12-2023

Customer cybersecurity and supplier cost management strategy

Xu YANG

Peng LIANG

Nan HU
Singapore Management University, nanhu@smu.edu.sg

Fujing XUE

Customers' Cybersecurity Risk and Suppliers' Cost Management Strategies: Evidence from Data Breaches

Nan Hu
School of Information Systems
Singapore Management University
nanhu@smu.edu.sg

Rong Huang*
School of Management
Fudan University
ronghuang@fudan.edu.cn

Peng Liang
International Institute of Finance, School of Management
University of Science and Technology of China
pengliang@ustc.edu.cn

Fujing Xue
School of Business
Sun Yat-sen University
xuefj@mail.sysu.edu.cn

December 2023

Abstract: This study examines the effect of customers' cybersecurity risk on suppliers' cost management strategies. A firm's cost structure is affected by its expectations of future demand. Since customers' cybersecurity risk may impact suppliers' expectations regarding future demand, we expect suppliers to adjust their cost structure facing changes in customers' cybersecurity risk. Using customers' data breaches to measure changes in their cybersecurity risks and suppliers' cost stickiness to capture their cost management strategies, we find a negative association between customer data breaches and supplier cost stickiness, suggesting that such breaches reduce suppliers' optimism about future sales. This reduction is stronger if suppliers are managed by CEOs with high uncertainty avoidance and low long-term orientation. Employing the passage of data breach notification laws as a natural experiment, we find that the negative association between customer data breaches and supplier cost stickiness is less pronounced after these laws become effective. Our results are robust to measuring customer cybersecurity risk using the predicted probability of data breaches and controlling for supplier market competition and supplier data breaches. Collectively, our findings provide insights into the effect of data breaches and cybersecurity risks on cost management strategies along the supply chain network.

Keywords: data breach, cost stickiness, supply chain, managerial expectations, data breach notification laws

*Corresponding author, Lidasan Endowed Chair Professor of Accounting, School of Management, Fudan University, Shanghai, China, ronghuang@fudan.edu.cn.

"*In a digitally connected world, cybersecurity presents ongoing risks and threats to our capital markets and to companies operating in all industries, including public companies regulated by the Commission.*" ——Securities and Exchange Commission (SEC) (2018)

I. INTRODUCTION

Cybersecurity breaches are posing new and growing challenges for businesses due to the widespread adoption of information and communication technologies such as artificial intelligence, big data, and cloud computing (Kumar and Mallipeddi 2022). These breaches have proven to be quite costly, with an average cost of $9.44 million per data breach in the United States during 2022 according to the IBM Data Breach Report (IBM 2022). In light of the significant financial costs associated with data breaches and the substantial operational and financial interdependencies inherent in customer-supplier partnerships, data breaches can have spillover effects on supply chain partners (Luo and Choi 2022; Choi et al. 2016) that are susceptible to such cyberattacks (Zhang and Smith 2022). Based on a 2022 cybersecurity risk report published by BlueVoyant, 98% of firms across North America, Europe, and Asia Pacific suffered negative impacts stemming from data breaches within their supply chains.[1] Consistent with this evidence, prior research shows that data breaches have emerged as a major threat to firms' customer-supplier relationships (Luo and Choi 2022), causing dependent suppliers to reduce relationship-specific investments after major customers[2] experience data breaches (Do et al. 2023; He et al. 2020a). Despite the increasing prevalence and the profound spillover impacts of data breaches, existing studies have not examined how customer data breaches may affect supplier cost management strategies.

[1] See https://www.bluevoyant.com/press-releases/bluevoyant-research-reveals-defending-digital-supply-chains-remains-a-business-challenge.

[2] A firm's major customers (hereafter customers) refer to those representing a minimum of 10% of total sales and are mandated to be publicly disclosed in annual reports as per the guidelines of the Statements of Financial Accounting Standards (SFAS) No. 14 and No. 131 (Chen et al. 2022; Liang et al. 2023).

Cost management strategies are a fundamental and essential decision to support corporate business operations and performance (He et al. 2020b; Zhang et al. 2022), and are one of the crucial competitive strategies (Rosenzweig and Easton 2010) suppliers manage during daily operations (Liang et al. 2023). In this study, we focus on cost stickiness, a typical cost management strategy that reduces costs less when demand falls than increases costs for an equivalent demand increase (Anderson et al. 2003). Prior studies suggest that such asymmetric cost behavior occurs when top managers anticipate future demand to rebound, and thus make rational decisions to intentionally keep slack resources when sales decrease to lower adjustment costs (Anderson et al. 2003; Chen et al. 2019b). Considering that customer data breaches can fundamentally reshape suppliers' expectations about future customer demand (Do et al. 2023; He et al. 2020a), we expect that these breaches will induce suppliers to take real actions to adjust the allocations of resources.

Drawing upon data breach and cost stickiness studies, we expect that customer data breaches can affect supplier cost stickiness in the following ways. One the one hand, customer data breaches may decrease the degree of supplier cost stickiness. A data breach suffered by a customer not only impacts firm performance negatively (Juma'h and Alnsour 2020), but also adversely influences how suppliers perceive the customer's future business prospects (He et al. 2020a). This, in turn, discourages supplier managers from keeping slack cost capacity when demand decreases because of their pessimistic expectations of a future demand rebound (Liang et al. 2023; Chen et al. 2019b), leading to a lower level of cost stickiness. On the other hand, customer data breaches may positively affect supplier cost stickiness. Since cyberattacks have the potential to spread from the targeted firms to their supply chain partners (Crosignani et al. (2023), suppliers may allocate additional resources such as information technology (IT) investments to strengthen their cybersecurity measures and enhance their resilience to cyber risks (Ashraf 2022). Consequently, suppliers tend to delay cutting costs when sales fall, thereby

resulting in a higher level of cost stickiness. Collectively, whether and how suppliers adjust costs in response to customer data breaches is an empirical question.

We collect information on data breaches, supply chain relationships, and financial variables from multiple sources for a sample of 11,371 U.S. firm-year observations (2,153 firms) between 2005 and 2019. Following prior research, we focus on selling, general, and administrative (SG&A) cost stickiness because SG&A costs represent a significant portion of a firm's operational expenditures, and managers have a high degree of discretion over these costs and closely monitor them to ensure effective control (Anderson et al. 2003; Chang et al. 2022; Liang et al. 2023; Chen et al. 2023). We find a negative association between customer data breaches and supplier cost stickiness, suggesting that suppliers cut SG&A costs more rapidly in sales-decrease periods after their customers experience data breaches due to their pessimistic expectations of future demand.

We further examine whether the association between customer data breaches and supplier cost stickiness varies with managerial personal characteristics that may affect their expectations of future demand. Specifically, we investigate two types of culture-based personal characteristics proposed by Hofstede (2001) that could affect managers' future expectations: 1) uncertainty avoidance (UAI), conceptualized as "*the extent to which the members of a culture feel threatened by uncertain or unknown situations*" (Hofstede 2001); and 2) long-term orientation (LTO), defined as "*the fostering of virtues oriented towards future rewards, in particular, perseverance and thrift*". Considering that managers in more uncertainty-avoidant cultures tend to be more risk-averse and prone to avoiding potential losses in a likely worst-case scenario of future demand (Kitching et al. 2016; Hofstede et al. 2010), we hypothesize that the decrease in supplier cost stickiness following customer data breaches is more pronounced when suppliers are led by CEOs from high UAI cultures. In addition, managers from low LTO cultures are less likely to expect future demand to rebound (Kitching et al. 2016;

Hofstede et al. 2010). Therefore, we predict that the decrease in supplier cost stickiness in response to customer data breaches is stronger when suppliers are managed by CEOs from low LTO cultures. Our empirical analyses provide supports for these cross-sectional hypotheses.

To strengthen causality, we employ a staggered difference-in-differences methodology by leveraging the enactment of mandatory state-level data breach notification laws as a natural experiment. These laws mandate focal firms that experience data breaches to disclose the incidents to affected parties (Nikkhah and Grover 2022), which in turn incentivizes focal firms to implement actions to enhance their resilience to cyber risks (Ashraf and Sunder 2023). Therefore, we posit that suppliers' expectations of their customers' future demands may improve following the implementation of these laws, thereby leading to a slower reduction in costs when sales decline. Our empirical findings support this prediction, as we document that the decrease in supplier cost stickiness following customer data breaches is weakened after these laws are implemented in the states where the customer firms are located.

Another potential endogeneity concern is that the publicly reported data breaches may potentially underestimate the actual data breaches (Janvrin and Wang 2022). This, in turn, biases our documented effect of customer data breaches on suppliers cost stickiness. To mitigate this concern, we first construct a predicted customer data breach measure derived from a Probit model (Huang and Wang 2021) and then replicate the baseline analysis with this new independent variable. Our inferences remain the same.

Additionally, we find that our results are robust to (1) controlling for supplier product market competition (Zhang et al. 2022); (2) including data breaches encountered by suppliers themselves; (3) limiting our analysis to representative industries including the retail industry, the automobiles and trucks industry, and the electronic equipment industry; (4) focusing on hacking breaches; (5) employing alternative cost measures, such as cost of goods sold (COGS) (Weiss 2010) and operating costs (*XOPR*) (Lee et al. 2020); and (6) using alternative model

specifications that either remove the main effects of control variables while introduce two-way interactions with the log change in sales (Chang et al. 2022), or incorporate both the main effects of control variables and their interactions with the log change in sales (Liang et al. 2023).

