The economic cost of cybersecurity breaches: A broad-based analysis[*]

by

Jacob Haislip
Texas Tech University
jacob.haislip@ttu.edu

Kalin Kolev
Baruch College
kalin.kolev@baruch.cuny.edu

Robert Pinsker
Florida Atlantic University
rpinsker@fau.edu

Thomas Steffen
Yale University
thomas.steffen@yale.edu

This version: May 9, 2019

ABSTRACT: Cybersecurity breaches (CSBs) are prominent in the media and underlie a wave of recent regulation; however, there is a lack of consensus in academic research on whether their impact is economically meaningful. We posit that by focusing almost exclusively on targeted firms, researchers ignore a material component of CSB-related costs. This narrow perspective leads to an apparent rift between the active regulatory and media concern about CSBs on one hand and observed general lack of response by capital markets on the other. Adopting a broad-based, multi-faceted approach, we examine the effect of CSBs on non-breached industry peers through the lens of capital markets, auditors, and affected insurers. We find that non-breached peers experience significant negative equity returns around the announcement of a CSB in their industry, together with a material increase in audit fees during the year of the infraction. We also document significantly negative equity returns for insurers with material cybersecurity exposure. Our results reinforce the importance of considering the implications of an economic event beyond the targeted entity and offer a lower bound estimate of CSB costs.

JEL Codes: D8; M15; M41
Keywords: cybersecurity breach; industry contagion; information spillover; audit fees; insurance

[*] We appreciate the comments and suggestions of Xin Yuan, anonymous practitioners, and workshop participants at Baruch College. Kolev acknowledges the financial support of Baruch College and the PSC-CUNY Research Award Program. All errors are ours.

1. INTRODUCTION

We conduct a broad-based study of the cost of cybersecurity breaches (CSBs), with primary focus on the spillover effect to industry peers, auditors, and insurance providers. We undertake this analysis in an effort to reconcile the conflicting attitude towards CSBs between regulators and the media on one hand, and capital markets on the other. Specifically, although regulators and the media place heavy emphasis on the risks and costs of CSBs (Public Company Accounting Oversight Board [PCAOB] 2016; Securities and Exchange Commission [SEC] 2018), capital markets seem to largely treat the infractions as non-events (Hilary et al. 2016; Rajgopal and Srinivasan 2016; Richardson et al. 2019).[1] We conjecture that focusing exclusively on the breached firms ignores a large portion of the economic cost associated with a CSB. As such, we view our study as a step towards developing a more comprehensive understanding of the economic impact of CSBs.

The notion that information spillover exists in capital markets is not new (e.g., Firth 1976; Foster 1981). Prior research offers some evidence that such spillover effects extend to the CSB setting (e.g., Ettredge and Richardson 2003; Hinz et al. 2015); however, these studies generally focus on small, specialized, samples (e.g., a single industry or a limited number of breaches). Thus, although the extant CSB spillover literature offers important insights, its relatively narrow scope raises questions about the generalizability of the documented results across industries and time. Consistent with this observation, in a recent review of the CSB literature, Spanos and Angelis

[1] Other public sector-related activities include the Justice Department's recent creation of the Cyber-Digital Task Force and proposed Senate legislation (The Cybersecurity Disclosure Act of 2017 [S. 536]) requiring firms to explain in their SEC filings whether their boards possess cyber expertise and, if not, why this expertise is rendered unnecessary by other firm actions.

(2016, 226) conclude that spillover in the CSB setting remains a “controversial phenomenon” due to “contradicting results” in the literature.

We adopt a multi-faceted approach to examining CSBs in order to address the contradicting findings in the literature and the apparent rift in perception between academic research and regulators and the media. In particular, we use data on CSB disclosures provided by Audit Analytics to construct a broad sample of 353 external infractions over the period January 2010 – March 2018. To analyze the effect of the CSBs beyond the breached firm, we study the market reaction for the non-breached industry peers, the auditors’ response in terms of audit fee adjustments, and the market reactions for cybersecurity insurance providers. Although not an exhaustive set of the entities (potentially) affected by CSBs, we believe evidence based on these groups provides a meaningful assessment of the conjectured effect and offers an informative gauge of the lower bound of the economic cost arising from CSBs.[2]

Starting with industry peers, we note that a successful breach at a competitor could have counteracting effects in the industry. On one hand, a CSB may lead to consumers shunning the breached firm, regulatory scrutiny, and litigation. Each of these could lead to a loss of market share for the breached firm, which would benefit the non-breached competitors (i.e., a competition effect). On the other hand, news of a CSB in the industry plausibly increases the perceived likelihood non-breached firms could become targets or may have suffered a CSB that is not yet identified or disclosed (i.e., a contagion effect). In other words, the market reaction for non-breached firms around the announcement of a CSB in the industry may be positive, negative, or zero, depending on the relative strength of the competition and contagion effects. Thus, our

[2] Credit providers and taxpayers are other examples of parties likely affected by a CSB.

analysis provides a look at the net effect on non-breached peer firms arising from the infraction, shedding light on the impact of CSBs on the broader economy.

Analyses of the market response of non-breached peers to a breach announcement in the industry is a convenient and well-established approach to assessing the existence of a spillover effect. Such a test, however, relies heavily on assumptions about information arrival and market efficiency.[3] Moreover, the tension between the competition and contagion effects discussed above suggests that the observed market response would be muted as investors jointly consider the positive and negative implications of the peer breach. To alleviate these challenges, we capitalize on cross-sectional variation in characteristics of the non-breached peers to identify factors that are likely to shift the market's weighting between the competition and contagion effects. We consider measures related to the CSB, governance characteristics of the peer firm, the relative size of the breached and non-breached firms, and the industry competitiveness.

We next examine the response of external auditors, a key component of the firm's governance structure, to gain further insight into the impact of CSBs. Even though the potential increase in market share (competition effect) for non-breached peers should not materially affect the auditor's assessment of audit risk, the potential contagion effect likely does. In other words, if the revelation of a CSB in the industry is perceived as a negative externality for the non-breached peers, their assessed audit risk could increase, translating into higher audit fees.[4] Thus, evidence of an increase in the audit fees for non-breached peers in the period a CSB is disclosed in the

[3] For example, if investors learn of the CSB before the official disclosure by the breached firm (i.e., respond to the event before it is announced publicly), the lack of reaction would be misconstrued as lack of economic effect. Additionally, if the market overreacts or underreacts to the CSB announcement, the returns of the non-breached peers around the event date would provide an incorrect estimate of the magnitude of the inferred costs.

[4] Indeed, extant research provides evidence that audit fees increase significantly for breached firms (Li et al. 2017; Smith et al. 2019). We discuss the issue in detail in Section 2.3.2.

industry would provide strong evidence of the existence of the spillover effect, helping parse out the competition and contagion effects associated with that test.

Finally, we investigate how CSBs affect insurance firms with a large cybersecurity business. One of the arguments often put forward as an explanation for the muted market response to the revelation of a CSB is that insurance firms absorb a substantial amount of the direct costs associated with the infraction (Eling and Schnell 2016; PwC 2018). Similar to the non-breached-peers analysis, however, there are opposing forces in play. On the one hand, the revelation of a new CSB may positively affect the insurers' top line as demand for cyber insurance and/or premia charged is likely to increase. On the other hand, the CSB triggers a policy payout and may increase the assessed probability of an increase in future payouts.[5] Thus, the market reaction for the examined insurers around the examined events could be positive, negative, or zero. Although the net reaction remains an empirical question, a significantly negative effect is consistent with the claim that insurers shoulder (some of) the burden associated with the breach, supporting this channel as one of the likely explanations for the muted capital market response to the target firm's disclosure of a CSB.

