Received: 30 October 2023 | Accepted: 17 January 2024

DOI: 10.1002/jcaf.22695

RESEARCH ARTICLE

The Journal of Corporate Accounting & Finance WILEY

The importance of cybersecurity disclosures in customer relationships

Aaron Nelson | **Shensi Wang**

University of Texas at El Paso, Woody L. Hunt College of Business, El Paso, USA

Correspondence
Aaron Nelson, University of Texas at El Paso, Woody L. Hunt College of Business, El Paso, USA.
Email: ASNelson@Utep.edu

Abstract

The escalating use of digital technologies has spotlighted the crucial role of cybersecurity in safeguarding sensitive information within companies. This study explores the relationship between a firm's major customers and its cybersecurity awareness. Drawing on SEC-mandated disclosures, we employ four proxies to measure changes in customer-supplier relationships. Our findings reveal that customers increase their purchases from suppliers whose cybersecurity awareness scores improve. Additionally, we examine the interplay between customers and suppliers more susceptible to nonpublic adverse news, particularly during cyber events. The study emphasizes the importance of cybersecurity disclosure for regulators, supply chain partners, and corporate management. It also contributes to the literature on factors influencing the duration of customer-supplier relationships and underscores the significance of supplier characteristics. "Understanding and disclosing cybersecurity risks are" paramount in an increasingly digital business landscape.

KEYWORDS
cybersecurity, cybersecurity disclosure, supply-chain

1 | INTRODUCTION

The increasing use of digital and information technologies among companies has emphasized cybersecurity's importance in protecting the company's information. Cyber threats like data breaches have attracted sizeable public attention due to their cost to the firm and shareholders. More than 20% of breached firms experience a substantial loss of revenues, customer base, and business opportunities (Cisco, 2017). These companies spend millions of dollars repairing damage and expanding security procedures following the attacks. Thus, cybersecurity and related disclosures have become a significant concern for the board and executives (Shumsky, 2016). Using SEC required disclosures, Berkman et al. (2018) develop a measure of cybersecurity awareness and provide evidence that the market values cybersecurity awareness. This study investigates whether a firm's major customers similarly value cybersecurity awareness and discusses implications for firm management.

Crosignani et al. (2023) investigate the effects of the Ukrainian NotPetya attacks along the supply chain. Affected customers are more likely to end their relationships with attacked suppliers and select alternative suppliers, especially those less exposed to cybersecurity risks. The authors argue that "the disruption caused by the cyberattack served as a 'wake-up call' for the affected customers, which responded by selecting suppliers with a stronger cybersecurity posture, resulting in a more cyber-resilient supply chain." Customer companies should take preventative measures before an attack as well. Suppliers with high cybersecurity awareness have lower risks

of cyberattacks. Thus, customers may respond to suppliers' cybersecurity disclosures by altering purchases or switching suppliers when necessary.

To respond to the increasing cyber threats, the SEC issued the cybersecurity disclosure guidance in 2011 and updated it in 2018 to assist firms in disclosing related information. This guidance has led to a rapid increase in cybersecurity disclosures by firms in their 10-Ks. We use the cybersecurity scores provided by Berkman et al. (2018) to measure suppliers' cybersecurity awareness. Berkman et al. (2018) argues that cybersecurity disclosure relates to a firm's cybersecurity awareness because substantial risks are associated with disclosing vulnerabilities. Based on a glossary list from the National Initiative for Cybersecurity Careers and Studies (NICCS) and cyber-related Acts prepared by the Congressional Research Service, they compute the cybersecurity awareness score for each disclosed firm (check Appendix A for more details).

We use four proxies to measure changes in the customer-supplier relationship: (1) the sales percentage change to each customer, (2) the sales change to each customer, (3) an indicator variable equals one if the percentage change of sales of (1) is positive, and, (4) and indicator variable equals one if the sales change of (2) is positive. Across our empirical specifications, we find that customers increase their purchases from suppliers whose cybersecurity awareness scores improve compared to last year.

We also examine how customers relate to suppliers that are more likely to have nonpublic bad news. A firm's stock price crash risk is indicative of both markets and management not sharing bad news Hong and Stein (2003); Jin and Myers (2006); Kim et al. (2016). Withholding bad news would be particularly problematic to related parties in the event of a cyberevent. We find that the association between cybersecurity awareness and changes in the customer-supplier relationship is stronger when stock price crash risk is high.