Our study contributes to the literature in the following ways. First, we contribute to the literature on the economic consequences of data breaches. Regulators and researchers have studied the direct impacts of data breaches on firm operations (SEC 2018; see Janvrin and Wang 2022 for a comprehensive review). These studies show that such breaches are detrimental to firm reputation and revenue (D'Arcy et al. 2020; Gwebu et al. 2018), IT system efficiency (Sen and Borle 2015), financing activities (Huang and Wang 2021), and shareholder value (Kamiya et al. 2021; Ashraf and Sunder 2023). However, there is limited research on the implications of data breaches for their upstream suppliers' operational decisions (He et al. 2020a; Do et al. 2023). Our study fills this void by examining the effect of customer data breaches on suppliers' cost decisions. We also answer the call by Janvrin and Wang (2022) for more research on data breaches and cybersecurity in the accounting field.

Second, we contribute to the literature on the spillover effect of negative events along the supply chain. Prior studies have documented supply chain externalities of various events, such as bankruptcies, management turnover, credit supply shocks, and natural disasters. These events may have significant impact on supply chain partners' market value, credit risk, production output, SG&A expenses, profit margin, employment decision (Hertzel et al. 2008; Houston et al. 2016; Kolay et al. 2016; Costello 2020; Hendricks et al. 2020; Barrot and Sauvagnat 2016), etc. We extend this line of literature by documenting that cybersecurity risk caused by customers' data breach events, a significant risk for firms, can lead to a substantial spillover effect on the operations of suppliers.

Third, we contribute to the cost management literature by documenting the effect of customer-supplier relationship on cost stickiness. Prior studies on cost structure and cost

stickiness mainly focus on the focal firm's characteristics, such as asset intensity (Anderson et al. 2003), demand uncertainty (Banker et al. 2014), managerial incentives (Dierynck et al. 2012; Kama and Weiss 2013), and managerial perception of uncertainty (Chen et al. 2023), among others. However, there remains a paucity of research on whether customers' and suppliers' characteristics may affect the focal firm's cost decisions (Liang et al. 2023; Agarwal and Agarwal 2023). We add to this body of research by investigating whether customers' cybersecurity risk affects the supplier's cost management strategies. In particular, we offer valuable insights into the cost management literature by showing that customer data breaches play a crucial role in shaping supplier cost stickiness.

Finally, we contribute to the managerial expectations literature by developing a novel measure of managerial expectations regarding future demand. Prior studies typically capture managerial expectations using firm-specific variables, such as an indicator of whether sales revenue declined in the preceding period (Anderson et al. 2003; Chang et al. 2022; Dierynck et al. 2012) , and the tone of forward-looking statements (Liang et al. 2023; Chen et al. 2019b). We extend this line of research by measuring managerial expectations of future demand at the firm-manager level using CEOs' national cultural backgrounds of UAI and LTO as in the cross-cultural psychology literature (Hofstede et al. 2010; Hofstede 2001).

The remainder of this paper is structured as follows. Section 2 discusses related literature and develops main hypotheses. Section 3 provides details about the data, the measurements of key variables, and the research design. Section 4 reports the empirical findings and Section 5 concludes.

II. LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

2.1 Literature Review on Data Breach and Supply Chain Management

The Privacy Rights Clearinghouse (PRC) defines a data breach as "a security violation in which sensitive protected or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual or organization."[3] Such a breach can occur due to several reasons, such as hacking, theft of credit/debit card information, mishandling of sensitive data, as well as loss, theft, or improper disposal of documents or devices. Since data breaches are viewed as violations of trust and contracts, businesses face severe consequences such as financial loss, reputation damage, and consumer trust deterioration (Huang and Wang 2021; Janakiraman et al. 2018; Gwebu et al. 2018; Akey et al. 2021).

Researchers have examined how customers, investors, and creditors react to data breaches. Ponemon (2017) discovers that breached firms in the life science industry experience a 5.7 percent abnormal customer churn rate. Janakiraman et al. (2018) find that customers of breached firms significantly reduce their purchases. Additionally, breached firms face negative reactions from equity investors (Cavusoglu et al. 2004; Amir et al. 2018; Kamiya et al. 2021), as well as higher loan spreads and stricter collateral and covenant requirements (Huang and Wang 2021). Meanwhile, data breaches have spillover effects on firms within the same industry. Hinz et al. (2015) show that data breaches negatively impact not only the attacked firm but also the entire industry, leading to a reduction in stock prices of its peers. Peer data breaches may also cause a decrease in future internal control material weaknesses for non-breached firms (Ashraf 2022). However, improvements in data security after a breach receive positive market reactions for both the breached firm and its competitors (Jeong et al. 2019).

In addition to the above implications, data breaches could pose a significant risk to supply chain partners. Data breaches have emerged as a significant threat to supply chain

[3] See https://privacyrights.org/consumer-guides/what-do-when-you-receive-data-breach-notice.

relationships (Hoehle et al. 2022), making it necessary for firms to focus on supply chain management (Luo and Choi 2022). Some studies have examined the impact of data breaches along the supply chain. For example, both Do et al. (2023) and He et al. (2020a) document that suppliers decrease relationship-specific investments following customer data breaches, as such data breaches of customers impair the corresponding suppliers' perception of the customers' future market prospects. Crosignani et al. (2023) report that cyberattacks have the potential to spread from the targeted firms to their downstream trading partners, leading to substantial revenue losses for the impacted partners. Zhang and Smith (2022) show that customer data breaches are associated with an increase in audit fees for their suppliers. However, prior studies have not examined the spillover effects of customers' data breaches on suppliers' cost management strategies.

2.2 Literature Review on Cost Management

Cost management strategies are essential to firms' resource planning and operational decisions. Deliberate cost management strategies may lead to an asymmetric cost behavior called "cost stickiness" (Anderson et al. 2003; see Ibrahim et al. 2022 for a review), which shows that SG&A costs are sticky; that is, they move upward more during a rise in sales than they move downward during a fall in sales. A key reason for this sticky cost behavior is that managers deliberately hold slack resources in sales-decreasing periods to reduce adjustment costs in anticipation of a future sales rebound (Anderson et al. 2003).

Prior literature shows that managerial expectations of future demand are essential for managers' decisions to adjust costs when sales change, thereby affecting the degree of cost stickiness (Chen et al. 2019b; Banker and Byzalov 2014). For example, the decision of whether to release or maintain underutilized resources during periods of sales decrease is based on managerial anticipations of the adjustment costs associated with removing resources in the short term and replacing them when future sales return. If managers expect that the current

sales decline is temporary and future demand will quickly restore, they tend to carry slack resources instead of removing them, leading to a high level of cost asymmetry (Anderson et al. 2003). Liang et al. (2023) extend this line of research by analyzing cost asymmetry along supply chains. They find that suppliers' cost stickiness is positively associated with their customers' managerial expectations of future demand. Nevertheless, research on how suppliers make cost decisions when their customers experience data breaches is still nascent.

2.3 Hypothesis Development

Drawing from prior research on data breach and cost management, we expect that customer data breaches may affect suppliers' cost stickiness. In a customer-supplier relationship, suppliers are typically in a vulnerable position and subject to significant power and influence from customers (Chen et al. 2022). As such, suppliers' operational decisions are often influenced by negative events (e.g., credit shocks, payment distortions) experienced by their customers (Agca et al. 2022; Serrano et al. 2018; Hertzel et al. 2008). As a salient type of negative event, customer data breaches may impact suppliers' operational decisions significantly. Consistent with this notion, recent research shows that customer data breaches reshape suppliers' anticipations of the customers' future growth prospects (Do et al. 2023; He et al. 2020a). This, in turn, may influence a firm's cost management strategies and lead to changes in the level of cost stickiness (Anderson et al. 2003; Liang et al. 2023).

We first hypothesize that customer data breaches lead to significant reductions in supplier cost stickiness. Prior literature finds that customer data breaches weaken trading relationships between supply chain partners (Do et al. 2023; He et al. 2020a). However, suppliers cannot afford to lose a significant part of customer demand, because they typically rely on a limited number of major customers who are considerably large in size (Patatoukas 2012; Chen et al. 2019a). As a result, terminating existing trading relationships with customers who suffer data breaches is not a rational decision for suppliers as they need to invest

substantial additional efforts and resources in finding new customers to replace the lost business (Crook and Combs 2007). Therefore, suppliers are expected to act in a way to maintain the trading relationships with their major customers while adjusting their operational resources as a response to customer data breaches. In addition, customers' data breaches can lower suppliers' expectations for such customers' future business prospects (He et al. 2020a), as such breaches lead to a decline in the attacked firm's performance (Juma'h and Alnsour 2020). Consequently, suppliers tend to remove slack resources during a sales decline in the expectations of future demand deterioration (Liang et al. 2023; Chen et al. 2019b). This results in a decrease in cost stickiness among suppliers. Therefore, we propose the following hypothesis, stated in the alternative form:

H1. *Customer data breaches are associated with a decrease in supplier cost stickiness.*

Alternatively, the occurrence of customer data breaches can have a positive impact on supplier cost stickiness. Agca et al. (2022) document that customers' negative events (i.e., credit shocks) can permeate upstream and increase suppliers' risk. More related to our study, Crosignani et al. (2023) show that cyber threats can spread along the supply chain. Hence, customers' data breaches can lead to a higher level of potential cyber risk for suppliers that have not yet faced such situation. As a response, suppliers may strengthen their cybersecurity measures to minimize such potential risks by committing more resources such as additional investments in IT security and procurement of cybersecurity insurance (Ashraf 2022; Janvrin and Wang 2022). Therefore, suppliers may delay cutting costs during sales-decrease periods of falling sales, leading to an increase in supplier cost stickiness. Therefore, the exact association between customer data breaches and supplier cost stickiness is an empirical question.

2.4 The Moderating Role of Supplier CEOs' Characteristics

Since supplier managers' expectations about future demand may affect their cost decisions after customers experience data breaches, we examine whether the association

between customer data breach and supplier cost stickiness is conditional on supplier CEOs' personal attributes. We focus on CEOs' uncertainty avoidance and long-term orientation, two attributes that may significantly shape managerial expectations about future demand (Hofstede et al. 2010; Kitching et al. 2016; Brochet et al. 2019).

