The stock market reaction to data breaches: A stakeholder perspective

To be submitted to

Western Decision Sciences Institute Conference 2022

Digitalization efforts introduce new operational risks for firms, such as data breaches. Based on a sample of 219 firm announcements from publicly traded U.S. firms, we conduct an event study to examine the stock market reaction, finding a significantly negative reaction of -0.55% to data breaches. Our post-hoc analysis indicates a sustained negative impact on shareholder value. The negative stock market reaction is stronger when customer data is breached, the breach occurred along the supply chain, and more media attention was received. This study also adds to the emerging topics of digitalization and cybersecurity in operations and supply chain management.

Keywords: data breaches; digital risk; stock market reaction; event study

---

1 Introduction

In the wake of digitalization efforts across all industries, firms are increasingly collecting data. Leveraging employee, supplier, or customer data provides a basis for big data analytics (Song, Li, and Yu, 2021; Choi, Wallace, and Wang, 2018; Kache and Seuring, 2017), promises increased transparency (Hastig and Sodhi, 2020; Seyedghorban, Samson, and Tahernejad, 2020), streamlined processes, and optimized revenue streams (Kurpjuweit, Schmidt, Klöckner, and Wagner, 2021; Olsen and Tomlin, 2020).

On the downside, however, accelerating digitalization endeavors and the corresponding omnipresence of data entail new operational risks, pressuring operations managers to increase their sensitivity to data privacy and cybersecurity issues (Cheung, Bell, and Bhattacharjya, 2021; Massimino, Gray, and Lan, 2018). Fueled by rapid developments of digital technologies and the concurrent inattention of many organizations to data security (Sridhar, Ralph, and Copic, 2021; Massimino et al., 2018), firms are now increasingly vulnerable targets for cyber-attacks that oftentimes lead to unintentional data breaches. In fact, such data breaches were continuously growing over the last years (Gwebu, Wang, and Wang, 2018; Bourdon, 2017). Notable examples include the Sony PlayStation data breach (Goode, Hoehle, Venkatesh, and Brown, 2017), several data loss incidents at Facebook (Burt, 2019), or recent cyber-attacks at Lockheed Martin, SpaceX, and Tesla (Winder, 2020). The recent COVID-19 pandemic is expected to further exacerbate these developments, as many firms had to quickly shift to software-based remote working settings (Sharton, 2020).

While data breaches are rising in frequency and severity, they also increase in diversity, affecting multiple actors in the stakeholder ecosystem of the breached firm. Businesses are facing a growing spectrum of data breaches, varying in the breached data type (e.g., financial, identity), the data owner (e.g., employee, customer, supplier), or the point of attack. Referred to as supply chain breaches, the latter relate to incidents where the entry point of the cyber-attack is not the breached firm itself, but a third party, such as a supplier or an IT service provider. As attackers intentionally target the weakest point of connected supply chains, this phenomenon becomes increasingly pervasive, forcing firms to rethink their IT security strategy beyond their own boundaries (Stupp, 2019). Recent estimations reveal that approximately half of today's data breaches can be traced back to supply chain attacks (Armerding, 2019), and this share is expected to grow further (ENISA, 2021). Prominent examples include A.P. Møller-Maersk, facing breach-related costs of $300 million due to a cyber-attack at a small supplier (Columbus, 2019), or retailer Target, which lost millions of financial customer records after an air conditioning contractor had been hacked (Armerding, 2019).

Despite these severe consequences, only a limited body of academic studies across disciplines has already examined data breaches. For instance, Janakiraman, Lim, and Rishika (2018) demonstrate that data breaches result in a decline of customer spending and pressure customers to shift to unbreached retailer channels. Taking a different perspective, Goode et al. (2017) conduct a longitudinal field study of a single-case data breach, the Sony PlayStation network breach. They find, among other things, that post-breach compensation has a positive effect on customer continuance and repurchase intention. Further empirical studies examine the relationship between data breaches and stock market performance, finding largely negative implications for shareholder value (Gwebu et al., 2018; Martin, Borah, and Palmatier, 2017; Modi, Wiles, and Mishra, 2015; Malhotra and Kubowicz Malhotra, 2011). In addition, Modi et al. (2015), for instance, find the stock market reaction to be more negative for breaches due to front-end IT outsourcing. Gwebu et al. (2018) further explore different response strategies to data breaches, emphasizing the mitigating potential of moderate and image renewal response strategies.

The purpose of this study is to extend the literature on data breaches, identifying a set of factors that moderate the negative impact of data breach announcements on shareholder value. This may help firms to better understand and mitigate potentially negative financial consequences of data breaches as increasingly important operational risks. Against this backdrop, we take a stakeholder perspective to identify and empirically assess the influence of several stakeholder groups on the shareholder value impact of the breached firm (Donaldson and Preston, 1995; Freeman, 1984).

Based on a sample of 219 data breach announcements of publicly traded U.S. firms, we use an event study design to empirically assess the shareholder value implications of data breaches. Establishing a baseline for our moderation analysis and confirming prior work (e.g., Martin et al., 2017; Modi et al., 2015), we find that data breach announcements entail a significant negative mean abnormal return of -0.55% on the announcement date and the following trading day. We further show that the negative stock market reaction is stronger when customer data is involved, when external parties are responsible for the data breach, and for firms that receive greater media attention. We augment our analysis with multiple robustness and sensitivity checks, and extend the scope of our stakeholder perspective in two post-hoc analyses, exploring competition spillovers and long-term effects of data breaches.

Beyond our contribution to the interdisciplinary literature stream on data breaches (e.g., Gwebu et al., 2018; Martin et al., 2017; Modi et al., 2015), our findings also add to the emerging literature on digitalization in operations and supply chain management (Olsen and Tomlin, 2020; Li, 2020).

As such, we introduce data breaches as increasingly important operational risks and identify the stakeholder factors shaping the negative financial impact for firms, extending the body of research that emphasizes emerging risks that come along with operations and supply chain digitalization (Son, Kim, Hur, and Subramanian, 2021; Cheung et al., 2021; Massimino et al., 2018).

2 Theoretical Background and Hypotheses Development

2.1 A Stakeholder Perspective on Data Breaches

In this empirical study, we take a stakeholder perspective to extend the knowledge on the consequences and moderation factors of data breaches. Originating from Freeman (1984), the stakeholder management literature defines a stakeholder as a group or individual, "who can affect or [are] affected by the achievement of the organization's objectives" (p. 46). Consistent with this definition, typical stakeholders of a firm are investors or shareholders, customers, employees, supply chain partners, or communities (Donaldson and Preston, 1995). Stakeholders may be internal or external, and hold different positions in the strategic setting of the focal firm. Against this backdrop, employees, customers, or shareholders constitute the *resource base*, supply chain partners or trade associations the *industry structure*, and communities or the government the *social political arena* of the firm (Post, Preston, and Sachs, 2002).

In contrast to the neoclassical maxim, according to which firms should only address the needs of their shareholders, stakeholder theory implies that firms must go beyond the mere maximization of shareholder value, serving the needs of various stakeholder groups to create competitive advantage (Donaldson and Preston, 1995; Jones, 1995; Freeman, 1984). In other words, firms that practice active stakeholder management by aligning different interests and building sustainable and trustworthy relationships will benefit from superior performance (Post et al., 2002; Clarkson, 1995; Donaldson and Preston, 1995). Barney (2018), for instance, conceptually demonstrates that a pure shareholder focus logic is flawed, arguing that firms in competitive settings must recognize and address different stakeholder needs to secure crucial resources, which are essential to generate profits.

Our empirical context, data breaches, provides an illustrative example of how different stakeholder requirements need to be addressed. Hence, alike previous empirical work (e.g., Kim, Wagner, and Colicchia, 2019; Longoni and Cagliano, 2018), we take a stakeholder perspective to examine our phenomenon of interest. Our conceptual model is depicted in Figure 1, suggesting that our primary baseline effect is a negative association between data breach announcements and the focal firm's shareholder value (Hypothesis 1). In a subsequent step, we argue for moderating effects that are

related to stakeholder groups others than shareholders and investors. We consider stakeholders in different positions across the firm's strategic setting, such as the resource base (e.g., shareholders, Hypothesis 1; customers, Hypothesis 2), the industry structure (e.g., supply chain partners, Hypothesis 3), and the social political arena (e.g., the media, Hypothesis 4; government, Hypothesis 5).

2.2 Shareholder Value Effects

Historically, shareholders were considered the primary stakeholders of a firm, characterized by maximum claims on the firm's profits (Barney, 2018; Jensen, 2001). Though the dominance of shareholder interests has decreased, shareholders are still a particularly crucial group of stakeholders, constituting the resource base of the firm by providing equity capital (Post et al., 2002; Jones, 1995). The influence of shareholders is substantial, and also reflected in the law in form of obligations (Jones, 1995; Clarkson, 1995).

Given the justified economic interest of shareholders in the financial performance of the firm, it is conceivable that shareholders react to specific firm events that expectedly affect the firm's financial situation (Lo, Tang, Zhou, Yeung, and Fan, 2018; McWilliams and Siegel, 1997). Data breaches clearly are such events, and have become an increasingly important operational risk for firms. Data breaches are associated with substantial costs for firms, which can be both direct and indirect. Direct costs, for example, include necessary IT investments to adjust and safeguard the weak point in the IT infrastructure, legal penalties, or administrative processing costs (Jain and Ropple, 2018). Indirect costs, in contrast, relate to reputation damage, and consequential decreases in customer spending (Janakiraman et al., 2018). In the Sony PlayStation data breach case, for instance, direct costs were $171 million, while indirect costs, arising from adverse publicity and negative customer sentiment, were estimated to more than $1 billion (Goode et al., 2017).

Previous empirical research is consistent with these arguments, demonstrating that data breaches are associated with reduced customer spending (Janakiraman et al., 2018), direct costs (Goode et al., 2017), and drops in shareholder value (Martin et al., 2017; Modi et al., 2015). For instance, Modi et al. (2015) show that data breach announcement entail a negative short-term stock market reaction. More recently, Martin et al. (2017) and Gwebu et al. (2018) confirm this effect.

Taking up the anecdotal evidence and the findings of these studies, we argue that shareholders anticipate the additional direct and indirect costs associated with a data breach, and adjust their estimation of expected cash flows accordingly. As a key stakeholder group, we expect shareholders to hold the firm accountable for a data breach, manifested in a negative stock market reaction. Hence, as the baseline for this study, we formulate the following hypothesis:

Hypothesis 1 *Data breach announcements are associated with a negative stock market reaction.*

2.3 Moderating Stakeholder Effects

Taking up a stakeholder perspective, we argue that the severity of the negative stock market reaction to data breach announcements depends on specific characteristics of the data breach setting, defined by different stakeholders of the breached firm. In the following, we provide arguments on how these characteristics moderate the stock market reaction.

