. However, as noted previously, peer events are diverse and complex; spillover effects likely vary depending on the peer event and its source (e.g., regulatory inquiry or peer disclosure). While firms may take relatively low-cost actions (such as modifying risk factor disclosures) in response to SEC enforcement at a peer (Brown et al. 2018), it is unclear whether a non-enforcement negative peer event (such as a peer data breach) serves as a deterrent and encourages unaffected firms to make broad and costly improvements to corporate governance (such as strengthening internal controls).

Data Breaches Related Literature

Several prior and concurrent studies examine the impact of data breaches for breached firms, and there is some debate regarding how the market responds to breaches. On one hand, several studies find that data breaches have costly valuation implications for the average breached firm. For example, Acquisti, Friedman, and Telang (2006), Goel and Shawky (2009), Gatzlaff and McCullough (2010), A. Malhotra and C. Malhotra (2011), Gordon, Loeb, and Zhou (2011), and Amir, Levi, and Livne (2018) find significant negative abnormal returns for breached firms upon disclosure of a breach. Supporting these findings, the Ponemon Institute (2017a) reports an on-average 5 percent negative return for breached firms after a breach is disclosed. On the other hand, Richardson et al. (2019) argue that while data breaches can cause catastrophic losses in *extreme* cases, market reaction to the *average* breached firm is statistically negative, but economically limited.

Beyond firm value implications, the Ponemon Institute (2017b) finds that breached firms incur an average total cost of $225 per record leaked in a breach, such as the costs of forgone business opportunities and customer turnover. Similarly, Janakiraman, Lim, and Rishika (2018) examine customer-level transaction data at a multichannel retailer and find that after a data breach, impacted customers either completely stop shopping at the retailer or decrease the amount of business they do with the firm, leading to an average 33 percent decrease in purchases. Likewise, Cisco (2017) reports that 38 percent of breached

[6] One such capital markets study is Gleason et al. (2008), who find that non-restating firms experience a decrease in firm value when a peer discloses a restatement. Other extant literature that studies capital markets implications includes, but is not limited to, peer earnings announcements (Foster 1981; Baginski 1987; Ramnath 2002), peer shareholder litigation (Gande and Lewis 2009), and peer SEC enforcement actions (Silvers 2016).

[7] Kedia et al. (2015) provide some evidence that firms do not begin earnings management if the restating peer firm faces enforcement activity. However, Kedia et al. (2015) do not find evidence of a *decrease* in earnings management after a peer's restatement.

firms have lost 20 percent or more of their revenue. Further, other studies find that after a data breach, breached firms exhibit an increase in the cost of private debt, an increase in future restatements and SEC comment letters, an increase in audit fees, greater CEO turnover, and a decrease in sales growth (Sheneman 2017; Lawrence et al. 2018; Lending, Minnick, and Schorno 2018; Smith, Higgs, and Pinsker 2019; Kamiya, Kang, Kim, Milidonis, and Stulz 2021). While firm valuation implications are debatable, prior and concurrent studies collectively provide evidence of negative non-valuation consequences of data breaches for breached firms. In addition, there are valid conceptual reasons why breached firms can experience material negative consequences, as suggested by several studies, but Richardson et al. (2019) still find no material impact on firm value for the average breached firm.[8]

At the same time, there are conflicting findings in the literature regarding data breaches and internal controls, specifically. Lawrence et al. (2018) find that breached firms who experience a breach are more likely to have a future material weakness in internal controls. In contrast, Richardson et al. (2019) find no significant association in a similar setting. While extant literature focuses on the association of data breaches and internal controls for *breached* firms, I examine the real actions of *non*-breached firms after a *peer* data breach. Regardless of whether breaches have a material firm value impact for breached firms, on average, breaches can have catastrophic firm value consequences for breached firms in extreme cases (Richardson et al. 2019). Consequently, if peer data breaches shine a light on the *risk* that the non-breached firm may also experience a breach and the *risk* that this breach may turn out to be catastrophic—also known as tail risk (Ashraf and Sunder 2021)—then peer breaches should serve as deterrents and induce non-breached firms to reduce exposure to cyber risk after a peer breach. This notion is supported by Haislip, Kolev, Pinsker, and Steffen (2019), who provide evidence of negative abnormal returns for non-breached firms around the disclosure of a peer breach.

Hypothesis Development

Firms in the same industry share similar institutional and economic environments, and theory asserts that disclosure about one firm may contain information that is relevant to peers (e.g., Dye 1990; Admati and Pfleiderer 2000; Dye and Hughes 2018; Gao and Zhang 2019). In particular, negative peer events may lead to information spillovers that, conceptually, help unaffected firms take real actions to enhance governance (e.g., Leuz and Wysocki 2016). Related to my setting, I argue that peer data breaches are a signal of non-breached firms' exposure to *actual* or *perceived* cyber risk. Actual cyber risk is when a peer breach leads to an information spillover wherein the managers, boards, and shareholders of non-breached firms are now aware of new vulnerabilities that they did not know about previously. Perceived cyber risk is when a peer breach highlights—to a non-breached firm's board and shareholders—the cybersecurity risks that already exist at the non-breached firm, but which may have hitherto been ignored or withheld by management.

In both scenarios, boards and shareholders receive new information about non-breached firms' cyber risk. Either stakeholder can use this new information to mitigate non-breached firms' exposure to cyber risk *vis-à-vis* oversight over management (Leuz and Wysocki 2016). For example, equipped with new information about cyber risk, a board can ask more informed and pointed questions of management, force management to deploy the necessary resources to resolve outstanding concerns, critically evaluate management's remediation plans, and—if necessary—employ disciplining mechanisms when management is noncompliant (Ashraf et al. 2020).[9]

At the same time, conceptually, it is not necessary for boards and shareholders to actively engage with management about cyber risk after a peer breach in order to reduce exposure to cyber risk. This is because non-breached firms should have existing mechanisms in place that discipline management in the event of undesirable behavior, and a decrease in information asymmetry between management and the board or shareholders (*vis-à-vis* new information contained in peer breaches) helps empower those mechanisms. In turn, the increased ability of the board or shareholders to initiate disciplining mechanisms should incentivize management to choose to mitigate exposure to cyber risk—independent of any active oversight by the board or shareholders. For example, Shleifer and Vishny (1989) argue that information asymmetry is used by managers to entrench themselves and weaken the threat of replacement as a disciplining mechanism; any decrease in information asymmetry

[8] For example, it is possible that the market may *ex ante* price in the risk of being breached for breached firms and, therefore, the price reaction is limited when a breach does occur, except in extreme cases when the breach magnitude exceeds market expectations and a stronger price response ensues.

[9] Arguably, neither managers, boards, nor investors desire a breach. However, the uncertain payoff for managers from committing resources to cybersecurity gives rise to managers potentially underplaying cyber risk. Resources committed to cybersecurity tend to help firms avoid costs rather than generate revenue and, in general, managers prefer to make revenue-generating investments rather than cost-savings investments (Gordon 2007). The problem is exacerbated specifically for cybersecurity because the costs saved through stronger cybersecurity (e.g., preventing a breach) are generally unobservable (Gordon, Loeb, Lucyshyn, and Zhou 2018). Further, managers do not necessarily always bear the costs of poor cybersecurity because of the uncertain timing of breaches (i.e., a breach may not happen until after the current decisionmakers have left the firm). Consequently, self-interested managers—who must decide how to deploy the firm's finite resources—tend to commit inadequate resources to cybersecurity (e.g., U.S. Treasury Department 2013).

strengthens existing mechanisms, such as the threat of replacement, that can be deployed to discipline management if necessary.

Given the preceding arguments, I state my hypothesis in its alternative form:

H: Peer data breaches are positively associated with enhanced corporate governance at non-breached firms.

As noted previously, my proxy for enhanced corporate governance is internal control material weaknesses. Since material weaknesses are an inverse measure of corporate governance, my hypothesis predicts a *negative* relation between peer breaches and material weaknesses.

III. RESEARCH DESIGN, DATA, AND SAMPLE SELECTION

Research Design

I study my research question using the following linear probability model:

$$\begin{aligned} MATERIAL\_WEAKNESS_{it} = \sum \beta_k Firm\text{-}Year\ Fixed\ Effects + \beta_1 PEER\_BREACH_{it-1} + \beta_2 SIZE_{it} + \beta_3 SALES\_GROWTH_{it} \\ + \beta_4 INV_{it} + \beta_5 LOSS_{it} + \beta_6 Z\_SCORE_{it} + \beta_7 ANNOUNCE\_RESTATEMENT_{it} \\ + \beta_8 INST\_OWNERSHIP_{it} + \beta_9 FOREIGN_{it} + \beta_{10} ACQUISITION_{it} + \beta_{11} RESTRUCTURE_{it} \\ + \beta_{12} Q4_{it} + e_{it} \end{aligned} \tag{1}$$

where i indexes firm and t indexes quarters.[10] The main dependent variable in this study is *MATERIAL_WEAKNESS,* which equals 1 if firm i has a material weakness in SOX 302 internal controls in quarter t (0 otherwise). The independent variable of interest is $PEER\_BREACH_{t-1}$, which equals 1 if any of firm i's industry peers exhibit a data breach during firm i's quarter t–1 (0 otherwise).[11] A negative coefficient on $PEER\_BREACH_{t-1}$ would be consistent with non-breached firms taking real actions to improve corporate governance after a peer data breach.

To calculate my test variable, I identify industry peers based on the Hoberg-Phillips text-based network industry classifications (TNIC). TNIC is an industry classification system that categorizes firms as peers if they operate in a similar product space (Hoberg and Phillips 2010, 2016). The advantage of this industry classification over more traditional measures is twofold. First, non-breached firms can only react to peer data breaches if they know about the breaches. It is considerably more likely that a non-breached firm is knowledgeable about events at firms that it shares a product space with rather than by virtue of being in the same SIC. While being in the same SIC arguably is a proxy of being in the same product space, TNIC is a more direct measure of the construct. For example, Hoberg and Phillips (2016) provide evidence that TNIC is able to classify firms as peers that managers themselves consider to be actual rivals. Second, TNIC is a time-varying intransitive industry classification system, which reduces noise in my measure by better identifying competitors as a firm's product space evolves over time.[12]

Importantly, I incorporate firm-year fixed effects in Equation (1), which help mitigate endogeneity concerns by removing between-firm-year variation. Firm-year fixed effects particularly help address the reflection problem that is common to all peer effect studies. In short, firms self-select into their industries and industry peers share institutional and economic environments, which leads to the concern that any peer-based measure may proxy for an industry-driven omitted latent factor that is simultaneously correlated with my test and dependent variables (Manski 1993; Leary and Roberts 2014). By allowing me to compare within-firm-year variation, firm-year fixed effects strongly address concerns about self-selection, as well as concerns about correlated omitted time-*invariant* and time-*varying* firm characteristics (which, also, naturally controls for industry-level unobservable characteristics).