We begin our analysis by confirming the observation that equity markets, on average, treat the disclosure of a CSB as a negative, yet largely insignificant, event. Using a sample of CSBs ranging from January 2010 through March 2018, we find that although abnormal returns are on average negative across the windows we consider, they are significant in only one of them. Even in that window, however, the effect is marginal at conventional levels. The analysis paints a different picture when we examine the non-breached industry peers: not only are the returns on average negative across windows, but they are also persistently and economically significant. This

[5] Chen et al. (2012) appeal to similar arguments in their study of the impact of CSBs on information technology (IT) consultants.

evidence supports equity investors treating the revelation of CSBs as bad news for the non-breached industry peers, pointing to the existence of an economically important spillover effect.[6] The results are also economically significant. Using the three-day window around the industry infraction as an example, the average buy-and-hold abnormal return is -13.36 basis points for the non-breached peers, translating into a loss of roughly $148 million per infraction totaled across the non-breached peers.[7] The effect increases with the measurement window length, reaching over $840 million per CSB over the [-5, +10] window around the disclosure of the infraction.[8]

The cross-sectional analyses further support the inferences, pointing to a change in the strength of the effect in the expected direction across most of the examined dimensions. The assurance analysis also yields consistent findings – we document an economically and statistically significant increase in the audit fees paid by non-breached peers in the year of the announcement of a CSB in their industry. Finally, our analysis of an index of insurance providers with large cyber insurance books points to a negative market reaction around the revelation of the CSB.

Our study bridges work in the accounting information systems and capital markets domains, contributing to the burgeoning CSB and information spillover literatures. Motivated by the discrepancy between the breached-firm-level evidence of muted capital market reaction to the disclosure of a CSB (e.g., Hilary et al. 2016; Richardson et al. 2019) and the active regulatory and media attention to the infractions, we argue a systematic assessment of the spillover effect of CSBs

[6] We note the significant difference between the size of the CSB and peer samples. Using a simulation, we find an attenuation in the significance of the peer results when we bootstrap the standard errors such that the samples are of comparable size. Importantly, we note that as the bootstrapped sample size increases, the statistical significance of the peer returns also increases. This simulation offers another possible explanation for the general lack of results in other studies focusing on breached firms: statistical power of the tests. We discuss the issue in more detail later on.

[7] In our sample, the average peer-firm market cap (number of peers per breach) is roughly $3.35 billion (33).

[8] To put these estimates in perspective, the Ponemon Institute (2017) survey places the per-CSB average cost for the breached firm at $7.35 million. This estimate is at the high end of the range, with other sources estimating the average cost per infraction for the target firm at less than $1 million (e.g., https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf).

to economic entities linked to the target could offer a more complete understanding of the issue. Our foray relies on a multi-pronged approach examining industry peers, assurance providers, and insurers. Although this does not comprise a complete list of the affected parties, we believe our analysis offers compelling evidence that the costs stemming from CSBs are borne by a broad range of related entities. As such, we view our results as providing a lower bound assessment of the economic cost of CSBs.

Our findings inform a broad audience. Specifically, regulators such as the PCAOB and SEC are actively revising guidance related to CSB, and auditors are investing heavily in the development of cybersecurity assurance procedures and services (PwC 2018). In addition, our study serves as a current and more expansive investigation of the spillover effects of CSB, offering evidence from a broad sample and multiple affected parties. Collectively, our multi-faceted approach expands our understanding of how CSBs affect the economy and offers a step toward reconciling the apparent tension in the perception of CSBs by capital markets and regulators.

2. LITERATURE REVIEW AND MOTIVATION

Cyber intrusion has become the norm, rather than the exception. The revelation of a number of recent high profile CSBs underscore the point. Among the many examples, the 2017 breach of Equifax affected over 150 million credit reports; the 2014 breach of Yahoo compromised half a billion accounts; the 2013 breach at Target led to the loss of tens of millions credit and debit cards; and the 2016 cyber breach of the Bangladesh Central Bank resulted in an initial misappropriation of $101 million. Not surprisingly, regulators and the public have taken notice, raising concerns about cybersecurity risk. Firms have also taken steps to mitigate the effect of such infractions.[9] In

[9] At a recent ISACA conference attended by one of the authors, Equifax's Chief Information Security Officer (CISO) noted that the firm made significant investments in information technology (IT) resources post-breach including hiring

other words, CSBs are economically important, harming a broad range of stakeholders. Although analyses of highly specialized samples occasionally provide evidence of negative effects, academic research generally suggests CSBs have little, if any, impact (e.g., Hillary et al. 2016; Richardson et al. 2019). Next, we provide a brief overview of the CSB and spillover literatures, and motivate our hypotheses.

2.1 CSBs

Tautologically, a cybersecurity breach requires the implementation of an IT system. As such, the CSB literature is relatively young, gaining momentum in recent years. Examinations of the equity market reaction to the revelation of CSBs trace back to Ettredge and Richardson (2003), Campbell et al. (2003), Cavusoglu et al. (2004), Gordon and Loeb (2002, 2006), and Goel and Shawky (2009), who generally note a negative response. Recent studies deploying larger samples, however, note that equity investors treat CSBs as non-events, on average.[10] As an example, Amir et al. (2018) argue that firms are often successful in hiding their CSB attacks. Contrasting CSB disclosures originating with the breached firm and those from external sources, the authors note that the negative market returns around both types of disclosure are only significant in the latter case. Hilary et al. (2016) further question the economic significance of CSBs. Despite noting a modest increase in disclosure following the reporting of a breach, the authors find a three-day negative market-adjusted return of only half a percent, which, they note, is much smaller than the 1.3 percent average drop in price in response to the announcement of an asset impairment. Similarly, Richardson et al. (2019) find that, with the exception of a few catastrophic breaches, the

their first ever Chief Privacy and Data Governance Officer. The CISO also stated that Equifax, two years removed from their CSB, still was not certain how many records were compromised.

[10] One notable exception is Kamya et al. (2018), who document a significantly negative market reaction to the revelation of CSBs, as well as operating and governance changes following the infraction. Similar to earlier studies, however, they note that the effect is concentrated among a subsample of the CSBs.

market reaction to CSBs is trivial, and dissipates within days of the disclosure. The evidence in Hilary et al. (2016) and Richardson et al. (2019) also fails to support the idea that breached firms differ from their peers with respect to subsequent performance.

Extant research on the response to and effects of CSBs yields important evidence on the disclosure policies, real actions, and capital markets' response to the infractions. Earlier studies, however, often target very specific settings (as an example, Ettredge and Richardson, 2003, examine four firms and one breach type over a three-day window). Recent studies relax this constraint, favoring large sample analyses. Primarily focusing on the breached firms, they provide evidence capital markets generally shrug off the infractions.

In summary, academic research confirms CSBs are common, but, outside specific subsamples, generally fails to provide evidence of negative impacts commensurate with the degree of reaction from regulators and the media. We conjecture that the discrepancy may arise from focusing on a single dimension of the problem, effectively obscuring the broader question of the aggregate economic impact of CSBs. Specifically, we posit the effects of CSBs are far-reaching, affecting the entities economically linked to the breached firms.

2.2 Spillover

Starting with Firth (1976) and Foster (1981), a large body of research demonstrates that shocks to a firm also affect related firms, even if that shock does not directly impact them. Typically referred to as "spillover effects" (e.g., Bushman and Smith 2001), evidence supports these effects exist for a wide range of "related firms" (industry peers and supply chain partners, among others) and "shocks" (e.g., earnings announcements, restatements, and fraud). For example, Gleason et al. (2008) find that when a firm experiences negative returns around an accounting restatement, its non-restating industry peers also suffer stock price declines. As another example, Durnev and Mangen (2009) document that industry peers adjust downwards their investment growth in the year after a competitor restates, indicating that peers incorporate the information into their investment decisions. Focusing on fraud, Beatty et al. (2013) investigate the actions of fraudulent firms' peers in the years leading up to the revelation of the malfeasance. The results suggest peer firms overinvest during the fraud period. Li (2016) extends the analysis, documenting that the effect extends to DOJ and SEC accounting-misstatement-related enforcement actions. Relatedly, Zhang and Zhang (2016) find evidence of a negative fraud spillover effect for the fraudulent firms' suppliers and customers over both the short term and long term. The spillover effect increases with business tie closeness and industry concentration, but varies across fraud types. Spillover effects among related firms have also been established with respect to bankruptcy (Hertzel et al. 2008), tax avoidance behavior (Cho et al. 2016), and in disclosure practices (e.g., Jung 2013).

We focus on spillover effects in the setting of CSBs. In contrast to the issues discussed above, the effects of CSBs relate more closely to operational performance (e.g., internal controls, security resource budget allocation decisions, and intellectual capital) than financial issues (Benaroch and Chernobai 2017; Kamiya et al. 2018). Moreover, a CSB could have opposing effects on the economically related non-breached firms as the contagion and competition effects comingle.