As data breaches increase in diversity, many different data types and owners are affected. Data owners may include firm-internal stakeholders, such as employees, or firm-external stakeholders, such as business partners (e.g., suppliers) or customers. Customers are an important external stakeholder for all businesses, constituting a crucial part of the firm's resource base, and consequently considered one of the primary stakeholders of any firm (Post et al., 2002; Clarkson, 1995). Customers dominantly shape firm reputation and brand loyalty, both directly affecting sales, and hence the performance bottom line of the firm (Post et al., 2002). Clearly, customer satisfaction and customer value are established drivers of competitive advantage (Payne, Frow, and Eggert, 2017). However, both customer satisfaction and customer value, in turn, are increasingly determined by digitalization endeavors and data-based business models, where market and customer data are extensively used to co-create value with downstream customers (Kohtamäki, Parida, Patel, and Gebauer, 2020).

At the same time, customers are becoming more sensitive about data privacy issues (Martin et al., 2017). For example, a recent survey of more than 2,500 adults shows that approximately one third of all respondents care about data privacy and have already switched service providers or firms due to data-related policies and incidents (Redman and Waitman, 2020). In addition, firms are increasingly overwhelmed by the complexity of customer data interfaces and the corresponding legislation, further fueling the development of increasing customer sensitivity (Kamleitner, Mitchell, Stephen, and Kolah, 2018).

Recent legislation efforts, for instance the EU General Data Protection Regulation (GDPR), have put substantial fines on the loss of customer data, driving the direct costs associated with a data breach for firms (Kamleitner et al., 2018). Even more importantly, it seems reasonable to assume that there are higher indirect costs when customer data is involved in the data breach. If customer data are put at risk, we argue that the corresponding reputation damage entails reduced sales due to negative customer sentiment. Previous research has also revealed that data breaches create customer vulnerability, which negatively affects financial firm performance (Martin et al., 2017). Hence, we posit as follows:

Hypothesis 2 *The negative stock market reaction to data breach announcements is stronger when the data breach involves customer data.*

Suppliers and service providers, among others, constitute the industry structure of a firm, corresponding to important stakeholder groups (Post et al., 2002). Recently, the phenomenon of supply chain breaches (or supply chain attacks), in which suppliers, service providers, or other external parties are targeted vehicles to gain access to data of the focal firm, has become increasingly dominant. The European Union Agency for Cybersecurity (ENISA) considers supply chain attacks as an increasing operational risk for firms, stating that these data breach types have exploded in frequency and increased in sophistication (ENISA, 2021). Based on four arguments, we expect supply chain breaches to receive a more pronounced negative stock market reaction.

First, supply chain breaches are likely associated with greater operational costs, due to a higher number of involved organizations, resulting in more interactions, coordination, and diagnosis or recovery activities (Modi et al., 2015; Craighead, Karwan, and Miller, 2004). Furthermore, due to the inter-organizational integration of IT architectures, such data breaches can also induce cascading effects along the supply chain or a firm's general business ecosystem (ENISA, 2021). This may also drive the overall direct costs associated with the data breach.

Second, supply chain breaches are an indication of elevated inter-organizational complexity, which demands more advanced data security strategies, beyond the boundaries of the focal firm. While data security generally improved over the last years, attackers successfully targeted the remaining weak points of interconnected supply chains, which could be suppliers or other external parties (ENISA, 2021; Armerding, 2019). Against this backdrop, firms are justifiably perceived as vulnerable, despite having potentially robust own data security structures (ENISA, 2021).

Third, customers might view a supply chain breach as a signal that the firm shares potentially sensitive data with multiple other organizations (Modi et al., 2015). As customers are increasingly sensitive towards data privacy, this may negatively affect customer sentiment, which in turn results in reduced sales and future cash flows.

Finally, from a stakeholder management perspective, it seems conceivable that supply chain breaches negatively affect the relationship between the focal firm and the stakeholders that are involved in the data breach. Once trustful relationships may turn into purely operational or even opportunistic relationships, contrary to fruitful stakeholder management (Post et al., 2002; Jones, 1995). Hence, taken together, we formulate the following hypothesis:

Hypothesis 3 *The negative stock market reaction to data breach announcements is stronger when*

the data breach is a supply chain breach.

The media is a powerful stakeholder from the social political arena, and has been shown to mobilize public opinion and affect a firm's behavior (Shipilov, Greve, and Rowley, 2019; Kim et al., 2019; Donaldson and Preston, 1995). In contrast to primary stakeholders like customers or investors, the media is considered a secondary stakeholder, which may influence, but is not engaged in transactions with a firm (Clarkson, 1995).

While firms are operating under continuous public scrutiny, it seems also clear that the media attention, reflecting the intensity of this public scrutiny, greatly varies between firms. During adverse events such as data breaches, increased public scrutiny may exacerbate the already negative perception of the affected firm. Oftentimes, media coverage draws elevated attention to adverse firm events, and shapes the perception of communities and other stakeholders, which can cause substantial (reputational) damage to a firm (Vanacker, Forbes, Knockaert, and Manigart, 2020; Wiersema and Zhang, 2013; Clarkson, 1995).

Multiple studies have demonstrated the major role of media attention for firm behavior and resulting performance implications. For instance, Liu and Shankar (2015) show that consumers, as primary stakeholders, react more negatively to product recalls that received more media attention. Likewise, Shipilov et al. (2019) find direct and indirect media pressure to affect the adoption of governance practices, while Jeong and Kim (2019) show that both positive and negative publicity explain firm spending for legitimacy management. In the empirical context of data breaches, we expect that the media similarly influences stakeholder perceptions, reflected in a more negative stock market reaction:

Hypothesis 4 *The negative stock market reaction to data breach announcements is stronger when the breached firm receives more media attention.*

Institutions, such as government agencies, are stakeholders operating in the social political arena of a firm (Post et al., 2002). Such public stakeholders provide infrastructure, enforce laws and regulations, and claim taxes or other obligations (Clarkson, 1995). Given these interdependencies, it seems evident that good relationships between, for instance, government agencies and firms are essential.

Such interdependencies are likely even more prevalent when institutions hold shares of the focal firm. As such, the underlying ownership structure of a firm not only influences its performance, but also affects its interactions with stakeholders, particularly shareholders (Gupta, Crilly, and Greckhamer, 2020). Increased institutional ownership in a firm relates to a higher degree of effective

control over the firm (Gupta et al., 2020), which might be beneficial during adverse events like data breaches, and potentially sends reassurance signals to investors.

Furthermore, consistent with the argumentation of Lo et al. (2018), we expect a higher degree of institutional ownership, particularly government ownership, to be associated with a higher likelihood of financial and legal support in the context of adverse incidents like data breaches. Since the interests between the firm and government institutions are better aligned by the presence of equity stakes, government agencies may be more likely to support the diagnosis of and recovery from data breaches more effectively. Furthermore, institutional investors like government agencies are less likely to promptly withdraw and sell shares after negative incidents. In quite contrast, it seems more reasonable to do the opposite, providing additional financial support through higher equity stakes. Consequently, to summarize, we argue that institutional ownership might function as a buffer during data breach incidents, mitigating the negative stock market reaction. Our hypothesis is as follows:

Hypothesis 5 *The negative stock market reaction to data breach announcements is weaker when the share of institutional ownership in the breached firm is higher.*

3 Research Method

3.1 Sample Construction

We obtain a list of firms that have experienced data breaches from the Identity Theft Resource Center (ITRC) database.[1] The ITRC is a widely recognized non-profit organization, transparently reporting data breaches in the U.S. since 2005, and it has been used as a data resource in previous empirical studies (e.g., Modi et al., 2015). In this study, we follow the ITRC in defining a data breach as an incident, in which an individual's name plus confidential information, such as social security number, medical record, or financial details, are put at risk due to exposure (ITRC, 2019). All data breach events are published along with corresponding announcement texts from various media or governmental sources, including detailed information on the data breach type, the affected company, and the announcement date.

We restrict our data breach sample to a five-year period between January 2014 and December 2018. We identify a total of 2,506 data breaches in the ITRC category "business" (i.e., not considering data breaches from public authorities, military, private healthcare institutions etc.). From these, enabling us to examine the stock market reaction to data breaches, we only include publicly traded U.S. firms on the New York Stock Exchange (NYSE) and the NASDAQ (Schmidt, Wuttke, Ball, and

[1] https://www.idtheftcenter.org/

Heese, 2020). This process leaves us with 267 potential data breach events. We further eliminate 33 events of firms with insufficient financial data available in the Thomson Reuters Eikon database. In a final step, ensuring the isolation of the data breach as our effect of interest, we remove 15 events with confounding information (e.g., announcements of quarterly earnings, lawsuits, or dividends) within a two-day period surrounding the announcement date (Modi et al., 2015; MacKinlay, 1997).

Consequently, our final sample comprises 219 data breach events from 165 unique firms. Table 1 presents the distribution of our sample event across announcement years (Panel A) and industries (Panel B). As indicated by our temporal sample distribution, we note that data breaches are increasing in frequency over the years, with 37 events (17%) in 2014 and 51 (23%) in 2018 (see Panel A in Table 1). From an industry perspective, most data breaches relate to the Consumer Discretionary sector (57, 26%), followed by Industrials (40, 18%), and Communication Services (30, 14%) (see Panel B in Table 1). Alike prior work, we follow the commonly applied Global Industry Classification Standard (GICS)[2] (e.g., Bellamy, Dhanorkar, and Subramanian, 2020; Hwang, Liberti, and Sturgess, 2019).

3.2 Measurements

We consider a number of variables to assess the moderating stakeholder effects of the stock market reaction to data breach announcements. Table 2 presents an overview of all measures.

3.2.1 Hypothesized Variables

To examine whether *customer data breached* affects the stock market reaction to data breaches, we coded the announcement texts based on the type of the data breached. We created a dummy variable equaling 1 when customer-specific data (e.g., name, address, social security number), in contrast to employee or business partner data, was put at risk. Likewise, we assessed our sample announcement texts with regard to the point of origin of the data breach. Specifically, we coded the variable *supply chain breach* as 1 when the breach was due to a third-party, such as a supplier or service provider.

As we are further interested in the role of the general public as an important stakeholder, we measure *media attention* based on a ratio of news wire hits and firm size during the one-year period prior to the data breach event. Finally, we use the share of strategic long-term shareholders, especially government institutions, to proxy the *institutional ownership* in the breached firm.

[2]https://www.msci.com/our-solutions/indexes/gics

3.2.2 Control Variables

In line with previous event studies, we control for the effects of key breach-, firm-, industry-, and time-factors. As it is conceivable that investors react differently when *financial data* is *breached*, we consider a dummy variable capturing whether the data breach involves financial information, such as a credit card or bank account number (Malhotra and Kubowicz Malhotra, 2011). We further control for key firm financials. As such, we control for *firm size*, measured as the natural logarithm of total assets (Jacobs and Singhal, 2014). Assessing potential under- or overvaluation of a certain stock, we also include the *market-to-book ratio* as a firm-level control (Gwebu et al., 2018). Likewise, we consider the financial *leverage* to account for differences in firms' capital structure (Hendricks, Hora, and Singhal, 2015; Fama and French, 1993). Finally, we include *year* and *industry dummies* to capture temporal and industry effects that may affect the stock market reaction (Bose and Leung, 2019; Modi et al., 2015). Table 3 presents descriptive statistics for all hypothesized and control variables.