[10] I use a linear probability model rather than a logistic regression for two reasons. First, complex fixed effect structures can cause biased coefficients and standard errors in nonlinear models due to the incidental parameters problem (Greene 2004). Second, it can be difficult to interpret interactions in nonlinear models (Ai and Norton 2003). The main result is generally consistent in a conditional (fixed effects) logistic regression (untabulated).

[11] I lag *PEER_BREACH* because the benefits of oversight triggered by a peer data breach in quarter t may not manifest until the next quarter, given that firms require time to implement changes that improve internal controls. That, however, raises the concern of whether it is plausible for a non-breached firm to enhance internal controls in one quarter after a peer breach. Based on the Compustat universe during my sample period, of the firm-quarters that report an existence of a material weakness during quarter t–1, 21.3 percent remediate that weakness by quarter t (untabulated). This suggests that firms can effectively make internal control changes in one quarter and that it is plausible for a non-breached firm to do so, as well.

[12] Intransitive classification means that firms are not peers by association. For example, under SIC (a transitive classification), if firm A and firm B are peers to firm C, then A and B are also peers. Under TNIC, it is possible for both A and B to be peers of C and for A and B to not be peers to each other. A byproduct of intransitivity is that every firm potentially has a unique set of peers and, thus, there are no distinct industry groups, such as the ones with traditional industry classifications.

TABLE 1

Data Breach Incidents and Sample Selection

Panel A: Data Breach Incidents

	n
Total data breach incidents from 2005 to 2017 (Privacy Rights Clearinghouse)	7,841
Less: Government, not for profit, and education (private schools and universities) organizations	(1,681)
Less: Observations not on Compustat (e.g., private firms)	(4,876)
Final sample of data breach incidents	1,284
Types of data breach incidents in final sample	
Data breaches caused by a hack by outside party	349
Data breaches caused by an insider (e.g., employee)	412
Data breaches caused by loss or theft of physical device	443
Other types of data breaches	80

Panel B: Sample Selection

Main Internal Controls Sample	**n**
Firm-quarter observations from 2005 to 2017 with non-missing CIKs (Compustat)	438,314
Less: Observations of firms that exhibit one or more breaches at any point in the sample	(26,249)
Less: Missing data on SOX 302 internal control material weaknesses or observations that do not possess at least one peer (Audit Analytics; TNIC)	(191,444)
Less: Missing data to calculate required control variables (Compustat or Audit Analytics)	(68,405)
Final main internal controls sample of firm-quarter observations	152,216
Total number of firms in main internal controls sample	5,567

While firm-year fixed effects go a long way in addressing the reflection problem, there remains the possibility that $PEER\_BREACH_{t-1}$ is correlated with industry-driven within-firm-year characteristics of the firm, and these characteristics, rather than peer data breaches, account for my treatment effect. To mitigate this concern, I control for a vector of firm-quarter characteristics that extant studies have shown to be correlated with the effectiveness of a firm's internal controls. Following Ashbaugh-Skaife, Collins, and Kinney (2007) and Doyle, Ge, and McVay (2007), I control for the following variables in my regression model: *SIZE, SALES_GROWTH, INV, LOSS, Z_SCORE, ANNOUNCE_RESTATEMENT, INST_OWNERSHIP, FOREIGN, ACQUISITION,* and *RESTRUCTURE*. I also control for *Q4,* an indicator variable that equals 1 if quarter *t* is the fourth quarter for firm *i*'s fiscal year, because auditors perform an audit of internal controls at the end of the fiscal year. All of these firm-quarter variables are defined in detail in Appendix A.

Data and Sample Selection

Table 1, Panel A presents my sample of data breach incidents. I collect data breach incidents from the Privacy Rights Clearinghouse (PRC), which has tracked publicly known data breaches since 2005. PRC's database includes data breaches "reported through either government agencies or verifiable media sources" (Privacy Rights Clearinghouse 2017), and PRC focuses on breaches that result in leakage of people's personal information, most often customer records. For every data breach observation, PRC provides the name of the breached firm and the date the breach is first publicly known, which I use to construct my sample of data breaches that occur at public firms.

I begin with 7,841 data breach incidents available on PRC between January 2005 and December 2017. I exclude 1,681 incidents where the breached firm is a government, not-for-profit organization, or private school or university. Next, I manually match data breach incidents to firm-quarter observations on Compustat, which leads to the deletion of 4,876 data breach incidents that occurred at private firms (or firms not on Compustat) and results in a final sample of 1,284 data breaches that occurred at public U.S. breached firms between 2005 and 2017. Of these breaches, 349 are caused by a hack, 412 are caused by an insider (e.g., employee), 443 are caused by loss of physical device, and 80 are in none of these categories. I use the 1,284 observations to calculate my test variable $PEER\_BREACH_{t-1}$ for non-breached firms.

TABLE 2

Descriptive Statistics

Panel A: Descriptive Statistics for Internal Controls Sample (n = 152,216)

Variable	Mean	Std. Dev.	25%	Median	75%
Test Variables					
PEER_BREACH$_{t-1}$ (binary)	0.27	0.44	0.00	0.00	1.00
No. of Peer Breaches$_{t-1}$	0.55	1.23	0.00	0.00	1.00
PEER_BREACH_LEADER$_{t-1}$ (binary)	0.01	0.10	0.00	0.00	0.00
Dependent Variable					
MATERIAL_WEAKNESS (binary)	0.07	0.26	0.00	0.00	0.00
Control Variables					
ACQUISITION (binary)	0.15	0.36	0.00	0.00	0.00
ANNOUNCE_RESTATEMENT (binary)	0.01	0.10	0.00	0.00	0.00
FOREIGN (binary)	0.22	0.41	0.00	0.00	0.00
INST_OWNERSHIP	0.55	0.34	0.23	0.59	0.85
INV	0.11	0.13	0.00	0.07	0.17
LOSS (binary)	0.46	0.50	0.00	0.00	1.00
Q4 (binary)	0.22	0.42	0.00	0.00	0.00
RESTRUCTURE (binary)	0.25	0.43	0.00	0.00	0.00
SALES_GROWTH	0.07	0.43	−0.06	0.02	0.11
SIZE ($millions)	2,245.60	5,646.56	94.28	387.54	1,554.16
Z_SCORE	0.56	5.46	0.32	0.99	1.76

Panel B: Other Descriptive Statistics

	Mean	Std. Dev.	Min.	Median	Max.
No. of Data Breach Incidents Per Quarter	22.48	11.92	1.00	24.00	42.00
No. of Non-Breached Peer Firms Per Data Breach Incident	68.57	75.24	1.00	39.00	304.00

Table 2 presents descriptive statistics for the internal controls sample. Continuous variables are winsorized at the 1 and 99 percentiles. *SIZE* is logged in subsequent multivariate analyses.
All variables are defined in Appendix A.

Table 1, Panel B presents my sample selection for subsequent multivariate regression analyses. I begin with 438,314 firm-quarter observations in Compustat with non-missing CIKs and eliminate 26,249 observations that belong to firms that exhibit a data breach at any point in my sample (i.e., I restrict my analysis exclusively to non-breached firms).[13] I also exclude 191,444 firm-quarters with missing data on SOX 302 internal control material weaknesses or that do not possess at least one peer per TNIC. Finally, I delete 68,405 observations with missing data to calculate required control variables, resulting in a final sample of 152,216 non-breached firm-quarter observations.

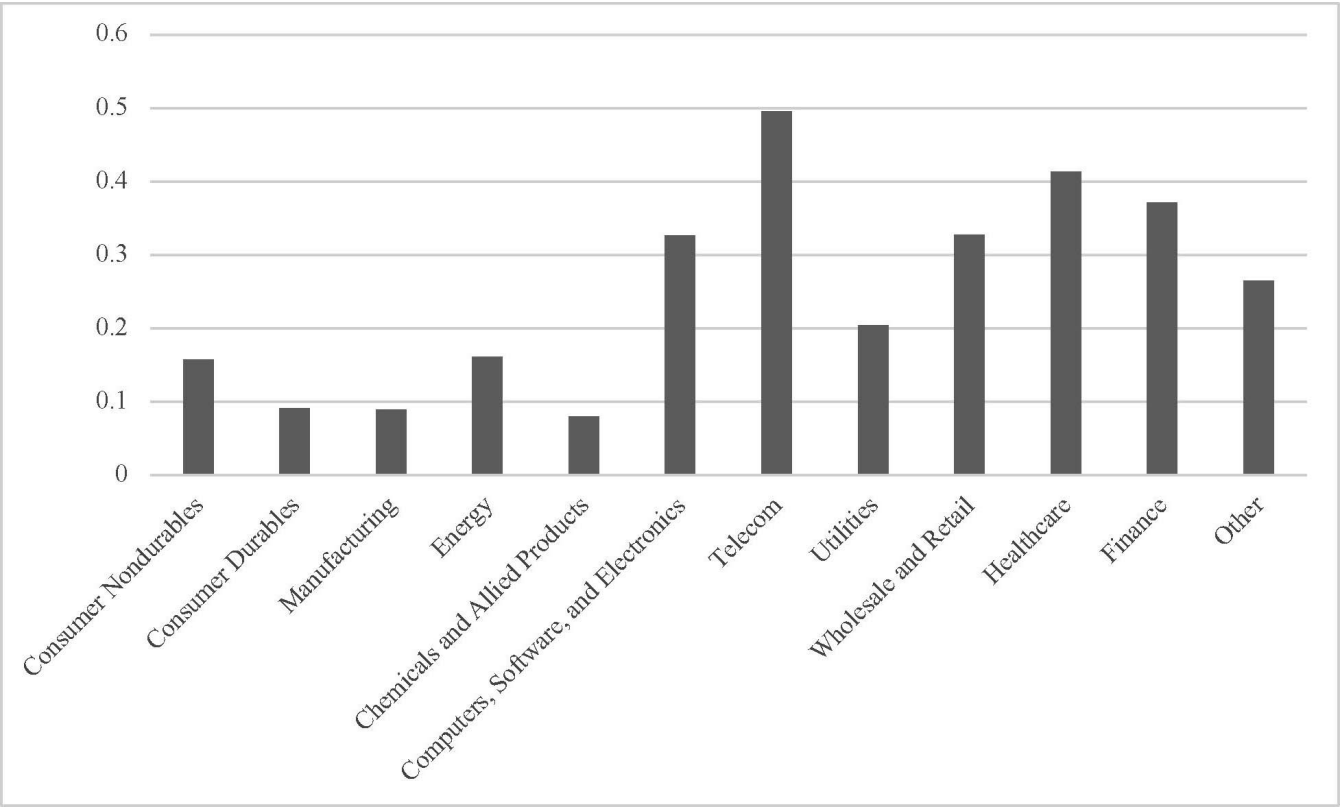
IV. RESULTS

Descriptive Statistics and Pearson Correlations

Table 2, Panels A and B present the descriptive statistics for my internal controls sample. Twenty-seven percent of observations exhibit a peer data breach in the prior quarter, while 7 percent of observations in my sample exhibit an internal control material weakness, which is consistent with extant literature (e.g., Ashraf et al. 2020). All other control variables are also generally consistent with extant literature (e.g., Ashbaugh-Skaife et al. 2007; Doyle et al. 2007; Ashraf et al. 2020).

