Customer Cybersecurity and Supplier Cost Management Strategy

Xu Yang
Xi'an Jiaotong University, yx1102@stu.xjtu.edu.cn

Peng Liang
University of Science and Technology of China, pengliang@ustc.edu.cn

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

Fujing Xue
Sun Yat-sen University, xuefj@mail.sysu.edu.cn

ICIS 2023 Hyderabad, The Spillover Effect of Cybersecurity on Cost Management

Completed Research Paper

Xu Yang
Xi'an Jiaotong University
Xi'an, Shaanxi, China
yx1102@stu.xjtu.edu.cn

Peng Liang
University of Science and Technology of China
Hefei, Anhui, China
pengliang@ustc.edu.cn

Nan Hu
Singapore Management University
81 Victoria Street, Singapore
nanhu@smu.edu.sg

Fujing Xue
Sun Yat-sen University
Shenzhen, Guangdong, China
xuefj@mail.sysu.edu.cn

Abstract

In this paper, we explore the spillover effect of customer firms' data breaches on their upstream supplier firms' cost management strategies, proxied by cost stickiness. Our primary analyses suggest that data breaches suffered by customer firms are associated with a decrease in cost stickiness among supplier firms. Furthermore, the reductions in supplier cost stickiness are stronger if suppliers are managed by CEOs from national cultural groups with high uncertainty avoidance, low long-term orientations, and/or low individualism. In sum, the findings contribute to both Information Systems (IS) and Operations Management (OM) disciplines in terms of data breach, cost management strategy, and the role of national culture in OM. In particular, the findings can facilitate the management and regulation of data breaches for managers and regulators.

Keywords: Data breach, cybersecurity, cost management, supply chain, national culture

Introduction

Data breaches are posing new and growing challenges for businesses of all sizes and across diverse industries, 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 the average cost of a data breach in the United States (global) totaling $9.44 ($4.35) million in 2022 according to the IBM Data Breach Report (IBM 2022). Consequently, regulators have paid particular attention to this issue (SEC 2018), while academia has embraced it as a crucial area of research within the fields of Operations Management (OM) and Information Systems (IS) (see Guha and Kumar (2018), Kumar and Mallipeddi (2022), and Schlackl et al. (2022)).

Due to the significant costs associated with data breaches, prior research has indicated that the direct impact of such data breaches can be disastrous on firm reputation and revenue losses (D'Arcy et al. 2020; Gwebu et al. 2018), information technology (IT) system (Sen and Borle 2015), bank loans (Huang and Wang 2021), and shareholder value (Ashraf and Sunder 2023; Kamiya et al. 2021). Apart from the effects on the directly attacked firms, data breaches can also create spillover effects on the affected firms' stakeholders, especially on supply chain partners (Choi et al. 2016; Luo and Choi 2022), because supply chain partners are susceptible to such cyberattacks (Zhang and Smith 2022). In this context, Crosignani et al. (2023) document that cyberattacks could propagate from the directly hit firms to their trading partners, leading to significant revenue losses for the affected businesses. Similarly, He et al. (2020a) find that when customers

experience data breaches, their key suppliers tend to reduce relationship-specific investments in the subsequent year because such data breaches of customers impair the corresponding suppliers' perception of the customers' future market prospects. Despite these consequences and their growing prevalence, a systematic understanding of how major customers' data breaches affect their suppliers' cost management strategies is still limited. This is a gap both in the OM and IS literatures.

In this study, we attempt to shed some light on the above gap by investigating whether customers' data breaches induce dependent suppliers to take real actions to adjust the allocations of cost resources. While customer data breaches potentially affect many types of supplier operational strategies, we focus on cost management strategies for the reason that cost resource allocations are a fundamental and essential behavior to support corporate business operations and performance (He et al. 2020b; Liang et al. 2023; Zhang et al. 2021), and are one of the crucial competitive capabilities (Rosenzweig and Easton 2010). Specifically, this paper examines firm sticky cost behavior, i.e., *cost stickiness*, a prevalent resource management strategy to avoid the costs of decreasing present capacity and increasing resources in the future (Anderson et al. 2003). Cost stickiness occurs when confronted with a decrease in demand, managers tend to reduce costs less than that they would increase in response to an equivalent increase in demand (Anderson et al. 2003). The theory of cost stickiness is grounded in the notion that managers make rational decisions to intentionally keep slack resource capacity when sales decrease, anticipating future demand to rebound to lower adjustment costs (Anderson et al. 2003; Banker et al. 2010). Additionally, we study the propagation of data breaches from customers to suppliers (instead of the other way around) because: 1) suppliers are subject to significant power and influence from customers (Chen et al. 2022); and 2) customer risk exposures could propagate to upstream suppliers (Agca et al. 2022; Serrano et al. 2018), which further affect the suppliers' business operations and managerial decision making (Hertzel et al. 2008).

Building on the significantly operational and financial bonds between customers and suppliers, we expect that customers' data breaches will decrease suppliers' cost stickiness. Data breaches could result in increases in bankruptcy risk for firms (Boasiako and O'Connor Keefe 2021; Huang and Wang 2021). Moreover, customers' enlarged default risk due to data breaches could travel up the supply chain (Agca et al. 2022), further leading to a higher level of default risk for the suppliers (Hertzel et al. 2008; Lian 2017). Consequently, as a reaction to the increased default risk, suppliers will cut costs more quickly when sales fall to improve earnings (Dai et al. 2023), resulting in a lower level of cost stickiness.

We further explore the moderation effect of national cultural backgrounds of top managers (i.e., Chief Executive Officer (CEO)) of suppliers. Modern supply chains are characterized by their global nature, with companies operating in multiple countries and engaging with diverse international partners. As highlighted by social psychologists, individuals belonging to different nationalities or countries tend to exhibit diverse decision-making behaviors (Hofstede et al. 2010). This necessitates a deep understanding of the impact that national cultures can have on business interactions between cross-cultural supply chain partners (Gray and Massimino 2014; Gupta and Gupta 2019). As such, recognizing the influence of national cultures within supply chains is becoming more and more vital in today's business landscape. To shed light on whether suppliers' cost management strategies following customers' data breaches is contingent on national cultural backgrounds of supplier CEOs, we turn to cross-cultural psychology and identity three dimensions of national culture identified by Hofstede (2001) (uncertainty avoidance (UAI), long-term orientation (LTO), and individualism (IND)), which we posit are related to customer data breaches and supplier cost stickiness. Our focus is on the ethnic cultural backgrounds at the firm top manager level because managers' ethnicity reveals their inherited culture, which can in turn provide insight into their managerial behaviors (Brochet et al. 2019).