3.3 Data Analysis

We follow a two-step procedure to test our hypothesized relationships. First, assessing the shareholder value effects of data breach announcements (Hypothesis 1), we conduct an event study. Second, we estimate a set of random effects regression models to test the moderating stakeholder effects (Hypotheses 2–5).

3.3.1 Event Study Analysis

A short-term event study is an efficient approach to measure the stock market reaction to discrete events (MacKinlay, 1997; Brown and Warner, 1985). The method relies on the assumption of an efficient market, in which publicly available information are instantaneously absorbed by stock prices (Dam and Petkova, 2014; Brown and Warner, 1985). Event studies have been frequently applied and validated in empirical operations management, for instance to examine the shareholder value effects of sustainability programs (Dam and Petkova, 2014), environmental incidents (Lo et al., 2018), or 3D printing (Lam, Ding, Cheng, and Zhou, 2019). Kothari and Warner (2006) and MacKinlay (1997) provide excellent summaries on the event study method.

In our empirical context, the method allows us to quantify the implications of data breach announcements (i.e., our event of interest) for firms' shareholder value. As such, the event study procedure requires to compute *abnormal returns*, which are defined as the difference between observed (raw) stock returns and expected returns (Xiong, Lam, Kumar, Ngai, Xiu, and Wang, 2021;

MacKinlay, 1997). To facilitate the handling of stock market data, we first translate calendar days into trading days, where Day 0 is the day of the data breach announcement, Day -1 the prior trading day, Day 1 the subsequent trading day, and so forth. Announcements on non-trading days (e.g., weekend days or public holidays) were shifted to the following trading day (Hendricks et al., 2015). We estimate expected returns (i.e., returns that we would have expected in the absence of the event of interest) using the commonly applied Fama-French four-factor model (Fama and French, 1993; Carhart, 1997),

$$R_{it} = \alpha_i + \beta_i R_{mit} + \gamma_i SMB_{it} + \delta_i HML_{it} + \theta_i UMD_{it} + \varepsilon_{it}, \tag{1}$$

where R_{it} is the observed (raw) return for stock i on day t, R_{mt} is the U.S. market return, proxied by the S&P 500 Index on day t, SMB_{it} is the small-minus-big-size portfolio return for stock i on day t, HML_{it} is the high-minus-low-book-to-market portfolio return for stock i on day t, UMD_{it} is the momentum factor, introduced by Carhart (1997), for stock i on day t, α_i, β_i, γ_i, δ_i, and θ_i are linear regression coefficients, and ε_{it} is the residual error. Consistent with previous work (e.g., Liu, Wei, Si, Xie, and Chen, 2020; Modi et al., 2015), we run an ordinary least squares (OLS) regression over a period of 200 trading days, with an offset of 10 trading days prior to the announcement date. We then use the resulting estimators $\hat{\alpha}_i$, $\hat{\beta}_i$, $\hat{\gamma}_i$, $\hat{\delta}_i$, and $\hat{\theta}_i$ to calculate the abnormal returns AR_{it} as the difference between observed and expected returns,

$$AR_{it} = R_{it} - E(R_{it}) = R_{it} - (\hat{\alpha}_i + \hat{\beta}_i R_{mt} + \hat{\gamma}_i SMB_{it} + \hat{\delta}_i HML_{it} + \hat{\theta}_i UMD_{it}). \tag{2}$$

We then average the abnormal returns for day t, yielding the mean abnormal abnormal return $\overline{AR}_t$ as given by,

$$\overline{AR}_t = \frac{1}{N} \sum_{i=1}^{N} AR_{it}. \tag{3}$$

We also compute cumulative abnormal returns over a given window (t_1, t_2) by aggregating abnormal returns,

$$CAR_{i,(t_1,t_2)} = \sum_{t=t_1}^{t_2} AR_{it}. \tag{4}$$

Consistent with the computation of the mean abnormal return, the mean cumulative abnormal return over the period (t_1, t_2) is then given by,

$$\overline{CAR}_{(t_1,t_2)} = \frac{1}{N} \sum_{i=1}^{N} CAR_{i,(t_1,t_2)}. \tag{5}$$

As mean (cumulative) abnormal returns might be disproportionately affected by outliers, we further compute and report the median and the percentage of negative (cumulative) abnormal returns (Liu et al., 2020; Modi et al., 2015).

Assessing the statistical significance of the mean abnormal return, we follow previous literature and compute the event study-specific t-test statistic TS_t for day t as follows (Hendricks et al., 2015),

$$TS_t = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} \frac{AR_{it}}{\hat{\sigma}_{\varepsilon_{it}}}, \tag{6}$$

where $\hat{\sigma}_{\varepsilon_{it}}$ is the estimated standard error from Equation (1), divided to get the standardized abnormal return (Hendricks et al., 2015). Similarly, the test statistic can be derived for the mean cumulative abnormal return over the multiple-day period (t_1, t_2),

$$TS_{(t_1,t_2)} = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} \frac{AR_{it}}{\sqrt{\sum_{t=t_1}^{t_2} \hat{\sigma}^2_{\varepsilon_{it}}}}. \tag{7}$$

For the median (cumulative) abnormal return, we implement commonly used nonparametric Wilcoxon signed rank tests (e.g., Liu et al., 2020; Hendricks et al., 2015), which rely on the rank distribution of abnormal returns on day t. We test the percentage of negative abnormal stock returns applying the generalized sign test (Cowan, 1992). While a standard binomial sign test assumes a 50% benchmark for abnormal returns, the generalized sign test tests against the stock-specific share of negative abnormal returns during the respective estimation period (Brandon-Jones, Dutordoir, Neto, and Squire, 2017).

3.3.2 Regression Analysis

To test Hypotheses 2–5, we estimate random effects regression models (e.g., Schmidt et al., 2020). This model specification allows us to account for the panel structure of our sample, as 32 of our 165 unique firms have experienced more than one data breach (Martin et al., 2017). Specifically, we regress the cumulative abnormal return on Day 0 and Day 1 on our set of hypothesized and control variables for our full sample of $N = 219$ data breach announcements,

$$\begin{aligned} CAR_{ij,(0,1)} = {} & \beta_1 + \beta_2 CUSTOMER_{ij} + \beta_3 SCBREACH_{ij} + \beta_4 MEDIA_{ij} + \beta_5 INSTOWNER_{ij} \\ & + \beta_6 FINANCIAL_{ij} + \beta_7 FIRMSIZE_{ij} + \beta_8 MTB_{ij} + \beta_9 LEVERAGE_{ij} \\ & + \beta_{10-13} YEAR_{ij} + \beta_{14-20} INDUSTRY_{ij} + u_i + w_{ij}, \end{aligned} \tag{8}$$

where j denotes the data breach announcement for every firm i, and β_{1-20} are the regression coefficients for all covariates, defined in Table 2. We sequentially add the hypothesized variables to the regression model and report all interim estimates. To assess the significance of the coefficients, two-tailed t-tests with robust standard errors are used.

4 Empirical Results

4.1 Event Study Results

In Hypothesis 1, we argue for a negative stock market reaction to data breach announcements. Table 4 presents the corresponding event study results for a five-day event window surrounding the data breach announcement date (Modi et al., 2015; Kalaignanam, Kushwaha, Steenkamp, and Tuli, 2013). As indicated by Columns 3 and 4, there is a significantly negative stock market reaction on the announcement date (Day 0) and the following trading day (Day 1). On Day 0, the mean (median) abnormal return is -0.23% (0.02%), statistically significant at the 5% (10%) level ($t = -1.80$, $p < 0.05$; $Z_{Wilcoxon} = -1.54$, $p < 0.10$). On the following day, these metrics further decrease, as our sample firms experience a mean (median) abnormal return of -0.32% (-0.18%) ($t = -3.04$, $p < 0.01$; $Z_{Wilcoxon} = -2.22$, $p < 0.05$). Aggregating Day 0 and Day 1, we see a significantly negative mean (-0.55%, $t = -3.42$, $p < 0.01$) and median (-0.24%, $Z_{Wilcoxon} = -3.01$, $p < 0.10$) cumulative abnormal return, equating to an average loss of approximately $208 million in shareholder value. Furthermore, as indicated by Column 6, 57.53% of all sample firms experience a negative cumulative abnormal return during the announcement date and the following trading day ($Z_{Generalized} = 2.07$, $p < 0.05$). Collectively, these results confirm Hypothesis 1.

4.2 Regression Results

In Hypotheses 2–5, we propose several moderating stakeholder effects. Table 5 provides pairwise correlation coefficients between our dependent variable, the cumulative abnormal return in the (0,1) period, and all explanatory variables. Table 6 presents the estimation results from Equation (8). Column 1 shows a control model, Columns 1–4 all interim regression models with sequentially added hypothesized effects, and Column 5 the full model including all hypothesized and control variables. We note that all variance inflation factors (*VIFs*) are well below the threshold of 2, which suggests that our estimation results are not affected by multicollinearity issues (Modi et al., 2015; Kutner, Nachtsheim, Neter, and Li, 2005).

In support of Hypothesis 2, the coefficient of our *customer data breached* dummy variable is statistically significant across all models ($\beta_2 = -0.007$, $p < 0.10$, Column 5), emphasizing the

sensitive role of customer-related data in breach incidents. We further predicted the negative stock market reaction to be stronger when the data breach is a *supply chain breach*, as argued for in Hypothesis 3. Our results strongly support this effect ($\beta_3 = -0.008$, $p < 0.05$, Column 5). Likewise, we find the negative stock market reaction to be significantly more negative when the breached firm receives more *media attention*, consistent with Hypothesis 4 ($\beta_4 = -0.008$, $p < 0.05$, Column 5). Finally, we argue that *institutional ownership*, proxying the role of the government, may mitigate the negative effect on a firm's shareholder value, functioning as a buffer during adverse events like data breaches. However, Hypothesis 5 cannot be supported by our analysis ($\beta_5 = -0.004$, *ns*, Column 5).

5 Robustness and Sensitivity of Results

5.1 Sample Selection

Our sample consists of firms experiencing data breaches. Arguably, being affected by a data breach is not exogenous, but most likely dependent on certain firm characteristics. As a result, our sample is (per definition) constructed by a non-random self-selection process, which may introduce endogeneity issues (Boyd, Kannan, and Slotegraaf, 2019; Modi et al., 2015; Heckman, 1979). To assess and account for the risk of a potential sample selection-induced endogeneity bias, we use two empirical strategies, a propensity score matching (PSM) approach and a two-stage Heckman model (Xiong et al., 2021; Dam and Petkova, 2014; Heckman, 1979).

5.1.1 Propensity Score Matching

Consistent with prior work (e.g., Xiong et al., 2021; Boyd et al., 2019; Modi et al., 2015), we implement PSM, introduced by Rosenbaum and Rubin (1983), to identify a set of control firms, which match our sample firms in key characteristics, but did not announce a data breach during the event period. Following the approach of Hendricks et al. (2015), we then use these control firms to construct a benchmark, as an alternative abnormal return computation.