2.4.1 Uncertainty Avoidance (UAI)

UAI influences individuals' tendencies to actively avoid uncertain outcomes. Members from cultures with high UAI tend to exhibit an aversion to uncertainty and behave more conservatively (Hofstede 2001). For example, managers from cultures characterized by a higher degree of uncertainty avoidance often exhibit increased risk aversion and a tendency to steer clear of potential losses (Hofstede 2001; Hofstede et al. 2010; Kanagaretnam et al. 2014), particularly when facing uncertain future demand (Kitching et al. 2016). Specifically, managers who prioritize avoiding uncertainty may place more emphasis on current demand signals that are certain, whereas overlooking future demand prospects that are inherently uncertain (Kitching et al. 2016). As a result, supplier managers from high UAI cultures are more likely to behave conservatively facing customer data breaches, such as quickly cutting unutilized costs and removing excess capacity. This cost management strategy contributes to a more pronounced reduction in cost stickiness. Therefore, we anticipate that the decline in supplier cost stickiness associated with customer data breaches could be magnified for supplier CEOs from national cultures with high levels of UAI, stated as follows:

H2. *The decrease in supplier cost stickiness following customer data breaches is stronger if suppliers are managed by CEOs from high UAI cultures.*

2.4.2 Long-term Orientation (LTO)

Next, we expect that the decline in supplier cost stickiness following customer data breaches is attenuated for supplier CEOs from national cultures with high LTO. LTO reflects the willingness of individuals to forego short-term benefits for the sake of long-term gains.

Long-term orientated people usually exhibit a forward-thinking approach and emphasize future implications in making decisions (Hofstede 2001; Hofstede et al. 2010). Hence, managers from cultures with high LTO are more inclined to consider the possibility of future sales reversals and hold a more optimistic view (Kitching et al. 2016), leading them to hold slack capacity in demand-decreasing periods after customer data breaches.

In contrast, supplier managers from cultures with a short-term orientation (i.e., low LTO) prefer to make long-term sacrifices for short-term gratification (Skowronski et al. 2022). Since retaining excessive resource capacity is typically costly in the short term (Anderson et al. 2003), those managers would act in a way to remove slack costs more aggressively when sales drop following customer data breaches to increase near-term earnings. Furthermore, these CEOs tend to hold pessimistic anticipations regarding a potential future demand recovery (Kitching et al. 2016). This leads to a greater reduction in supplier cost stickiness. Thus, we present the following hypothesis:

H3. *The decrease in supplier cost stickiness following customer data breaches is stronger if suppliers are managed by CEOs from low LTO cultures.*

III. METHODOLOGY

3.1 Sample and Data Sources

We obtain a sample of 9,025 reported data breach events in the U.S. from the Privacy Rights Clearinghouse (PRC) database[4] over the period 2005[5] to 2019. We choose the U.S. sample because the breached firms are required to notify affected organizations under data breach notification laws in the U.S. (Nikkhah and Grover 2022; Kamiya et al. 2021). This ensures that the affected business partners, including the suppliers, are aware of the data breach incidents of their customers. A key advantage of the PRC database is that it provides detailed

[4] The information is available at: https://www.privacyrights.org/data-breaches.
[5] We use 2005 as the starting year because PRC tracks publicly reported data breaches since 2005.

information on data breaches such as the name of the breached firm, the reported date of the breach, the type of breach, and the detailed description of breach. A number of recent studies in various settings across multiple disciplines have confirmed the validity, reliability and usefulness of reported data breach events in the PRC database (Haislip et al. 2021; Ashraf 2022; Li et al. 2022; Kamiya et al. 2021).

For the 9,025 reported data breaches, we use fuzzy name-matching algorithm to match company names found in the PRC database against those listed in Compustat and the Center for Research in Securities Prices (CRSP). We retain only matched records that achieve a similarity score of 80% or higher, leading to a reduced sample of 3,600 reported data breaches. To ensure the accuracy of our analysis, we perform the following procedure. First, we manually check these matches and remove cases where the match is unclear or the name abbreviation corresponds to multiple companies. Second, we follow Huang and Wang (2021) and restrict the sample to the most severe data breach incidents that have the highest number of records lost if firms experience multiple data breach events in a year. The above procedure yields a final sample of 602 data breach events.

Table 1 summarizes our sample selection process. Consistent with recent research (Chiu et al. 2019; Houston et al. 2016; Li et al. 2023; Serpa and Krishnan 2018), we identify a supplier's major customers based on the widely used "*WRDS Supply Chain with IDs (Compustat Segment)*" database[6] that is built on Compustat segment files, with an initial sample of 50,639 distinct supplier-customer-year pairs. From this sample, we exclude 189 parent-subsidiary pairs where the customer and supplier share the same identifier (GVKEY), as well as 15,563 observations that have missing values in suppliers' sales to customers. Moreover, to address the potential issue of dependence among observations in our empirical

[6] https://wrds-www.wharton.upenn.edu/pages/get-data/linking-suite-wrds/supply-chain-with-ids-compustat-segment/.

regressions (i.e., multiple firm-year observations from the same supplier), we limit our analysis to the most significant customer (based on suppliers' sales percentages) for each supplier-year (Cho et al. 2020; Bauer et al. 2018). This procedure removes 17,758 supplier-customer-year observations. In addition, we exclude 271 observations with missing data in suppliers' sales. We then merge the supplier-customer-year sample with customer data breaches from PRC, excluding 2,647 observations without lagged customer data breaches. Finally, we delete 254 observations from the financial industry (SIC 6000-6999) and 1,691 observations without available data for constructing main variables. Our final sample contains 11,371 unique supplier-year observations, with 2,153 unique suppliers, 1,017 unique customers, and 526 customer data breach events.

3.2 Research Design

We use the following cost stickiness model developed by Anderson et al. (2003) and augmented by Zhang et al. (2022):[7]

$$\begin{aligned}\Delta LOG(SG\&A_{i,t}) = {} & \beta_0 + \beta_1 \Delta LOG(SALES_{i,t}) + \beta_2 DEC_{i,t} * \Delta LOG(SALES_{i,t}) \\ & + \{\beta_3 CDB_{i,t-1} + \beta_4 AI_{i,t} + \beta_5 EI_{i,t} + \beta_6 SUCC_{i,t} + \beta_7 RDI_{i,t}\} \\ & * DEC_{i,t} * \Delta LOG(SALES_{i,t}) \\ & + \{\beta_8 CDB_{i,t-1} + \beta_9 AI_{i,t} + \beta_{10} EI_{i,t} + \beta_{11} SUCC_{i,t} + \beta_{12} RDI_{i,t}\} + \mu_{i,t}, \quad (1)\end{aligned}$$

where $\Delta LOG(SG\&A_{i,t})$ is the log-change in SG&A costs and $\Delta LOG(SALES_{i,t})$ is the log-change in total sales revenue, for firm *i* in year *t*, respectively. $CDB_{i,t-1}$ is customer data breach in the preceding year, defined as a binary indicator equal to 1 if any of supplier firm *i*'s most significant customer exhibits a data breach in year *t-1*, and 0 otherwise. $DEC_{i,t}$ is a dummy variable equal to 1 if there is a decrease in sales in year *t*, and 0 otherwise. Our main coefficient of interest is β_3, which characterizes the impact of customer data breaches on supplier cost

[7] In Section 4.5, we find our main inferences are robust to alternative cost stickiness models.

stickiness. A positive value for β_3 would suggest that supplier SG&A costs are less sticky after customer data breaches, consistent with *H1*.

To account for various economic factors that are likely to affect cost stickiness, we incorporate an array of control variables that have been identified in prior research. Asset intensity ($AI_{i,t}$) is the ratio of total assets over sales; employee intensity ($EI_{i,t}$) is the ratio of number of employees scaled by total sales; successive revenue decreases $SUCC_{i,t}$ takes a value of 1 if sales decrease in both the current and the preceding years, and 0 otherwise; $RDI_{i,t}$ is the proxy for research and development (R&D) intensity, defined as the ratio of total R&D expenses to total sales. Appendix A provides details on variable definitions. All continuous variables are winsorized at the top and bottom 1% levels to reduce the influence of outliers. We estimate Equation (1) using ordinary least squares (OLS) with year and four-digit SIC code industry fixed effects.

3.3 Measuring the Moderators

Consistent with existing literature (Merkley et al. 2020; Jung et al. 2019; Pan et al. 2020), we measure the CEO's cultural attributes utilizing the CEO's surname to identify his or her country of origin. Prior research indicates that ancestry has an enduring cultural impact that can last for multiple generations (Guiso et al. 2006). Therefore, we can reasonably attribute cultural backgrounds even if an individual's family has resided in the United States for multiple generations (Du et al. 2017). Furthermore, managers' ethnic cultural backgrounds reveal their inherited culture, which in turn can provide insight into their behaviors (Brochet et al. 2019).

To measure CEOs' cultural-based UAI and LTO, we use a three-step approach. First, we collect surnames of CEOs from Standard & Poor's ExecuComp database, which includes executives of S&P 1500 firms dating back to 1992, and supplement top managers' surnames with data from conference calls transcripts. In the second step, we adopt the name-matching approach proposed by Jung et al. (2019) and Merkley et al. (2020) to determine the cultural

origin of CEOs. Specifically, we use two ancestral dictionaries, the Oxford Dictionary of American Family Names and Ancestry.com, to map CEO surnames to their respective countries of origin. The Oxford Dictionary is preferred due to its academic credibility and reliability (Merkley et al. 2020), while Ancestry.com is used as a supplement (Pan et al. (2020); Jung et al. (2019). This allows us to assign a specific country of origin to each CEO based on his or her surname.

Third, we match the country of origin to Hofstede's national cultural database, which provides the country-level UAI and LTO indexes, and obtain CEOs' attitudes toward uncertainty and time orientation, respectively (Hofstede 2001; Hofstede et al. 2010). As such, we obtain the CEO's ethnic cultural backgrounds for each firm-year.