To provide a systematic understanding of the impact of customer data breaches on supplier cost stickiness, we collect data breach events of U.S. public firms from the Privacy Rights Clearinghouse (PRC) database[1] over the period 2005 to 2019. A key advantage of PRC database is that it provides detailed information on data breaches (e.g., the name of the breached firm, the reported date of the breach, type of breach, detailed description of breach), and the breached firms are required to notify affected organizations under data breach notification laws in the United States (Kamiya et al. 2021; Nikkhah and Grover 2022). Additionally, consistent with extant research (e.g., Cen et al. (2017), Chen et al. (2022), Chu et al. (2019), Liang et al.

[1] More information can be found at: https://www.privacyrights.org/data-breaches.

(2023)), we identify a supplier's major customers based on the widely used "*WRDS Supply Chain with IDs (Compustat Segment)*" database[2] that is built on Compustat segment files.

Our main analysis shows that suppliers manage selling, general, and administrative (SG&A) costs more conservatively in reaction to customer data breaches. The results are robust to alternative cost measures and alternative model specifications. We further indicate that this effect is stronger for supplier CEOs with national cultural backgrounds that are more uncertainty-avoiding, less long-term orientated, and/or less individualistic. Moreover, we address several potential concerns that our main results could be shaped by other supplier firm characteristics, such as industry competition (Zhang et al. 2021) and suppliers' own data breaches. Finally, using the enactment of mandatory staggered state-level data breach notification laws as natural experiments that generates plausibly exogenous variation in customer data breaches, we employ a staggered difference-in-differences approach and document that the decrease in supplier cost stickiness following customer data breaches is weakened after these laws became effective in the states where the customer firms are headquartered. Finally, suppliers are found to be more inclined towards recruiting a cybersecurity expert to join their top management team subsequent to a customer data breach.

Our research makes three contributions to the interface between OM and IS regarding data breach, cost management strategy, and the role of national culture in OM. First, we advance our understanding of the spillover effects of data breaches along supply chains. Prior studies have investigated firms' reactions to data breaches in many ways (e.g., Nikkhah and Grover (2022), Huang and Wang (2021)), but little research exists that explores the spillover effects of customer data breaches on supplier operational decision-making (Do et al. 2023; He et al. 2020a; Zhang and Smith 2022). Our analyses expand this line of literature by indicating that suppliers take real actions to reallocate cost resources in the face of customer data breaches, which can help managers better understand cybersecurity risks. This paper also responds to the call by Kumar and Mallipeddi (2022) for more studies on data breaches and cybersecurity in operations and supply chain management.

Second, we emphasize the significance of cost management strategy from OM perspective, extending beyond the boundaries of the accounting field. We complement the current cost management literature that introduces the theory of cost stickiness, a prevalent but underexplored phenomenon in operations management, in the context of operations management to capture operational resource adjustments (Liang et al. 2023; Zhang et al. 2021). Specifically, our study offers novel insights to the literature on the determinants of cost stickiness by showing that suppliers release cost resources more rapidly in sales-decreasing periods in responding to customer data breaches.

Third, we contribute to cross-cultural psychology and recent research on the pertinent role of national cultures in the domain of OM. Social psychologists suggest that individuals from different countries and nationalities have their own unique national cultural values (Ribbink and Grimm 2014), which can result in different decision-making behaviors (Hofstede et al. 2010). Given the global nature of today's supply chains, we examine and confirm that supplier CEO national cultural origins could moderate the supplier's responses to customer data cybersecurity issues in cost resource allocations. This research also addresses the need for further exploration into how national culture influences operational decision-making within the OM field (Gupta and Gupta 2019; Gupta and Gupta 2021).

Literature Review and Hypotheses Development

Research 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

[2] For details, see: https://wrds-www.wharton.upenn.edu/pages/get-data/linking-suite-wrds/supply-chain-with-ids-compustat-segment/.

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

consequences in terms of financial loss, long-lasting damage to reputation, and loss of consumer trust (Akey et al. 2021; Gwebu et al. 2018; Huang and Wang 2021; Janakiraman et al. 2018).

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 (Amir et al. 2018; Cavusoglu et al. 2004; 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 have positive market reactions for both the breached firm and its competitors (Jeong et al. 2019).

Beyond the above implications, data breaches could pose a significant risk to supply chain partners. Data breaches have emerged as a major threat to firms' customer-supplier relationships (Hoehle et al. 2022), which highlights the need for increased attention to supply chain management (Luo and Choi 2022). Despite this, few studies have explored the impact of data breaches on companies in a supply chain. For instance, 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. Other literature shows that customer data breaches exhibit an increase in audit fees for their suppliers (Zhang and Smith 2022). However, to date, there appears to be a lack of research on the spillover effects of customer data breaches on supplier cost management strategies.

Research on Cost Management Strategy

Asymmetric cost behavior is a firm's typical operational cost management strategy. Anderson et al. (2003)'s seminal research identifies an asymmetric cost behavior called "cost stickiness" (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 is that managers deliberately hold slack resources in sales-decreasing periods in anticipation of a future rebound in sales to lower adjustment costs (Anderson et al. 2003).

There are two major factors that may shape the extent of asymmetry in cost behavior. Frist, managerial expectations of future demand are responsible for managers' choices to adjust cost resources when sales increase or decrease (Banker and Byzalov 2014; Chen et al. 2019b; Liang et al. 2023). According to Anderson et al. (2003), the decision of whether to release or maintain underutilized resources during periods of sales falling is based on managerial anticipations of the adjustment costs related to cutting cost resources in the short term and replacing them when future sales return. If managers expect future demand to restore during a sales decline, they are encouraged to carry slack resources instead of remove them, leading to cost asymmetry (Anderson et al. 2003). Second, cost stickiness also depends on the degree of firm default risk. For example, Dai et al. (2023) document that when experiencing increased bankruptcy risk, firms choose to cut costs more quickly in sales-decreasing periods to enhance liquidity and increase earnings, ultimately avoiding the need for covenant renegotiations and violations. Such cost resource adjustment decisions result in a decrease in cost asymmetry.