Consistent with our main sample construction approach, we consider all NYSE- and NASDAQ-listed U.S. firms as potential matching candidates. We use logistic regression (logit) models to estimate *propensity scores*, representing the likelihood of belonging to our sample, given a set of observable firm factors. Instead of estimating a pooled logit model over the whole period covered, we follow prior recommendations and estimate cross-sectional logit models per announcement year (Boyd et al., 2019; Hendricks et al., 2015). We consider the key firm financial controls from our main model, *firm size*, *market-to-book* ratio, and *leverage*, as well as the *industry* affiliation as matching

variables, yielding the following logit equation for each announcement year,

$$P(Sample = 1 \mid X) = \Lambda(\gamma_1 + \gamma_2 FIRMSIZE_i + \gamma_3 MTB_i + \gamma_4 LEVERAGE_i + \gamma_{5-14} INDUSTRY_i + u_i), \tag{9}$$

where X denotes the set of explanatory variables and γ_{1-14} are the regression coefficients based on a maximum likelihood estimation approach. $\Lambda(X'\gamma)$ is the logistic regression function, defined by $\Lambda(X'\gamma) = \frac{exp(X'\gamma)}{1+exp(X'\gamma)}$. Appendix Table A1 presents the estimates of all cross-sectional logit models. To construct the control group, we use the logit predictions and apply nearest neighbor matching with replacement based on the predicted propensity scores. We use the five nearest neighbors for each sample observation within the same four-digit GICS industry (Hendricks et al., 2015). Descriptive statistics for our sample firms and their matches are comparatively displayed in Appendix Table A2.

Analogous to Hendricks et al. (2015), we then use the equally-weighted mean abnormal returns of the five nearest neighbor firms as benchmark portfolio returns for the computation of abnormal returns, instead of expected returns based on the Fama-French four-factor model as outlined in Section 3.3.1. Appendix Table A3 presents the event study results for this alternative approach, indicating structural consistency with our main results (see Table 4 for comparison). Collectively, this robustness check suggests that our event study results may not be biased by sample selection.

5.1.2 Heckman Two-Step Model

We further estimate a two-stage Heckman model to assess the risk of sample selection-induced endogeneity issues for our moderating regression analysis (Boyd et al., 2019; Dam and Petkova, 2014; Heckman, 1979). In a first step, the Heckman procedure requires the estimation of a probit regression, modeling the likelihood of a data breach, based on a combined sample of breached- and non-breached firms. In the second step, the main effects can then be re-estimated while correcting for a potential sample selection bias considering the *Inverse Mills Ratio* (*IMR*) (Hendricks et al., 2015).

To construct the combined sample for the first-stage probit regression, we deploy a one-to-one matching of our sample observations with the nearest neighbors obtained from the PSM approach described previously (see Section 5.1.1), resulting in first-stage sample of 438 observations. Considering the key firm financial controls from our main model, as well as industry and year effects, we

estimate the following probit equation,

$$P(data\ breach\ = 1 \mid X) = \Phi(\delta_1 + \delta_2 FIRMSIZE_i + \delta_3 MTB_i + \delta_4 LEVERAGE_i + \delta_{5-8} YEAR_i + \delta_{9-18} INDUSTRY_i + \varepsilon_i), \tag{10}$$

where the δ_{1-18} are the regression parameters from a maximum likelihood estimation. Column 1 of Appendix Table A4 presents the resulting probit estimates. We use these estimates to compute the *IMR*, given by $\phi(X_1'\hat{\delta})/\Phi(X_1'\hat{\delta})$, with X_1' being the vector of explanatory variables from the first-stage probit regression and ϕ (Φ) denoting the probability (cumulative) density function of the standard normal distribution. We then use the IMR_i as an additional regressor in our main model (Equation 8), correcting for a potential sample selection bias. Column 2 of Appendix Table A4 presents the second-stage regression results considering the IMR_i, based on our main sample of 219 data breach announcements. All moderating effects are consistent with our original results and the IMR_i is insignificant ($p = 0.82$), providing strong support that sample selection does not introduce endogeneity issues (Hendricks et al., 2015).

5.2 First Data Breaches

In our sample, 32 out of 165 unique firms announce more than one data breach during our data collection period. It may be conceivable that subsequent data breach announcements are valued structurally different on the stock market, potentially biasing our findings. To assess the consequence of a potential bias, we consider only the first data breach announcement of each sample firm, reducing the sample size from 219 to 165 announcements. We then re-evaluate our event study results and the regression estimates based on this sample. Appendix Table A5 presents the event study results, which are structurally similar to our original results. The re-estimation of the regression models portrays a comparable pattern. As illustrated in Appendix Table A6, all hypothesized effects are consistent with our original results. Collectively, this robustness check strongly supports the validity of our main findings.

5.3 Alternative Expected Return Models

Short-term event studies structurally rely on the estimation of expected returns, which provide a benchmark for the actually observed firm returns to compute abnormal returns. However, the estimation of expected returns depends on certain design choices, most importantly the selection of the underlying expected return model. In this study, we use the most advanced and commonly applied Fama-French four-factor model (Xiong et al., 2021; Modi et al., 2015; Fama and French,

1993; Carhart, 1997). To explore the sensitivity of our results to this particular design choice, we also compute abnormal returns based on alternative approaches, the Fama-French three-factor model, the simple market model, the mean-adjusted model, and the market-adjusted model (e.g., Xiong et al., 2021; Brandon-Jones et al., 2017). Appendix Table A7 presents the corresponding event study results for the four alternative approaches, indicating that our findings are most likely not driven by the choice of the expected return model, as all approaches show consistent abnormal return metrics.

5.4 Outlier Analysis

In a final robustness check, we evaluate the influence of outliers on our regression estimates. This is particularly important as we partially work with secondary data from large accounting databases like Thomson Reuters. Exploring the sensitivity of our regression estimates to outliers, we re-estimate our main models using 1%-winsorized versions of the measures that are based on raw financial or accounting data. Appendix Table A8 presents the corresponding regression estimates. As indicated by Column 5 (Model 4), the results are consistent with our original findings, suggesting that the risk of outliers driving our results is reasonably low.

6 Post-hoc Analyses

6.1 Competition Spillover Effects

In the universe of potential firm stakeholders, competitors are usually excluded (Post et al., 2002; Donaldson and Preston, 1995). This is reasonable, as stakeholders usually show an interest in the economic benefit of the firm, making the relations between a firm and its competitors usually structurally different (Post et al., 2002). Quite contrary, competitors may even gain (competitive) advantage, when the firm is not successful (Donaldson and Preston, 1995).

Given our specific context of data breaches, it might be conceivable that competitors even benefit from the data breaches of their rivals. In a first post-hoc analysis, we explore this facet. To assess whether the data breaches of our sample firms induce positive spillover effects for competitors, we first construct a sample of suitable rival firms. We identify competitors following a PSM approach based on the matching variables described in Section 5.1.1, and take the propensity score-based nearest neighbor of each sample firm observation within the same, most-granular sub-industry level (8-digit GICS). We then conduct an event study for the competitor sample, using the corresponding data breach announcement dates of our sample firms. For the event study, we follow the procedure described in Section 3.3.1. Table 7 presents the event study results for the competitors. However,

we cannot find any evidence for positive competition spillover effects, contrary to previous research (Martin et al., 2017).

A potential explanation might rely on a competing mechanism, according to which firm-specific adverse events may induce negative performance effects for industry peers (Post et al., 2002). As such, a negative incident like a data breach may be interpreted as a cue for systemic industry problems that negatively affect all firms. Consistent with this logic, illustrative example include accusations against Arthur Anderson that affected the whole accounting industry (Post et al., 2002), or data breaches of leading social media platforms that adversely impact the whole social media industry, including non-breached competitors. These mechanisms might cancel out the expected positive spillover effects based on gaining competitive advantages, and may partially explain our results.

6.2 Long-term Stock Market Effects

In this study, we estimate the short-term stock market reaction to data breach announcements, providing a baseline for subsequent moderation analyses. To further extend the knowledge on the financial consequences of data breaches (Gwebu et al., 2018; Modi et al., 2015), we also explore the long-term implications for shareholder value. This analysis may approach the question to which extent the negative effect on shareholder value is sustained.

In the empirical operations management and information systems literature long-term event studies are scarce, mainly because the question of statistical inference is a key issue (Kothari and Warner, 2006). However, example event studies explore the long-term stock market effects of product recalls (Liu, Shankar, and Yun, 2017), new product announcements (Warren and Sorescu, 2017), or supply chain disruptions (Hendricks and Singhal, 2005).

We follow the long-term event study approach outlined in Hendricks and Singhal (2005), computing buy-and-hold abnormal returns (*BHARs*) based on a one-to-one matched control group of firms. As control firms, we use the nearest neighbors based on the PSM approach described in Section 5.1.1. We then compute the *BHAR* for firm i as the difference of compounded returns between our sample firm observations and their corresponding matches (Hendricks and Singhal, 2005),

$$BHAR_i = \prod_{t=1}^{T}(1 + R_{it}) - \prod_{t=1}^{T}(1 + R_{ct}), \tag{11}$$

where R_{it} is the observed return of firm i on day t and R_{ct} is the return of the matched control firm c on day t. We compute BHARs in monthly increments (approximately 20 trading days) over a symmetric period of ten months surrounding the announcement date (Day 0). Table 8 presents

the corresponding event study results. As indicated by Columns 1–4, there are no significant stock market effects in the five-, four-, three-, or two-month period prior to the data breach announcement. Focusing on only the one-month period prior to the data breach (i.e., Days -20 to -1), we see a positive effect, implying that our sample firms did comparatively better than the control group. However, after the data breach (Day 0), this picture is inverted. As suggested by Column 6, there are negative stock market effects during the first month after the data breach (mean *BHAR* of -0.90%, $t = -1.30$, $p < 0.10$). The negative long-term impact is increasing over time after the data breach announcement, up to a mean (median) *BHAR* of -3.34% (-2.21%) for the post-breach five-month period ($t = -1.97$, $p < 0.05$; $Z_{Wilcoxon} = -2.31$, $p < 0.05$). In other words, while there were no consistently significant stock market effects prior to the data breach, we see that the non-breached control firms outperform our sample firms after the data breach in terms of stock market performance. These findings provide indications for sustained negative shareholder value implications of data breaches.

7 Discussion, Implications, and Future Research

7.1 Summary and Discussion

Based on a sample of 219 data breach announcements from public firms listed on U.S. stock exchanges, we demonstrate that these announcements evoke a decline of -0.55% in shareholder value within a two-day event window spanning the announcement date and the subsequent trading day. This short-term abnormal return is also economically substantial, corresponding to an average $208 million decrease in shareholder value. In addition to this direct effect, we further identify multiple moderating factors, relating to the stakeholder ecosystem of the breached firm. We find evidence for a more negative stock market reaction when customer data is breached, emphasizing the key role of customers as primary stakeholders that constitute the resource base of the firm. As hypothesized, we also show the shareholder impact to be stronger for supply chain breaches, a breach type that spans inter-organizational boundaries and is becoming an increasing risk for firms. According to our results, the negative financial consequences of data breaches are also more severe when the breached firm receives more media attention, which underpins the critical role of the media as a stakeholder that shapes the public opinion about a firm. Finally, we could not demonstrate that institutional ownership mitigates the negative stock market reaction to data breach announcements. While our hypothesis derivation was based on ownership control and support arguments, a potential counter-explanation could be that institutional investors, such as government agencies, perceive the data breach as an investment threat. Against this backdrop, instead of providing (financial) support, these institutions

may even reduce their equity stakes accordingly.