IV. EMPIRICAL ANALYSES

4.1 Sample Distribution and Descriptive Statistics

Table 2 presents the distribution of 526 customer data breach events by incidence type (Panel A) and the Fama-French 48 industry (Panel B). Of these breaches, 117 (22.24%) are caused by unintended disclosure, 104 (19.77%) are caused by portable device, and 101 (19.20%) are caused by hacking or malware. Such distribution is consistent with that reported by Huang and Wang (2021). We also observe that the retail industry accounts for the highest number of data breaches (241), followed by the automobiles and trucks industry (50), and the electronic equipment industry (41).

Table 3 reports the descriptive statistics (Panel A) and the correlation matrix (Panel B) for our sample. Consistent with recent studies on asymmetric cost behavior (Chang et al. 2022; Chen et al. 2023), our sample exhibits right-skewed distributions for SG&A costs and sales revenue, with mean (median) values of $446.794 ($76.659) and $2,622.837 ($423.378) million, respectively. Furthermore, the mean value of customer data breach is 0.045 with a standard deviation of 0.207, which is in line with the numbers provided in extant research (He et al.

2020a). The distributions of other control variables are also largely consistent with those in prior studies (Chen et al. 2019b; Liang et al. 2023; Zhang et al. 2022).

4.2 Baseline Results

We present the results of our main analysis in Table 4. Column (1) provides the results using only the basic cost asymmetry model proposed by Anderson et al. (2003). We find a positive and significant coefficient on $\Delta LOG(SALES)$ (coefficient = 0.480, t-statistic = 30.60) and a significantly negative coefficient on $DEC*\Delta LOG(SALES)$ (coefficient = −0.174, t-statistic = −6.81), suggesting that SG&A costs are sticky.

Column (2) reports the expanded model (i.e., Equation (1)) that includes our main variable of interest and the control variables. Consistent with *H1*, we find a positive and significant coefficient on $DEC*\Delta LOG(SALES)*CDB$ (coefficient = 0.143, t-statistic = 3.23).[8] The coefficient is also economically significant, i.e., a one-standard-deviation increase in *CDB* from its mean value results in a 2.7% (coefficient*standard deviation of *CDB* = 0.143* 0.207 = 0.027) reduction in supplier cost stickiness. That is, when customers suffer data breaches, suppliers tend to expedite cutting excess capacity during a sales decline. This finding supports *H1* that customer data breaches lead to a lower degree of cost stickiness among suppliers.

4.3 Results of the Moderating Effects

Next, we investigate the moderating effects of supplier CEOs' characteristics of uncertainty avoidance (*H2*) and long-term orientation (*H3*). We first divide our sample into low and high subsamples based on the median value of conditioning variables (i.e., UAI and LTO). We then estimate Equation (1) separately for firms in the low and high subsamples, respectively. Tables 5 reports the estimation results.

[8] We also find that all the variance inflation factors (VIFs) are well below the threshold of 10 (O'brien 2007), indicating that multicollinearity is not a concern in our study.

Columns (1) and (2) of Table 5 show that the estimated coefficients on *DEC*ΔLOG(SALES)*CDB* are both positive and significant for the low and the high UAI subsamples (coefficient = 0.754, t-statistic = 1.95 for the low UAI subsample; coefficient = 1.350, t-statistic = 2.46 for the high UAI subsample). However, the coefficient is significantly larger for the high UAI than for the low UAI subsamples. The difference in the coefficients across two subsamples are statistically significant (F-statistic = 2.80; p-value < 10%). This finding is consistent with *H2*, indicating that the reduction in supplier cost stickiness after customer data breaches is more pronounced when suppliers are managed by uncertainty-avoiding CEOs.

Columns (3) and (4) show that the coefficient on *DEC*ΔLOG(SALES)*CDB* is positive and significant in the low LTO subsample (coefficient = 0.907, t-statistic = 2.43), while it is insignificant in the high LTO subsample (coefficient = 0.929, t-statistic = 1.52). The results support *H3* that supplier CEOs with short-term orientation are more inclined to cut excess resources during periods of decreased sales compared to long-term oriented supplier CEOs.

4.4 Addressing Endogeneity

4.4.1 A Natural Experiment: Data Breach Notification Laws

To examine the causal relationship between customer data breaches and supplier cost management strategies, we use the enactment of data breach notification laws (hereafter notification laws)[9] as a quasi-experimental setting. Fifty-one states in the United States enacted notification laws at different points in time between 2003 and 2018 (see Appendix B). These laws require breached companies to disclose data breaches to affected parties (Nikkhah and Grover 2022), and are largely exogenous to breached and affected firms (Huang and Wang 2021). While notification laws may incur costs for breached firms (e.g., notification expenses)

[9] Available at: https://www.perkinscoie.com/images/content/1/9/v2/197566/SecurityBreach-Notification-Law-Chart-June-2018.pdf.

(Huang and Wang 2021), they assist in mitigating shareholder risk by motivating managers to take concrete actions to minimize firms' vulnerability to cyber threats (Ashraf and Sunder 2023). As such, we contend that suppliers may hold more positive views of customers' future demand following the implementation of these laws in the states where their customers are based, thereby delaying cutting costs when sales fall.

Using the staggered implementation of these mandatory state-level laws, we examine the difference-in-difference impact of these laws on the relation between customer breaches and supplier cost stickiness. Specifically, we introduce an indicator variable, *POSTLAW*, that takes a value of 1 if a customer data breach occurs after the effective date of the data breach notification law in the state where the customer firm is located, and 0 otherwise. We then estimate the following equation:

$$\begin{aligned}\Delta LOG(SG\&A_{i,t}) = {} & \beta_0 + \beta_1 \Delta LOG(SALES_{i,t}) + \beta_2 DEC_{i,t} * \Delta LOG(SALES_{i,t}) \\ & + \{\beta_3 CDB_{i,t-1} + \beta_4 POSTLAW_{i,t} + \sum Controls_{i,t}\} \\ & * DEC_{i,t} * \Delta LOG(SALES_{i,t}) \\ & + \beta_5 CDB_{i,t-1} * POSTLAW_{i,t} * DEC_{i,t} * \Delta LOG(SALES_{i,t}) \\ & + \beta_6 CDB_{i,t-1} + \beta_7 POSTLAW_{i,t} + \sum Controls_{i,t} + \mu_{i,t} \end{aligned} \quad (2)$$

Our main variable of interest is *DEC*ΔLOG(SALES)*CDB*POSTLAW*, which captures the causal effect of notification laws. Results in Table 6 show a significantly negative coefficient on this variable (coefficient = −0.371; t-statistic = −1.93), suggesting that supplier cost stickiness after a customer data breach is attenuated after the passage of these laws. This finding supports the argument that the implementation of notification laws reduces customers' exposures to cyber risks in the future, ultimately enhancing suppliers' optimism in customers' future demands.

4.4.2 Two-stage Analysis: The Predicted Probability of Customer Data Breach

Our analysis relies on data breach incidents that have been publicly disclosed by customer firms. However, this approach may potentially underestimate the actual frequency of customer data breaches and thus overestimate their impact on suppliers. Publicly observable data breaches are a function of both the presence and the reporting of a data breach event. In cases where organizations opt not to publicly report the existence of data breaches (Janvrin and Wang 2022), this potential underestimation occurs. To mitigate this endogeneity concern, we adopt a two-stage procedure by first estimating the likelihood of customer data breaches and then re-estimate Equation (1) using this predicted likelihood.

In the first stage, following Huang and Wang (2021), we use a Probit model to predict the likelihood of a data breach event as follows:

$$Prob(BREACH_{i,t}) = SIZE_{i,t-1} + ROA_{i,t-1} + LEVERAGE_{i,t-1} + PPE_{i,t-1} + ZSCORE_{i,t-1} + MTB_{i,t-1} + SEGMENT_{i,t-1} + EVOL_{i,t-1} + ICW_{i,t-1} + \varepsilon_{i,t} \quad (3)$$

The dependent variable *BREACH* is a binary indicator that equals 1 if firm *i* experiences a data breach in year *t*, and 0 otherwise. Consistent with Huang and Wang (2021), all explanatory variables are lagged by one year to predict the likelihood of a data breach. These explanatory variables include firm size (*SIZE*), performance (*ROA*), financial leverage (*LEVERAGE*), tangibility (*PPE*), financial conditions (*ZSCORE*), market-to-book ratio (MTB), complexity of operations (*SEGMENT*), volatility of operations (*EVOL*), and internal control (*ICW*). Appendix A provides details on variable definitions and Appendix C tabulates the estimation results.

Next, we utilize the estimated coefficients from Equation (3) to calculate the data breach probability for each firm-year. Then we match this predicted probability to our benchmark sample and obtain the likelihood of a customer data breach, *P(CDB)*. In the second stage, we replace the independent variable *CDB* in model (1) with *P(CDB)* and present the estimation

results in Table 7. We show that the coefficient on *DEC*ΔLOG(SALES)*P(CDB)* remains positive and significant, further supporting *H1*.

4.5 Additional Analyses

4.5.1 Addressing Alternative Explanations

Our findings may be potentially confounded by product market competition among suppliers, because Zhang et al. (2022) document that the presence of competition increases firms' investment in sticky SG&A spending. To rule out this confounding factor, we follow Zhang et al. (2022) and include a control variable for supplier product market competition in our baseline specification, proxied by the Herfindahl-Hirschman index (*HHI*). As shown in Column (1) of Table 8, we find that our main findings remain after controlling for suppliers' product market competition.

We also consider the possibility that the observed effects on supplier cost stickiness are driven by supplier data breaches rather than customer data breaches. To mitigate this concern, we control for supplier data breaches (i.e., *SDB*) and its interaction with the sales decrease dummy and the log change in sales (i.e., *DEC*ΔLOG(SALES)*SDB*). Column (2) of Table 8 confirms that our main results are robust to controlling for the occurrence of supplier data breaches.