[13] Throughout this study, my sample is restricted to firm-quarter observations with fiscal quarter-ends between June 30, 2005 and December 31, 2017 (inclusive). I begin on June 30, 2005 because I calculate my test variable *PEER_BREACH*$_{t-1}$ over a non-breached firm's full fiscal quarter *t*−1 and PRC began tracking data breaches in January 2005. I end on December 31, 2017 because that is the latest date for which TNIC data are available.

FIGURE 1
***PEER_BREACH*$_{t-1}$ by Fama-French 12 Industries**



Further, in my sample of data breach incidents, there is an average (median) of 22 (24) breach incidents per quarter and an average (median) of 69 (39) non-breached peers per breach incident.

I plot my test variable *PEER_BREACH*$_{t-1}$ by industry in Figure 1.[14] Consistent with IBM (2017), *PEER_BREACH*$_{t-1}$ is above the sample mean for technology, telecom, wholesale and retail, healthcare, and finance firms. Importantly, the use of firm-year fixed effects in my analyses mitigates any impact that industry-level characteristics may have on my inferences.

One concern with my main test variable *PEER_BREACH*$_{t-1}$ is that non-breached firms may not be knowledgeable about breaches at *all* of their peers. Using TNIC as my industry classification is intended to mitigate this concern because, as already discussed, firms are more likely to be knowledgeable of an event if it occurs at a peer with whom a firm shares a product market. Following Brown et al. (2018), I further mitigate this concern with a supplementary test variable that focuses on peer breaches that occur at industry leaders. *PEER_BREACH_LEADER*$_{t-1}$ is calculated the same as *PEER_BREACH*$_{t-1}$ except it equals 1 only when there is a breach at a peer industry leader, where an industry leader is a firm that has 20 percent or more of the industry's total yearly sales (Brown et al. 2018). One percent of observations in my sample have a peer industry leader that exhibits a breach in quarter $t-1$.[15]

Table 3 presents the Pearson correlations for my internal controls sample. *PEER_BREACH*$_{t-1}$ is significantly negatively (p-value $\leq$ 0.01) correlated with *MATERIAL_WEAKNESS*. This is univariate evidence consistent with the notion that peer

[14] As noted previously, TNIC is an intransitive industry classification scheme that has no distinct industry groups. Thus, for descriptive purposes, in Figure 1, *PEER_BREACH*$_{t-1}$ is plotted by the focal non-breached observation's Fama-French 12 group.

[15] 12.4 percent of my sample possesses two peers who are industry leaders, 21.0 percent of my sample possesses one peer who is an industry leader, and the remaining 66.6 percent of the sample do not possess any peer who is an industry leader (untabulated). For these latter observations, *PEER_BREACH_LEADER*$_{t-1}$ always equals 0 since an industry leader cannot be breached if there is no industry leader. If I restrict my sample to the observations that do possess an industry leader, the mean of *PEER_BREACH_LEADER*$_{t-1}$ is 0.03 and subsequent main results are consistent (untabulated). Results are also consistent if, for non-breached firms that possess more than one peer who is an industry leader, I restrict the leader to being the one with the largest sales (untabulated).

TABLE 3

Pearson Correlations for Internal Controls Sample

		(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
(1)	*PEER_BREACH*$_{t-1}$												
(2)	*MATERIAL_WEAKNESS*	**−0.01**											
(3)	*ACQUISITION*	**0.11**	**0.00**										
(4)	*ANNOUNCE_RESTATEMENT*	**−0.01**	**0.18**	**−0.02**									
(5)	*FOREIGN*	**0.01**	**0.03**	**0.11**	0.00								
(6)	*INST_OWNERSHIP*	**0.08**	**−0.10**	**0.16**	**−0.02**	**0.09**							
(7)	*INV*	**−0.14**	**0.01**	**−0.07**	0.00	**0.02**	**−0.03**						
(8)	*LOSS*	**0.01**	**0.10**	**−0.08**	**0.02**	**−0.05**	**−0.41**	**−0.02**					
(9)	*Q4*	0.00	**−0.01**	**−0.05**	**0.04**	**−0.03**	**0.01**	0.00	**0.01**				
(10)	*RESTRUCTURE*	0.00	**0.01**	**0.17**	0.00	**0.15**	**0.20**	**0.01**	**−0.04**	**−0.07**			
(11)	*SALES_GROWTH*	**0.01**	**0.01**	0.00	0.00	**−0.02**	**−0.05**	**−0.04**	**−0.02**	**−0.08**	**−0.04**		
(12)	*SIZE*	**0.09**	**−0.12**	**0.21**	**−0.03**	**0.11**	**0.64**	**−0.15**	**−0.54**	**0.02**	**0.18**	**−0.03**	
(13)	*Z_SCORE*	**−0.03**	**−0.05**	**0.03**	**−0.01**	**0.01**	**0.16**	**0.07**	**−0.17**	**0.01**	**−0.03**	**−0.03**	**0.16**

Table 3 presents Pearson correlations for the internal controls sample. Bold values indicate significance at the 0.10 level or lower.

events assist unaffected firms to improve corporate governance. I explore the relation between peer breaches and internal controls further in subsequent multivariate analyses.

Main Internal Control Analyses

I present the results of my main analysis in Panel A of Table 4. Across the first three columns of Panel A, the coefficient on *PEER_BREACH*$_{t-1}$ is negative and significant (p-values $\leq$ 0.01). Based on Column (3), the economic significance of experiencing a peer data breach is a reduction in the incidence rate of material weaknesses by 6.6 percent (relative to the sample mean). The coefficient on *PEER_BREACH_LEADER*$_{t-1}$ in Column (4) is also significantly negative (p-value $\leq$ 0.05), and the economic significance of a peer industry leader being breached is relatively larger than a breach at any peer firm: a 12.6 decrease in material weaknesses, relative to the sample mean. Results are consistent when, instead of firm-year fixed effects, I conduct a changes analysis in Panel B (p-values $\leq$ 0.05 or lower). Overall, the results of Table 4 suggest that peer events have positive governance externalities for unaffected firms.

Cross-Sectional Internal Control Analyses

I reinforce my inferences with four cross-sectional analyses. The theory of why a peer event may impact the corporate governance of unaffected firms is based on the notion of information transfers between peers (Leuz and Wysocki 2016)—or the idea that a peer event provides unaffected firms with new information that can be used to help mitigate governance problems. Consequently, I first study if my main effect is stronger when the peer breach is a stronger signal of cyber risk (i.e., has greater information spillovers). I proxy for this construct with the variables *PEER_BREACH_CATASTROPHIC*$_{t-1}$ and *PEER_BREACH_HACKED*$_{t-1}$.

PEER_BREACH_CATASTROPHIC$_{t-1}$ is a binary indicator that loads as a 1 when any of firm *i*'s industry peers exhibit a catastrophic data breach during firm *i*'s quarter *t*−1, where a catastrophic breach is when the breached firm experiences a 10 percent or larger negative cumulative abnormal return in the [−1, 1] window around breach disclosure date. This variable is based on the argument that when the breached firm experiences a catastrophic negative impact on firm value, then that breach is a stronger signal of a vulnerability that non-breached firms may also be exposed to.

PEER_BREACH_HACKED$_{t-1}$ is a binary indicator that loads as a 1 when any of firm *i*'s industry peers exhibit a data breach during firm *i*'s quarter *t*−1 that is a result of a hack by an outside party. Because operating and institutional environments (such as policies, procedures, information systems, network of customers and supplies, etc.) are similar among peer firms, conceptually, all types of peer breaches contain some information about vulnerabilities that non-breached firms may also be exposed to. However, relative to vulnerabilities that require physical or insider access in order to be exploited, remote outsiders can just as easily target a vulnerability at a non-breached firm as they did at the breached firm. Thus, the risk of being breached should be relatively higher for non-breached firms when the peer breach is a hacking event relative to other types of peer breaches.

TABLE 4

The Effect of Peer Data Breaches on Non-Breached Firms' Internal Controls

Panel A: Levels Analysis

		Dependent Variable: *MATERIAL_WEAKNESS*			
Independent Variables	**Pr.**	**No Controls or Fixed Effects (1)**	**No Controls (2)**	**Full Model (3)**	**Peer Industry Leader Breaches Only (4)**
Test Variables					
$PEER\_BREACH_{t-1}$	−	−0.0107***	−0.0032***	−0.0046***	
[t-stat.]		[−5.11]	[−2.89]	[−3.39]	
(p-value)		(≤0.010)	(≤0.010)	(≤0.010)	
$PEER\_BREACH\_LEADER_{t-1}$	−				−0.0088**
[t-stat.]					[−1.87]
(p-value)					(0.031)
Control Variables					
SIZE	−			−0.0030	−0.0031*
SALES_GROWTH	+			0.0000	0.0000
INV	+			−0.0069	−0.0069
LOSS	+			0.0055***	0.0055***
Z_SCORE	−			−0.0004**	−0.0004**
ANNOUNCE_RESTATEMENT	+			0.1450***	0.1451***
INST_OWNERSHIP	−			0.0031	0.0031
FOREIGN	+			0.0049**	0.0049**
ACQUISITION	+			0.0059**	0.0059**
RESTRUCTURE	+			0.0062**	0.0062**
Q4	−			−0.0094***	−0.0094***
Firm-Year Fixed Effects		No	Yes	Yes	Yes
n		220,621	220,621	152,216	152,216
Adjusted R^2		0.04%	60.18%	61.85%	61.85%

(continued on next page)

The results of both analyses are presented in Table 5. Consistent with expectations, the coefficient on the interactions in both columns is significantly negative and the "total effect" is, as well (p-values $\leq$ 0.10 or lower).[16] Importantly, the economic impact of a peer breach being catastrophic or being a hack is larger than the on-average effect in Table 4—a 15.4 and 10.7 percent decrease, respectively, in the incidence of a material weakness relative to the sample mean.