In a post-hoc analysis, we further examine whether data breaches induce positive spillover effects for competitor firms, which we could not confirm. Investors perceiving data breaches as cues to systemic industry-wide issues might be an opposite effect, cancelling out the expected positive spillover effects. Finally, assessing the long-term shareholder value consequences of data breaches, our second post-hoc analysis shows that there are indeed indications of sustained negative effects, highlighting the downside potential of data breaches as operational risks.

7.2 Theoretical Implications

Our study contributes to the extant literature in multiple ways. First, demonstrating that data breaches are associated with a significant decline in shareholder value as a baseline for our moderating analysis, we confirm the results of previous event studies (e.g., Gwebu et al., 2018; Martin et al., 2017; Modi et al., 2015; Malhotra and Kubowicz Malhotra, 2011), presenting empirical evidence from a more contemporary sample of data breaches. Our effect size of a mean cumulative abnormal return of -0.55% within a two-day period is consistent with prior research. For instance, Gwebu et al. (2018) find a -0.41% decrease in shareholder value for the same window; Martin et al. (2017) present an abnormal return of -0.29%. For a three-day event window, Modi et al. (2015) find the drop to be -1.17%. Likewise, Malhotra and Kubowicz Malhotra (2011) estimate a slightly higher impact of -0.78% within a three-day period surrounding the data breach announcement date.

Second, more importantly, taking a stakeholder perspective (Kim et al., 2019; Longoni and Cagliano, 2018; Donaldson and Preston, 1995), we introduce data breaches as an emerging risk that requires elevated attention in the field of operations and supply chain management. Identifying and assessing the stakeholder factors that influence the magnitude of the stock market reaction to data breaches represents an application of the stakeholder view (Post et al., 2002; Clarkson, 1995; Freeman, 1984), and advances our general understanding of data breaches. In this regard, we add three novel and crucial moderation factors that should be taken into account when examining data breaches, or stock market reactions to adverse events in general. Specifically, we show the stock market reaction to data breach announcements to be more negative when customer data is involved, consistent with current discussions on data privacy and security (Cheung et al., 2021). Finding that supply chain breaches evoke a more negative stock market reaction may further extend the literature on data breaches, emphasizing the increasing diversity and complexity of cybersecurity risks. We also show media attention to impact the magnitude of the shareholder value decline associated with data breaches. While often overlooked in operations and supply chain management research, this

highlights the exacerbating effect of public scrutiny, not limited to the case of data breaches, but adverse events in general.

Finally, our work adds to the emerging stream of cybersecurity in operations and supply chain management (Cheung et al., 2021), and well resonates with recent examinations of supply chain digitalization risks (Son et al., 2021). While security and privacy issues that accompany digitalization efforts have gained comparatively limited attention (Massimino et al., 2018), our study empirically substantiates these issues by introducing the case of data breaches. Our stakeholder-based moderation framework helps to understand which factors determine the magnitude of the negative financial consequences associated with data breaches. Eventually, this may also extend the larger discussion on digitalization in operations and supply chain management (e.g., Olsen and Tomlin, 2020; Li, 2020), shedding light on the consequences and mitigation of associated risks.

7.3 Managerial Implications

Based on our empirical findings, we derive a set of actionable insights and recommendations for managers. First, we emphasize the severe short- and long-term financial consequences of data breaches for firms. In the wake of the rapid and cross-functional digitalization developments, managers must consider data breaches as an increasingly harmful operational risk. Therefore, we encourage practitioners to re-evaluate and optimize the firm's IT security strategy. As we see data breaches increasing in number, volume, and diversity, it seems crucial to extend the scope of the IT security strategy beyond the boundaries of the own firm. Supply chain breaches, targeting the weakest point of a digital supply chain, are becoming pervasive cyber-attack strategies. Against this backdrop, purely focusing on the own firm's security structure may not be sufficient any more.

Second, based the results of our moderation analysis, it appears crucial to be specifically cautious in instances where customer data is involved. While leveraging customer data through analytics tools may be a relevant source of competitive advantage for firms, we aim to emphasize the corresponding risks. Arguably, customers – key stakeholders for every business – are becoming more sensitive to data privacy issues, and it should be a key pillar of every firm's IT security strategy to focus on safeguarding customer data, maintaining privacy. Our findings indicate that the loss of customer data is particularly costly, negatively affecting firm reputation and customer spending, both resulting in negatively adjusted investor expectations and a loss in shareholder value.

Third, as we find a firm's media attention to amplify the negative shareholder value impact of data breach announcements, we emphasize the role of firm media coverage. Firms receiving intensive media attention should be particularly cautious, and must be aware that the increased public scrutiny

may accentuate the risks associated with data breaches.

7.4 Limitations and Future Research

As with any study, our research does not come without limitations. Specifically, we discuss three limitations, opening up avenues for future studies on data breaches. First, due to the availability of public data wregarding data breaches and firm financials, we consider U.S. firms only. Future research should extend the geographical scope to potentially identify systematic differences and generally enrich our understanding of contingency factors influencing the financial consequences of data breaches. Second, inherent to our event study approach, we focus on firms that are publicly traded. In general, these firms are often larger and might not be representative for the effects of data breaches on small and medium sized firms, as these firms are not commonly traded on stock markets and also receive less (or no) media attention. It might be worthwhile to also investigate the consequences and contingencies of data breaches for small and medium sized firms, leveraging alternative data sources. Third, to study financial consequences of data breaches, we utilize an event study, examining the effects on short- and long-term shareholder value. While shareholder value is a key dimension of financial firm performance, we encourage future studies to also investigate the implications on alternative operational firm performance measures.

References

Armerding, T.. 2019. It's not just you they're after – it's your supply chain too. *Forbes Magazine*, April 10 (2019).

Barney, J. B.. 2018. Why resource-based theory's model of profit appropriation must incorporate a stakeholder perspective. *Strategic Management Journal*, 39 (13), 3305–3325.

Bellamy, M. A., S. Dhanorkar, and R. Subramanian. 2020. Administrative environmental innovations, supply network structure, and environmental disclosure. *Journal of Operations Management* 66, 895–932.

Bose, I. and A. C. M. Leung. 2019. Adoption of identity theft countermeasures and its short- and long-term impact on firm value. *MIS Quarterly*, 43 (1), 313–327.

Bourdon, B.. 2017. The avoidable mistakes executives continue to make after a data breach. *Harvard Business Review Digital Articles*, November 20 (2017).

Boyd, D. E., P. Kannan, and R. J. Slotegraaf. 2019. Branded apps and their impact on firm value: A design perspective. *Journal of Marketing Research*, 56 (1), 76–88.

Brandon-Jones, E., M. Dutordoir, J. Q. F. Neto, and B. Squire. 2017. The impact of reshoring decisions on shareholder wealth. *Journal of Operations Management* 49-51, 31–36.

Brown, S. J. and J. B. Warner. 1985. Using daily stock returns: The case of event studies. *Journal of Financial Economics*, 14 (1), 3–31.

Burt, A.. 2019. Can Facebook ever be fixed? *Harvard Business Review Digital Articles*, April 8 (2019).

Carhart, M. M.. 1997. On persistence in mutual fund performance. *The Journal of Finance*, 52 (1), 57–82.

Cheung, K. F., M. G. H. Bell, and J. Bhattacharjya. 2021. Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review* 146, 102217.

Choi, T., S. W. Wallace, and Y. Wang. 2018. Big data analytics in operations management. *Production and Operations Management*, 27 (10), 1868–1883.

Clarkson, M. B.. 1995. A stakeholder framework for analyzing and evaluating corporate social performance. *Academy of Management Review*, 20 (1), 92–117.

Columbus, L.. 2019. Why manufacturing supply chains need zero trust. *Forbes Magazine*, April 29 (2019).

Cowan, A. R.. 1992. Nonparametric event study tests. *Review of Quantitative Finance and Accounting*, 2 (4), 343–358.

Craighead, C. W., K. R. Karwan, and J. L. Miller. 2004. The effects of severity of failure and customer loyalty on service recovery strategies. *Production and Operations Management*, 13 (4), 307–321.

Dam, L. and B. N. Petkova. 2014. The impact of environmental supply chain sustainability programs on shareholder wealth. *International Journal of Operations & Production Management*, 34 (5), 586–609.

Donaldson, T. and L. E. Preston. 1995. The stakeholder theory of the corporation: Concepts, evidence, and implications. *Academy of Management Review*, 20 (1), 65–91.

ENISA. 2021. ENISA threat landscape for supply chain attacks. *European Union Agency for Cybersecurity (ENISA)*, July (2021).

Fama, E. F. and K. R. French. 1993. Common risk factors in the returns on stocks and bonds. *Journal of Financial Economics*, 33 (1), 3–56.

Freeman, R. E.. 1984. *Strategic management: A stakeholder approach*. Boston, MA: Pitman.

Goode, S., H. Hoehle, V. Venkatesh, and S. A. Brown. 2017. User compensation as a data breach recovery action: An investigation of the Sony Playstation network breach. *MIS Quarterly*, 41 (3), 703–727.

Gupta, K., D. Crilly, and T. Greckhamer. 2020. Stakeholder engagement strategies, national institutions, and firm performance: A configurational perspective. *Strategic Management Journal*, 41 (10), 1869–1900.

Gwebu, K. L., J. Wang, and L. Wang. 2018. The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, 35 (2), 683–714.

Hastig, G. M. and M. S. Sodhi. 2020. Blockchain for supply chain traceability: Business requirements and critical success factors. *Production and Operations Management*, 29 (4), 935–954.

Heckman, J. J.. 1979. Sample selection bias as a specification error. *Econometrica: Journal of the Econometric Society*, 47 (1), 153–161.

Hendricks, K. B., M. Hora, and V. R. Singhal. 2015. An empirical investigation on the appointments of supply chain and operations management executives. *Management Science*, 61 (7), 1562–1583.

Hendricks, K. B. and V. R. Singhal. 2005. An empirical analysis of the effect of supply chain disruptions on long-run stock price performance and equity risk of the firm. *Production and Operations Management*, 14 (1), 35–52.

Hwang, B.-H., J. M. Liberti, and J. Sturgess. 2019. Information sharing and spillovers: Evidence from financial analysts. *Management Science*, 65 (8), 3624–3636.

ITRC. 2019. 2018 end-of-year data breach report. *Identity Theft Resource Center (ITRC)*, November 17 (2019).

Jacobs, B. W. and V. R. Singhal. 2014. The effect of product development restructuring on shareholder value. *Production and Operations Management*, 23 (5), 728–743.

Jain, S. C. and L. M. Ropple. 2018. Stopping data breaches will require help from governments. *Harvard Business Review Digital Articles*, December 14 (2018).

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.