4.5.2 Additional Robustness Checks

We conduct several additional robustness tests and present the results in Table 9. First, the sample distribution by industry in Panel B of Table 2 indicates that customer data breaches are concentrated in the retail industry, the automobiles and trucks industry, and the electronic equipment industry. Therefore, we repeat the analysis in these three representative industries. Column (1) of Table 9 shows that the main results continue to hold.

Second, we examine variations in the types of data breaches. The PRC database categorizes data breaches into eight types (as reported in Panel A of Table 2). Among these

types, a data breach caused by a hacking (malware) event causes the highest direct and reputational costs (Ponemon 2017), as well as the largest default and information risks for firms (Huang and Wang 2021). Therefore, we focus our analysis on this severe case of data breach and report our findings in Column (2) of Table 9. Specifically, we replace *CDB* with an alternative indicator variable that equals 1 if the breach involves hacking or malware, and 0 otherwise (Huang and Wang 2021). We continue to find a significantly positive coefficient on our variable of interest.

Third, we follow previous studies and employ cost categories other than SG&A, such as cost of goods sold (*COGS*) (Weiss 2010) and operating costs (*XOPR*) (Lee et al. 2020), to capture cost management strategy. We repeat our analysis by replacing the dependent variable with these two alternative cost measures. Columns (3) and (4) of Table 9 show that our main results continue to hold.

Finally, to further enhance the reliability of our findings, we consider two alternative cost stickiness models in recent studies. The first model, introduced by Chang et al. (2022), removes the main effects of economic factors and incorporates the effects of two-way interactions between these control variables and the log change in sales. We also examine Liang et al. (2023)'s cost stickiness model that includes both the main effects of economic factors and their interactions with the log change in sales. Results in Columns (5) and (6) suggest that our results are robust to using these two alternative sticky cost models.

V. CONCLUSION

This study investigates whether the rapidly increasing phenomenon of data breaches affect firms' cost management strategies along the supply chain. Our analyses reveal several key findings. We first document that customer data breaches result in a decline in the degree of suppler cost stickiness, indicating that these breaches reduce suppliers' optimism regarding future sales. Using managers' national cultural charcteristics to capture their expectations of

future sales, we find that the negative association between customer data breaches and supplier cost stickiness is more pronounced among supplier CEOs with high uncertainty avoidance and low long-term orientation. To address potential endogeneity concerns, we use the enactment of data breach notification laws as a quasi-experimental setting and employ a two-stage regression analysis, and find consistent findings. Additionally, our results are not driven by alternative explanations such as competition in the supplier product market or data breaches suffered by suppliers. Our main inference is also robust when we restrict our sample to criminal data breaches caused by hacking or malware, analyze representative industries, employ alternative measures of cost stickiness, and use alternative model specifications.

Our findings have important implications for understanding and mitigating cybersecurity risks along the supply chain. First, our findings indicate that top management teams are aware of the potential spillover effects of their customers' data breaches, as these breaches have become one of the major threats to firms' customer-supplier relationships (Hoehle et al. 2022; Luo and Choi 2022). The decrease in cost stickiness observed in the study suggests that supplier firms tend to be more conservative in managing their costs to mitigate the negative impact of customer data breaches. Future research can be conducted along several dimensions, such as investigating the effect of customer data breaches on supply firms' investing, financing, and contracting decisions.

Second, our analyses have policy implications for regulators, particularly with respect to the adoption of mandatory state-level data breach notification laws. The ever-increasing cybersecurity risks that companies face have received considerable attention from the regulators (SEC 2018). We document that mandatory state-level data breach notification laws can have a positive impact on supplier firms' cost management strategies after customer data breaches. Regulators can leverage this evidence to encourage the adoption of such laws to reduce the negative effects of data breaches on firm stakeholders. Further mandating and

facilitating firms to disclose data breach events is one potential way for regulators to help minimize the growing risks accompanied by cybersecurity incidents.

REFERENCES

Agarwal, N., and S. Agarwal. 2023. Cost decisions of supplier firms: A study based on the customer-supplier link. *Management Accounting Research*:100856.

Agca, S., V. Babich, J. R. Birge, and J. Wu. 2022. Credit shock propagation along supply chains: Evidence from the CDS market. *Management Science* 68 (9):6506-6538.

Akey, P., S. Lewellen, I. Liskovich, and C. Schiller. 2021. Hacking corporate reputations. *Rotman School of Management Working Paper* (3143740).

Amir, E., S. Levi, and T. Livne. 2018. Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies* 23:1177-1206.

Anderson, M. C., R. D. Banker, and S. N. Janakiraman. 2003. Are selling, general, and administrative costs "sticky"? *Journal of Accounting Research* 41 (1):47-63.

Ashraf, M. 2022. The role of peer events in corporate governance: Evidence from data breaches. *The Accounting Review* 97 (2):1-24.

Ashraf, M., and J. Sunder. 2023. Can shareholders benefit from consumer protection disclosure mandates? Evidence from data breach disclosure laws. *The Accounting Review* 98 (4):1-32.

Banker, R. D., and D. Byzalov. 2014. Asymmetric cost behavior. *Journal of Management Accounting Research* 26 (2):43-79.

Banker, R. D., D. Byzalov, and J. M. Plehn-Dujowich. 2014. Demand uncertainty and cost behavior. *The Accounting Review* 89 (3):839-865.

Barrot, J.-N., and J. Sauvagnat. 2016. Input specificity and the propagation of idiosyncratic shocks in production networks. *The Quarterly Journal of Economics* 131 (3):1543-1592.

Bauer, A. M., D. Henderson, and D. P. Lynch. 2018. Supplier internal control quality and the duration of customer-supplier relationships. *The Accounting Review* 93 (3):59-82.

Brochet, F., G. S. Miller, P. Naranjo, and G. W. Yu. 2019. Managers' cultural background and disclosure attributes. *The Accounting Review* 94 (3):57-86.

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.

Chang, H., X. Dai, E. Lohwasser, and Y. Qiu. 2022. Organized labor effects on SG&A cost behavior. *Contemporary Accounting Research* 39 (1):404-427.

Chen, C., J. B. Kim, M. Wei, and H. Zhang. 2019a. Linguistic information quality in customers' forward-looking disclosures and suppliers' investment decisions. *Contemporary Accounting Research* 36 (3):1751-1783.

Chen, G., X. S. Tian, and M. Yu. 2022. Redact to protect? Customers' incentive to protect information and suppliers' disclosure strategies. *Journal of Accounting and Economics* 74 (1):101490.

Chen, J. V., I. Kama, and R. Lehavy. 2019b. A contextual analysis of the impact of managerial expectations on asymmetric cost behavior. *Review of Accounting Studies* 24 (2):665-693.

———. 2023. The managerial perception of uncertainty and cost elasticity. *Journal of Accounting and Economics, Forthcoming*.

Chiu, T. T., J. B. Kim, and Z. Wang. 2019. Customers' risk factor disclosures and suppliers' investment efficiency. *Contemporary Accounting Research* 36 (2):773-804.

Cho, Y. J., Y. Kim, and Y. Zang. 2020. Information externalities and voluntary disclosure: Evidence from a major customer's earnings announcement. *The Accounting Review* 95 (6):73-96.

Choi, B. C., S. S. Kim, and Z. Jiang. 2016. Influence of firm's recovery endeavors upon privacy breach on online customer behavior. *Journal of Management Information Systems* 33 (3):904-933.

Costello, A. M. 2020. Credit market disruptions and liquidity spillover effects in the supply chain. *Journal of Political Economy* 128 (9):3434-3468.

Crook, T. R., and J. G. Combs. 2007. Sources and consequences of bargaining power in supply chains. *Journal of Operations Management* 25 (2):546-555.

Crosignani, M., M. Macchiavelli, and A. F. Silva. 2023. Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics* 147 (2):432-448.

D'Arcy, J., I. Adjerid, C. M. Angst, and A. Glavas. 2020. Too good to be true: Firm social performance and the risk of data breach. *Information Systems Research* 31 (4):1200-1223.
Dierynck, B., W. R. Landsman, and A. Renders. 2012. Do managerial incentives drive cost behavior? Evidence about the role of the zero earnings benchmark for labor cost behavior in private Belgian firms. *The Accounting Review* 87 (4):1219-1246.
Do, T. K., H. H. Huang, and A.-T. Le. 2023. Cybersecurity risk through the supply chain: Evidence from relationship-specific investment. *Working paper*.
Du, Q. Q., F. Yu, and X. Y. Yu. 2017. Cultural proximity and the processing of financial information. *Journal of Financial and Quantitative Analysis* 52 (6):2703-2726.
Guiso, L., P. Sapienza, and L. Zingales. 2006. Does culture affect economic outcomes? *Journal of Economic perspectives* 20 (2):23-48.
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.
Haislip, J., J.-H. Lim, and R. Pinsker. 2021. The impact of executives' IT expertise on reported data security breaches. *Information Systems Research* 32 (2):318-334.
He, C., J. HuangFu, M. J. Kohlbeck, and L. Wang. 2020a. The impact of customer's reported cybersecurity breaches on key supplier's relationship-specific investments and relationship duration. *Working paper*.
He, J., X. Tian, H. Yang, and L. Zuo. 2020b. Asymmetric cost behavior and dividend policy. *Journal of Accounting Research* 58 (4):989-1021.
Hendricks, K. B., B. W. Jacobs, and V. R. Singhal. 2020. Stock market reaction to supply chain disruptions from the 2011 Great East Japan Earthquake. *Manufacturing & Service Operations Management* 22 (4):683-699.
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.
Hinz, O., M. Nofer, D. Schiereck, 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.
Hoehle, H., V. Venkatesh, S. A. Brown, B. J. Tepper, and T. Kude. 2022. Impact of customer compensation strategies on outcomes and the mediating role of justice perceptions: A longitudinal study of target's data breach. *MIS Quarterly* 46 (1).
Hofstede, G. 2001. *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations*: Thousand Oaks, CA: Sage Publications.
Hofstede, G., G. J. Hofstede, and M. Minkov. 2010. *Cultures and organizations: Software of the mind. Revised and Expanded*. Vol. 2: Mcgraw-Hill New York.
Houston, J. F., C. Lin, and Z. Zhu. 2016. The financial implications of supply chain changes. *Management Science* 62 (9):2520-2542.
Huang, H. H., and C. Wang. 2021. Do banks price firms' data breaches? *The Accounting Review* 96 (3):261-286.
IBM. 2022. Cost of a data breach report 2022. *https://www.ibm.com/reports/data-breach*.
Ibrahim, A. E. A., H. Ali, and H. Aboelkheir. 2022. Cost stickiness: A systematic literature review of 27 years of research and a future research agenda. *Journal of International Accounting Auditing and Taxation* 46:100439.
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.
Janvrin, D. J., and T. W. Wang. 2022. Linking cybersecurity and accounting: An event, impact, response framework. *Accounting Horizons* 36 (4):67-112.
Jeong, C. Y., S.-Y. T. Lee, and J.-H. Lim. 2019. Information security breaches and IT security investments: Impacts on competitors. *Information & Management* 56 (5):681-695.
Juma'h, A. H., and Y. Alnsour. 2020. The effect of data breaches on company performance. *International Journal of Accounting & Information Management*.