As my second cross-sectional analysis, I study the incremental effect of peer breaches for non-breached firms that have existing governance problems, which I proxy for with $MATERIAL\_WEAKNESS_{t-1}$ and $GOING\_CONCERN_{t-1}$ (binary indicator that equals 1 if firm *i*'s audit report for quarter *t*−1's fiscal year indicates a going concern opinion).[17] The intuition behind this analysis is noted in Section II. If management has hitherto downplayed existing problems at the firm, then the new information that peer breaches provide the board and shareholders should enable either stakeholder to better question or push back on management's assertions (e.g., significance of existing problems or remediation plans). Conceptually, both $MATERIAL\_WEAKNESS_{t-1}$ and $GOING\_CONCERN_{t-1}$ proxy for existing problems and, therefore, peer breaches should have a stronger effect for these non-breached firms. The results of these analyses are presented in Table 6 and are consistent with

[16] I exclude the main effect of both $PEER\_BREACH\_CATASTROPHIC_{t-1}$ and $PEER\_BREACH\_HACKED_{t-1}$ because of collinearity; $PEER\_BREACH_{t-1}$ always equals 1 when these variables equal 1 and both these variables always equal 0 when $PEER\_BREACH_{t-1}$ equals 0. In other words, the main effects of these variables are the same as the interaction variables in Table 5.

[17] $GOING\_CONCERN_{t-1}$ is a signal of problems that exist during the quarter, even if the opinion itself is *ex post* and issued after the whole fiscal year has ended.

TABLE 4 (continued)

Panel B: Changes Analysis

		Dependent Variable: Δ*MATERIAL_WEAKNESS*			
Independent Variables	**Pr.**	**No Controls or Fixed Effects (1)**	**No Controls (2)**	**Full Model (3)**	**Peer Industry Leader Breaches Only (4)**
Test Variables					
Δ*PEER_BREACH*$_{t-1}$	−	−0.0018**	−0.0018**	−0.0028***	
[t-stat.]		[−2.05]	[−2.07]	[−2.62]	
(p-value)		(0.020)	(0.019)	(≤0.010)	
Δ*PEER_BREACH_LEADER*$_{t-1}$	−				−0.0089***
[t-stat.]					[−2.39]
(p-value)					(≤0.010)
Control Variables					
Δ*SIZE*	−			−0.0028*	−0.0028*
Δ*SALES_GROWTH*	+			−0.0006	−0.0006
Δ*INV*	+			−0.0307	−0.0306
Δ*LOSS*	+			0.0028**	0.0028**
Δ*Z_SCORE*	−			−0.0002	−0.0002
Δ*ANNOUNCE_RESTATEMENT*	+			−0.0049	−0.0049
Δ*INST_OWNERSHIP*	−			0.0032	0.0032
Δ*FOREIGN*	+			0.0020	0.0021
Δ*ACQUISITION*	+			0.0000	0.0000
Δ*RESTRUCTURE*	+			0.0043***	0.0043***
Δ*Q4*	−			−0.0073***	−0.0073***
Year Fixed Effects		No	Yes	Yes	Yes
n		215,267	215,267	147,763	147,763
Adjusted R^2		0.00%	0.17%	0.30%	0.30%

***, **, * Indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests if coefficient sign is consistent with the predicted direction, and two-tailed tests otherwise.
Table 4 presents the analysis of the effect of peer data breaches in quarter *t*−1 on internal control material weaknesses in quarter *t*. Panel A is a levels analysis. Panel B is a changes analysis. All models are linear probability models with robust standard errors clustered by firm.
All variables are defined in Appendix A.

expectations (p-values ≤ 0.05 or lower). The economic significance of a peer breach for observations with existing problems is a 40.9 and 35.3 percent reduction in material weaknesses (relative to sample mean), respectively.[18]

I next study whether my main effect varies for non-breached firms that possess complementary governance mechanisms, using two proxies: *BOARD_INDEPENDENCE*$_{t-1}$ (binary indicator that equals 1 if firm *i*'s number of independent directors scaled by total number of directors is in the top quartile in quarter *t*−1) and *BOARD_CYBER_EXPERT*$_{t-1}$ (a binary indicator for whether a director on firm *i*'s board in quarter *t*−1 has professional work experience as a Chief Information Officer, Chief Information Security Officer, or Chief Security Officer). The former is a proxy of board monitoring, as the literature provides evidence that independent directors tend to provide more oversight than non-independent directors (Armstrong et al. 2010). The latter is a proxy for the board's level of expertise related to cybersecurity—expertise that better enables the board to advise management. Both are proxies of complementary corporate governance mechanisms and, conceptually, new information that arises from a peer breach should be more effectively utilized by more independent boards and boards with more relevant expertise.

[18] Material weaknesses in quarter *t* can clearly be improved for firms that have material weaknesses in quarter *t*−1. However, it is important to note that internal controls in quarter *t* can also be improved for firms that do *not* have material weaknesses in quarter *t*−1, because of two reasons. First, firms are dynamic institutions that are constantly in flux, and every firm has an X percent chance that a new material weakness may arise during the normal course of business (whatever that X percent may be). My evidence suggests that this X percent is lower when *PEER_BREACH*$_{t-1} = 1$, arguably due to the already discussed governance externalities. Second, material weaknesses are the most extreme form of internal control problems (PCAOB 2007). It is possible—in fact, likely—that some firms have existing internal control deficiencies in quarter *t*−1 and these problems were not significant enough to report as a material weakness, but may precipitate into a material weakness in quarter *t* if corrective action is not taken. My evidence suggests that there is a lower likelihood of these less extreme forms of internal controls problems turning into more extreme material weaknesses when *PEER_BREACH*$_{t-1} = 1$.

TABLE 5

Is the Effect Stronger When the Peer Breach is a Stronger Signal of Cyber Risk?

		Dependent Variable: *MATERIAL_WEAKNESS*	
Independent Variables	**Pr.**	**(1)**	**(2)**
Test Variables			
$PEER\_BREACH_{t-1}$	−	−0.0043***	−0.0031**
[t-stat.]		[−3.12]	[−2.03]
(p-value)		(≤0.010)	(0.021)
$PEER\_BREACH_{t-1} * PEER\_BREACH\_CATASTROPHIC_{t-1}$	−	−0.0065*	
[t-stat.]		[−1.60]	
(p-value)		(0.055)	
$PEER\_BREACH_{t-1} * PEER\_BREACH\_HACKED_{t-1}$	−		−0.0044**
[t-stat.]			[−2.10]
(p-value)			(0.018)
Control Variables			
SIZE	−	−0.0031	−0.0031
SALES_GROWTH	+	0.0000	−0.0001
INV	+	−0.0072	−0.0070
LOSS	+	0.0055***	0.0055***
Z_SCORE	−	−0.0004**	−0.0004**
ANNOUNCE_RESTATEMENT	+	0.1450***	0.1450***
INST_OWNERSHIP	−	0.0031	0.0032
FOREIGN	+	0.0049**	0.0048**
ACQUISITION	+	0.0058**	0.0059**
RESTRUCTURE	+	0.0062**	0.0062**
Q4	−	−0.0095***	−0.0095***
Firm-Year Fixed Effects		Yes	Yes
n		152,216	152,216
Adjusted R^2		61.86%	61.86%
$PEER\_BREACH_{t-1} + PEER\_BREACH_{t-1} * PEER\_BREACH\_CATASTROPHIC_{t-1}$	−	−0.0108***	
[t-stat.]		[−2.66]	
(p-value)		(≤0.010)	
$PEER\_BREACH_{t-1} + PEER\_BREACH_{t-1} * PEER\_BREACH\_HACKED_{t-1}$	−		−0.0075***
[t-stat.]			[−3.93]
(p-value)			(≤0.010)

***, **, * Indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests if coefficient sign is consistent with the predicted direction, and two-tailed tests otherwise.

Table 5 presents cross-sectional variation in the analysis of the effect of peer data breaches in quarter *t*−1 on internal control material weaknesses in quarter *t*. All models are linear probability models with robust standard errors clustered by firm.

All variables are defined in Appendix A.

The results of these analyses are presented in Table 7. Consistent with expectations, the negative relation between *PEER_BREACH*$_{t-1}$ and *MATERIAL_WEAKNESS* is stronger when the board is more independent (p-value $\leq$ 0.05). Similarly, a non-breached firm whose board possesses a cyber expert exhibits a stronger improvement in internal controls relative to firms with boards that do not possess this expertise (p-value $\leq$ 0.10). The economic significance of a peer breach is an 11.0 percent and 16.0 percent decrease in material weaknesses (relative to the sample mean) for non-breached firms that possess either a more independent board or a cyber expert on the board, respectively.

For my final cross-sectional analysis, I study whether it is, in fact, the external auditor that drives my treatment effect. External auditors focus on auditing SOX 404 internal controls at the end of the year for accelerated filers; they do not audit SOX 302 controls (PCAOB 2007). However, auditors do perform quarterly reviews of financial statements (Krishnan and Zhang 2005). Thus, it is possible that auditors perceive a peer breach as an increase in risk for non-breached firms and, therefore, encourage the non-breached firms to address the risk. Further, given the inherent connection between SOX 302 and SOX 404 internal controls, it is possible that auditors may indirectly account for my treatment effect: non-breached firms who

TABLE 6

Is the Effect Stronger for Non-Breached Firms with Existing Governance Problems?