Jensen, M. C.. 2001. Value maximization, stakeholder theory, and the corporate objective function. *Journal of Applied Corporate Finance*, 14 (3), 8–21.

Jeong, Y.-C. and T.-Y. Kim. 2019. Between legitimacy and efficiency: An institutional theory of corporate giving. *Academy of Management Journal*, 62 (5), 1583–1608.

Jones, T. M.. 1995. Instrumental stakeholder theory: A synthesis of ethics and economics. *Academy of*

Management Review, 20 (2), 404–437.

Kache, F. and S. Seuring. 2017. Challenges and opportunities of digital information at the intersection of big data analytics and supply chain management. *International Journal of Operations & Production Management*, 37 (1), 10–36.

Kalaignanam, K., T. Kushwaha, J.-B. E. Steenkamp, and K. R. Tuli. 2013. The effect of CRM outsourcing on shareholder value: A contingency perspective. *Management Science*, 59 (3), 748–769.

Kamleitner, B., V. W. Mitchell, A. Stephen, and A. Kolah. 2018. Your customers may be the weakest link in your data privacy defenses. *MIT Sloan Management Review*, May 22 (2018).

Kim, S., S. M. Wagner, and C. Colicchia. 2019. The impact of supplier sustainability risk on shareholder value. *Journal of Supply Chain Management*, 55 (1), 71–87.

Kohtamäki, M., V. Parida, P. C. Patel, and H. Gebauer. 2020. The relationship between digitalization and servitization: The role of servitization in capturing the financial potential of digitalization. *Technological Forecasting and Social Change* 151, 119804.

Kothari, S. and J. B. Warner. 2006. *Econometrics of event studies.* Handbook of corporate finance: Empirical corporate finance, Vol A (Handbooks in Finance Series). Amsterdam: Elsevier.

Kurpjuweit, S., C. G. Schmidt, M. Klöckner, and S. M. Wagner. 2021. Blockchain in additive manufacturing and its impact on supply chains. *Journal of Business Logistics*, 42 (1), 46–70.

Kutner, M. H., C. J. Nachtsheim, J. Neter, and W. Li. 2005. *Applied linear statistical models*, Volume 5. New York: McGraw-Hill Irwin.

Lam, H. K. S., L. Ding, T. C. E. Cheng, and H. G. Zhou. 2019. The impact of 3D printing implementation on stock returns: A contingent dynamic capabilities perspective. *International Journal of Operations & Production Management*, 39 (6/7/8), 935–961.

Li, F.. 2020. Leading digital transformation: Three emerging approaches for managing the transition. *International Journal of Operations & Production Management*, 40 (6), 809–817.

Liu, W. H., W. Y. Wei, C. Si, D. Xie, and L. J. Chen. 2020. Effect of supply chain strategic collaboration announcements on shareholder value: An empirical investigation from China. *International Journal of Operations & Production Management*, 40 (4), 389–414.

Liu, Y. and V. Shankar. 2015. The dynamic impact of product-harm crises on brand preference and advertising effectiveness: An empirical analysis of the automobile industry. *Management Science*, 61 (10), 2514–2535.

Liu, Y., V. Shankar, and W. Yun. 2017. Crisis management strategies and the long-term effects of product recalls on firm value. *Journal of Marketing*, 81 (5), 30–48.

Lo, C. K., C. S. Tang, Y. Zhou, A. C. Yeung, and D. Fan. 2018. Environmental incidents and the market value of firms: An empirical investigation in the Chinese context. *Manufacturing & Service Operations Management*, 20 (3), 422–439.

Longoni, A. and R. Cagliano. 2018. Inclusive environmental disclosure practices and firm performance: The role of green supply chain management. *International Journal of Operations & Production Management*, 38 (9), 1815–1835.

MacKinlay, A. C.. 1997. Event studies in economics and finance. *Journal of Economic Literature*, 35 (1), 13–39.

Malhotra, A. and C. Kubowicz Malhotra. 2011. Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research*, 14 (1), 44–59.

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

Massimino, B., J. V. Gray, and Y. C. Lan. 2018. On the inattention to digital confidentiality in operations and supply chain research. *Production and Operations Management*, 27 (8), 1492–1515.

McWilliams, A. and D. Siegel. 1997. Event studies in management research: Theoretical and empirical issues. *Academy of Management Journal*, 40 (3), 626–657.

Modi, S. B., M. A. Wiles, and S. Mishra. 2015. Shareholder value implications of service failures in triads: The case of customer information security breaches. *Journal of Operations Management* 35, 21–39.

Olsen, T. L. and B. Tomlin. 2020. Industry 4.0: Opportunities and challenges for operations management. *Manufacturing & Service Operations Management*, 22 (1), 113–122.

Payne, A., P. Frow, and A. Eggert. 2017. The customer value proposition: Evolution, development, and application in marketing. *Journal of the Academy of Marketing Science*, 45 (4), 467–489.

Post, J. E., L. E. Preston, and S. Sachs. 2002. Managing the extended enterprise: The new stakeholder view. *California Management Review*, 45 (1), 6–28.

Redman, T. C. and R. M. Waitman. 2020. Do you care about privacy as much as your customers do? *Harvard Business Review Digital Articles*, January 28 (2020).

Rosenbaum, P. R. and D. B. Rubin. 1983. The central role of the propensity score in observational studies for causal effects. *Biometrika*, 70 (1), 41–55.

Schmidt, C. G., D. A. Wuttke, G. P. Ball, and H. S. Heese. 2020. Does social media elevate supply chain importance? An empirical examination of supply chain glitches, Twitter reactions, and stock market returns. *Journal of Operations Management*, 66 (6), 646–669.

Seyedghorban, Z., D. Samson, and H. Tahernejad. 2020. Digitalization opportunities for the procurement function: Pathways to maturity. *International Journal of Operations & Production Management*, 40 (11), 1685–1693.

Sharton, B. R.. 2020. Will coronavirus lead to more cyber attacks? *Harvard Business Review Digital Articles*, March 16 (2020).

Shipilov, A. V., H. R. Greve, and T. J. Rowley. 2019. Is all publicity good publicity? The impact of direct and indirect media pressure on the adoption of governance practices. *Strategic Management Journal*, 40 (9), 1368–1393.

Son, B.-G., H. Kim, D. Hur, and N. Subramanian. 2021. The dark side of supply chain digitalisation: Supplier-perceived digital capability asymmetry, buyer opportunism and governance. *International Journal of Operations & Production Management*, 41 (7), 1220–1247.

Song, H., M. Li, and K. Yu. 2021. Big data analytics in digital platforms: How do financial service providers customise supply chain finance? *International Journal of Operations & Production Management*, 41 (4), 410–435.

Sridhar, K., D. Ralph, and J. Copic. 2021. 3 strategies to secure your digital supply chain. *Harvard Business Review Digital Articles*, August 9 (2021).

Stupp, C.. 2019. Malware attack on Asus computers raises concerns. *The Wall Street Journal*, March 26 (2019).

Vanacker, T., D. P. Forbes, M. Knockaert, and S. Manigart. 2020. Signal strength, media attention, and resource mobilization: Evidence from new private equity firms. *Academy of Management Journal*, 63 (4), 1082–1105.

Warren, N. L. and A. Sorescu. 2017. Interpreting the stock returns to new product announcements: How the past shapes investors' expectations of the future. *Journal of Marketing Research*, 54 (5), 799–815.

Wiersema, M. F. and Y. Zhang. 2013. Executive turnover in the stock option backdating wave: The impact of social context. *Strategic Management Journal*, 34 (5), 590–609.

Winder, D.. 2020. Lockheed Martin, SpaceX and Tesla caught in cyber attack crossfire. *Forbes Magazine*, March 2 (2020).

Xiong, Y. C., H. K. S. Lam, A. Kumar, E. W. T. Ngai, C. Y. Xiu, and X. Y. Wang. 2021. The mitigating role of blockchain-enabled supply chains during the COVID-19 pandemic. *International Journal of Operations & Production Management*, 41 (9), 1495–1521.

Figures

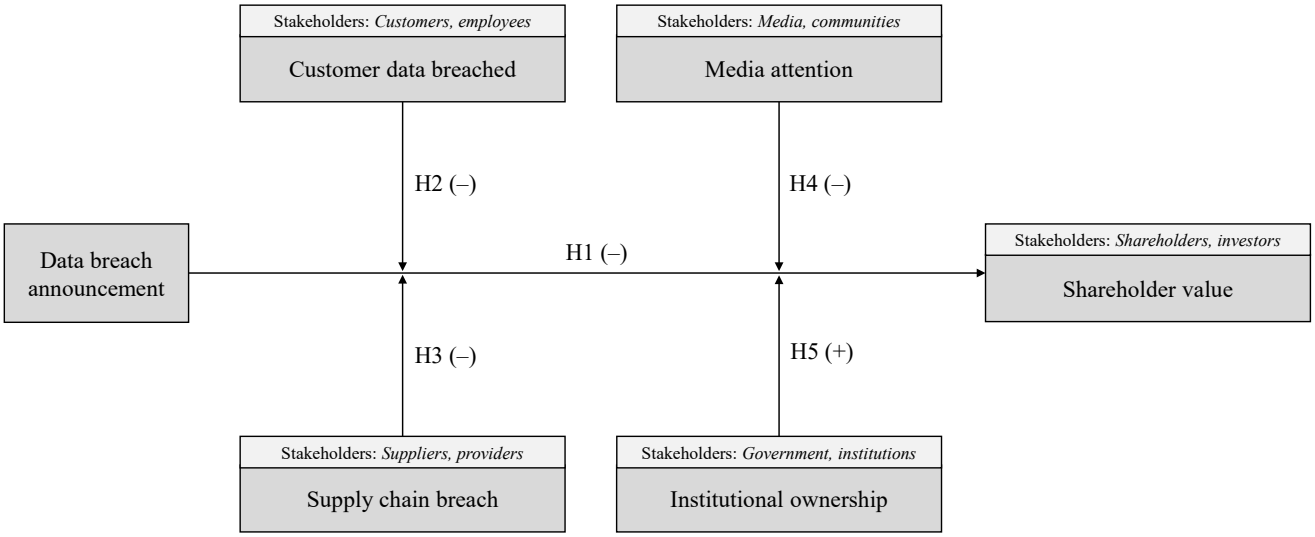

Figure 1: Conceptual model.

Tables

Table 1: Sample summary statistics.

	Frequency	Percentage
Panel A: Year		
2018	51	23%
2017	48	22%
2016	43	20%
2015	40	18%
2014	37	17%
Total	*219*	*100%*
Panel B: Industry		
Consumer Discretionary	57	26%
Industrials	40	18%
Communication Services	30	14%
Financials	27	12%
Information Technology	27	12%
Consumer Staples	14	6%
Health Care	10	5%
Other	14	6%
Total	*219*	*100%*

Table 2: Measurement details for hypothesized and control variables.