A CSB is a criminal offense (a form of internet fraud) against the target. That is, unlike financial reporting fraud and restatements, the infraction originates outside the firm. The breaches, however, affect the target's reputation, could lead to legal actions, and may result in customers taking their business elsewhere. If investors believe a breach in the industry increases the likelihood other firms would become targets or already have been breached, but have not identified or disclosed the infraction yet, equity prices for the non-breached peers may decline at the revelation of the CSB. We label this a *contagion* effect. Alternatively, investors who flee the breached firm could perceive related, non-breached, firms to be a good investment, pushing their stock price up.[11] We refer to this as a *competition* effect. Thus, it is ex ante unclear whether the contagion or competition spillover effect dominates when CSBs are disclosed.

Consistent with this observation, spillover analyses in the CSB setting fail to provide conclusive results. As a confounding factor, most extant studies favor small samples or highly specialized settings. As an example, Hinz et al. (2015) analyze a sample of six data thefts, documenting that companies in the same industry suffer a decrease in stock price. Similarly, using a sample of four breached internet firms, Ettredge and Richardson (2003) highlight the existence of information transfer to other internet firms. Chen et al. (2012) find that the value of IT consulting firms increases when their clients are breached, but the effect reverses as the number of breaches increases. Zafar et al. (2012) and Jeong et al. (2017) both study the effect on competitors when a data breach occurs, but arrive at opposite conclusions. In particular, Zafar et al. (2012) identify a contagion effect (the competitors' stock price moves in the same direction as the breached firm), while Jeong et al. (2017) document a competition effect (the competitors' stock price moves in the opposite direct of the breached firm). Not surprisingly, in a recent review of the CSB literature, Spanos and Angelis (2016, p. 226) conclude that spillover in the CSB setting remains "a controversial phenomenon." By employing a broad sample of over 350 CSB across many industries and years to study spillover effects for several types of related parties, we aim to enhance the understanding of the economic costs of CSBs.

[11] Among the reasons for this dynamic is expectations of market share re-distribution and supply chain re-alignment as customers and suppliers leave the breached firm.

2.3 Hypotheses

2.3.1 CSBs, Market Reaction, and Spillover

The frequency and severity of CSBs have intensified over the past decade, drawing the attention of regulators, investors, practitioners, and the media (e.g., the SEC's [2018] recent guidance). Academic and anecdotal evidence indicates that the economic costs associated with CSBs, from prevention to detection and ultimately to remediation, can be significant (Higgs et al. 2016; Kashmiri et al. 2017; Ponemon Institute 2017). The heightened regulatory interest and push for disclosure and implementation of safeguard protocols supports this notion; however, empirical analyses of the capital market's response to the revelation of a CSB suggest investors treat these infractions as a minor nuisance (Hilary et al. 2016; Rajgopal and Srinivasan 2016; Richardson et al. 2019). What drives this disparity? Do regulators and investors truly disagree on the cost of CSBs? Or, does focusing primarily on the breached firm and its investors ignore an economically important portion of the impact of the infraction?

We conjecture that a likely explanation pertains to a failure to identify the full set of costs associated with CSBs. Calling on the spillover literature highlighted in the prior section, we posit that non-breached peers could also feel the effects of a CSB in the industry. Specifically, the revelation of the event may trigger a reassessment of the likelihood that a non-breached peer either (1) may become a target in the future, or (2) already has been breached, but the infraction has not been identified or disclosed. Such concerns may lead to costly actions by the board/management and negative responses by investors, both pointing to a decrease in stock price. As noted earlier (e.g., Chen et al. 2012), it is also possible that non-breached peers benefit from the infraction via product market competition as they absorb business lost by the breached firm. Thus, the direction of the associated spillover (positive, negative, or net zero) becomes an empirical question. We state our first hypothesis in the null as follows:

Hypothesis 1: The revelation of a CSB in a firm does not affect the equity returns of its peers.

2.3.2 CSBs and Peers' Audit Fees

We supplement the examination of the response of equity investors with an analysis of the response by assurance providers. Auditors are external monitors tasked with detecting potential problems with their clients' financial statements and internal controls (Smith et al. 2019). A CSB, at its core, attests to a weakness in internal controls. Although recent Center for Audit Quality (CAQ; 2016, 2017) and PCAOB (2016) statements attempt to clarify the role of the auditor with respect to a client's CSB, Li et al. (2017, p. 3) openly question whether auditors would include procedures specifically identified with CSB risk in the absence of clear audit guidance. Their analysis, however, points to an increase in audit fees for firms that fallen victim to a CSB. Lawrence et al. (2018) and Smith et al. (2019) similarly note an increase in audit fees for breached firms. Although each of the studies offers a nuanced analysis (e.g., Lawrence et al. note their combination of imperfect operational risk proxies), the preponderance of the evidence suggests that auditors are mindful of CSBs and treat the infractions as an increase in audit risk.

Turning to non-breached peers, if auditors perceive that a CSB in the industry translates into higher audit risk or a need for additional procedures, audit fees for the peer firms would increase during the year of the infraction. If the auditors treat CSBs as non-events, then there should not be a material change in audit fees during the treatment period.[12] Thus, we state our second hypothesis in the null as follows:

Hypothesis 2: There is no effect of a CSB on a non-breached peer firm's audit fees.

[12] A convenient feature of the setting is that unlike the case of equity investors, it is difficult to come up with a plausible story for a decrease in the audit fees. In other words, failing to find a result is informative on its own.

2.3.3 Providers of Cybersecurity Insurance

Our final analysis focuses on providers of cybersecurity insurance. Even though insurance has been cited as a potential explanation for the muted market reactions to revealed CSBs (Eling and Schnell 2016; PwC 2018), we are not aware of empirical evidence on the impact of CSBs on insurance providers.[13] If insurers indeed absorb a large portion of the direct costs arising from a CSB, then failing to consider them overlooks a significant component of the economic burden imposed by these infractions. Mirroring the arguments on the potential impact on non-breached peers, the effect on insurers is two-sided. On the one hand, the disclosure of a CSB mechanically triggers the payout on the respective insurance policy and (potentially) increases the assessed likelihood that future payouts would become due as more firms are breached. On the other hand, the higher threat of cyberattacks could drive demand for the insurer's products and may justify an increase in the relevant premiums.[14] The prior effect implies a negative market reaction for the insurer around the revelation of a material CSB; whereas, the latter implies a positive one. Which force dominates, i.e. whether the net effect is positive, negative, or zero, is an empirical question. Thus, we state our third hypothesis in the null form:

Hypothesis 3: *A CSB disclosure does not affect the equity returns of cybersecurity insurance providers.*

3. SAMPLE AND RESEARCH DESIGN

3.1 Breach Sample

[13] Conversations with practitioners reveal the cyber insurance products are heterogeneous, as the field is relatively young. These products, however, are gaining popularity among both insurance providers and customers. Although we recognize this test likely has low power and is (somewhat) tangential to the other analyses in the study, we believe it provides an important insight on the scale and scope of CSBs.

[14] This logic applies to a broad spectrum of entities economically linked with the breached firm. As an example noted earlier, Chen et al. (2012) study the effect of client breaches on IT consulting firms, juxtaposing the increase in demand for their services to loss of reputation capital.

We begin the analysis by constructing a comprehensive sample of material CSBs. We obtain the data from Audit Analytics. As shown in Panel A of Table 1, our initial sample comprises 405 breaches with disclosure dates from January 2010 through March 2018.[15] We drop CSBs without available Compustat and CRSP identifiers, GICS (industry) data, as well as CSBs disclosed within two days of earnings announcements and CSBs in firms with stock price less than $1 during the short window surrounding the breach disclosure date. These selection criteria result in a final sample of 353 CSB disclosure events. In Panel B of Table 1 we present the distribution of CSB by type, as reported by Audit Analytics. Within our sample, 29 percent of CSBs are classified as “financial” breaches, 57 percent as “personal” breaches, and 14 percent as “other.” Turning to Panel C, we note that with the exception of real estate, all GICS industries are affected by a CSB during the examined period. Not surprisingly, the sectors affected most often are consumer discretionary firms (36 percent), information technology firms (24 percent), and financial firms (13 percent). Finally, Panel D presents the sample composition by year. Notably, the frequency of disclosed CSB increases over time, underscoring the importance of the issue (the smaller number in 2018 is due to our CSB data ending in March of 2018).