		Dependent Variable: *MATERIAL_WEAKNESS*	
Independent Variables	**Pr.**	**(1)**	**(2)**
Test Variables			
$PEER\_BREACH_{t-1}$	−	−0.0025**	−0.0037***
[t-stat.]		[−2.24]	[−2.69]
(p-value)		(0.013)	(≤0.010)
$PEER\_BREACH_{t-1} * MATERIAL\_WEAKNESS_{t-1}$	−	−0.0261**	
[t-stat.]		[−2.10]	
(p-value)		(0.018)	
$PEER\_BREACH_{t-1} * GOING\_CONCERN_{t-1}$	−		−0.0210***
[t-stat.]			[−2.35]
(p-value)			(≤0.010)
Control Variables			
$MATERIAL\_WEAKNESS_{t-1}$	+	0.0095	
$GOING\_CONCERN_{t-1}$	+		0.0352***
SIZE	−	−0.0028	−0.0019
SALES_GROWTH	+	−0.0001	0.0005
INV	+	−0.0095	−0.0179
LOSS	+	0.0055***	0.0047***
Z_SCORE	−	−0.0004**	−0.0003*
ANNOUNCE_RESTATEMENT	+	0.1427***	0.1499***
INST_OWNERSHIP	−	0.0040	0.0036
FOREIGN	+	0.0037*	0.0059**
ACQUISITION	+	0.0062**	0.0060**
RESTRUCTURE	+	0.0060**	0.0068**
Q4	−	−0.0093***	−0.0083***
Firm-Year Fixed Effects		Yes	Yes
n		150,818	144,017
Adjusted R^2		61.89%	61.70%
$PEER\_BREACH_{t-1} + PEER\_BREACH_{t-1} * MATERIAL\_WEAKNESS_{t-1}$	−	−0.0286***	
[t-stat.]		[−2.33]	
(p-value)		(≤0.010)	
$PEER\_BREACH_{t-1} + PEER\_BREACH_{t-1} * GOING\_CONCERN_{t-1}$	−		−0.0247***
[t-stat.]			[−2.79]
(p-value)			(≤0.010)

***, **, * Indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests if coefficient sign is consistent with the predicted direction, and two-tailed tests otherwise.

Table 6 presents cross-sectional variation in the analysis of the effect of peer data breaches in quarter *t*−1 on internal control material weaknesses in quarter *t*. All models are linear probability models with robust standard errors clustered by firm.

All variables are defined in Appendix A.

expect a SOX 404 audit at the end of the year may address the issue more strongly during the year to prevent any issues from cropping up during the SOX 404 audit. Consequently, I study whether my treatment effect is stronger for non-breached firms audited by industry expert auditors ($INDUSTRY\_EXPERT\_AUDITOR_{t-1}$, which is a binary indicator for whether firm *i*'s external auditor for quarter *t*−1's fiscal year is an industry expert) or non-breached firms that are accelerated filers ($ACCELERATED\_FILER_{t-1}$, which is a binary indicator for whether firm *i* is an accelerated filer for quarter *t*−1's fiscal year).[19]

[19] An auditor is deemed an industry expert if it has the highest market share in the industry in an MSA-year. Results are consistent if I alternatively define an auditor as an industry expert if it has 30 percent or more industry market share in an MSA-year (untabulated).

TABLE 7

Is the Effect Stronger When Non-Breached Firms Possess Complementary Corporate Governance Mechanisms?

		Dependent Variable: *MATERIAL_WEAKNESS*	
Independent Variables	**Pr.**	**(1)**	**(2)**
Test Variables			
$PEER\_BREACH_{t-1}$	−	−0.0024*	−0.0034***
[t-stat.]		[−1.43]	[−2.35]
(p-value)		(0.077)	(≤0.010)
$PEER\_BREACH_{t-1} * BOARD\_INDEPENDENCE_{t-1}$	−	−0.0053**	
[t-stat.]		[−1.92]	
(p-value)		(0.028)	
$PEER\_BREACH_{t-1} * BOARD\_CYBER\_EXPERT_{t-1}$	−		−0.0078*
[t-stat.]			[−1.48]
(p-value)			(0.069)
Control Variables			
$BOARD\_INDEPENDENCE_{t-1}$	−	0.0013	
$BOARD\_CYBER\_EXPERT_{t-1}$	?		0.0088
SIZE	−	−0.0024	−0.0024
SALES_GROWTH	+	−0.0004	−0.0004
INV	+	−0.0029	−0.0031
LOSS	+	0.0036**	0.0036**
Z_SCORE	−	−0.0004*	−0.0004*
ANNOUNCE_RESTATEMENT	+	0.1470***	0.1470***
INST_OWNERSHIP	−	−0.0018	−0.0018
FOREIGN	+	0.0073***	0.0073***
ACQUISITION	+	0.0049*	0.0049*
RESTRUCTURE	+	0.0078***	0.0079***
Q4	−	−0.0080***	−0.0079***
Firm-Year Fixed Effects		Yes	Yes
n		136,437	136,437
Adjusted R^2		60.23%	60.23%
$PEER\_BREACH_{t-1} + PEER\_BREACH_{t-1} * BOARD\_INDEPENDENCE_{t-1}$	−	−0.0077***	
[t-stat.]		[−3.43]	
(p-value)		(≤0.010)	
$PEER\_BREACH_{t-1} + PEER\_BREACH_{t-1} * BOARD\_CYBER\_EXPERT_{t-1}$	−		−0.0112**
[t-stat.]			[−2.22]
(p-value)			(0.013)

***, **, * Indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests if coefficient sign is consistent with the predicted direction, and two-tailed tests otherwise.

Table 7 presents cross-sectional variation in the analysis of the effect of peer data breaches in quarter $t-1$ on internal control material weaknesses in quarter t. All models are linear probability models with robust standard errors clustered by firm.

All variables are defined in Appendix A.

Beyond being considered by the literature to be higher-quality auditors (e.g., Reichelt and Wang 2010), industry-expert auditors are arguably better equipped than other auditors to assess the risk signal of a peer breach and, therefore, to encourage non-breached firms to address that risk. Further, accelerated filers are the firms that must obtain a SOX 404 audit at the end of the year. If the effect of peer breaches is really driven by the external auditor (directly or indirectly), then my treatment effect should be partially or fully subsumed by these variables. The results of these analyses are presented in Table 8, where the coefficient on the interaction term in both columns is insignificant (p-values = 0.42 and 0.55). These insignificant results

TABLE 8

Is the Effect Stronger When Non-Breached Firms are Audited by an Industry Expert Auditor or Must Obtain a SOX 404 Audit at the End of the Year?

		Dependent Variable: *MATERIAL_WEAKNESS*	
Independent Variables	**Pr.**	**(1)**	**(2)**
Test Variables			
$PEER\_BREACH_{t-1}$	−	−0.0053***	−0.0064**
[t-stat.]		[−2.53]	[−1.95]
(p-value)		(≤0.010)	(0.026)
$PEER\_BREACH_{t-1} * INDUSTRY\_EXPERT\_AUDITOR_{t-1}$	−	0.0022	
[t-stat.]		[0.80]	
(p-value)		(0.423)	
$PEER\_BREACH_{t-1} * ACCELERATED\_FILER_{t-1}$	−		0.0021
[t-stat.]			[0.59]
(p-value)			(0.553)
Control Variables			
$INDUSTRY\_EXPERT\_AUDITOR_{t-1}$	?	0.0098***	
$ACCELERATED\_FILER_{t-1}$	?		0.0045
SIZE	−	−0.0036*	−0.0027
SALES_GROWTH	+	−0.0005	−0.0001
INV	+	0.0050	−0.0327
LOSS	+	0.0051***	0.0043**
Z_SCORE	−	−0.0004**	−0.0003
ANNOUNCE_RESTATEMENT	+	0.1481***	0.1517***
INST_OWNERSHIP	−	0.0040	0.0004
FOREIGN	+	0.0056**	0.0059**
ACQUISITION	+	0.0051*	0.0045
RESTRUCTURE	+	0.0062**	0.0080***
Q4	−	−0.0094***	−0.0090***
Firm-Year Fixed Effects		Yes	Yes
n		145,109	142,319
Adjusted R^2		61.08%	61.65%
$PEER\_BREACH_{t-1} + PEER\_BREACH_{t-1} * INDUSTRY\_EXPERT\_AUDITOR_{t-1}$	−	−0.0031**	
[t-stat.]		[−1.76]	
(p-value)		(0.039)	
$PEER\_BREACH_{t-1} + PEER\_BREACH_{t-1} * ACCELERATED\_FILER_{t-1}$	−		−0.0043***
[t-stat.]			[−2.94]
(p-value)			(≤0.010)

***, **, * Indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests if coefficient sign is consistent with the predicted direction, and two-tailed tests otherwise.

Table 8 presents cross-sectional variation in the analysis of the effect of peer data breaches in quarter *t*−1 on internal control material weaknesses in quarter *t*. All models are linear probability models with robust standard errors clustered by firm.

All variables are defined in Appendix A.

suggest there is no evidence to support the notion that my treatment effect varies between these two characteristics. Thus, external auditors are unlikely to drive my treatment effect.[20]

[20] Inferences regarding the role of auditors remain consistent if I focus on Big 4 auditors or audit fees instead of accelerated files and industry specialists (untabulated).

TABLE 9

Falsification Test: Are Managers Improving Internal Controls or Underreporting Internal Control Material Weaknesses?

Independent Variables	Pr.	Dependent Variable: *MATERIAL_WEAKNESS* (1)
Test Variable		
PEER_BREACH$_{t-1}$	?	0.0010
[t-stat.]		[0.09]
(p-value)		(0.927)
Control Variables		
SIZE	?	−0.0255*
SALES_GROWTH	?	−0.0088
INV	?	−0.1200
LOSS	?	0.0253**
Z_SCORE	?	−0.0011
ANNOUNCE_RESTATEMENT	?	0.1851***
INST_OWNERSHIP	?	0.0998*
FOREIGN	?	0.0655**
ACQUISITION	?	0.0720***
RESTRUCTURE	?	0.0064
Q4	?	−0.0538***
Firm-Year Fixed Effects		Yes
n		8,195
Adjusted R^2		55.34%

***, **, * Indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests if coefficient sign is consistent with the predicted direction, and two-tailed tests otherwise.
Table 9 presents the analysis of the effect of peer data breaches in quarter $t-1$ on internal control material weaknesses in quarter t, restricted to a subsample of observations whose financial statements were subsequently restated (i.e., firm-quarters who likely possess internal control material weaknesses, but may not have reported them prior to restatement). The model is a linear probability model with robust standard errors clustered by firm.
All variables are defined in Appendix A.