In addition, recent studies extend our understanding of cost stickiness from OM perspective beyond the domain of the accounting field. Zhang et al. (2021) provide evidence that sticky cost behavior could be explained by the level of competition. Liang et al. (2023) analyze cost asymmetry along supply chains and find that suppliers' cost stickiness is positively associated with their customers' managerial expectations of future demand. Nevertheless, research on how suppliers make decisions regarding cost resources when their customers experience data breaches is still nascent.

Linking Data Breach to Cost Management Strategy Along Supply Chains

Drawing on prior research on data breach and cost management strategy, we predict that customer data breaches will lead to significant reductions in supplier cost stickiness due to the following two reasons. On the one hand, Boasiako and O'Connor Keefe (2021) and Huang and Wang (2021) confirm that data breaches could increase default risk for firms. Agca et al. (2022) further show that customer default risk could travel up the supply chain, thereby resulting in an increase in default risk for suppliers (Lian 2017). In this case, suppliers experiencing increased bankruptcy risk tend to cut costs more rapidly during periods of falling sales. This is done to improve liquidity and increase performance, ultimately helping the firm avoid the need for covenant renegotiations and violations (Dai et al. 2023). As a result of these cost resource adjustment decisions, there is a decrease in cost stickiness of suppliers.

On the other hand, prior work finds that customer data breaches could weaken trading relationships between supply chain partners (Do et al. 2023; He et al. 2020a). However, suppliers cannot afford to lose a major portion of demand from their customers, upon whom they depend (Chen et al. 2019a). On the contrary, ending existing trading relationships with customers who suffer data breaches is not a rational decision for suppliers. This is due to the fact that more than 80% of companies around the world suffer data breaches (IBM 2022). Thus, suppliers will need to invest substantial efforts and resources in finding new customers to replace the lost business (Crook and Combs 2007). Moreover, customers' data breaches lower suppliers' expectations for such customers' future business prospects (He et al. 2020a), as data breaches lead to a decline in firm performance (Juma'h and Alnsour 2020). Consequently, suppliers tend to remove slack in cost resource capacity during a sales decline in the expectations of future demand disappearing (Liang et al. 2023). This results in a lower level of supplier cost stickiness. Therefore, we hypothesize the following:

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

The Moderating Role of Supplier CEOs' National Cultural Backgrounds

Uncertainty Avoidance (UAI)

More related to our study, Kitching et al. (2016) conduct a cross-country research and analyze how high UAI management adjusts cost resources. According to their findings, uncertainty-avoiding managers make more aggressive cuts in costs in sales downturns, through reducing managerial empire-building incentives (Chen et al. 2012), thereby resulting in a decrease in cost stickiness. Therefore, in cultures with a low tolerance for uncertainty, CEOs of suppliers will take a more conservative approach to cost management (i.e., hold less unutilized resources during a decrease in demand) in reaction to customer data breaches. Following this logic, we anticipate that the decline in supplier cost stickiness associated with customer data breaches could be magnified for supplier CEOs in national cultures with high levels of UAI.

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

Long-term Orientation (LTO)

We expect that the decline in supplier cost stickiness responding to customer data breaches will be attenuated for supplier CEOs in national cultures with high LTO. In high-LTO cultures, supplier managers prioritize the establishment of market positions and strong relationships with trading partners (e.g., customers) (Lui and Ngo 2012; Skowronski et al. 2022) by spending more resources in long-term strategies (Flammer and Bansal 2017). In addition, managers in cultures with high LTO are more inclined towards taking into account the likelihood of future sales reversals when making decisions (Kitching et al. 2016). Therefore, long-term oriented suppliers are likely to hold slack capacity in demand-decreasing periods following customer data breaches in expectation of a future rebound in demand. In contrast, supplier managers in 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,

instead of tolerating such short-term costs. This leads to a greater reduction in supplier cost stickiness. Thus, we hypothesize

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

Individualism (IND)

In terms of individualism/collectivism, we predict that the decline in supplier cost stickiness reacting to customer data breaches will be diminished for supplier CEOs in national cultures with high IND. First, IND captures the extent to which a society prioritizes individual interests and values over group interests and values (Hofstede 2001). As highlighted by Chui et al. (2010), societies with high levels of IND are positively related to overconfidence. However, overconfident CEOs often exhibit excessive optimism regarding their ability to recover sales, thereby overestimating the probability of a sales rebound in the near future (Kuang et al. 2015). Hence, when responding to customer data breaches, managers at suppliers in high-IND cultures are more likely to preserve slack cost resources in case of declining sales, bringing about higher cost asymmetry.

H4. *A decrease in supplier cost stickiness following customer data breaches is stronger if suppliers are managed by CEOs in low IND cultures.*

Sample

We started by identifying supplier-customer pairs for the period from 2005 to 2019, resulting in an initial sample of 50,639 unique supplier-customer-year pairs. We removed 189 parent-subsidiary pairs where the customer and supplier share the same GVKEY. We eliminate 15,563 observations that have missing values in suppliers' sales to customers, and we only retain the most significant customer for each supplier, resulting in a reduced sample of 17,758 supplier–customer–year relationships. Our data on reported data breach events from 2005 to 2019 is obtained from the Chronology of Data Breaches maintained by the PRC. We merged the supplier–customer–year sample with customer data breaches from the Chronology. We then merged the sample with fundamental financial data, such as SG&A costs from COMPUSTAT, and matched the stock return data from the Center for Research of Security Prices (CRSP) at the supplier-year level. We excluded 254 observations from the financial services industry (SIC 6000-6999) and 1,691 observations without sufficient data to construct regression variables. Following these procedures, we obtained a final sample of 11,371 unique supplier-year pairs.