[Insert Table 1 about here]

3.2 Industry Peer Spillover

To construct our sample of non-breached industry peers, we follow Gleason et al. (2008) and start by identifying all firms in the same GICS subsector as the breached firm for each of the 353 CSB disclosures described in Table 1. We then impose requirements similar to those used for the breached firms: we require Compustat and CRSP firm identifiers, and we exclude peers if they

[15] The Audit Analytics database contains eight CSB disclosure events from 2004 through 2009. We choose to start our sample period in 2010 when the coverage appears to become more comprehensive.

have an earnings announcement within 2 days of the CSB disclosure or have a stock price less than \$1 during the event window. We also exclude all CSB firms from the set of non-breached peer firms.[16] For our initial tests of Hypothesis 1, we construct buy-and-hold abnormal returns (BHAR) for four different event windows relative to the CSB disclosure date: [-1, 1], [-2, 2], [-5, 5], and [-5, 10]. We calculate BHAR as the buy-and-hold return of the firm minus the buy-and-hold return on the value-weighted market return over the respective window. Similar to Gleason et al. (2008), we first perform *t*-tests to investigate whether the mean BHAR is significantly different from zero across each of the event windows. Because the sample sizes (and resulting statistical power) are very different for the breached firm and non-breached peer firm subsamples, we also perform bootstrapped *t*-tests with varying sample sizes and bootstrap repetitions in order to provide evidence on the impact of sample size in CSB market reaction tests.

To shed additional light on the factors that might influence the magnitude of a non-breached peer firm's market reaction, we then consider drivers of cross-sectional variation in the peer firms' market reactions by estimating the following regression model:

$$\text{BHAR}_{p,t} = \alpha_0 + \alpha_1\text{TRAIT}_{p,t} + \alpha_2\text{SIZE}_{p,t} + \alpha_3\text{BTM}_{p,t} + \alpha_4\text{LEV}_{p,t} + \gamma_y + \varepsilon_{p,t} \qquad (1)$$

In equation (1), *p* refers to the non-breached peer firm, and *t* refers to a particular CSB disclosure date. BHAR is the buy-and-hold abnormal return described above, and we include control variables considered by prior spillover research (e.g., Gleason et al. 2008; Silvers 2016). Specifically, we include SIZE, BTM, and LEV to control for firm size, growth opportunities, and leverage, respectively. We also consider calendar year fixed effects (γ_y) as a control for macroeconomic factors. TRAIT is one of five traits that we expect to be associated with the magnitude of the non-breached peer firm's market reaction. The first is BREACHNUM, defined

[16] We present descriptive statistics in Table 2.

as the natural log of the number of CSB disclosed in the GICS subindustry. For example, if breach *t* is the second CSB disclosed in a particular GICS subindustry, BREACHNUM = *ln*(2) for the peer firms linked to that CSB event. If CSB become more severe over time, we might see a negative coefficient on BREACHNUM, indicating a more negative market reaction for peer firms as the number of CSBs increases in an industry. If peer firms' investors become less surprised and less worried as CSBs become more commonplace, however, we might observe a positive coefficient on BREACHNUM.

The second TRAIT variable is COMPETITION, defined as the Herfindahl index based on Compustat firms' sales in the same GICS subindustry from the year prior to CSB *t*. Larger values of COMPETITION indicate less competition (more highly concentrated competitors). The third trait we consider is BREACHSIZE, defined as the decile rank of the breached firm's market capitalization based on daily rankings constructed using CRSP data. The fourth TRAIT variable is SIZEDIFF, defined as BREACHSIZE minus the decile rank of the peer firm's market capitalization. Therefore, positive (negative) values of SIZEDIFF indicate that the breached firm is larger (smaller) than the respective non-breached peer. Since the impact of industry concentration, breached firm size, and size difference on BHAR would differ depending on whether the contagion or competition effect dominates, we do not predict the sign of COMPETITION, BREACHSIZE, or SIZEDIFF. Our last TRAIT variable is TECHCOMM, an indicator set to one if the peer firm has a technology committee in place during the year of the CSB disclosure. Similar to the other traits, we do not predict the sign of TECHCOMM, because although the presence of a technology committee could indicate better cybersecurity preparedness (Higgs et al. 2016), it could also capture technology dependency and thus the attractiveness of the firm as a future breach target. By examining how these various TRAIT variables are associated with cross-sectional variation in CSB disclosure event BHARs, we hope to shed light on the factors that drive CSB information spillover.

3.3 Audit Fees

To test Hypothesis 2, we use the same initial set of GICS subindustry peers described in the previous section, but we do not screen on proximity to earnings announcements, stock price, or availability of CRSP data. We then limit the sample to firms with all of the required data from Compustat and Audit Analytics to estimate our audit fee model. The procedure yields 9,080 non-breached peer firm observations. The control group comprises all non-breached, non-peer firm observations with all required data from Compustat and Audit Analytics. In total, this sample comprises 47,386 firm-year observations. Following Li et al. (2017), estimate the following model:

$$\text{LNFEES}_{i,t} = \alpha_0 + \alpha_1\text{PEER}_{i,t} + \alpha_2\text{SIZE}_{i,t} + \alpha_3\text{INVREC}_{i,t} + \alpha_4\text{SEGMENTS}_{i,t} + \alpha_5\text{FOREIGN}_{i,t} + \alpha_6\text{MERGER}_{i,t} + \alpha_7\text{SPECIAL}_{i,t} + \alpha_8\text{LOSS}_{i,t} + \alpha_9\text{GROWTH}_{i,t} + \alpha_{10}\text{BTM}_{,t} + \alpha_{11}\text{BIG4}_{i,t} + \alpha_{12}\text{GC}_{i,t} + \alpha_{13}\text{INITIAL}_{i,t} + \alpha_{14}\text{ROA}_{i,t} + \alpha_{15}\text{LEV}_{i,t} + \alpha_{16}\text{QUICK}_{i,t} + \alpha_{17}\text{ICMW}_{i,t} + \gamma_y + \mu_\mu + \varepsilon_{i,t} \quad (2)$$

In Equation (2), *i* indicates a firm, and *t* refers to year. The dependent variable, LNFEES is the natural log of audit fees (we define all variables in Appendix A). The variable of interest is PEER, which is an indicator set to one if the firm is in the GICS subsector of a firm that discloses a breach in year *t*. We interpret a positive coefficient on PEER (α_1) in support of the existence of a contagion effect associated with CSB. The vector of controls follows prior research (e.g., Li et al. 2017) and comprises variables shown to be associated with audit fees. Specifically, we include constructs capturing size (SIZE), complexity (INVREC, SEGMENTS, FOREIGN, MERGER, and SPECIAL), performance (LOSS, GROWTH, BTM, ROA, LEV, and QUICK), and other audit characteristics (BIG4, GC, INITIAL, and ICMW). We also include year (γ_y) and industry (μ_μ) fixed effects.[17]

3.4 Cybersecurity Insurance Providers

To test Hypothesis 3, we construct a sample of insurance firms, comparing those with vs. without significant cybersecurity insurance exposure. The test focuses on equity returns during the event windows surrounding CSB disclosures. We begin by identifying 320 unique dates from the 353 CSB disclosures described in Table 1. We then construct the pool of insurers by retaining firms with GICS subindustry codes of 40301030 (multi-line insurance) and 40301040 (property and casualty insurance). Similar to the prior analyses, we remove breached firms from this sample and require CRSP and Compustat identifiers, eliminate firms having earnings announcements within two days of a CSB disclosure, and firms with stock price below \$1 during the event window. Next, we construct BHAR for the various event windows applying the same methodology we adopt for the peer-firm market-reaction tests. We first report *t*-tests of mean BHARs for the non-cyber and cyber-exposed insurers and then estimate the following model:

$$BHAR_{i,t} = \alpha_0 + \alpha_1 CYBER_{i,t} + \alpha_2 SIZE_{i,t} + \alpha_3 BTM_{i,t} + \alpha_4 LEV_{i,t} + \gamma_y + \varepsilon_{i,t} \qquad (3)$$

Equation (3) is similar to equation (1) except that *i* refers to insurance firms, and CYBER is an indicator set to one for firms we identify as significant providers of cybersecurity insurance. The final sample of insurance firms comprises 96 insurance providers, 10 of which we identify as having significant cybersecurity insurance exposure (CYBER = 1).[18] As we note in the hypothesis

[17] To differentiate from our process of identifying peer firms, we define the industry fixed effects over two-digit SIC codes. Inferences remain the same if the model does not include industry fixed effects.