Jung, J. H., A. Kumar, S. S. Lim, and C. Y. Yoo. 2019. An analyst by any other surname: Surname favorability and market reaction to analyst forecasts. *Journal of Accounting & Economics* 67 (2-3):306-335.
Kama, I., and D. Weiss. 2013. Do earnings targets and managerial incentives affect sticky costs? *Journal of Accounting Research* 51 (1):201-224.
Kamiya, S., J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz. 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics* 139 (3):719-749.
Kanagaretnam, K., C. Y. Lim, and G. J. Lobo. 2014. Influence of national culture on accounting conservatism and risk-taking in the banking industry. *The Accounting Review* 89 (3):1115-1149.
Kitching, K., R. Mashruwala, and M. Pevzner. 2016. Culture and cost stickiness: A cross-country study. *The International Journal of Accounting* 51 (3):402-417.
Kolay, M., M. Lemmon, and E. Tashjian. 2016. Spreading the misery? Sources of bankruptcy spillover in the supply chain. *Journal of Financial and Quantitative Analysis* 51 (6):1955-1990.
Kumar, S., and R. R. Mallipeddi. 2022. Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. *Production and Operations Management* 31 (12):4488-4500.
Lee, W. J., J. Pittman, and W. Saffar. 2020. Political uncertainty and cost stickiness: Evidence from national elections around the world. *Contemporary Accounting Research* 37 (2):1107-1139.
Li, C., N. Li, and F. Zhang. 2023. Using economic links between firms to detect accounting fraud. *The Accounting Review* 98 (1):399-421.
Li, W., A. C. M. Leung, and W. T. Yue. 2022. Where is IT in Information security? The interrelationship among IT investment, security awareness, and data breaches. *MIS Quarterly, forthcoming*.
Liang, P., H. Cavusoglu, and N. Hu. 2023. Customers' managerial expectations and suppliers' asymmetric cost management. *Production and Operations Management, forthcoming*.
Luo, S. Y., and T. M. Choi. 2022. E-commerce supply chains with considerations of cyber-security: Should governments play a role? *Production and Operations Management* 31 (5):2107-2126.
Merkley, K., R. Michaely, and J. Pacelli. 2020. Cultural diversity on Wall Street: Evidence from consensus earnings forecasts. *Journal of Accounting and Economics* 70 (1).
Nikkhah, H. R., and V. Grover. 2022. An empirical investigation of company response to data breaches. *MIS Quarterly* 46 (4):2163-2196.
O'brien, R. M. 2007. A caution regarding rules of thumb for variance inflation factors. *Quality & quantity* 41 (5):673-690.
Pan, Y., S. Siegel, and T. Yue Wang. 2020. The cultural origin of CEOs' attitudes toward uncertainty: Evidence from corporate acquisitions. *The Review of Financial Studies* 33 (7):2977-3030.
Patatoukas, P. N. 2012. Customer-base concentration: Implications for firm performance and capital markets. *The Accounting Review* 87 (2):363-392.
Ponemon, L. 2017. Cost of data breach study. *Ponemon Institute*.
Rosenzweig, E. D., and G. S. Easton. 2010. Tradeoffs in manufacturing? A meta-analysis and critique of the literature. *Production and Operations Management* 19 (2):127-141.
SEC. 2018. Commission statement and guidance on public company cybersecurity disclosures. *https://federalregister.gov/d/2018-03858*.
Sen, R., and S. Borle. 2015. Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems* 32 (2):314-341.
Serpa, J. C., and H. Krishnan. 2018. The impact of supply chains on firm-level productivity. *Management Science* 64 (2):511-532.
Serrano, A., R. Oliva, and S. Kraiselburd. 2018. Risk propagation through payment distortion in supply chains. *Journal of Operations Management* 58:1-14.
Skowronski, K., W. C. Benton, and S. Handley. 2022. The moderating influence of supplier culture on the relationship between buyer power and supplier shirking. *Journal of Operations Management* 68 (3):270-301.
Weiss, D. 2010. Cost behavior and analysts' earnings forecasts. *The Accounting Review* 85 (4):1441-1471.

Zhang, R. G., M. Hora, S. John, and H. A. Wier. 2022. Competition and slack: The role of tariffs on cost stickiness. *Journal of Operations Management* 68 (8):855-880.
Zhang, Y., and T. J. Smith. 2022. The impact of customer firm data breaches on the audit fees of their suppliers. *Working paper*.

APPENDIX A

Variable Definitions

Variable	Definition
CDB_{t-1}	A binary indicator that loads as 1 if any of supplier firm *i*'s most significant customer exhibits a data breach in year t-1, and 0 otherwise.
SG&A	Total selling, general, and administration expenses.
SALES	Total sales revenue.
DEC	A binary indicator that loads as 1 if there is a decrease in sales in year t, and 0 otherwise.
SUCC	A binary indicator that loads as 1 if sales revenue in year t-1 are less than those in year t-2, and 0 otherwise.
AI	Asset intensity, defined as total assets scaled by total sales revenue.
EI	Employee intensity, defined as number (thousand) of employees scaled by total sales revenue.
RDI	The ratio of total R&D expenses on total sales. Missing R&D values are set to 0.
UAI	Measure of CEO uncertainty avoidance.
LTO	Measure of CEO long-term orientation.
IND	Measure of CEO individualism.
SDB_{t-1}	A binary indicator that loads as 1 if any of supplier firm *i* exhibits a data breach in year t-1, and 0 otherwise.
HHI	Sum of squared market shares for all firms in the same industry (2−digit SIC), where the market share of an individual firm is the proportion of the firm's sales to the entire industry's sales.
CIO	A binary indicator that loads as 1 if firm *i*'s top management team in year *t* includes a Chief Information Officer, Chief Information Security Officer, or Chief Security Officer, and 0 otherwise.
$BREACH_t$	A binary indicator that loads as 1 if firm *i* exhibits a data breach in year t, and 0 otherwise.
SIZE	Natural logarithm of market value.
LEVERAGE	Long-term debt scaled by total assets.
PPE	Gross property, plant, and equipment scaled by total assets.
ZSCORE	Measured as 1.2 * (current asset – current liabilities) / total assets + 1.4 * retained earnings / total assets + 3.3 * earnings before interest and taxes / total assets + 0.6 * market value of equity / total liabilities + 0.999 * sales / total assets.
MTB	Market-to-book ratio, measured as market value scaled by book value.
SEGMENT	Natural logarithm of the number of business segments.
EVOL	Standard deviation of yearly cash flows from operations divided by total assets over the past five fiscal years.
ICW	A binary indicator that loads as 1 if the firm has an internal control weakness under SOX 302, and 0 otherwise.
SG	Year-to-year change in sales.

APPENDIX B

Effective Date of Data Breach Notification Laws

State	Effective Date	State	Effective Date	State	Effective Date
Alabama	2018/6/1	Louisiana	2006/1/1	Oklahoma	2008/11/1
Alaska	2009/7/1	Maine	2006/1/31	Oregon	2007/10/1
Arizona	2006/12/31	Maryland	2008/1/1	Oregon	2013/9/12
Arkansas	2005/8/12	Massachusetts	2007/10/31	Pennsylvania	2006/6/20
California	2003/7/1	Michigan	2007/7/2	Rhode Island	2016/7/2
California	2014/9/30	Michigan	2011/4/1	South Carolina	2009/7/1
Colorado	2006/9/1	Minnesota	2006/1/1	South Carolina	2013/4/23
Connecticut	2006/1/1	Mississippi	2011/7/1	South Dakota	2018/7/1
Delaware	2005/6/28	Missouri	2009/8/28	Tennessee	2005/7/1
Delaware	2010/6/10	Montana	2006/3/1	Tennessee	2016/7/1
DC	2007/7/1	Nebraska	2006/4/10	Tennessee	2017/4/4
Florida	2014/7/1	Nebraska	2016/7/20	Texas	2009/4/1
Georgia	2005/5/5	Nevada	2005/10/1	Texas	2013/6/14
Hawaii	2007/1/1	Nevada	2006/1/1	Utah	2007/1/1
Hawaii	2008/4/17	Nevada	2008/1/1	Utah	2009/5/12
Idaho	2006/7/1	Nevada	2011/10/1	Vermont	2012/5/8
Illinois	2006/6/27	New Hampshire	2007/1/1	Vermont	2013/5/13
Illinois	2012/1/1	New Jersey	2006/1/1	Virginia	2008/7/1
Illinois	2017/1/1	New Mexico	2017/6/16	Virginia	2011/1/1
Indiana	2006/7/1	New York	2005/12/7	Virginia	2017/7/1
Indiana	2009/7/1	North Carolina	2005/12/31	Washington	2005/7/24
Iowa	2008/7/1	North Carolina	2009/7/27	Washington	2010/7/1
Iowa	2014/7/1	North Dakota	2005/6/1	West Virginia	2008/6/6
Kansas	2007/1/1	North Dakota	2013/4/18	Wisconsin	2006/3/31
Kentucky	2014/7/15	Ohio	2006/02/29	Wyoming	2007/7/1
Kentucky	2015/1/1	Ohio	2007/3/30		

Notes*:* This table presents the dates when the data breach notification laws came into effect in each state (Huang and Wang (2021).