Falsification Test and IT Material Weaknesses

Publicly observable internal control material weaknesses are a function of both the *presence* and the *reporting* of a material weakness. Consequently, one potential concern regarding my main analysis is the possibility that managers are not actually improving internal controls, but rather choosing not to publicly report material weaknesses. While this is unlikely, given that the CEO and CFO are personally liable for any misreporting in the post-SOX era (i.e., the cost-benefit trade-off for managers to withhold the reporting of a material weakness is in favor of reporting), it is possible—especially because disclosing a material weakness could actually make non-breached firms a target for malicious third parties.

To address this concern, I conduct a falsification analysis by studying the effect of *PEER_BREACH*$_{t-1}$ on *MATERIAL_WEAKNESS* in a subsample of observations that subsequently restate their financial statements. Because misstatements generally have an associated underlying failure in internal controls (e.g., Rice and Weber 2012), each observation in this sample likely possesses an internal control material weakness; however, not all of these observations necessarily report that weakness prior to restating their financial statements. If the negative relation between *PEER_BREACH*$_{t-1}$ and *MATERIAL_WEAKNESS* in my main analysis is really just managers withholding the disclosure of material weaknesses, then that relation should be negative and significant in this subsample, as well. However, as shown in Table 9, there is no significant association between *PEER_BREACH*$_{t-1}$ and *MATERIAL_WEAKNESS* in this analysis (p-value = 0.93), which supports the notion that firms are actually improving internal controls after a peer data breach rather than just not publicly reporting them.

I further probe my main inferences by bifurcating material weaknesses into IT-related material weaknesses and non-IT-related material weaknesses.[21] This analysis helps to pin down whether non-breached firms are improving IT and cybersecurity

[21] Following Ashraf et al. (2020), IT-related material weaknesses are the ones categorized by Audit Analytics as code 52 (information technology, software, access/security issues) or code 51 (segregation of duty issues) while non-IT-related material weaknesses are the ones that are not categorized as such.

TABLE 10

Information Technology and Non-Information Technology Internal Controls

Independent Variables	Pr.	Dependent Variable: *IT_MATERIAL_WEAKNESS* (1)	Dependent Variable: *NON_IT_MATERIAL_WEAKNESS* (2)
Test Variable			
PEER_BREACH$_{t-1}$	−/?	−0.0033***	−0.0013*
[t-stat.]		[−2.63]	[−1.81]
(p-value)		(≤0.010)	(0.071)
Control Variables			
SIZE	−	−0.0049**	0.0018
SALES_GROWTH	+	0.0003	−0.0004
INV	+	−0.0020	−0.0049
LOSS	+	0.0060***	−0.0005
Z_SCORE	−	−0.0004**	−0.0001
ANNOUNCE_RESTATEMENT	+	0.1120***	0.0330***
INST_OWNERSHIP	−	0.0020	0.0011
FOREIGN	+	0.0019	0.0029**
ACQUISITION	+	0.0051*	0.0008
RESTRUCTURE	+	0.0025	0.0037***
Q4	−	−0.0069***	−0.0026***
Firm-Year Fixed Effects		Yes	Yes
n		152,216	152,216
Adjusted R^2		64.04%	31.20%

***, **, * Indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests if coefficient sign is consistent with the predicted direction, and two-tailed tests otherwise.
Table 10 presents the analysis of the effect of peer data breaches in quarter *t*−1 on information technology and non-information technology internal control material weaknesses in quarter *t*. All models are linear probability models with robust standard errors clustered by firm.
All variables are defined in Appendix A.

only or if they are improving the control environment as a whole. If non-breached firms improve cybersecurity specifically after a peer breach, then that should manifest as an improvement in IT-related internal controls because the two share common IT platforms (e.g., Lawrence et al. 2018). If peer breaches shine a light on the internal control environment in general rather than just cybersecurity in particular, then that should manifest as an improvement in internal controls that are not directly related to IT or cybersecurity. For instance, the National Institute of Standards and Technology Cybersecurity Framework requires firms to obtain a deep understanding of their business, governance, and control environment in order to develop effective cyber protection strategies. A byproduct of this process is enhanced knowledge, and potential improvement, of a firm's overall internal control environment.

Conceptually, if peer breaches contain information about non-breached firms' exposure to cyber risk, then, at the very least, IT material weaknesses should be improved. In contrast, it remains an open question whether non-IT material weaknesses are improved, as well. Non-breached firms may focus only on improving cybersecurity, in which case there may not be a decrease in non-IT material weaknesses. Alternatively, if peer breaches draw non-breached firms' attention to the control environment as a whole, then there may be a reduction in non-IT material weaknesses, as well.

The results of this analysis are presented in Table 10.[22] Not surprisingly, there is a negative and significant relation between *PEER_BREACH*$_{t-1}$ and IT material weaknesses in Column (1) (p-value $\leq$ 0.01). Interestingly, there is also a negative and significant relation between *PEER_BREACH*$_{t-1}$ and non-IT material weaknesses in Column (2) (p-value $\leq$ 0.10). Altogether, this evidence supports the notion that peer breaches contain information spillovers that are relevant to non-breached firms' exposure to cyber risk, *and* the evidence supports the notion that peer breaches draw non-breached firms' attention to the whole control environment rather than just cybersecurity.

[22] The means of *IT_MATERIAL_WEAKNESS* and *NON_IT_MATERIAL_WEAKNESS* are 0.06 and 0.01, respectively (untabulated).

TABLE 11

The Effect of Peer Data Breaches on Non-Breached Firms' Top Management Team

Independent Variables	Pr.	Dependent Variable: *CYBER_EXPERT* (1)
Test Variable		
$PEER\_BREACH_{t-1}$	+	0.0017**
[t-stat.]		[2.06]
(p-value)		(0.020)
Control Variables		
SIZE	+	0.0024*
SALES_GROWTH	+	0.0001
LEVERAGE	+	−0.0055
ROA	+	0.0008
MTB	?	−0.0001*
INST_OWNERSHIP	+	0.0178***
FOREIGN	+	0.0058***
ACQUISITION	+	0.0073***
RESTRUCTURE	+	0.0045**
Firm-Year Fixed Effects		Yes
n		193,959
Adjusted R^2		94.83%

***, **, * Indicate significance at the 0.01, 0.05, and 0.10 levels, respectively, using one-tailed tests if coefficient sign is consistent with the predicted direction, and two-tailed tests otherwise.

Table 11 presents the analysis of the effect of peer data breaches in quarter $t-1$ on having a Chief Information Officer, Chief Information Security Officer, or Chief Security Officer a firm's top management team in quarter t. The model is a linear probability model with robust standard errors clustered by firm. All variables are defined in Appendix A.

Cyber Expertise on Top Management Team

The focus of this study is on material weaknesses as a proxy for corporate governance. While there are strong conceptual reasons why I choose to study material weaknesses (see discussion in Section II), there are also downsides to this proxy (see Dechow et al. 2010). Consequently, to ensure my inferences are robust to my research design choice, as my final analysis, I study the effect of peer breaches on a different proxy: having a cyber expert on the top management team, where *CYBER_EXPERT* equals 1 when firm *i* has a Chief Information Officer, Chief Information Security Officer, or Chief Security Officer on the top management team in quarter *t* (0 otherwise). The results of this analysis are presented in Table 11.[23] The positive and significant coefficient on $PEER\_BREACH_{t-1}$ (p-value ≤ 0.05) suggests that non-breached firms are more likely to have a cyber expert on the top management team after a peer breach, which is another indicator of enhanced oversight over cyber risk.

V. CONCLUSION

In this study, I examine the role of peer events in corporate governance, using peer data breaches and internal controls as my empirical setting. I find that peer data breaches are associated with a lower incidence rate of future internal control material weaknesses for non-breached firms, suggesting that peer events have market-wide spillovers that help enhance corporate governance at unaffected firms. The finding is consistent in a levels analysis with firm-year fixed effects and in a changes analysis; the effect varies cross-sectionally with breach, firm, and board characteristics, but not with auditor characteristics; and the effect is likely not attributable to managers withholding the public reporting of a material weakness. The evidence further suggests that peer data breaches are associated with an improvement in both information technology-related and unrelated internal controls, implying that information spillovers from peer events can have broad implications for corporate governance. Finally, my inferences are robust to using the presence of a cyber expert on the top management team as a proxy of governance instead of internal controls.

[23] While having or not having a cyber expert on the top management team is likely a sticky choice quarter-over-quarter, the firm-year fixed effects enable me to capture the effect of $PEER\_BREACH_{t-1}$ when there *is* within-firm-year variation of *CYBER_EXPERT* (Wooldridge 2002).

As a whole, my findings should be of interest to both academics and non-academics, including regulators, boards, and shareholders. Given that strong governance is critical to the functioning of modern capital markets, understanding the deterrent role peer events play in shaping market-wide corporate governance is of first-order importance. Likewise, identifying positive market-wide governance externalities of negative disclosures provides one economic justification for mandatory disclosure requirements (Leuz and Wysocki 2016).

Finally, my evidence suggests that firms do enhance corporate governance in response to cybersecurity concerns and boards do take cyber risks seriously, which has implications not only for regulators who are concerned about firms' ability to manage cyber risk (e.g., SEC 2018a), but also for shareholders who have strong incentives to mitigate exposure to this risk (e.g., PwC 2018). Importantly, my analysis speaks to the concern that firms may opt to just manage the consequences of a breach after the fact rather than proactively strengthen cybersecurity (e.g., Gordon et al. 2018). My findings are particularly relevant given that cybersecurity is a relatively new and growing risk faced by firms. As noted by the Depository Trust and Clearing Corporation (2018, 16), cyber risks "may have become the most important near-term threat to financial stability [of the economy]."

REFERENCES

Acquisti, A., A. Friedman, and R. Telang. 2006. *Is there a cost to privacy breaches? An event study*. *ICIS 2006 Proceedings*. Available at: https://aisel.aisnet.org/icis2006/94

Admati, A. R., and P. Pfleiderer. 2000. Forcing firms to talk: Financial disclosure regulation and externalities. *Review of Financial Studies* 13 (3): 479–519. https://doi.org/10.1093/rfs/13.3.479

Ai, C., and E. C. Norton. 2003. Interaction terms in logit and probit models. *Economics Letters* 80 (1): 123–129. https://doi.org/10.1016/S0165-1765(03)00032-6

Altman, E. 1983. *Corporate Financial Distress: A Complete Guide to Predicting, Avoiding, and Dealing with Bankruptcy*. New York, NY: Wiley.