[18] The cybersecurity firms in the sample include AIG, CNA Financial, Chubb, Markel, XL Group, Travelers, Axis Capital Holdings, and Allied World Assurance. We identify them through internet searches for lists such as those found at https://www.propertycasualty360.com/2017/11/13/top-10-writers-of-cybersecurity-insurance/ and https://cyberpolicy.com/cybersecurity-education/the-top-5-cyber-insurance-carriers-in-the-market.

development section, it is ex ante unclear whether cybersecurity insurance providers are positively (due to increased demand for their services) or negatively (due to revisions in the expectation of insurance payouts) affected when insured firms disclose a CSB. Moreover, conversations with practitioners indicate that while the cybersecurity insurance business is growing, the products remain in a very early stage. As such, we do not make a prediction on the sign of the CYBER coefficient and turn to the empirical results to shed light on how disclosed CSBs impact cybersecurity insurance providers.

4. FINDINGS

4.1 Breached Firms

Prior to testing our hypotheses, we examine the market reaction for the breach firms in our sample of 353 CSB disclosure events (described in Table 1). We present the distribution of BHARs for the breach firms in Panel A of Table 3. The average market reaction is -17.83 basis points for the [-1, 1] event window and increases in magnitude to approximately -50 basis points for the longer event windows. Although consistently negative, only the [-5, 5] event window has an average return that is statistically different from zero ($p < 0.10$). These results generally confirm broad-sample evidence in prior research that equity investors do not respond in an unambiguously negative way to the revelation of a CSB.

4.2 Non-breached Industry Peers

Turning to Panel B, we examine the average market reaction for the non-breached peer firms. Although the [-1, 1] BHAR is less negative than that for the breached firms during the same window (-13.36 basis points vs. -17.83 basis points for the breached firms), a *t*-test indicates that the peer firm result is highly significant ($p < 0.01$). In addition, the magnitude of the negative market reaction increases as the event window widens, going from -13.36 basis points over the [-

1, 1] window to -76.20 basis points over the [-5, 10] window. Moreover, all of the average BHARs are significantly different from zero at the 1 percent level. The results in Panel B support that non-breached peer firms experience significant negative spillover when a peer firm announces a CSB, suggesting that contagion effects dominate any potential competition effects. In other words, ignoring the effect of CSB on the non-breached industry peers materially understates the assessed cost of these infractions.

[Insert Table 3 about here]

However, one of the obvious differences between the results in Panels A and B of Table 3 is the sample size of the breached firms (353) vs. the sample size of the non-breached peer firms (11,508). As a result, the power of the test differs greatly between the two samples. To investigate the effects of these sample size differences, we perform bootstrapped *t*-tests using the peer firm sample with various sample sizes and bootstrap repetitions. We present the results in Table 4. In Panel A, we draw 353 observations for each bootstrap repetition (to match the number of observations in the breach firm sample) and vary the number of repetitions (ranging from 100 to 5,000 and indicated in the column headings). The results indicate that only the BHAR from the [-5, 10] window remains significant across all numbers of repetitions.

In Panel B, we hold constant the number of bootstrap repetitions at 1,000 and instead vary the number of observations drawn per repetition (ranging from 353 to 5,000 and indicated in the column headings). Similar to Panel A, only the BHAR from the [-5, 10] window is significant across all numbers of observations. As expected, statistical significance in both panels is stronger as the number of observations and repetitions increases, although the effect is stronger for the number of observations shown in Panel B. For example, using 353 observations, only the BHAR from the [-5, 10] window is significant, but even increasing the sample size to 500 shows that other return windows start to show statistical significance. To summarize, the results in Table 4 indicate that one of the reasons we generally observe insignificant results for the breached firms in Table 3 with significant results for the peer firms is due to differences in statistical power. We believe this result may also help explain the lack of statistically significant results in the literature studying market reactions to CSBs. As time goes on and more CSBs occur, researchers will likely be able to detect significant market reactions.

[Insert Table 4 about here]

We next consider the set of TRAITS that could affect the strength of the examined effect across peer firms. We present the results in Table 5 with BHAR [-5, 10] as the dependent variable. We choose to focus on the [-5, 10] window because it is the most robust result considering the bootstrap analyses in Table 4.

The sign of the BREACHNUM estimated coefficient is positive when considered in isolation (column 1 of Table 5) but is not significant one all the TRAIT variables are considered together (column 6). Thus, there is some evidence that peer firms' market reactions are less negative as more breaches occur (i.e., investors are perhaps desensitized and view CSBs as more commonplace), but the number of previous CSBs in an industry is not among the primary drivers of the examined contagion. The COMPETITION coefficient, however, is consistently positive (recall that larger values of COMPETITION indicate more concentrated, less competitive, industries). This implies that when there are fewer players in an industry, the peer firms' market responses to the revelation of a CSB in the industry are more positive (or less negative), suggesting higher (lower) weight of the competition (contagion) effect. We also observe that the estimated coefficients on BREACHSIZE are positive and significant across specifications. This result indicates that peer firms are impacted less negatively when the breached firm is larger, suggesting that the weight of the competition (contagion) effect increases (decreases) in the size of the target.

Turning to SIZEDIFF, the coefficient is not significant when it enters the model as the sole TRAIT variable (column 4), but when included simultaneously with the other TRAIT variables (column 6), it is significantly negative ($p < 0.01$). This implies that after controlling for the size of the breached firm, BREACHSIZE, the larger the breached firm relative to its peer firm, the stronger the contagion effect. Finally, the estimated coefficient on the TECHCOMM variable is positive and significant ($p < 0.05$ in column 5, $p < 0.10$ in column 6). This finding is consistent with the notion that investors are less concerned about contagion effects when peer firms have better quality IT governance in place.

[Insert Table 5 about here]

4.3 Audit Fees

We present the results of the test of Hypothesis 2 on audit fees in Table 6. In column 1, the coefficient of interest (PEER) is positive and significant, suggesting the peers of breach firms do pay higher audit fees in the year of the breach. Further, the positive and significant coefficient in column 2 (*Lag* PEER) indicates that the increase in audit fees for peer firms persists in the year following the breach. The *Lag* PEER coefficient in column 2 (0.052), however, is lower than the PEER coefficient in column 1 (0.063), suggesting an attenuation of the effect over time. In economic terms, in the year of a CSB disclosure, non-breached peer firms' audit fees are higher by approximately 6 percent, which is material. This finding again underscores the importance of considering contagion effects when evaluating the economic costs of CSBs.

[Insert Table 6 about here]

4.4 Cybersecurity Insurance Providers

We present the analyses related to cybersecurity insurance providers (Hypothesis 3) in Table 7. Similar to the peer-firm-equity-returns analyses, we consider four measurement windows for BHAR around the CSB disclosure date. For completeness, we present BHAR summary statistics and *t*-tests for the means for non-cyber insurance firms (Panel A) and those insurance firms with heavier cybersecurity exposure (Panel B). The non-cyber insurance firms have significantly positive returns in the [-1, 1] and [-2, 2] windows, while the cybersecurity insurers have significantly negative returns in the [-5, 5] window ($p < 0.05$). However, we are most interested in the differential market reaction, and Panel C presents regression results. The estimated coefficients on CYBER across all BHAR windows are negative, and CYBER is significant for three of the four windows ($p < 0.10$). Collectively, this set of results supports the conclusion that the policy payouts triggered by CSBs, as well as the revised assessment of expected future payouts, outweigh the potential increase in revenue. Similar to the evidence from the other analyses, these results reinforce the notion that the costs from CSBs extend well beyond the breached firm itself. Moreover, this analysis provides evidence in support of the claim that insurers absorb CSB-related costs (Eling and Schnell 2016; PwC 2018), adding a piece to the puzzle of investors' apparent disinterest in the disclosure of the infraction at the breached firm.