Research Design

Model Specification

We study our research questions using the following standard cost stickiness model developed by Anderson et al. (2003) and extended by Zhang et al. (2021):[4]

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

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. We focus on SG&A costs because SG&A costs represent a significant portion of a firm's operational expenditures, and as such, managers tend to 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). $CUSTBREACH_{i,t-1}$ is the one-year lagged proxy for customer data breach, defined as a binary indicator that loads as a 1 if any of supplier firm i's most significant customer exhibits a data breach

[4] In Robustness section, we find our main inferences are robust to alternative cost stickiness models.

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 zero otherwise.

In this model, the coefficient β_1 measures the elasticity of SG&A costs to sales. That is, it reflects the percentage change in SG&A costs when current sales increase by 1%. The coefficient β_2 captures the base-level degree of SG&A cost stickiness. The sum of the coefficients ($\beta_1 + \beta_2$) reveals the percentage change in SG&A costs when current sales decrease by 1%. Based on prior cost stickiness studies (e.g., Anderson et al. (2003), Liang et al. (2023), Zhang et al. (2021)), β_1 is expected to be positive and β_2 is expected to be negative, which means $\beta_1 + \beta_2$ is lower than β_1. This indicates that costs decrease less when sales decline than they increase when sales increase by the same amount, i.e., managers hold unused resources during periods of sales falling. A more negative β_2 corresponds to a higher level of cost stickiness. Our main coefficient of interest is β_3, which characterizes the impact of customer data breaches on supplier cost stickiness. A positive value for β_3 would suggest that supplier SG&A costs are less sticky after customer data breaches, which is our prediction for the main hypothesis.

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 revenue if sales decrease in both the current year and the preceding year, 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 on total sales. Appendix 1 provides details on variable definitions. All continuous variables are winsorized at the top and bottom 1% level to reduce the influence of outliers. We estimate ordinary least squares (OLS) regressions with year and 4-digit SIC industry fixed effects.

Measuring the Moderators

In accordance with existing literature (Jung et al. 2019; Merkley et al. 2020; Pan et al. 2020), we assess the cultural attributes of firm top executives by utilizing CEO surnames to identify the regions that are most likely to represent the CEO's country of origin. Prior studies indicate 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).

To measure CEO national cultures in terms of UAI, LTO, and IND, we use a three-step approach. First, we collect surnames of CEOs from Standard & Poor's ExecuComp database, which contains data on 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 supplementary data, based on previous studies by Pan et al. (2020) and Jung et al. (2019). This allows us to assign a specific country of origin to each CEO based on their surname.

Third, we match the country of origin to Hofstede's national cultural database, which provides the country-level UAI, LTO, and IND to capture CEOs' attitudes toward uncertainty, time orientation, and individualism, respectively (Hofstede 2001; Hofstede et al. 2010). These indexes range from low values close to zero to high values close to 100 (Hofstede et al. 2010). As such, we obtain the ethnic cultural backgrounds at the firm top manager level.

Findings

Baseline Results

We present the results of estimating the relationship between customers' data breach and suppliers' cost management in Table 1. We employed ordinary least squares regression to estimate our model, while taking into account the potential issue of heteroskedasticity using heteroskedasticity-robust and firm-clustered standard errors (Petersen, 2009). Moreover, following the approach of Anderson et al. (2003), we checked

for multicollinearity and found that the mean variance inflation factors (VIFs) for all models in Table 1 were less than 5, indicating that multicollinearity was not a concern in our study.

We first estimate the basic cost asymmetry model in column (1). In line with prior literature, we find that the coefficient on $\Delta LOG(SALES_{i,t})$ is positively significant at the 1% level (coefficient = 0.480, t-statistic = 30.60) while the coefficient on $DECREASE_{i,t} * \Delta LOG(SALES_{i,t})$ is negative and significant (coefficient = −0.174, t-statistic = −6.81). This indicates that a 1% increase in sales revenue results in a 0.480% increase in SG&A expenses while a 1% decrease in sales revenue results in only a 0.306% (= 0.480% − 0.174%) decrease in SG&A expenses, providing support for the cost stickiness hypothesis.

Continuing with Table 1, column (2) shows a positive and highly significant coefficient (coefficient = 0.143, t-statistic = 3.23) for the three-way interaction term $DECREASE_{i,t} * \Delta LOG(SALES_{i,t}) * CUST\_BREACH_{i,t-1}$, economically implying that a 1 standard deviation increase in *CUST_BREACH* from its mean value brings about a 3.0% decrease in supplier cost asymmetry. This evidence suggests that data breach of downstream firms can travel up the supply chain and weaken the cost asymmetry of their dependent upstream supplier.

	(1)△LOG(SG&A)	(2)△LOG(SG&A)
△LOG(SALES)	0.480***	0.467***
	(30.60)	(29.28)
DECREASE*△LOG(SALES)	-0.174***	-0.188***
	(-6.81)	(-6.33)
DECREASE*△LOG(SALES)*CUST_BREACH (t-1)		0.143***
		(3.23)
DECREASE*△LOG(SALES)*AI		0.000
		(0.15)
DECREASE*△LOG(SALES)*EI		-0.000
		(-0.24)
DECREASE*△LOG(SALES)* SUCC		0.067***
		(3.13)
DECREASE*△LOG(SALES)*RDI		-0.001
		(-0.08)
CUST_BREACH (t-1)		-0.001
		(-0.16)
CONSTANT	0.051**	0.038
	(2.07)	(1.58)
CONTROLS	YES	YES
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

Table 1. Customers' Data Breaches and Suppliers' Cost Management

Moderation Effects

For cross-sectional analyses, we first divide our sample into three high and low subsamples based on the median value of our moderation variables, respectively. In Columns (1) and (2) of Table 2,these results lend support that when customer data beach, supplier CEOs with a more uncertainty-avoiding cultural heritage will have a lower tendency to retain unutilized resources during periods of reduced sales if those suppliers deliver offer specialized goods to their major customers. Second, in Columns 3 and 4, these findings support the notion that following a customer data breach, supplier CEOs with a cultural heritage that does not emphasize long-term orientation are less inclined to retain unused resources during periods of reduced sales if those suppliers offer specialized goods to their major customers. Third, the results obtained from columns 5 and 6 provide evidence that in the event of a customer data breach, supplier CEOs with a cultural heritage that is less individualistic are less likely to retain unused resources during periods of declining sales if those suppliers provide specialized goods to their major customers.