Amir, E., S. Levi, and T. Livne. 2018. Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies* 23 (3): 1177–1206. https://doi.org/10.1007/s11142-018-9452-4

Armstrong, C. S., W. R. Guay, and J. P. Weber. 2010. The role of information and financial reporting in corporate governance and debt contracting. *Journal of Accounting and Economics* 50 (2–3): 179–234. https://doi.org/10.1016/j.jacceco.2010.10.001

Ashbaugh-Skaife, H., D. W. Collins, and W. R. Kinney. 2007. The discovery and reporting of internal control deficiencies prior to SOX-mandated audits. *Journal of Accounting and Economics* 44 (1–2): 166–192. https://doi.org/10.1016/j.jacceco.2006.10.001

Ashbaugh-Skaife, H., D. W. Collins, W. R. Kinney, 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

Ashraf, M., and J. Sunder. 2021. *Can shareholders benefit from consumer protection disclosure mandates? Evidence from data breach disclosure laws and the cost of equity*. Working paper, Michigan State University and The University of Arizona. Available at: http://dx.doi.org/10.2139/ssrn.3308551

Ashraf, M., P. N. Michas, and D. Russomanno. 2020. The impact of audit committee information technology expertise on the reliability and timeliness of financial reporting. *The Accounting Review* 95 (5): 23–56. https://doi.org/10.2308/accr-52622

Baginski, S. P. 1987. Intraindustry information transfers associated with management forecasts of earnings. *Journal of Accounting Research* 25 (2): 196. https://doi.org/10.2307/2491015

Beatty, A., S. Liao, and J. J. Yu. 2013. The spillover effect of fraudulent financial reporting on peer firms' investments. *Journal of Accounting and Economics* 55 (2–3): 183–205. https://doi.org/10.1016/j.jacceco.2013.01.003

Beyer, A., D. A. Cohen, T. Z. Lys, and B. R. Walther. 2010. The financial reporting environment: Review of the recent literature. *Journal of Accounting and Economics* 50 (2–3): 296–343. https://doi.org/10.1016/j.jacceco.2010.10.003

Brown, S. V., X. Tian, and J. W. U. Tucker. 2018. The spillover effect of SEC comment letters on qualitative corporate disclosure: Evidence from the risk factor disclosure. *Contemporary Accounting Research* 35 (2): 622–656. https://doi.org/10.1111/1911-3846.12414

Cheng, M., D. Dhaliwal, and Y. Zhang. 2013. Does investment efficiency improve after the disclosure of material weaknesses in internal control over financial reporting? *Journal of Accounting and Economics* 56 (1): 1–18. https://doi.org/10.1016/j.jacceco.2013.03.001

Chiu, P. C., S. H. Teoh, and F. Tian. 2013. Board interlocks and earnings management contagion. *The Accounting Review* 88 (3): 915–944. https://doi.org/10.2308/accr-50369

Cisco. 2017. *Annual cyber security report*. Available at: https://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf

Costello, A. M., and R. Wittenberg-Moerman. 2011. The impact of financial reporting quality on debt contracting: Evidence from internal control weakness reports. *Journal of Accounting Research* 49 (1): 97–136. https://doi.org/10.1111/j.1475-679X.2010.00388.x

Dechow, P., W. Ge, and C. Schrand. 2010. Understanding earnings quality: A review of the proxies, their determinants and their consequences. *Journal of Accounting and Economics* 50 (2–3): 344–401. https://doi.org/10.1016/j.jacceco.2010.09.001

Deloitte. 2015. *Audit committee resource guide*. Available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/center-for-corporate-governance/us-aers-audit-committee-resource-guide-2015-032615.pdf

Depository Trust and Clearing Corporation. 2018. *The next crisis will be different*. Available at: https://www.dtcc.com/~/media/Files/Downloads/WhitePapers/Systemic-Risk-White-Paper-962018.pdf

Dhaliwal, D., C. Hogan, R. Trezevant, and M. Wilkins. 2011. Internal control disclosures, monitoring, and the cost of debt. *The Accounting Review* 86 (4): 1131–1156. https://doi.org/10.2308/accr-10043

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

Dye, R. A. 1990. Mandatory versus voluntary disclosures: The cases of financial and real externalities. *The Accounting Review* 65 (1): 1–24.

Dye, R. A., and J. S. Hughes. 2018. Equilibrium voluntary disclosures, asset pricing, and information transfers. *Journal of Accounting and Economics* 66 (1): 1–24. https://doi.org/10.1016/j.jacceco.2017.11.003

Ettredge, M., 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

Foster, G. 1981. Intra-industry information transfers associated with earnings releases. *Journal of Accounting and Economics* 3 (3): 201–232. https://doi.org/10.1016/0165-4101(81)90003-3

Frolov, M. 2019. If security breaches are inevitable what do organisations do about it? *Computer Business Review*. Available at: https://techmonitor.ai/techonology/data/if-security-breaches-are-inevitable-what-do-organisations-do-about-it

Gande, A., and C. M. Lewis. 2009. Shareholder-initiated class action lawsuits: Shareholder wealth effects and industry spillovers. *Journal of Financial and Quantitative Analysis* 44 (4): 823–850. https://doi.org/10.1017/S0022109009990202

Gao, P., and G. Zhang. 2019. Accounting manipulation, peer pressure, and internal control. *The Accounting Review* 94 (1): 127–151. https://doi.org/10.2308/accr-52078

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

Gleason, C. A., N. T. Jenkins, and W. B. Johnson. 2008. The contagion effects of accounting restatements. *The Accounting Review* 83 (1): 83–110. https://doi.org/10.2308/accr.2008.83.1.83

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

Gordon, L. A. 2007. *Incentives for improving cybersecurity in the private sector: A cost-benefit perspective*. Testimony for the House Committee on Homeland Security's Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.549.7147&rep=rep1&type=pdf

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

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and L. Zhou. 2015. The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy* 34 (5): 509–519. https://doi.org/10.1016/j.jaccpubpol.2015.05.001

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and L. Zhou. 2018. Empirical evidence on the determinants of cybersecurity investments in private sector firms. *Journal of Information Security* 9 (02): 133–153. https://doi.org/10.4236/jis.2018.92010

Gormley, T. A., and D. A. Matsa. 2014. Common errors: How to (and not to) control for unobserved heterogeneity. *Review of Financial Studies* 27 (2): 617–661. https://doi.org/10.1093/rfs/hht047

Greene, W. 2004. The behaviour of the maximum likelihood estimator of limited dependent variable models in the presence of fixed effects. *Econometrics Journal* 7 (1): 98–119. https://doi.org/10.1111/j.1368-423X.2004.00123.x

Haislip, J., K. Kolev, R. Pinsker, and T. Steffen. 2019. *The economic cost of cybersecurity breaches: A broad-based analysis*. Working paper, Baruch College–CUNY, Florida Atlantic University, Texas Tech University, and Yale University. Available at: https://weis2017.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_13.pdf

Hoberg, G., and G. Phillips. 2010. Product market synergies and competition in mergers and acquisitions: A text-based analysis. *Review of Financial Studies* 23 (10): 3773–3811. https://doi.org/10.1093/rfs/hhq053

Hoberg, G., and G. Phillips. 2016. Text-based network industries and endogenous product differentiation. *Journal of Political Economy* 124 (5): 1423–1465. https://doi.org/10.1086/688176

Hoitash, R., U. Hoitash, and K. M. Johnstone. 2012. Internal control material weaknesses and CFO compensation. *Contemporary Accounting Research* 29 (3): 768–803. https://doi.org/10.1111/j.1911-3846.2011.01122.x

Hoitash, U., R. Hoitash, and J. C. Bedard. 2009. Corporate governance and internal control over financial reporting: A comparison of regulatory regimes. *The Accounting Review* 84 (3): 839–867. https://doi.org/10.2308/accr.2009.84.3.839

IBM. 2014. *IBM security services 2014 cyber security intelligence index*. Available at: https://omnipush.com/docs/IBM_Cyber_Security_Intelligence_20450.pdf

IBM. 2017. *IBM X-force threat intelligence index*. Available at: https://web.archive.org/web/20180910071036/https://public.dhe.ibm.com/common/ssi/ecm/wg/en/wgl03140usen/WGL03140USEN.PDF

Janakiraman, R., J. H. Lim, and R. Rishika. 2018. The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing* 82 (2): 85–105. https://doi.org/10.1509/jm.16.0124

Kamiya, S., J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz. 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics* 139 (3): 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kedia, S., K. Koh, and S. Rajgopal. 2015. Evidence on contagion in earnings management. *The Accounting Review* 90 (6): 2337–2373. https://doi.org/10.2308/accr-51062

Krishnan, J., and Y. Zhang. 2005. Auditor litigation risk and corporate disclosure of quarterly review report. *Auditing: A Journal of Practice & Theory* 24 (Supplement): 115–138. https://doi.org/10.2308/aud.2005.24.s-1.115

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

Leary, M. T., and M. R. Roberts. 2014. Do peer firms affect corporate financial policy? *Journal of Finance* 69 (1): 139–178. https://doi.org/10.1111/jofi.12094

Lending, C., K. Minnick, and P. J. Schorno. 2018. Corporate governance, social responsibility, and data breaches. *Financial Review* 53 (2): 413–455. https://doi.org/10.1111/fire.12160

Leuz, C., and P. D. Wysocki. 2016. The economics of disclosure and financial reporting regulation: Evidence and suggestions for future research. *Journal of Accounting Research* 54 (2): 525–622. https://doi.org/10.1111/1475-679X.12115

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

Manski, C. F. 1993. Identification of endogenous social effects: The reflection problem. *Review of Economic Studies* 60 (3): 531. https://doi.org/10.2307/2298123

Omer, T. C., M. K. Shelley, and F. M. Tice. 2020. Do director networks matter for financial reporting quality? Evidence from audit committee connectedness and restatements. *Management Science* 66 (8): 3361–3388. https://doi.org/10.1287/mnsc.2019.3331

Ponemon Institute. 2017a. *Cost of data breach study: United States*. Available at: https://web.archive.org/web/20171031044450/http://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf

Ponemon Institute. 2017b. *The impact of data breaches on reputation & share value*. Available at: https://www.centrify.com/media/4737054/ponemon_data_breach_impact_study.pdf