[Insert Table 7 about here]

5. CONCLUSION

The frequency and severity of cybersecurity breaches are on the rise. Extant research analyzing the costs at the breached-firm level generally find that capital markets are not too concerned with CSBs. We posit that focusing primarily on the target firms ignores an important component of the economic costs associated with these infractions. To this end, we conduct a large-scale, multi-faceted analysis of the spillover effects of CSBs, examining non-breached peers, assurance providers, and cybersecurity insurance providers.

Our analyses reveal that non-breached peers suffer significantly negative equity returns around the announcement of a CSB in their industry, together with a material increase in audit fees during the year of the infraction. We also document negative equity returns for insurers with significant cybersecurity exposure. Overall, our results suggest that the costs of CSBs are more extensive and affect a number of entities other than the breached firm. These findings speak to the significant concerns expressed by regulators and the media with respect to CSBs. Moreover, our findings contribute to the CSBs and information spillover literatures, demonstrating the contagion effect of CSBs in a broad sample spanning several years and considering multiple potentially affected entities.

Our study is not without limitations. First, we limit our sample of CSBs to a single data set, which contains one breach type – hacks. Future research could examine the generalizability of our findings to other data sets and breach types. Similarly, we are limited to CSBs that are publicly disclosed. Finally, although we consider multiple CSB stakeholders, we do not consider the full set of potentially affected parties. Analyzing these parties represents an important opportunity for future research. Nevertheless, we believe our findings provide an important stepping-stone in providing a more complete picture of the economic costs of CSBs and offer a path to reconciling the on-the-surface conflicting perceptions of CSBs by regulators and the media on the one hand, and capital markets on the other.

Appendix A
Variable Definitions

Variable **Definition**

BHAR (-A, B) Buy-and-hold abnormal returns starting A days before the breach disclosure date and ending B days after the disclosure date. Abnormal returns are calculated as the firm's buy-and-hold return minus the buy-and-hold value-weighted market return. We present the BHAR variables in basis points.

BIG4 An indicator variable set to one if the firm retains a Big 4 auditor during the year, 0 otherwise.

BREACHNUM The natural log of the number of breaches experienced in the GICS subindustry (i.e., BREACHNUM = ln(2) if the examined breach disclosure is the second breach disclosed in that GICS subindustry).

BREACHSIZE Decile rank of the breached firm's market capitalization, where market capitalization ranks are determined each day using CRSP data.

BTM Book-to-market value of equity (Compustat items SEQ / (LT + (CSHO * PRCC_F)).

COMPETITION Herfindahl index using sales data for all firms listed on Compustat in the year prior to the breach disclosure year.

CYBER An indicator variable set to one if the insurance firm is a significant provider of cybersecurity insurance, 0 otherwise.

FOREIGN An indicator variable set to one if the firm has foreign operations in year t, 0 otherwise.

GC An indicator variable set to one if the firm receives a going concern opinion in year t, 0 otherwise.

GROWTH Percentage change in sales relative to year t-1.

ICMW An indicator variable set equal to one if the firm reports a material weakness in internal controls in year t, 0 otherwise.

INVREC Inventory and accounts receivable divided by total assets (Compustat items (INVT+RECT)/AT).

INITIAL An indicator variable set to one if the firm switched auditors in year t.

LEV Compustat items (DLC + DLTT) / AT.

LNFEES The natural log of audit fees in year t, as reported by Audit Analytics.

LOSS An indicator variable set to one if the firm reports negative net income before extraordinary items (Compustat item IB) in year t, 0 otherwise.

MERGER An indicator variable set to one if the firm has merger activity in year t (Compustat item AQA), 0 otherwise.

PEER An indicator variable set to one if the firm is in the same industry as a breached firm in year t, 0 otherwise.

QUICK Current assets minus inventory divided by current liabilities (Compustat items (ACT – INVT) / LCT).

ROA Operating income scaled by total assets (Compustat items OIBDP / AT).

SEGMENTS The firm’s operating segments for the year, as reported by Compustat.

SIZE The natural log of total assets (Compustat item AT).

SIZEDIFF BREACHSIZE minus the decile rank of the non-breached peer’s market capitalization.

SPECIAL An indicator variable set to one if the firm reports special items in year t, 0 otherwise.

TECHCOMM An indicator variable set to one if the non-breached peer firm has a technology committee in the year of the breach disclosure, 0 otherwise.

Lag The lag operator.

REFERENCES

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.

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

Benaroch M., and A. Chernobai. 2017. Operational IT failures, IT value-destruction, and board-level IT governance changes. *MIS Quarterly*. Forthcoming.

Bushman, R. M. and A. J. Smith. 2001. Financial accounting information and corporate governance. *Journal of Accounting and Economics* 32: 237–333.

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

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

Center for Audit Quality. 2016. Understanding cybersecurity and the external audit. Available at: http://www.thecaq.org/understanding-cybersecurity-and-external-audit. Last accessed October 6, 2016.

Center for Audit Quality. 2017. The CPA's role in addressing cybersecurity risk. Available at: http://www.thecaq.org/cpas-role-addressing-cybersecurity-risk. Last accessed December 19, 2017.

Chen, J. V., H. C. Li, D. C. Yen, and K. V. Bata. 2012. Did IT consulting firms gain when their clients were breached? *Computers in Human Behavior* 28: 456–464.

Cho, H., S. Lee, and J. A. Meade. 2016. Does news of IRS tax litigation affect assessments of tax risk? Working paper. Abstract available at SSRN.

Durnev, A., and C. Mangen. 2009. Corporate investments: Learning from restatements. *Journal of Accounting Research* 47 (3): 679–720.

Eling, M. and W. Schnell. 2016. What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance* 17 (5): 474–491.

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

Firth, M. 1976. The impact of earnings announcements on the share price behavior of similar type firms. *The Economic Journal* 86 (342): 296–306.

Foster, G. 1981. Intra-industry information transfers associated with earnings releases. *Journal of Accounting and Economics* 3 (3): 201–232.

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

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

Gordon, L. A. and M. P. Loeb. 2002. The economics of information security investment. *ACM Transactions on Information and System Security*, (November 2002): 438–457.

Gordon, L. A. and M. P. Loeb. 2006. Process for deciding on information security expenditures: empirical evidence. *Communications of the ACM* (January 2006): 121–125.

Gwebu, K. L., J. Wang, and W. Xie. 2014. Understanding the cost associated with data breaches. *Pacific Asia Conference on Information Systems Proceedings.*

Haislip, J., J-H. Lim, and R. Pinsker. 2018. The role of IT governance mechanisms in data security breaches. Presented at the 2018 American Accounting Association's Accounting Information Systems Midyear Meeting, Newport Beach, CA.

Hertzel, M. G., Z. Li,, M. S. Officer, and K. J. Rodgers. 2008. Inter-Firm Linkages and the wealth effects of financial distress along the supply chain. *Journal of Financial Economics* 87 (2): 374–387.

Higgs, J. L, R. E. Pinsker, T. J. Smith, and G. R. Young. 2016. The relationship between board - level technology committees and reported security breaches. *Journal of Information Systems* 30 (3): 79–98.

Hilary, G., B. Segal, and M. H. Zhang. 2016. Cyber-risk disclosure: Who cares? Working paper, Georgetown University, available on SSRN.

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

Jeong, C. Y., S.-Y. T. Lee, and J.-H. Lim. 2017. The impact of information security breaches and IT security investments on a firm's competitors. *Association for Information Systems ICIS 2017 Proceedings*.

Jung, M. J. 2013. Investor overlap and diffusion of disclosure practices. *Review of Accounting Studies* 18(1): 167–206.

Kamiya, S., J. K. Kang, J. Kim, A. Milidonis, and R. M. Stulz. 2018. What is the impact of successful cyberattacks on target firms? Working paper. Available at NBER.

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

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

Li, H., W. G. No, and J. E. Boritz. 2017. Are external auditors concerned about cyber incidents? Evidence from audit fees. Working paper presented at the 2017 AAA AIS/SET Midyear Meeting, Orlando, FL.

Li, V. 2016. Do false financial statements distort peer firms' decisions? *The Accounting Review* 91 (1): 251‒278.

Ponemon Institute. 2017. 2017 Cost of Data Breach Study: Global Analysis. Available at www.ncsl.org/documents/taskforces/IBM_Ponemon2017CostofDataBreachStudy.pdf. Last accessed April 22, 2019.

Public Company Accounting Oversight Board (PCAOB). 2016. PCAOB Update – Recent Activities and Next Steps Speech by Jay D. Hansen, PCAOB Board Member. June 9, 2016.