	Uncertainty Avoidance		Long-term Orientation		Individualism	
DV=△LOG(SG&A)	(1) Low	(2) High	(3) Low	(4) High	(5) Low	(6) High
△LOG(SALES)	0.493***	0.504***	0.511***	0.453***	0.498***	0.504***
	(16.63)	(14.19)	(18.72)	(10.51)	(21.67)	(3.90)
DECREASE*△LOG(SALES)	-0.194***	-0.251***	-0.183***	-0.197*	-0.229***	0.194
	(-3.70)	(-3.45)	(-3.62)	(-1.88)	(-5.41)	(0.58)
DECREASE*△LOG(SALES)	0.754*	1.350**	0.907**	0.929	0.910***	0.480
*CUST_BREACH (t-1)	(1.95)	(2.46)	(2.43)	(1.52)	(2.98)	(0.24)
DECREASE	0.001	-0.021*	0.000	-0.027	0.000	-0.023
*△LOG(SALES)*AI	(0.93)	(-1.70)	(0.36)	(-1.60)	(0.28)	(-0.11)
DECREASE	0.001	0.034***	0.000	0.017**	-0.000	0.014
△LOG(SALES) EI	(0.81)	(3.88)	(0.16)	(2.09)	(-0.05)	(1.15)
DECREASE	0.009	0.083	0.013	0.098	0.053	-0.330
△LOG(SALES) SUCC	(0.20)	(1.34)	(0.27)	(1.45)	(1.39)	(-0.92)
DECREASE	-0.009	-0.451***	-0.003	-0.259**	-0.002	0.583
*△LOG(SALES)*RDI	(-0.91)	(-3.12)	(-0.31)	(-2.26)	(-0.21)	(0.45)
CUST_BREACH (t-1)	0.022	0.012	0.018	0.022	0.024***	-0.116*
	(1.60)	(1.09)	(1.49)	(1.48)	(2.71)	(-1.78)
CONSTANT	0.011	-0.079***	0.025	-0.067**	0.005	-0.256***
	(0.64)	(-4.18)	(1.57)	(-2.21)	(0.35)	(-3.62)
Difference	2.80 (p< 10%)		3.14 (p< 10%)		7.81 (p< 1%)	
CONTROLS	YES	YES	YES	YES	YES	YES
Year FE	YES	YES	YES	YES	YES	YES
Industry FE	YES	YES	YES	YES	YES	YES
Observations	3,324	1,791	3,474	1,641	4,845	270
Adj-R^2	0.370	0.412	0.391	0.371	0.372	0.615

Table 2. The Moderating Effects of Supplier CEO National Cultural Backgrounds

Robustness Checks

We conduct several robustness tests to bolster our inferences and present the results in Table 3. First, we replace *CUSTBREACH* with an alternative indicator variable that equals 1 if the breach involved hacking or malware and zero otherwise (Huang and Wang 2021). Second, except for asymmetric SG&A cost activities, previous studies also employ other proxies to capture firm cost management strategy, such as cost of goods sold (*COGS*) (Weiss 2010) and operating costs (*XOPR*) (Lee et al. 2020). We repeat our analysis by replacing the dependent variable with these two alternative cost measures in Table 3, respectively. Finally, to further enhance the reliability of our findings, we examine Liang et al. (2023)'s cost stickiness model that include both the main effects of economic factors and their interactions with the log change in sales. Results in Table 3 reveal that our results continue to hold under diverse robustness checks.

	Hacking	Alternative sticky costs		Alternative model
	△LOG(SG&A)	△LOG(COGS)	△LOG(XOPR)	△LOG(SG&A)
△LOG(SALES)	0.507***	0.864***	0.684***	0.571***
	(5.89)	(36.56)	(35.86)	(19.63)
DEC*△LOG(SALES)	-0.359*	-0.136**	-0.112**	-0.192***
	(-1.73)	(-2.26)	(-2.45)	(-6.36)
DEC*△LOG(SALES)*	0.512*	0.911**	1.026**	0.094*
CUSTBREACH (t-1)	(1.95)	(2.12)	(2.57)	(1.91)
DEC*△LOG(SALES)*AI	0.044	0.000	-0.001	-0.000
	(0.70)	(0.10)	(-0.49)	(-0.06)
DEC*△LOG(SALES)*EI	-0.009	-0.000	-0.002	-0.001
	(-0.23)	(-0.18)	(-0.97)	(-0.50)
DEC*△LOG(SALES)*SUCC	0.242	0.115**	0.048	0.082***
	(1.58)	(1.99)	(1.19)	(3.16)
DEC*△LOG(SALES)*RDI	-0.675*	-0.000	0.006	0.001
	(-1.76)	(-0.04)	(0.59)	(0.15)
△LOG(SALES)				0.327
*CUSTBREACH (t-1)				(1.49)
△LOG(SALES)*AI				-0.051***
				(-6.00)
△LOG(SALES)*EI				0.008**
				(2.22)
△LOG(SALES)*SUCC				-0.025
				(-1.01)
△LOG(SALES)*RDI				-0.351***
				(-3.50)
CUSTBREACH (t-1)	0.071*	0.006	0.001	-0.015
	(1.87)	(0.75)	(0.15)	(-1.46)
CONSTANT	-0.001	0.006	0.039*	0.035
	(-0.01)	(0.35)	(1.66)	(1.47)
CONTROLS	YES	YES	YES	YES

Year FE	YES	YES	YES	YES
Industry FE	YES	YES	YES	YES
Observations	526	11,363	11,368	11,371
Adj-R^2	0.387	0.482	0.512	0.357

Table 3. Robustness checks

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 as a quasi-experimental setting. 51 states in the United States enacted data breach notification laws (hereafter notification laws)[5] that the government imposes on breached firms at different points in time between 2003 and 2018. These laws require breached companies to disclose data breaches to inform affected individuals (Nikkhah and Grover 2022), and are largely exogenous to individual firms (Huang and Wang 2021). While notification laws may incur costs for breached firms (e.g., notification expenses) (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 are inclined to view customer future demands more positively following the implementation of these laws in the states where their customers are based, thereby cutting costs less rapidly when sales fall.