APPENDIX C

First-Stage Analysis: Predicting the Probability of Data Breaches

	(1) BREACH (t)
SIZE (t-1)	0.182***
	(8.08)
ROA (t-1)	0.071
	(0.28)
LEVERAGE (t-1)	0.386**
	(2.39)
PPE (t-1)	-0.515***
	(-3.19)
ZSCORE (t-1)	0.012*
	(1.93)
MTB (t-1)	-0.007
	(-1.12)
SEGMENT (t-1)	0.001
	(0.02)
EVOL (t-1)	-1.341**
	(-2.24)
ICW (t-1)	0.169
	(1.22)
CONSTANT	-4.014***
	(-19.28)
Observations	25,785
Pseudo-R^2	0.108

Notes: This table reports the results of predicting the probability of data breaches for each firm-year.

TABLE 1

Sample Selection Procedure

Step	Number of observations
All customer-supplier-year pairs (with GVKEYs) from fiscal year 2005 to 2019	50,639
Less:	
Customer and supplier with the same identifier (GVKEY)	(189)
Missing data in suppliers' sales to customers	(15,563)
Customers that are not the most significant for each supplier	(17,755)
Missing data in suppliers' sales	(271)
Firm-years without customer data breaches in the last year	(2,647)
Supplier firms in financial industries (SIC 6000–6999)	(1,152)
Missing data in constructing main variables	(1,691)
Total number of supplier-customer-year pairs in the final sample	**11,371**

Notes: This table presents the sample selection procedure.

TABLE 2

Distribution of Customer Data Breach Events

Panel A: Distribution of Customer Data Breach Events by Type

	Freq.	Percent	Cum.
Payment card fraud	83	15.78	15.78
Unintended disclosure	117	22.24	38.02
Hacking or malware	101	19.20	57.22
Insider	71	13.50	70.72
Physical loss	24	4.56	75.29
Portable device	104	19.77	95.06
Stationary device	12	2.28	97.34
Unknown	14	2.66	100.00
Total	526	100.00	

Panel B: Distribution of Customer Data Breach Events by Fama-French 48 Industries

	Fama-French Industry	Number of data breach events		Fama-French Industry	Number of data breach events
1	Agriculture	0	25	Shipbuilding, Railroad Equipment	0
2	Food Products	0	26	Defense	4
3	Candy & Soda	2	27	Precious Metals	0
4	Alcoholic Beverages	0	28	Nonmetallic Mining	0
5	Tobacco Products	0	29	Coal	0
6	Recreational Products	0	30	Petroleum and Natural Gas	9
7	Entertainment	0	31	Utilities	1
8	Printing and Publishing	0	32	Telecommunications	36
9	Consumer Goods	0	33	Personal Services	0
10	Apparel	0	34	Business Services	12
11	Healthcare	5	35	Computers	2
12	Medical Equipment	4	36	Electronic Equipment	41
13	Pharmaceutical Products	5	37	Measuring and Control Equipment	0
14	Chemicals	1	38	Business Supplies	0
15	Rubber and Plastic Products	0	39	Shipping Containers	0
16	Textiles	0	40	Transportation	9
17	Construction Materials	2	41	Wholesale	21
18	Construction	0	42	Retail	241
19	Steel Works, etc.	0	43	Restaurant, Hotels Motels	4
20	Fabricated Products	0	44	Banking	26
21	Machinery	0	45	Insurance	12
22	Electrical Equipment	0	46	Real Estate	3
23	Automobiles and Trucks	50	47	Trading	0
24	Aircraft	36	48	Other Industries	0

Notes: This table presents the distribution of 526 customer data breach events. Panel A presents the distribution of customer data breach events by type. Panel B presents the distribution of customer data breach events by Fama-French 48 industries.

TABLE 3

Descriptive Statistics and Correlations Matrix

Panel A: Descriptive Statistics

Variables		N	Mean	Std. Dev.	Q1	Median	Q3
1	SG&A	11,371	446.794	76.659	1,219.443	25.844	274.403
2	SALES	11,371	2,622.837	423.378	7,221.096	100.601	1,707.699
3	CDB_{t-1}	11,371	0.045	0.000	0.207	0.000	0.000
4	DEC	11,371	0.340	0.000	0.474	0.000	1.000
5	SUCC	11,371	0.406	0.000	0.491	0.000	1.000
6	AI	11,371	1.768	1.189	1.772	0.753	2.001
7	EI	11,371	4.473	3.097	5.490	1.707	4.954
8	RDI	11,371	0.092	0.013	0.185	0.000	0.117

Panel B: Correlation Matrix

Variables		1	2	3	4	5	6	7	8
1	SG&A		**0.867**	**0.093**	**-0.082**	**-0.117**	-0.008	**-0.152**	**0.135**
2	SALES	**0.774**		**0.083**	**-0.098**	**-0.126**	**-0.079**	**-0.262**	**-0.200**
3	CDB_{t-1}	**0.062**	**0.075**		**-0.025**	**-0.017**	**-0.065**	0.002	**-0.021**
4	DEC	**-0.026**	**-0.031**	-0.012		**0.138**	-0.002	**0.063**	**0.027**
5	SUCC	**-0.039**	**-0.050**	**-0.024**	**0.138**		0.013	**0.052**	0.008
6	AI	**-0.040**	**-0.086**	**-0.059**	**0.027**	**0.058**		**-0.174**	**0.128**
7	EI	**-0.099**	**-0.117**	**-0.020**	**0.036**	**0.045**	**-0.030**		**0.203**
8	RDI	0.001	**-0.089**	**-0.037**	**0.073**	**0.061**	**0.230**	**0.145**	

Notes: This table reports summary statistics and the Pearson (lower diagonal) and the Spearman (upper diagonal) correlations among variables in our baseline analysis. A correlation coefficient in bold indicates a significance level of 10% or lower.

TABLE 4

Customer Data Breaches and Supplier Cost Management Strategy

	(1) ΔLOG(SG&A)	(2) ΔLOG(SG&A)
ΔLOG(SALES)	0.480***	0.467***
	(30.60)	(29.28)
DEC*ΔLOG(SALES)	-0.174***	-0.188***
	(-6.81)	(-6.33)
DEC*△LOG(SALES)*CDB$_{t-1}$		**0.143*** **
		(3.23)
DEC*ΔLOG(SALES)*AI		0.000
		(0.15)
DEC*ΔLOG(SALES)*EI		-0.000
		(-0.24)
DEC*ΔLOG(SALES)*SUCC		0.067***
		(3.13)
DEC*ΔLOG(SALES)*RDI		-0.001
		(-0.08)
CDB$_{t-1}$		-0.001
		(-0.16)
AI		0.014***
		(6.70)
EI		0.001
		(1.33)
SUCC		-0.037***
		(-9.60)
RDI		0.026
		(1.41)
CONSTANT	0.051**	0.038
	(2.07)	(1.58)
Year FE	YES	YES
Industry FE	YES	YES
Observations	11,371	11,371
Adj-R^2	0.331	0.348
Mean VIF	2.14	2.39

Notes: This table presents the results of estimating the association between customer data breaches and supplier cost management strategy. Variables are defined in Appendix A. Robust standard errors are clustered at the firm level. *, ** and *** denote significance at the 10%, 5% and 1% levels, respectively.

TABLE 5

Moderating Effects of Supplier CEO Characteristics

	Uncertainty Avoidance		Long-term Orientation	
DV=ΔLOG(SG&A)	(1) Low UAI	(2) High UAI	(3) Low LTO	(4) High LTO
ΔLOG(SALES)	0.493***	0.504***	0.511***	0.453***
	(16.63)	(14.19)	(18.72)	(10.51)
DEC*ΔLOG(SALES)	-0.194***	-0.251***	-0.183***	-0.197*
	(-3.70)	(-3.45)	(-3.62)	(-1.88)
DEC*ΔLOG(SALES)*CDB$_{t-1}$	**0.754***	**1.350****	**0.907****	**0.929**
	(1.95)	**(2.46)**	**(2.43)**	**(1.52)**
DEC*ΔLOG(SALES)*AI	0.001	-0.021*	0.000	-0.027
	(0.93)	(-1.70)	(0.36)	(-1.60)
DEC*ΔLOG(SALES)*EI	0.001	0.034***	0.000	0.017**
	(0.81)	(3.88)	(0.16)	(2.09)
DEC*ΔLOG(SALES)* SUCC	0.009	0.083	0.013	0.098
	(0.20)	(1.34)	(0.27)	(1.45)
DEC*ΔLOG(SALES)*RDI	-0.009	-0.451***	-0.003	-0.259**
	(-0.91)	(-3.12)	(-0.31)	(-2.26)
CDB$_{t-1}$	0.022	0.012	0.018	0.022
	(1.60)	(1.09)	(1.49)	(1.48)
AI	0.014***	0.010*	0.011***	0.018***
	(4.11)	(1.84)	(3.36)	(3.07)
EI	-0.001	0.000	-0.001	0.001
	(-0.59)	(0.13)	(-1.43)	(0.58)
SUCC	-0.040***	-0.026***	-0.039***	-0.024**
	(-5.48)	(-3.20)	(-5.66)	(-2.56)
RDI	0.047	0.018	0.057	0.008
	(1.39)	(0.30)	(1.59)	(0.17)
CONSTANT	0.011	-0.079***	0.025	-0.067**
	(0.64)	(-4.18)	(1.57)	(-2.21)
F-statistic of difference (p-value)	2.80 (p < 10%)		3.14 (p < 10%)	
Year FE	YES	YES	YES	YES
Industry FE	YES	YES	YES	YES
Observations	3,324	1,791	3,474	1,641
Adj-R^2	0.370	0.412	0.391	0.371

Notes: This table presents the results of estimating the moderating effects of supplier CEO characteristics on the association between customer data breaches and supplier cost management strategy. Variables are defined in Appendix A. Robust standard errors are clustered at the firm level. *, ** and *** denote significance at the 10%, 5% and 1% levels, respectively.