PwC. 2018. Insurance 2020 & beyond: Reaping the dividends of cyber resilience. Available at: https://www.pwc.com/gx/en/industries/financial-services/publications/insurance-2020-cyber.html.

Rajgopal, S. and S. Srinivasan. 2016. Why the market yawned when Yahoo was hacked. *The Wall Street Journal*, Oct. 3, 2016. http://www.wsj.com/articles/why-the-market-yawned-when-yahoo-was-hacked-1475537076?mod=djemRiskCompliance.

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*, forthcoming.

Securities and Exchange Commission (SEC). 2018. Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Release Nos. 33-10459, 34-82746). Published February 21, 2018.

Silvers, R. 2016. The valuation impact of SEC enforcement actions on nontarget foreign firms. *Journal of Accounting Research* 54 (1): 187–233.

Smith, T., J. L. Higgs, and R. Pinsker. 2019. Do auditors price breach risk in their audit fees? *Journal of Information Systems*, forthcoming.

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

United States Congress (2017) The cybersecurity disclosure act of 2017, Report, https://www.congress.gov/115/bills/s536/BILLS-115s536is.pdf.

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

Zhang, B., and Z. Zhang. 2016. The spillover effect of corporate fraud: Evidence from firm level supply chain data. Working paper, University of Warwick. Available on SSRN.

Table 1
Breach Sample Composition

Panel A: Breach sample

Audit Analytics breaches disclosed between Jan. 2010 and Mar. 2018	405
Less breaches without Compustat GVKEY	(6)
Less breaches without CRSP PERMNO	(22)
Less breaches without GICS industry	(1)
Less breaches disclosed within two days of an earnings announcement	(22)
Less breaches with stock price < $1 during event window	(1)
Breaches in sample	353
Unique firms in breach sample	248

Panel B: Breach types

Audit Analytics Type	Frequency	Percent
Financial	103	29.2 percent
Personal	202	57.2 percent
Other	48	13.6 percent
Total	353	100.0 percent

Panel C: Industry distribution

GICS Sector	Frequency	Percent
10 (Energy)	7	2.0 percent
15 (Materials)	6	1.7 percent
20 (Industrials)	27	7.6 percent
25 (Consumer Discretionary)	126	35.7 percent
30 (Consumer Staples)	21	5.9 percent
35 (Healthcare)	16	4.5 percent
40 (Financials)	47	13.3 percent
45 (Information Technology)	83	23.5 percent
50 (Telecom)	15	4.2 percent
55 (Utilities)	5	1.4 percent
60 (Real Estate)	0	0.0 percent
Total	353	100.0 percent

Panel D: Year distribution

Breach Disclosure Year	Frequency	Percent
2010	17	4.8 percent
2011	22	6.2 percent
2012	35	9.9 percent
2013	37	10.5 percent
2014	53	15.0 percent
2015	43	12.2 percent
2016	60	17.0 percent
2017	73	20.7 percent
2018	13	3.7 percent
Total	353	100.0 percent

Table 2
Descriptive Statistics

Panel A: Non-breached peer sample from Table 4 (n = 11,508)

	Mean	St. Dev.	5 percent	25 percent	Median	75 percent	95 percent
BREACHNUM	1.40	1.03	0.00	0.69	1.39	2.20	3.14
COMPETITION	0.13	0.10	0.03	0.07	0.09	0.18	0.34
BREACHSIZE	7.55	2.03	4.00	6.00	9.00	9.00	9.00
SIZEDIFF	2.31	3.21	-3.00	0.00	2.00	5.00	8.00
TECHCOMM	0.06	0.25	0.00	0.00	0.00	0.00	1.00
SIZE	6.78	2.05	3.63	5.33	6.68	8.03	10.54
BTM	0.28	0.24	0.02	0.11	0.21	0.39	0.74
LEV	0.18	0.21	0.00	0.00	0.11	0.30	0.61

Panel B: Audit fee sample from Table 5 (n = 47,386)

	Mean	St. Dev.	5 percent	25 percent	Median	75 percent	95 percent
LNFEES	13.29	1.65	10.45	12.16	13.45	14.39	15.83
PEER	0.19	0.39	0.00	0.00	0.00	0.00	1.00
Lag PEER	0.17	0.38	0.00	0.00	0.00	0.00	1.00
SIZE	5.91	3.15	0.10	4.19	6.33	7.98	10.36
INVREC	0.22	0.23	0.00	0.03	0.15	0.34	0.71
SEGMENTS	1.93	3.84	1.00	1.00	1.00	1.00	10.00
FOREIGN	0.41	0.49	0.00	0.00	0.00	1.00	1.00
MERGER	0.23	0.42	0.00	0.00	0.00	0.00	1.00
SPECIAL	0.99	0.10	1.00	1.00	1.00	1.00	1.00
LOSS	0.40	0.49	0.00	0.00	0.00	1.00	1.00
GROWTH	0.00	0.00	-0.49	-0.03	0.03	0.15	0.91
BTM	0.27	0.29	0.01	0.06	0.20	0.38	0.83
BIG4	0.61	0.49	0.00	0.00	1.00	1.00	1.00
GC	0.13	0.33	0.00	0.00	0.00	0.00	1.00
INITIAL	0.11	0.31	0.00	0.00	0.00	0.00	1.00
ROA	-3.94	165.46	-2.26	-0.10	0.01	0.05	0.15
LEV	0.24	0.23	0.00	0.02	0.18	0.41	0.68
QUICK	2.70	36.65	0.00	0.12	1.05	2.09	7.75
ICMW	0.12	0.33	0.00	0.00	0.00	0.00	1.00

Panel C: Insurance firm sample from Table 6 (n = 19,917)

	Mean	St. Dev.	5 percent	25 percent	Median	75 percent	95 percent
CYBER	0.13	0.33	0.00	0.00	0.00	0.00	1.00
SIZE	8.54	1.94	5.13	7.19	8.56	9.90	11.59
BTM	0.27	0.12	0.10	0.20	0.26	0.32	0.50
LEV	0.07	0.08	0.00	0.03	0.05	0.08	0.17

This table presents descriptive statistics for the variables used in the analyses presented in Tables 4 through 7.

Table 3
Market Reaction to Breach Disclosures for Breached Firms and Non-breached Peer Firms

Panel A: Breach firm returns around breach disclosure dates

	N	Mean	Std Dev	5 percent	25 percent	Median	75 percent	95 percent
BHAR [-1, 1]	353	-17.83	289.11	-392.41	-135.96	-0.87	125.26	408.84
BHAR [-2, 2]	353	-7.12	364.72	-611.38	-165.09	4.70	177.65	541.42
BHAR [-5, 5]	353	-50.63*	529.47	-857.30	-312.55	-51.15	222.69	782.70
BHAR [-5, 10]	353	-50.11	679.12	-1142.16	-355.32	-58.22	294.46	1015.27

Panel B: Peer firm returns around breach disclosure dates

	N	Mean	Std Dev	5 percent	25 percent	Median	75 percent	95 percent
BHAR [-1, 1]	11508	-13.36***	319.18	-510.01	-180.09	-19.48	148.11	503.28
BHAR [-2, 2]	11508	-34.23***	405.99	-677.27	-244.32	-35.25	170.82	620.42
BHAR [-5, 5]	11508	-52.32***	595.91	-995.10	-368.10	-68.78	250.51	918.32
BHAR [-5, 10]	11508	-76.20***	715.42	-1240.82	-474.50	-91.35	304.88	1098.56

This table presents descriptive statistics for buy-and-hold abnormal returns in basis points (BHAR) around breach disclosure dates for breached firms (Panel A) and non-breached peer firms (Panel B). The BHAR measures are calculated for various event windows in each panel and are calculated as the buy-and-hold return for the firm minus the buy-and-hold value-weighted market return over the same event window. We perform *t*-tests to measure whether the mean of each BHAR measure is different from zero, and statistical significance is indicated by *** for $p < 0.01$, ** for $p < 0.05$ and * for $p < 0.10$ (two-tailed tests).