Using the staggered variations in data breaches generated by the passage of mandatory state-level notification laws, we examine the difference-in-differences impact of these laws on the relationship 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 zero otherwise. Then we estimate:

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

Our main coefficient of interest is β_5 , the coefficient on the four-way interaction *DEC*ΔLOG(SALES)*CUSTBREACH*POSTLAW* that captures the causal effect of notification laws. Results in Table 4 show a significantly negative estimation on β_5 (p-value< 10%), suggesting that supplier cost stickiness subsequent to a customer data breach is attenuated after these laws. This finding supports the argument that the implementation of notification laws reduces customers' exposures to cyber risks, ultimately enhancing suppliers' trust in customers' future demands.

[5] To review data breach notification laws, see: https://www.perkinscoie.com/images/content/1/9/v2/197566/SecurityBreach-Notification-Law-Chart-June-2018.pdf.

	△LOG(SG&A)
△LOG(SALES)	0.467***
	(29.28)
DEC*△LOG(SALES)	-0.186***
	(-6.23)
DEC*△LOG(SALES)	0.155***
*CUSTBREACH (t-1)	(3.41)
DEC*△LOG(SALES)	-0.055
*POSTLAW	(-0.51)
DEC*△LOG(SALES)	-0.371*
*CUSTBREACH (t-1)*POSTLAW	(-1.93)
POSTLAW	-0.003
	(-0.42)
CUSTBREACH (t-1)	-0.002
	(-0.26)
CONSTANT	0.039
	(1.58)
CONTROLS	YES
Year FE	YES
Industry FE	YES
Observations	11,371
Adj-R^2	0.348

Table 4. The Effect of Data Breach Notification Law

Ruling Out the Potential Alternative Explanations

Our findings might be potentially confounded by product market competition among suppliers, because Zhang et al. (2021) document that the presence of competition increases firms' investment in sticky SG&A spending. To filter out this confounding factor, we follow Zhang et al. (2021) and include a control variable for supplier product market competition in our baseline specification, proxied by the Herfindahl-Hirschman index (*HHI*) defined in Appendix 1. As shown in Column (1) of Table 5, we find that the key inference remains consistent with supplier product market competition controlled.

We also consider the possibility that the observed effects on supplier cost management strategies are driven by supplier data breaches rather than customer data breaches. To mitigate such a concern, we control for the main effect of supplier data breaches (i.e., *SUPPBREACH*, as defined in Appendix 1) and its interaction with the log change in sales and sales decrease (i.e., *DEC*ΔLOG(SALES)* SUPPBREACH*). Continuing with Table 5, the results in Column (2) confirm that the observed main findings are robust after controlling for the influence of supplier data breaches.

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)	0.144***	0.143***
*CUSTBREACH (t-1)	(3.27)	(3.24)
DEC*△LOG(SALES)*HHI	0.297	
	(1.36)	
DEC*△LOG(SALES)		-0.155
*SUPPBREACH (t-1)		(-1.35)
CUSTBREACH (t-1)	-0.001	-0.001
	(-0.18)	(-0.15)
HHI	0.018	
	(0.73)	
SUPP_BREACH (t-1)		-0.019
		(-1.22)
CONSTANT	0.025	0.038
	(0.76)	(1.57)
CONTROLS	YES	YES
Year FE	YES	YES
Industry FE	YES	YES
Observations	11,371	11,371
Adj-R^2	0.348	0.348

Table 5. Ruling Out the Potential Alternative Explanations

Conclusion

This study aims to investigate the impact of data breaches suffered by customer firms on their suppliers' cost behaviors. We explore whether data breaches induce suppliers to adjust their cost resource allocation. Our findings suggest that customer data breaches are associated with a decrease in cost stickiness of their supplier firms. This reduction is more significant among supplier CEOs who have cultural backgrounds that are more uncertainty-avoiding, less long-term orientated, and/or less individualistic. Our results are robust to alternative measures of cost stickiness and alternative models. In addition, the significant evidence persists when we use alternative measures of data breach. We also provide evidence that our main findings are not driven by suppliers' industry competition, managerial incentives, and suppliers' own data breaches. To establish causality, we use mandatory state-level data breach notification laws as natural experiments, which generate plausibly exogenous variation in customer data breaches. Our analysis shows that the negative effect of customer data breaches on supplier cost stickiness is reduced after these laws became effective in the states where breached firms are headquartered. Finally, we find that suppliers are more likely to hire cybersecurity experts on the top management team following data breaches suffered by customers.

References

Agca, S., Babich, V., Birge, J. R., and Wu, J. 2022. "Credit Shock Propagation Along Supply Chains: Evidence from the Cds Market," *Management Science* (68:9), pp. 6506-6538.

Akey, P., Lewellen, S., Liskovich, I., and Schiller, C. 2021. "Hacking Corporate Reputations," *Rotman School of Management Working Paper*, 3143740.

Amir, E., Levi, S., and Livne, T. 2018. "Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets," *Review of Accounting Studies* (23), pp. 1177-1206.

Anderson, M. C., Banker, R. D., and Janakiraman, S. N. 2003. "Are Selling, General, and Administrative Costs "Sticky"?," *Journal of Accounting Research* (41:1), pp. 47-63.

Ashraf, M. 2022. "The Role of Peer Events in Corporate Governance: Evidence from Data Breaches," *The Accounting Review* (97:2), pp. 1-24.

Ashraf, M., and Sunder, J. 2023. "Can Shareholders Benefit from Consumer Protection Disclosure Mandates? Evidence from Data Breach Disclosure Laws," *The Accounting Review* (98:4), pp. 1-32.

Banker, R. D., and Byzalov, D. 2014. "Asymmetric Cost Behavior," *Journal of Management Accounting Research* (26:2), pp. 43-79.

Banker, R. D., Byzalov, D., and Plehn-Dujowich, J. M. 2010. "Sticky Cost Behavior: Theory and Evidence," *Working Paper*.

Boasiako, K. A., and O'Connor Keefe, M. 2021. "Data Breaches and Firm Credit Risk," *Working paper*.