PricewaterhouseCoopers (PwC). 2018. *Global investor survey*. Available at: https://www.pwc.com/gx/en/ceo-survey/2018/deep-dives/pwc-global-investor-survey-2018.pdf

Privacy Rights Clearinghouse. 2017. *Chronology of data breaches: FAQ*. Available at: https://web.archive.org/web/20170617004210/https://www.privacyrights.org/chronology-data-breaches-faq

Public Company Accounting Oversight Board (PCAOB). 2007. *Auditing Standard No. 5: An audit of internal control over financial reporting that is integrated with an audit of financial statements. Release No. 2007-005A*. Available at: https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/rulemaking/docket_021/2007-06-12_release_no_2007-005a.pdf?sfvrsn=9685a498_0

Rajgopal, S., and S. Srinivasan. 2016. Why the market yawned when Yahoo was hacked. *Wall Street Journal*. Available at: https://www.wsj.com/articles/why-the-market-yawned-when-yahoo-was-hacked-1475537076

Ramnath, S. 2002. Investor and analyst reactions to earnings announcements of related firms: An empirical analysis. *Journal of Accounting Research* 40 (5): 1351–1376. https://doi.org/10.1111/1475-679X.t01-1-00057

Reichelt, K. J., and D. Wang. 2010. National and office-specific measures of auditor industry expertise and effects on audit quality. *Journal of Accounting Research* 48 (3): 647–686. https://doi.org/10.1111/j.1475-679X.2009.00363.x

Rice, S. C., and D. P. Weber. 2012. How effective is internal control reporting under SOX 404? Determinants of the (non-)disclosure of existing material weaknesses. *Journal of Accounting Research* 50 (3): 811–843. https://doi.org/10.1111/j.1475-679X.2011.00434.x

Richardson, V. J., R. E. Smith, and M. W. Watson. 2019. Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems* 33 (3): 227–265. https://doi.org/10.2308/isys-52379

Securities and Exchange Commission (SEC). 2018a. *Commission statement and guidance on public company cybersecurity disclosures*. Available at: https://federalregister.gov/d/2018-03858

Securities and Exchange Commission (SEC). 2018b. *Report of investigation pursuant to Section 21(a) of the Securities Exchange Act of 1934 regarding certain cyber-related frauds perpetrated against public companies and related internal accounting controls requirements*. Available at: https://www.sec.gov/litigation/investreport/34-84429.pdf

Securities and Exchange Commission (SEC). 2018c. *SEC investigative report: Public companies should consider cyber threats when implementing internal accounting controls*. Available at: https://www.sec.gov/news/press-release/2018-236

SeekingAlpha. 2017. *TransUnion's (TRU) CEO James Peck on Q3 2017 results—Earnings call transcript*. Available at: https://seekingalpha.com/article/4117600-transunions-tru-ceo-james-peck-on-q3-2017-results-earnings-call-transcript

Sheneman, A. G. 2017. *Cybersecurity risk and the cost of debt*. Working paper, The Ohio State University. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3406217

Shleifer, A., and R. W. Vishny. 1989. Management entrenchment: The case of manager-specific investments. *Journal of Financial Economics* 25 (1): 123–139. https://doi.org/10.1016/0304-405X(89)90099-8

Silvers, R. 2016. The valuation impact of SEC enforcement actions on nontarget foreign firms. *Journal of Accounting Research* 54 (1): 187–234. https://doi.org/10.1111/1475-679X.12098

Sloan, R. G. 2001. Financial accounting and corporate governance: A discussion. *Journal of Accounting and Economics* 32 (1–3): 335–347. https://doi.org/10.1016/S0165-4101(01)00039-8

Smith, T., J. Higgs, and R. Pinsker. 2019. Do auditors price breach risk in their audit fees? *Journal of Information Systems* 33 (2): 177–204. https://doi.org/10.2308/isys-52241

Sonnemaker, T. 2019. *Facing inevitable data breaches and new privacy laws, companies shift focus to response*. Available at: https://news.medill.northwestern.edu/chicago/facing-inevitable-data-breaches-and-new-privacy-laws-companies-shift-focus-to-response/

Srinivasan, S., L. Paine, and N. Goyal. 2019. *Cyber breach at Target*. Harvard Business School Case 117-027. Available at: https://www.hbs.edu/faculty/Pages/item.aspx?num=51339

U.S. Treasury Department. 2013. *Report to the president on cybersecurity incentives pursuant to executive order 13636*. Available at: https://www.treasury.gov/press-center/Documents/Supporting%20Analysis%20Treasury%20Report%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf

Viebeck, E. 2015. *Wal-Mart continually tests net post-Target breach*. Available at: https://thehill.com/policy/cybersecurity/240643-walmart-continually-tests-networks-post-target-breach

Wooldridge, J. M. 2002. *Econometric Analysis of Cross Section and Panel Data*. Cambridge, MA: MIT Press.

APPENDIX A

Variable Definitions

Variable		Definition [Data Source]
$ACCELERATED\_FILER_{t-1}$	=	1 if firm i is an accelerated filer for quarter $t-1$'s fiscal year (0 otherwise) [Audit Analytics].
ACQUISITION	=	1 if there is an acquisition by firm i in quarter t (0 otherwise) [Compustat].
ANNOUNCE_RESTATEMENT	=	1 if firm i announces a restatement in quarter t (0 otherwise) [Audit Analytics].
$BOARD\_CYBER\_EXPERT_{t-1}$	=	1 if firm i's board of directors in quarter $t-1$ possesses a director with prior work experience as a Chief Information Officer, Chief Information Security Officer, or Chief Security Officer (0 otherwise) [BoardEx].
$BOARD\_INDEPENDENCE_{t-1}$	=	1 if firm i's number of independent directors scaled by total number of directors is in the top quartile in quarter $t-1$ (0 otherwise); all terms are calculated for firm i's quarter $t-1$ [BoardEx].
CYBER_EXPERT	=	1 if firm i's top management team in quarter t possesses a Chief Information Officer, Chief Information Security Officer, or Chief Security Officer (0 otherwise) [BoardEx].
FOREIGN	=	1 if firm i exhibits non-missing foreign exchange income in quarter t (0 otherwise) [Compustat].
$GOING\_CONCERN_{t-1}$	=	1 if firm i's audit report for quarter $t-1$'s fiscal year indicates a going concern opinion (0 otherwise) [Audit Analytics].
$INDUSTRY\_EXPERT\_AUDITOR_{t-1}$	=	1 if firm i's external auditor for quarter $t-1$'s fiscal year is an industry expert auditor (0 otherwise); an auditor is deemed an industry expert if it has the highest market share in an industry in an MSA-year [Audit Analytics].
INST_OWNERSHIP	=	the percentage of firm i owned by institutional investors in quarter t [Thomson Reuters].
INV	=	total inventory scaled by total assets for firm i in quarter t [Compustat].
IT_MATERIAL_WEAKNESS	=	1 if firm i's SOX 302 report indicates a material weakness in internal controls for quarter t that is categorized by Audit Analytics as code 52 (information technology, software, access/security issues) or code 51 (segregation of duty issues) (0 otherwise) (Ashraf et al. 2020) [Audit Analytics].
LEVERAGE	=	long-term debt scaled by total assets for firm i in quarter t [Compustat].
LOSS	=	1 if firm i exhibits net income less than zero in quarter t (0 otherwise) [Compustat].
MATERIAL_WEAKNESS	=	1 if firm i's SOX 302 report indicates a material weakness in internal controls for quarter t (0 otherwise) [Audit Analytics].
MTB	=	market value of equity scaled by book value of equity for firm i in quarter t [Compustat].
NON_IT_MATERIAL_WEAKNESS	=	1 if firm i's SOX 302 report indicates a material weakness in internal controls for quarter t that is *not* categorized by Audit Analytics as code 52 (information technology, software, access/security issues) and code 51 (segregation of duty issues) (0 otherwise) [Audit Analytics].
$PEER\_BREACH\_CATASTROPHIC_{t-1}$	=	1 if any of firm i's Hoberg-Phillips TNIC industry peers exhibit a catastrophic data breach during firm i's quarter $t-1$ (0 otherwise); a peer breach is catastrophic when the breached firm experiences a 10 percent or larger negative cumulative abnormal return in the [−1, 1] window around breach disclosure date [CRSP, Privacy Rights Clearinghouse].
$PEER\_BREACH\_HACKED_{t-1}$	=	1 if any of firm i's Hoberg-Phillips TNIC industry peers exhibit a data breach during firm i's quarter $t-1$ that was a result of a hack by an outsider party (0 otherwise) [Privacy Rights Clearinghouse].

(continued on next page)

APPENDIX A (continued)

Variable		Definition [Data Source]
$PEER\_BREACH\_LEADER_{t-1}$	=	1 if any of firm *i*'s Hoberg-Phillips TNIC industry leader peers exhibit a data breach during firm *i*'s quarter *t*−1 (0 otherwise); a firm is an industry leader if that firm has at least 20 percent of the industry's total sales during year *t*−1 (Brown et al. 2018) [Compustat, Privacy Rights Clearinghouse].
$PEER\_BREACH_{t-1}$	=	1 if any of firm *i*'s Hoberg-Phillips TNIC industry peers exhibit a data breach during firm *i*'s quarter *t*−1 (0 otherwise) [Privacy Rights Clearinghouse].
Q4	=	1 if quarter *t* is the fourth quarter in firm *i*'s fiscal year (0 otherwise) [Compustat].
RESTRUCTURE	=	1 if firm *i* exhibited non-missing restructuring costs in quarter *t* (0 otherwise) [Compustat].
ROA	=	net income scaled by total assets for firm *i* in quarter *t* [Compustat].
SALES_GROWTH	=	sales for firm *i* in quarter *t* minus sales for firm *i* in quarter *t*−1, all scaled by sales for firm *i* in quarter *t*−1 [Compustat].
SIZE	=	the natural log of market value for firm *i* in quarter *t* [Compustat].
Z_SCORE	=	0.717 ∗ ((current assets − current liabilities)/total assets) + 0.847 ∗ (retained earnings/total assets) + 3.107 ∗ (earnings before interest and taxes/total assets) + 0.42 ∗ (book value of equity/total liabilities) + 0.998 ∗ (sales/total assets); all terms are calculated for firm *i* in quarter *t;* this variable is calculated following Altman (1983) [Compustat].