Table 4
Bootstrapped Peer Returns with Varying Repetitions and Observations

Panel A: Bootstrapped peer returns with varying repetitions and 353 observations per repetition

	100 repetitions	500 repetitions	1,000 repetitions	2,500 repetitions	5,000 repetitions
BHAR [-1, 1]	-13.36	-13.36	-13.36	-13.36	-13.36
BHAR [-2, 2]	-34.23	-34.23	-34.23	-34.23	-34.23
BHAR [-5, 5]	-52.32*	-52.32	-52.32	-52.32*	-52.32*
BHAR [-5, 10]	-76.20*	-76.20*	-76.20**	-76.20**	-76.20**

Panel B: Bootstrapped peer returns with varying observations and 1,000 repetitions

	353 observations	500 observations	1,000 observations	2,500 observations	5,000 observations
BHAR [-1, 1]	-13.36	-13.36	-13.36	-13.36**	-13.36***
BHAR [-2, 2]	-34.23	-34.23**	-34.23***	-34.23***	-34.23***
BHAR [-5, 5]	-52.32	-52.32**	-52.32***	-52.32***	-52.32***
BHAR [-5, 10]	-76.20**	-76.20**	-76.20***	-76.20***	-76.20***

This table presents bootstrapped *t*-tests for mean buy-and-hold abnormal returns in basis points (BHAR) around breach disclosure dates for peer firms. The BHAR measures are calculated for various event windows in each panel and are calculated as the buy-and-hold return for the firm minus the buy-and-hold value-weighted market return over the same event window. For each return window, the means reported here are identical to the means reported in Panel B of Table 3. However, we use bootstrapping with varying numbers of repetitions (Panel C) and varying observations per repetition (Panel D) to illustrate issues related to statistical power when examining breach event returns. Statistical significance is indicated by *** for $p < 0.01$, ** for $p < 0.05$ and * for $p < 0.10$ (two-tailed tests).

Table 5
Drivers of Cross-sectional Variation in the Market Response of Non-breached Peers

	(1)	(2)	(3)	(4)	(5)	(6)
BREACHNUM	19.34**					3.76
	(2.33)					(0.44)
COMPETITION		318.97***				207.46***
		(4.37)				(2.74)
BREACHSIZE			27.34***			55.50***
			(7.85)			(11.26)
SIZEDIFF				-1.92		-31.04***
				(-0.70)		(-7.90)
TECHCOMM					49.58**	41.61*
					(2.03)	(1.71)
Controls for SIZE, BTM, LEV, and Year FE	Yes	Yes	Yes	Yes	Yes	Yes
N	11,508	11,508	11,508	11,508	11,508	11,508
Adj. R-squared	0.005	0.007	0.010	0.005	0.005	0.017

This table presents results of models used to investigate cross-sectional variation in the market response of non-breached peer firms to breach disclosures. The dependent variable in each model is BHAR (-5, 10). We choose the (-5, 10) window for these cross-sectional tests because it is the only window that remains statistically significant in all of the bootstrapped variations in Table 4. BREACHNUM is the natural log of the number of breaches experienced in the particular GICS subindustry (i.e., BREACHNUM = ln(2) if the breach disclosure in question is the second breach disclosed in that GICS subindustry). COMPETITION is the Herfindahl index using sales data for all firms listed on Compustat in the year prior to the breach disclosure year. BREACHSIZE is the decile rank of the breached firm's market capitalization, where market capitalization ranks are determined each day using CRSP data. SIZEDIFF is BREACHSIZE minus the decile rank of the non-breached peer's market capitalization. TECHCOMM is an indicator = 1 if the non-breached peer firm has a technology committee in the year of the breach disclosure. Models are estimated using OLS with heteroskedasticity-robust standard errors. *t*-statistics are reported in parentheses, and statistical significance is indicated by *** for $p < 0.01$, ** for $p < 0.05$ and * for $p < 0.10$ (two-tailed tests).

Table 6
Audit Fees of Non-Breached Peer Firms

	(1)	(2)
PEER	0.063***	
	(5.781)	
Lag PEER		0.052***
		(4.293)
SIZE	0.431***	0.436***
	(90.933)	(85.113)
INVREC	0.107***	0.113***
	(3.434)	(3.409)
SEGMENTS	0.017***	0.016***
	(9.448)	(8.154)
FOREIGN	0.047***	0.040***
	(3.167)	(2.598)
MERGER	0.165***	0.161***
	(14.340)	(13.286)
SPECIAL	-0.065*	-0.063
	(-1.746)	(-1.572)
LOSS	0.101***	0.116***
	(8.369)	(8.918)
GROWTH	0.000	0.000
	(1.298)	(1.120)
BTM	-0.291***	-0.302***
	(-12.272)	(-11.883)
BIG4	0.585***	0.587***
	(33.255)	(31.413)
GC	0.104***	0.122***
	(4.386)	(4.725)
INITIAL	-0.180***	-0.153***
	(-12.075)	(-8.529)
ROA	-0.000*	-0.000*
	(-1.739)	(-1.600)
LEV	0.162***	0.122***
	(4.834)	(3.335)
QUICK	-0.000*	-0.001*
	(-1.649)	(-1.946)
ICMW	0.067***	0.072***
	(3.566)	(3.589)
CONSTANT	0.431***	0.436***
	(90.933)	(85.113)
Fixed effects for year and industry	Yes	Yes
N	47,386	38,369
Adj. R-squared	0.835	0.841

This table presents results of models used to investigate cross-sectional variation in the audit fees of non-breached peer firms to breach disclosures. The dependent variable in each model is LNFEES. PEER is an indicator variable set to one if the firm is in the same industry as a breached firm in year t, 0 otherwise. All control variables are defined in APPENDIX A. Models are estimated using OLS with heteroskedasticity-robust standard errors. *t*-statistics are reported in parentheses, and statistical significance is indicated by *** for $p < 0.01$, ** for $p < 0.05$ and * for $p < 0.10$ (two-tailed tests).

Table 7
Market Reaction to Breach Disclosures for Cyber Insurance Providers

Panel A: Non-CYBER insurance firm returns around breach disclosure dates

	N	Mean	Std Dev	5 percent	25 percent	Median	75 percent	95 percent
BHAR [-1, 1]	17372	8.29***	241.70	-346.59	-115.19	-0.80	119.12	403.87
BHAR [-2, 2]	17372	7.75***	305.61	-467.80	-151.93	-2.28	155.18	512.70
BHAR [-5, 5]	17372	-2.73	450.83	-695.44	-248.99	-21.59	222.75	739.81
BHAR [-5, 10]	17372	4.67	533.16	-817.93	-301.88	-12.06	289.85	872.93

Panel B: CYBER insurance firm returns around breach disclosure dates

	N	Mean	Std Dev	5 percent	25 percent	Median	75 percent	95 percent
BHAR [-1, 1]	2545	0.39	148.43	-233.97	-82.03	1.44	83.23	232.30
BHAR [-2, 2]	2545	2.37	194.23	-302.34	-103.46	3.86	118.01	311.57
BHAR [-5, 5]	2545	-12.14**	288.50	-491.58	-174.97	-8.20	155.45	451.47
BHAR [-5, 10]	2545	-9.56	340.98	-558.15	-216.15	-11.41	203.06	544.54

Panel C: Regression analysis comparing CYBER to non-CYBER insurance firms

	BHAR (-1, 1)	BHAR (-2, 2)	BHAR (-5, 5)	BHAR (-5, 10)
CYBER	-7.48*	-8.76	-15.60*	-16.95*
	(-1.77)	(-1.62)	(-1.95)	(-1.80)
Controls for SIZE, BTM, LEV, and Year FE	Yes	Yes	Yes	Yes
N	19,917	19,917	19,917	19,917
Adj. R-squared	0.005	0.009	0.020	0.022

This table presents descriptive statistics and panel regression analyses of the market reaction for providers of cybersecurity insurance relative to other insurance firms. The variable of interest in all panels is BHAR for various event windows relative to the breach disclosure dates for the breaches shown in Table 1. The sample is comprised of all insurance firms (firms with GICS subindustry of 40301030 or 40301040). CYBER is an indicator = 1 if the insurance firm is a significant provider of cybersecurity insurance. All models include controls for SIZE, BTM, LEVERAGE, and year fixed effects. Standard errors are heteroskedasticity-robust, and *t*-statistics are reported in parentheses. Statistical significance is indicated by *** for $p < 0.01$, ** for $p < 0.05$ and * for $p < 0.10$ (two-tailed tests).