Brochet, F., Miller, G. S., Naranjo, P., and Yu, G. W. 2019. "Managers' Cultural Background and Disclosure Attributes," *The Accounting Review* (94:3), pp. 57-86.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 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), pp. 70-104.

Cen, L., Maydew, E. L., Zhang, L. D., and Zuo, L. 2017. "Customer-Supplier Relationships and Corporate Tax Avoidance," *Journal of Financial Economics* (123:2), pp. 377-394.

Chang, H., Dai, X., Lohwasser, E., and Qiu, Y. 2022. "Organized Labor Effects on Sg&a Cost Behavior," *Contemporary Accounting Research* (39:1), pp. 404-427.

Chen, C., Kim, J. B., Wei, M., and Zhang, H. 2019a. "Linguistic Information Quality in Customers' Forward-Looking Disclosures and Suppliers' Investment Decisions," *Contemporary Accounting Research* (36:3), pp. 1751-1783.

Chen, C. X., Lu, H., and Sougiannis, T. 2012. "The Agency Problem, Corporate Governance, and the Asymmetrical Behavior of Selling, General, and Administrative Costs," *Contemporary Accounting Research* (29:1), pp. 252-282.

Chen, G., Tian, X. S., and Yu, M. 2022. "Redact to Protect? Customers' Incentive to Protect Information and Suppliers' Disclosure Strategies," *Journal of Accounting and Economics* (74:1), p. 101490.

Chen, J. V., Kama, I., and Lehavy, R. 2019b. "A Contextual Analysis of the Impact of Managerial Expectations on Asymmetric Cost Behavior," *Review of Accounting Studies* (24:2), pp. 665-693.

Choi, B. C., Kim, S. S., and Jiang, Z. 2016. "Influence of Firm's Recovery Endeavors Upon Privacy Breach on Online Customer Behavior," *Journal of Management Information Systems* (33:3), pp. 904-933.

Chu, Y. Q., Tian, X., and Wang, W. Y. 2019. "Corporate Innovation Along the Supply Chain," *Management Science* (65:6), pp. 2445-2466.

Chui, A. C. W., Titman, S., and Wei, K. C. J. 2010. "Individualism and Momentum around the World," *Journal of Finance* (65:1), pp. 361-392.

Crook, T. R., and Combs, J. G. 2007. "Sources and Consequences of Bargaining Power in Supply Chains," *Journal of Operations Management* (25:2), pp. 546-555.

Crosignani, M., Macchiavelli, M., and Silva, A. F. 2023. "Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains," *Journal of Financial Economics* (147:2), pp. 432-448.

D'Arcy, J., Adjerid, I., Angst, C. M., and Glavas, A. 2020. "Too Good to Be True: Firm Social Performance and the Risk of Data Breach," *Information Systems Research* (31:4), pp. 1200-1223.

Dai, J., Hu, N., Huang, R., and Yan, Y. 2023. "How Does Credit Risk Affect Cost Management Strategies? Evidence on the Initiation of Credit Default Swap and Sticky Cost Behavior," *Journal of Corporate Finance*, p. 102401.

Do, T. K., Huang, H. H., and Le, A.-T. 2023. "Cybersecurity Risk through the Supply Chain: Evidence from Relationship-Specific Investment," *Working paper*.

Du, Q. Q., Yu, F., and Yu, X. Y. 2017. "Cultural Proximity and the Processing of Financial Information," *Journal of Financial and Quantitative Analysis* (52:6), pp. 2703-2726.
Flammer, C., and Bansal, P. 2017. "Does a Long-Term Orientation Create Value? Evidence from a Regression Discontinuity," *Strategic Management Journal* (38:9), pp. 1827-1847.
Gray, J. V., and Massimino, B. 2014. "The Effect of Language Differences and National Culture on Operational Process Compliance," *Production and Operations Management* (23:6), pp. 1042-1056.
Guha, S., and Kumar, S. 2018. "Emergence of Big Data Research in Operations Management, Information Systems, and Healthcare: Past Contributions and Future Roadmap," *Production and Operations Management* (27:9), pp. 1724-1735.
Guiso, L., Sapienza, P., and Zingales, L. 2006. "Does Culture Affect Economic Outcomes?," *Journal of Economic perspectives* (20:2), pp. 23-48.
Gupta, M., and Gupta, S. 2019. "Influence of National Cultures on Operations Management and Supply Chain Management Practices—a Research Agenda," *Production and Operations Management* (28:11), pp. 2681-2698.
Gupta, S., and Gupta, M. 2021. "Production and Operations Management Call for Papers Special Issue: The Role of National Culture in Operations Management," *Production and Operations Management* (30:4), pp. 1178-1179.
Gwebu, K. L., Wang, J., and Wang, L. 2018. "The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management," *Journal of Management Information Systems* (35:2), pp. 683-714.
He, C., HuangFu, J., Kohlbeck, M. J., and Wang, L. 2020a. "The Impact of Customer's Reported Cybersecurity Breaches on Key Supplier's Relationship-Specific Investments and Relationship Duration," *Working paper*.
He, J., Tian, X., Yang, H., and Zuo, L. 2020b. "Asymmetric Cost Behavior and Dividend Policy," *Journal of Accounting Research* (58:4), pp. 989-1021.
Hertzel, M. G., Li, Z., Officer, M. S., and Rodgers, K. J. 2008. "Inter-Firm Linkages and the Wealth Effects of Financial Distress Along the Supply Chain," *Journal of Financial Economics* (87:2), pp. 374-387.
Hinz, O., Nofer, M., Schiereck, D., and Trillig, J. 2015. "The Influence of Data Theft on the Share Prices and Systematic Risk of Consumer Electronics Companies," *Information & Management* (52:3), pp. 337-347.
Hoehle, H., Venkatesh, V., Brown, S. A., Tepper, B. J., and Kude, T. 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., Hofstede, G. J., and Minkov, M. 2010. *Cultures and Organizations: Software of the Mind. Revised and Expanded*. Mcgraw-Hill New York.
Huang, H. H., and Wang, C. 2021. "Do Banks Price Firms' Data Breaches?," *The Accounting Review* (96:3), pp. 261-286.
IBM. 2022. "Cost of a Data Breach Report 2022," *https://www.ibm.com/reports/data-breach*.
Ibrahim, A. E. A., Ali, H., and Aboelkheir, H. 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), p. 100439.
Janakiraman, R., Lim, J. H., and Rishika, R. 2018. "The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer," *Journal of marketing* (82:2), pp. 85-105.
Jeong, C. Y., Lee, S.-Y. T., and Lim, J.-H. 2019. "Information Security Breaches and It Security Investments: Impacts on Competitors," *Information & Management* (56:5), pp. 681-695.
Juma'h, A. H., and Alnsour, Y. 2020. "The Effect of Data Breaches on Company Performance," *International Journal of Accounting & Information Management*.
Jung, J. H., Kumar, A., Lim, S. S., and Yoo, C. Y. 2019. "An Analyst by Any Other Surname: Surname Favorability and Market Reaction to Analyst Forecasts," *Journal of Accounting & Economics* (67:2-3), pp. 306-335.
Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., and Stulz, R. M. 2021. "Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms," *Journal of Financial Economics* (139:3), pp. 719-749.
Kitching, K., Mashruwala, R., and Pevzner, M. 2016. "Culture and Cost Stickiness: A Cross-Country Study," *The International Journal of Accounting* (51:3), pp. 402-417.