TABLE 6

Effect of Data Breach Notification Law

	(1) △LOG(SG&A)
△LOG(SALES)	0.467***
	(29.28)
DEC*△LOG(SALES)	-0.186***
	(-6.23)
DEC*△LOG(SALES)*CDB_{t-1}	0.155***
	(3.41)
DEC*△LOG(SALES)*POSTLAW	-0.055
	(-0.51)
DEC*△LOG(SALES)*CDB_{t-1}*POSTLAW	**-0.371***
	(-1.93)
DEC*△LOG(SALES)*AI	0.000
	(0.15)
DEC*△LOG(SALES)*EI	-0.000
	(-0.25)
DEC*△LOG(SALES)* SUCC	0.067***
	(3.12)
DEC*△LOG(SALES)*RDI	-0.001
	(-0.07)
POSTLAW	-0.003
	(-0.42)
CDB_{t-1}	-0.002
	(-0.26)
AI	0.014***
	(6.70)
EI	0.001
	(1.34)
SUCC	-0.037***
	(-9.60)
RDI	0.026
	(1.42)
CONSTANT	0.039
	(1.58)
Year FE	YES
Industry FE	YES
Observations	11,371
Adj-R^2	0.348

Notes: This table presents the results of estimating the effect of data breach notification law on the association between customer data breaches and supplier cost management strategy. Appendix B provides the dates when the data breach notification laws came into effect in each state. Variable definitions are shown in Appendix A. Robust standard errors are clustered at the firm level. *, ** and *** denote significance at the 10%, 5% and 1% levels, respectively.

TABLE 7

Two-stage Analysis: Predicted Probability of Customer Data Breach

	(1) ΔLOG(SG&A)
ΔLOG(SALES)	0.480***
	(23.06)
DEC*ΔLOG(SALES)	-0.140*
	(-1.81)
DEC*ΔLOG(SALES)*P(CDB)	**0.041***
	(1.78)
DEC*ΔLOG(SALES)*AI	0.001
	(0.46)
DEC*ΔLOG(SALES)*EI	0.001
	(0.50)
DEC*ΔLOG(SALES)* SUCC	0.099***
	(2.99)
DEC*ΔLOG(SALES)*RDI	-0.009
	(-0.47)
P(CDB)	0.007
	(0.77)
AI	0.020***
	(7.20)
EI	0.001*
	(1.71)
SUCC	-0.037***
	(-7.29)
RDI	0.023
	(0.87)
CONSTANT	0.031
	(0.67)
Year FE	YES
Industry FE	YES
Observations	6,300
Adj-R^2	0.366

Notes: This table presents the results of estimating the association between customer data breaches and supplier cost management strategy using a two-stage analysis. Variables are defined in Appendix A. Robust standard errors are clustered at the firm level. *, ** and *** denote significance at the 10%, 5% and 1% levels, respectively.

TABLE 8

Controlling for Alternative Explanations

DV=∆LOG(SG&A)	(1) Supplier Product Market Competition	(2) Supplier Data Breach
∆LOG(SALES)	0.466***	0.467***
	(29.26)	(29.27)
DEC*∆LOG(SALES)	-0.219***	-0.187***
	(-5.85)	(-6.32)
DEC*∆LOG(SALES)*CDB$_{t-1}$	**0.144*** **	**0.143*** **
	(3.27)	**(3.24)**
DEC*∆LOG(SALES)*HHI	0.297	
	(1.36)	
DEC*∆LOG(SALES)*SDB$_{t-1}$		-0.155
		(-1.35)
DEC*∆LOG(SALES)*AI	0.000	0.000
	(0.16)	(0.15)
DEC*∆LOG(SALES)*EI	-0.000	-0.000
	(-0.24)	(-0.25)
DEC*∆LOG(SALES)* SUCC	0.068***	0.067***
	(3.18)	(3.13)
DEC*∆LOG(SALES)*RDI	-0.001	-0.001
	(-0.08)	(-0.07)
CDB$_{t-1}$	-0.001	-0.001
	(-0.18)	(-0.15)
HHI	0.018	
	(0.73)	
SDB$_{t-1}$		-0.019
		(-1.22)
AI	0.014***	0.014***
	(6.66)	(6.70)
EI	0.001	0.001
	(1.35)	(1.33)
SUCC	-0.037***	-0.037***
	(-9.53)	(-9.60)
RDI	0.026	0.026
	(1.41)	(1.41)
CONSTANT	0.025	0.038
	(0.76)	(1.57)
Year FE	YES	YES
Industry FE	YES	YES
Observations	11,371	11,371
Adj-R^2	0.348	0.348

Notes: This table presents the results of estimating the association between customer data breaches and supplier cost management strategy after controlling for the impacts of supplier product market competition and supplier data breach. Variables are defined in Appendix A. Robust standard errors are clustered at the firm level. *, ** and *** denote significance at the 10%, 5% and 1% levels, respectively.

TABLE 9

Robustness Checks

	Representative industries	Hacking	Alternative sticky costs		Alternative specifications	
	(1) ΔLOG(SG&A)	(2) ΔLOG(SG&A)	(3) ΔLOG(COGS)	(4) ΔLOG(XOPR)	(5) ΔLOG(SG&A)	(6) ΔLOG(SG&A)
ΔLOG(SALES)	0.524***	0.507***	0.864***	0.684***	0.603***	0.571***
	(15.66)	(5.89)	(36.56)	(35.86)	(23.44)	(19.63)
DEC*ΔLOG(SALES)	-0.153**	-0.359*	-0.136**	-0.112**	-0.269***	-0.192***
	(-2.31)	(-1.73)	(-2.26)	(-2.45)	(-8.91)	(-6.36)
DEC*ΔLOG(SALES) *CDB$_{t-1}$	**0.132****	**0.512***	**0.911****	**1.026****	**0.118*****	**0.094***
	(2.55)	(1.95)	(2.12)	(2.57)	(2.71)	(1.91)
DEC*ΔLOG(SALES)* AI	-0.001	0.044	0.000	-0.001	-0.001	-0.000
	(-0.08)	(0.70)	(0.10)	(-0.49)	(-1.24)	(-0.06)
DEC*ΔLOG(SALES)* EI	-0.003	-0.009	-0.000	-0.002	-0.003**	-0.001
	(-0.45)	(-0.23)	(-0.18)	(-0.97)	(-2.03)	(-0.50)
DEC*ΔLOG(SALES)* SUCC	0.131**	0.242	0.115**	0.048	0.171***	0.082***
	(2.24)	(1.58)	(1.99)	(1.19)	(5.71)	(3.16)
DEC*ΔLOG(SALES)* RDI	-0.221**	-0.675*	-0.000	0.006	0.011	0.001
	(-2.32)	(-1.76)	(-0.04)	(0.59)	(1.40)	(0.15)
ΔLOG(SALES)* CDB$_{t-1}$					0.106	0.327
					(1.29)	(1.49)
ΔLOG(SALES)*AI					-0.030***	-0.051***
					(-4.97)	(-6.00)
ΔLOG(SALES)*EI					0.010***	0.008**
					(3.73)	(2.22)
ΔLOG(SALES)*SUCC					-0.093***	-0.025
					(-4.07)	(-1.01)
ΔLOG(SALES)*RDI					-0.441***	-0.351***
					(-6.04)	(-3.50)
CDB$_{t-1}$	-0.003	0.071*	0.006	0.001		-0.015
	(-0.29)	(1.87)	(0.75)	(0.15)		(-1.46)
AI	0.018**	0.010	0.006	0.010***		0.017***
	(2.01)	(0.70)	(1.48)	(4.10)		(8.09)
EI	0.001	0.000	0.001**	0.002***		0.000
	(0.93)	(0.29)	(2.35)	(3.95)		(0.06)
SUCC	-0.024***	-0.020	-0.021***	-0.031***		-0.034***
	(-4.08)	(-1.30)	(-3.92)	(-8.26)		(-8.62)
RDI	0.047	-0.193	-0.066**	0.020		0.030
	(1.17)	(-1.62)	(-2.37)	(1.06)		(1.61)
CONSTANT	0.008	-0.001	0.006	0.039*	0.041*	0.035
	(0.35)	(-0.01)	(0.35)	(1.66)	(1.72)	(1.47)
Year FE	YES	YES	YES	YES	YES	YES
Industry FE	YES	YES	YES	YES	YES	YES
Observations	3,496	526	11,363	11,368	11,371	11,371
Adj-R^2	0.412	0.387	0.482	0.512	0.350	0.357

Notes: This table presents the results on the robustness tests of estimating the association between customer data breaches and supplier cost management strategy. Variables are defined in Appendix A. Robust standard errors are clustered at the firm level. *, ** and *** denote significance at the 10%, 5% and 1% level, respectively.