Variable (label)	Operationalization	Data source	Reference
Customer data breached (*CUSTOMER*)	Dummy variable that equals 1 when customer data is breached (e.g., name, address, financial information), 0 otherwise	Coded	-
Supply chain breach (*SCBREACH*)	Dummy variable that equals 1 when data breach is due to an incident at a third-party (e.g., supplier, contractor, IT service provider, subsidiary), 0 otherwise	Coded	-
Media attention (*MEDIA*)	Ratio of number of news database hits for breached firm (from PR Newswire and Business Wire) within the year before the data breach announcement to total firm assets	LexisNexis, Thomson Reuters	-
Institutional ownership (*INSTOWNER*)	Ratio of number of long-term shareholders (i.e., government institutions, corporates etc.) to total number of outstanding shares	Thomson Reuters	-
Financial data breached (*FINANCIAL*)	Dummy variable that equals 1 when financial data is breached (e.g., bank account data, credit card information), 0 otherwise	Coded	-
Firm size (*FIRMSIZE*)	Logarithm of total assets in the fiscal year prior to the announcement	Thomson Reuters	Jacobs and Singhal (2014)
Market-to-book ratio (*MTB*)	Ratio of stock closing price to firm book value per share for the announcement date	Thomson Reuters	Gwebu et al. (2018)
Leverage (*LEVERAGE*)	Ratio of total debts to total equity in the fiscal year prior to the announcement	Thomson Reuters	Hendricks et al. (2015)
Year dummies (*YEAR*)	Dummy variables for announcement years	LexisNexis	Lo et al. (2018)
Industry dummies (*INDUSTRY*)	Dummy variables for two-digit GICS codes	Thomson Reuters	Modi et al. (2015)

Table 3: Descriptive statistics for explanatory variables.

Binary variables	Type	Mean	TRUE	FALSE		
Customer data breached	Hypothesis 2	0.61	133	86		
Supply chain breach	Hypothesis 3	0.20	43	176		
Financial data breached	Control	0.37	80	139		
Non-binary variables	Type	Mean	Stdev.	Median	Min.	Max.
Media attention	Hypothesis 4	13.81	36.73	3.88	0.00	447.35
Institutional ownership	Hypothesis 5	0.10	0.16	0.03	0.00	0.67
Firm size (in billions)	Control	47.32	95.41	6.82	0.02	719.89
Market-to-book ratio	Control	5.00	22.34	2.99	−121.82	191.48
Leverage	Control	2.86	10.37	0.86	−5.57	97.43

Variables are not logarithmized; N=219.

Table 4: Event study results.

	Day -2	Day -1	Day 0	Day 1	Day 2	Days (0, 1)
	(1)	(2)	(3)	(4)	(5)	(6)
Mean abnormal return	0.12%	0.15%	−0.23%	−0.32%	0.02%	−0.55%
t-test (t-statistic)	(1.53)*	(0.38)	(−1.80)**	(−3.04)***	(−0.06)	(−3.42)***
Median abnormal return	0.10%	−0.05%	0.02%	−0.18%	0.12%	−0.24%
Wilcoxon signed rank test (Z-statistic)	(1.51)*	(−0.49)	(−1.54)*	(−2.22)**	(1.30)*	(−3.01)***
Percent negative abnormal returns	44.75%	54.79%	48.86%	57.08%	44.29%	57.53%
Generalized sign test (Z-statistic)	(−1.71)**	(1.26)	(−0.50)	(1.94)**	(−1.85)**	(2.07)**

*p < 0.10, **p < 0.05, ***p < 0.01; all tests are one-tailed; N=219.
The computation of expected returns is based on the Fama-French four-factor model.

Table 5: Correlation matrix.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
(1) Cumulative abnormal return day in (0, 1) ($CAR_{(0,1)}$)	1							
(2) Customer data breached (*CUSTOMER*)	−0.02	1						
(3) Supply chain breach (*SCBREACH*)	−0.09	0.12*	1					
(4) Media attention (*MEDIA*)	−0.13*	−0.17*	−0.12*	1				
(5) Institutional ownership (*INSTOWNER*)	0.04	0.16*	−0.09	0.10	1			
(6) Financial data breached (*FINANCIAL*)	0.11*	0.30*	0.08	−0.11	0.10	1		
(7) Firm size (*FIRMSIZE*)	0.11	0.36*	0.21*	−0.47*	−0.15*	0.08	1	
(8) Market-to-book ratio (*MTB*)	0.02	−0.08	0.09	0.02	−0.27*	−0.03	0.10	1
(9) Leverage (*LEVERAGE*)	0.04	−0.05	0.18*	−0.02	−0.07	−0.00	0.04	0.40*

*p < 0.10, N=219.

Table 6: Random effects regression results.

Dependent variable: Cumulative abnormal return in (0, 1) ($CAR_{(0,1)}$)						
	Predicted sign	Controls (1)	Model 1 (2)	Model 2 (3)	Model 3 (4)	Model 4 (5)
Intercept		−0.026	−0.030	−0.034	−0.018	−0.020
		(0.028)	(0.028)	(0.028)	(0.028)	(0.030)
Hypothesized variables						
Customer data breached (*CUSTOMER*)	–		−0.008*	−0.007*	−0.007*	−0.007*
			(0.004)	(0.004)	(0.004)	(0.004)
Supply chain breach (*SCBREACH*)	–			−0.008**	−0.008**	−0.008**
				(0.004)	(0.004)	(0.004)
Media attention (*MEDIA*)	–				−0.000**	−0.000**
					(0.000)	(0.000)
Institutional ownership (*INSTOWNER*)	+					0.004
						(0.011)
Control variables						
Financial data breached (*FINANCIAL*)		0.006*	0.008**	0.008**	0.008**	0.008**
		(0.004)	(0.004)	(0.004)	(0.004)	(0.004)
Firm size (*FIRMSIZE*)		0.001	0.001	0.001	0.001	0.001
		(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
Market-to-book ratio (*MTB*)		0.000	0.000	0.000	0.000	0.000
		(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
Leverage (*LEVERAGE*)		−0.000	−0.000	0.000	0.000	0.000
		(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
Year dummies (*YEAR*)		Included	Included	Included	Included	Included
Industry dummies (*INDUSTRY*)		Included	Included	Included	Included	Included
χ^2		19.90	23.62*	27.11*	28.69*	28.71*
R^2		0.09	0.10	0.12	0.13	0.13
VIF_{max}		1.27	1.30	1.31	1.46	1.49
N		219	219	219	219	219

*p < 0.10, **p < 0.05, ***p < 0.01; Robust standard errors in parentheses.
$CAR_{(0,1)}$ based on Fama-French four-factor model.

Table 7: Event study results. Competition spillover effects.

	Day -2 (1)	Day -1 (2)	Day 0 (3)	Day 1 (4)	Day 2 (5)	Days (0, 1) (6)
Mean abnormal return	0.12%	0.04%	−0.16%	0.08%	−0.15%	−0.08%
t-test (t-statistic)	(1.09)	(−0.81)	(−0.81)	(0.21)	(−0.87)	(−0.42)
Median abnormal return	0.00%	−0.07%	−0.12%	−0.10%	−0.06%	−0.12%
Wilcoxon signed rank test (Z-statistic)	(0.78)	(−1.16)	(−1.50)*	(−0.08)	(−1.40)*	(−0.50)
Percent negative abnormal returns	49.77%	52.97%	54.79%	52.97%	52.97%	52.51%
Generalized sign test (Z-statistic)	(−0.26)	(0.68)	(1.23)	(0.68)	(0.68)	(0.55)

*p < 0.10, **p < 0.05, ***p < 0.01; all tests are one-tailed; N=219.
The computation of expected returns is based on the Fama-French four-factor model.

Table 8: Long-term event study results. Buy-and-hold abnormal returns (BHARs).

	Days [-100, -1] (1)	Days [-80, -1] (2)	Days [-60, -1] (3)	Days [-40, -1] (4)	Days [-20, -1] (5)	Days [1, 20] (6)	Days [1, 40] (7)	Days [1, 60] (8)	Days [1, 80] (9)	Days [1, 100] (10)
Mean BHAR	−0.21%	−1.73%	−0.32%	−0.02%	1.09%	−0.90%	−2.00%	−2.62%	−3.41%	−3.34%
t-test (t-statistic)	(−0.14)	(−1.19)	(−0.24)	(−0.01)	(1.54)*	(−1.30)*	(−2.03)**	(−2.16)**	(−2.31)**	(−1.97)**
Median BHAR	1.06%	−1.23%	−0.00%	−0.00%	0.93%	0.00%	−0.31%	−0.78%	−2.47%	−2.21%
Wilcoxon signed rank test (Z-statistic)	(0.05)	(−1.08)	(−0.25)	(−0.38)	(1.93)**	(−0.92)	(−1.02)	(−1.62)*	(−2.16)**	(−2.31)**
Percent negative BHARs	48.40%	51.60%	50.68%	50.23%	45.66%	49.32%	51.14%	53.42%	57.08%	55.71%
Binomial sign test (Z-statistic)	(−0.41)	(0.41)	(0.14)	(0.00)	(−1.22)	(−0.14)	(0.27)	(0.95)	(2.03)**	(1.62)*

*p < 0.10, **p < 0.05, ***p < 0.01; all tests are one-tailed; N=219.

The computation of expected returns is based on the Fama-French four-factor model.

Appendix

Table A1: Cross-sectional logit regression results.

Dependent variable: Sample firm (binary indicator)					
	2014	2015	2016	2017	2018
	(1)	(2)	(3)	(4)	(5)
Intercept	-18.186^{***}	-18.367^{***}	-11.253^{***}	-11.173^{***}	-18.268^{***}
	(2.147)	(2.112)	(1.629)	(1.610)	(1.954)
Firm size (*FIRMSIZE*)	0.702^{***}	0.668^{***}	0.416^{***}	0.400^{***}	0.672^{***}
	(0.090)	(0.087)	(0.072)	(0.070)	(0.080)
Market-to-book ratio (*MTB*)	−0.000	−0.000	−0.000	−0.000	0.000
	(0.000)	(0.000)	(0.001)	(0.000)	(0.001)
Leverage (*LEVERAGE*)	−0.000	−0.001	0.002	0.002	0.011
	(0.001)	(0.003)	(0.003)	(0.006)	(0.023)
Industry dummies (*INDUSTRY*)	Included	Included	Included	Included	Included
χ^2	118.62^{***}	103.31^{***}	87.44^{***}	83.05^{***}	146.51^{***}
McFadden $\tilde{R}^2$	0.29	0.24	0.19	0.16	0.27
N	3,182	3,374	3,559	3,770	3,919

$^{*}p < 0.10$, $^{**}p < 0.05$, $^{***}p < 0.01$. Robust standard errors in parentheses.

Table A2: Descriptive statistics for sample and matched firms.

	Sample firms		Matched firms (five nearest neighbors)	
	Median	Stdev.	Median	Stdev.
Propensity score	0.05	0.11	0.04	0.05
Firm size (in billions)	6.82	95.41	5.74	59.69
Market-to-book ratio	2.99	22.34	2.43	455.41
Leverage	0.86	10.37	0.68	11.18

Variables are not logarithmized; N=219.

Table A3: Event study results. Five nearest neighbors as benchmark.