Kuang, Y. F., Mohan, A., and Qin, B. 2015. "Ceo Overconfidence and Cost Stickiness," *Management Control & Accounting* (2), pp. 26-32.
Kumar, S., and Mallipeddi, R. R. 2022. "Impact of Cybersecurity on Operations and Supply Chain Management: Emerging Trends and Future Research Directions," *Production and Operations Management* (31:12), pp. 4488-4500.
Lee, W. J., Pittman, J., and Saffar, W. 2020. "Political Uncertainty and Cost Stickiness: Evidence from National Elections around the World," *Contemporary Accounting Research* (37:2), pp. 1107-1139.
Lian, Y. L. 2017. "Financial Distress and Customer-Supplier Relationships," *Journal of Corporate Finance* (43), pp. 397-406.
Liang, P., Cavusoglu, H., and Hu, N. 2023. "Customers' Managerial Expectations and Suppliers' Asymmetric Cost Management," *Production and Operations Management, forthcoming*.
Lui, S. S., and Ngo, H. y. 2012. "Drivers and Outcomes of Long-Term Orientation in Cooperative Relationships," *British Journal of Management* (23:1), pp. 80-95.
Luo, S. Y., and Choi, T. M. 2022. "E-Commerce Supply Chains with Considerations of Cyber-Security: Should Governments Play a Role?," *Production and Operations Management* (31:5), pp. 2107-2126.
Merkley, K., Michaely, R., and Pacelli, J. 2020. "Cultural Diversity on Wall Street: Evidence from Consensus Earnings Forecasts," *Journal of Accounting and Economics* (70:1).
Nikkhah, H. R., and Grover, V. 2022. "An Empirical Investigation of Company Response to Data Breaches," *MIS Quarterly* (46:4), pp. 2163-2196.
Pan, Y., Siegel, S., and Yue Wang, T. 2020. "The Cultural Origin of Ceos' Attitudes toward Uncertainty: Evidence from Corporate Acquisitions," *The Review of Financial Studies* (33:7), pp. 2977-3030.
Ponemon, L. 2017. "Cost of Data Breach Study," *Ponemon Institute*.
Ribbink, D., and Grimm, C. M. 2014. "The Impact of Cultural Differences on Buyer-Supplier Negotiations: An Experimental Study," *Journal of Operations Management* (32:3), pp. 114-126.
Rosenzweig, E. D., and Easton, G. S. 2010. "Tradeoffs in Manufacturing? A Meta-Analysis and Critique of the Literature," *Production and Operations Management* (19:2), pp. 127-141.
Schlackl, F., Link, N., and Hoehle, H. 2022. "Antecedents and Consequences of Data Breaches: A Systematic Review," *Information & Management*, p. 103638.
SEC. 2018. "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," *https://federalregister.gov/d/2018-03858*.
Sen, R., and Borle, S. 2015. "Estimating the Contextual Risk of Data Breach: An Empirical Approach," *Journal of Management Information Systems* (32:2), pp. 314-341.
Serrano, A., Oliva, R., and Kraiselburd, S. 2018. "Risk Propagation through Payment Distortion in Supply Chains," *Journal of Operations Management* (58), pp. 1-14.
Skowronski, K., Benton, W. C., and Handley, S. 2022. "The Moderating Influence of Supplier Culture on the Relationship between Buyer Power and Supplier Shirking," *Journal of Operations Management* (68:3), pp. 270-301.
Weiss, D. 2010. "Cost Behavior and Analysts' Earnings Forecasts," *The Accounting Review* (85:4), pp. 1441-1471.
Zhang, R., Hora, M., John, S., and Wier, H. A. 2021. "Competition and Slack: The Role of Tariffs on Cost Stickiness," *Journal of Operations Management*.
Zhang, Y., and Smith, T. J. 2022. "The Impact of Customer Firm Data Breaches on the Audit Fees of Their Suppliers," *Working paper*.

Appendix 1

Variables	Definitions
CUST_BREACH (t-1)	Indicator variable that equals 1 if any of firm *i*'s most significant customer exhibit a data breach during firm *i*'s year t-1, and 0 otherwise.
SG&A	Total selling, general, and administration expenses.
SALES	Total sales revenue.
DECREASE	A dummy variable equal to 1 if sales revenue in year t is lower than that in year t-1, and 0 otherwise.
SUCC	A dummy variable equal to one if sales revenue in year t-1 are less than those in year t-2, and zero 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 zero.
UAI	Measure of firm *i*'s CEO uncertainty avoidance score.
LTO	Measure of firm *i*'s CEO long-term orientation score.
IND	Measure of firm *i*'s CEO individualism score.
SUPPBREACH (t-1)	Indicator variable that equals 1 if any of supplier firm *i* exhibits a data breach in year t-1, and 0 otherwise.
HHI	The 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.

Table 6. Variable Definitions