	Day -2	Day -1	Day 0	Day 1	Day 2	Days (0, 1)
	(1)	(2)	(3)	(4)	(5)	(6)
Mean abnormal return	0.21%	0.14%	−0.18%	−0.24%	0.04%	−0.42%
t-test (t-statistic)	$(1.66)^{**}$	(0.70)	(−1.19)	$(-1.70)^{**}$	(0.42)	$(-2.12)^{**}$
Median abnormal return	0.11%	−0.10%	0.01%	−0.14%	0.16%	−0.19%
Wilcoxon signed rank test (Z-statistic)	$(1.35)^{*}$	(−0.26)	(−0.76)	$(-1.80)^{**}$	(1.24)	$(-2.13)^{**}$
Percent negative abnormal returns	46.58%	52.05%	49.32%	57.08%	44.29%	55.71%
Binomial sign test (Z-statistic)	(−0.95)	(0.54)	(−0.14)	$(2.03)^{**}$	$(-1.62)^{*}$	$(1.62)^{*}$

$^{*}p < 0.10$, $^{**}p < 0.05$, $^{***}p < 0.01$; all tests are one-tailed; N=219.

Generalized sign tests are not applicable for average abnormal returns from five firms.

Table A4: Two-stage Heckman model results.

Dependent variable:	Data breach announcement	Cum. abn. return in (0, 1) ($CAR_{(0,1)}$)
	First stage Probit	Second stage Random effects
	(1)	(2)
Intercept	−0.429	0.024
	(0.821)	(0.199)
Hypothesized variables		
Customer data breached (*CUSTOMER*)		−0.007*
		(0.004)
Supply chain breach (*SCBREACH*)		−0.008**
		(0.004)
Media attention (*MEDIA*)		−0.000**
		(0.000)
Institutional ownership (*INSTOWNER*)		0.005
		(0.011)
Control variables		
Financial data breached (*FINANCIAL*)		0.007
		(0.004)
Firm size (*FIRMSIZE*)	0.019	0.001
	(0.035)	(0.002)
Market-to-book ratio (*MTB*)	0.002	0.000
	(0.003)	(0.000)
Leverage (*LEVERAGE*)	0.013	−0.000
	(0.009)	(0.001)
Inverse Mills ratio (*IMR*)		−0.040
		(0.175)
Year dummies (*YEAR*)	Included	Included
Industry dummies (*INDUSTRY*)	Included	Included
χ^2	4.52	28.61*
McFadden $\tilde{R}^2$ / R^2	0.01	0.13
N	438	219

*p < 0.10, **p < 0.05, ***p < 0.01.
Robust standard errors in parantheses.
$CAR_{(0,1)}$ based on Fama-French four-factor model.

Table A5: Event study results. First data breach only.

	Day -2	Day -1	Day 0	Day 1	Day 2	Days (0, 1)
	(1)	(2)	(3)	(4)	(5)	(6)
Mean abnormal return	0.11%	0.26%	−0.21%	−0.34%	0.02%	−0.55%
t-test (t-statistic)	(1.13)	(1.02)	(−1.99)**	(−2.39)***	(−0.32)	(−3.10)***
Median abnormal return	0.21%	−0.05%	−0.08%	−0.14%	0.07%	−0.27%
Wilcoxon signed rank test (Z-statistic)	(1.79)**	(−0.07)	(−2.08)**	(−1.91)**	(0.77)	(−3.03)***
Percent negative abnormal returns	41.82%	53.94%	52.12%	55.15%	47.88%	60.00%
Generalized sign test (Z-statistic)	(−2.34)***	(0.78)	(0.31)	(1.09)	(−0.78)	(2.34)***

*p < 0.10, **p < 0.05, ***p < 0.01; all tests are one-tailed; N=165.
The computation of expected returns is based on the Fama-French four-factor model.

Table A6: OLS regression results. First data breach only.

Dependent variable: Cumulative abnormal return in (0, 1) ($CAR_{(0,1)}$)						
	Predicted sign	Controls (1)	Model 1 (2)	Model 2 (3)	Model 3 (4)	Model 4 (5)
Intercept		−0.009	−0.012	−0.017	0.002	0.002
		(0.028)	(0.028)	(0.028)	(0.028)	(0.029)
Hypothesized variables						
Customer data breached (*CUSTOMER*)	–		−0.008**	−0.008*	−0.008*	−0.008*
			(0.004)	(0.004)	(0.004)	(0.004)
Supply chain breach (*SCBREACH*)	–			−0.010**	−0.011**	−0.011**
				(0.004)	(0.004)	(0.004)
Media attention (*MEDIA*)	–				−0.000***	−0.000**
					(0.000)	(0.000)
Institutional ownership (*INSTOWNER*)	+					0.001
						(0.011)
Control variables						
Financial data breached (*FINANCIAL*)		0.006	0.008*	0.008*	0.008*	0.007*
		(0.004)	(0.004)	(0.004)	(0.004)	(0.004)
Firm size (*FIRMSIZE*)		−0.000	0.000	0.001	−0.000	−0.000
		(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
Market-to-book ratio (*MTB*)		0.000	0.000	0.000	0.000	0.000
		(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
Leverage (*LEVERAGE*)		0.000	0.000	0.000	0.000	0.000
		(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
Year dummies (*YEAR*)		Included	Included	Included	Included	Included
Industry dummies (*INDUSTRY*)		Included	Included	Included	Included	Included
F		1.13	1.35	1.57*	1.63*	1.53*
R^2		0.10	0.13	0.15	0.17	0.17
VIF_{max}		1.22	1.22	1.23	1.34	1.35
N		165	165	165	165	165

*p < 0.10, **p < 0.05, ***p < 0.01; Robust standard errors in parentheses.
$CAR_{(0,1)}$ based on Fama-French four-factor model.

Table A7: Event study results. Alternative expected return models.

	Day -2 (1)	Day -1 (2)	Day 0 (3)	Day 1 (4)	Day 2 (5)	Days (0, 1) (6)
Panel A: Fama-French three-factor model						
Mean abnormal return	0.15%	0.12%	−0.20%	−0.30%	0.03%	−0.50%
t-test (t-statistic)	(1.70)**	(0.10)	(−1.59)*	(−2.81)***	(0.06)	(−3.11)***
Median abnormal return	0.15%	−0.09%	0.02%	−0.16%	0.05%	−0.21%
Wilcoxon signed rank test (Z-statistic)	(1.83)**	(−0.92)	(−1.37)*	(−2.05)**	(1.17)	(−2.75)***
Percent negative abnormal returns	42.01%	55.25%	48.86%	56.16%	46.58%	57.08%
Generalized sign test (Z-statistic)	(−2.57)***	(1.35)*	(−0.55)	(1.62)*	(−1.22)	(1.89)**
Panel B: Market model						
Mean abnormal return	0.16%	0.21%	−0.26%	−0.35%	0.04%	−0.62%
t-test (t-statistic)	(1.59)*	(0.99)	(−2.07)**	(−3.13)***	(0.10)	(−3.67)***
Median abnormal return	0.05%	−0.07%	−0.05%	−0.18%	0.12%	−0.23%
Wilcoxon signed rank test (Z-statistic)	(1.26)	(−0.12)	(−1.81)**	(−2.22)**	(1.26)	(−3.12)***
Percent negative abnormal returns	48.86%	53.88%	52.51%	57.53%	44.75%	58.45%
Generalized sign test (Z-statistic)	(−0.51)	(0.98)	(0.57)	(2.06)**	(−1.72)**	(2.33)***
Panel C: Mean-adjusted model						
Mean abnormal return	0.12%	0.19%	−0.22%	−0.38%	−0.01%	−0.60%
t-test (t-statistic)	(0.91)	(0.92)	(−1.58)*	(−2.41)***	(−0.08)	(−3.13)***
Median abnormal return	0.05%	−0.04%	−0.22%	−0.02%	0.21%	−0.27%
Wilcoxon signed rank test (Z-statistic)	(1.22)	(−0.21)	(−1.73)**	(−1.45)*	(1.11)	(−2.89)***
Percent negative abnormal returns	46.12%	51.14%	58.90%	50.68%	42.47%	57.53%
Generalized sign test (Z-statistic)	(−1.12)	(0.36)	(2.66)***	(0.23)	(−2.21)**	(2.25)**
Panel D: Market-adjusted model						
Mean abnormal return	0.15%	0.19%	−0.24%	−0.38%	0.01%	−0.62%
t-test (t-statistic)	(1.30)*	(0.96)	(−1.84)**	(−2.64)***	(0.15)	(−3.45)***
Median abnormal return	0.06%	−0.06%	−0.12%	−0.22%	0.08%	−0.24%
Wilcoxon signed rank test (Z-statistic)	(1.31)*	(−0.26)	(−1.72)**	(−2.55)***	(1.12)	(−3.18)***
Percent negative abnormal returns	47.95%	55.71%	52.05%	58.90%	48.40%	55.71%
Generalized sign test (Z-statistic)	(−0.78)	(1.51)*	(0.43)	(2.46)***	(−0.65)	(1.51)*

*p < 0.10, **p < 0.05, ***p < 0.01; all tests are one-tailed; N=219.

Table A8: Random effects regression results. Winsorized sample.

Dependent variable: Cumulative abnormal return in (0, 1) ($CAR_{(0,1)}$)						
	Predicted sign	Controls (1)	Model 1 (2)	Model 2 (3)	Model 3 (4)	Model 4 (5)
Intercept		−0.027	−0.030	−0.034	−0.019	−0.021
		(0.026)	(0.026)	(0.026)	(0.026)	(0.028)
Hypothesized variables						
Customer data breached (*CUSTOMER*)	–		−0.007*	−0.006*	−0.006*	−0.006*
			(0.004)	(0.004)	(0.004)	(0.004)
Supply chain breach (*SCBREACH*)	–			−0.008**	−0.009**	−0.009**
				(0.004)	(0.004)	(0.004)
Media attention (*MEDIA*)	–				−0.000**	−0.000**
					(0.000)	(0.000)
Institutional ownership (*INSTOWNER*)	+					0.002
						(0.010)
Control variables						
Financial data breached (*FINANCIAL*)		0.005	0.007*	0.007*	0.007*	0.007*
		(0.003)	(0.004)	(0.004)	(0.004)	(0.004)
Firm size (*FIRMSIZE*)		0.001	0.001	0.001	0.001	0.001
		(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
Market-to-book ratio (*MTB*)		0.000	0.000	0.000	0.000	0.000
		(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
Leverage (*LEVERAGE*)		0.000	0.000	0.000	0.000	0.000
		(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
Year dummies (*YEAR*)		Included	Included	Included	Included	Included
Industry dummies (*INDUSTRY*)		Included	Included	Included	Included	Included
χ^2		19.28	22.77	27.31*	28.90**	28.81*
R^2		0.09	0.10	0.12	0.13	0.13
VIF_{max}		1.27	1.30	1.31	1.46	1.49
N		219	219	219	219	219

*p < 0.10, **p < 0.05, ***p < 0.01; Robust standard errors in parentheses.
$CAR_{(0,1)}$, *MTB*, and *LEVERAGE* winsorized at 1%.
$CAR_{(0,1)}$ based on Fama-French four-factor model.