This study underscores the importance of understanding cybersecurity disclosure. Regulators can help both investors and supply chain partners by requiring detailed disclosure on cybersecurity risks. Firm management can use these results as an indicator to share these risks with major partners to allow for collaborative problem solving, but because potential partners expect detailed disclosure. We also contribute to the literature on factors that affect the duration of the customer-supplier relationship (Bauer et al., 2018). We add cybersecurity awareness as an important factor in these relationships. Finally, the majority of supply chain research in finance and accounting focuses on customer characteristics affecting suppliers (Radhakrishnan et al., 2014). This study sheds light on the importance of supplier characteristics as well (Haapamĺaki & Sihvonen, 2019).

2 | LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

2.1 | Cybersecurity

Accounting and finance studies on cyber-related issues have focused mainly on the impact of cyberattacks. For example, Amir et al. (2018) provide evidence that firms underreport cyberattacks, withhold information on severe attacks, and experience a 3.6% stock price decline in the month a report is detected and disclosed. Consistent with academic evidence, Ponemon Insititute (2019) reports 5% negative returns for breached firms after a breach is disclosed. In contrast, Richardson et al. (2019) argue that market reaction to the cyberattack is generally negative but economically limited. Generally speaking, markets view cyberattacks negatively.

Cyberattacks have spillover effects. Cyberattacks negatively impact the breached firms and their peer firms, with the impact on peer firms depending on the severity of the cyberattacks (Hinz et al., 2015; Martin et al., 2017). However, Martin et al. (2017) reports that the effect turns positive when data breaches are highly severe because customers of breached firms are more likely to switch to rival firms.

Prior studies also find that a firm's cybersecurity is highly correlated with its governance. For example, Firms with better governance are less likely to withhold information about cyberattacks since stronger governance is associated with more substantial fiduciary responsibility (Amir et al., 2018). Similarly, Westland (2020) finds that firms with stronger internal controls experience fewer data breaches. Another trend of studies focuses on corporate governance changes following a cyber-related event. For example, Li (2016) finds a positive relationship between incidences of cyberattacks and auditing fees. Ashraf (2022) finds that unbreached firms are more likely to enhance internal controls when a peer firm experiences data breaches.

Crosignani et al. (2023) perform related work examining the effect of the NotPetya cyberattacks on customers of attacked firms. Petya was ransomware that circulated 2016. In 2017, Russian military intelligence released a virus that appeared to be an updated version but was designed specifically to stifle economic activity in Ukraine. NotPetya, as it came to be known, was successful in its mission, shutting down many Ukrainian suppliers and infecting their customers' systems as well.[1] Crosignani et al. (2023) finds that affected firms' customers experienced a sizeable drop in profits, with many of them terminating relations with the supplier.

Cybersecurity has also been a major topic for standard setters and policymakers. The American Institute of

Certified Public Accountants (AICPA) stated, "Cybersecurity is one of the top issues on the minds of management and boards in nearly every company in the world-large and small, public and private." Since investors ask for more information about cybersecurity risks and data breaches and how firms address those risks, it aims to increase transparency regarding material cyber-related issues (Shumsky, 2016; AICPA, 2018).

The SEC issued CF Disclosure Guidance in 2011: topic No.2 Cybersecurity to achieve this goal (Securities and Commission, 2011). The guidance highlights that firms facing material cyber-related issues must disclose related information. Firms need to provide disclosures related to cybersecurity, including management's discussion, analysis of the financial condition, and results of operation (MD&A); description of the business; description of legal proceedings; and in Item 1A, Risk factors. Firms should disclose the most significant factors related to the riskiness of investing in a company. The guidance encourages firms to generate disclosures with sufficient and appropriate information. In 2018, the SEC updated the guidance to assist corporations in preparing cybersecurity-related disclosures.

Berkman et al. (2018) uses the SEC-mandated disclosures to construct a cybersecurity awareness score. They argue that cyber-related disclosures are indicative of a firm's cybersecurity awareness because disclosure behaviors are associated with managers' reporting strategies. Berkman et al. (2018) finds that cybersecurity disclosures have become more prevalent over time and that cybersecurity awareness is positively valued by the market.

2.2 | Prior literature on customer relationship

Major customers are among the most important stakeholders of a firm. Recent research demonstrates that customer-base concentration has increased over time, indicating that these relationships are becoming more important Patatoukas (2012); Chen et al. (2021a). The Statement of Financial Accounting Standards No.131 (SFAS 131) requires firms to disclose external customers that account for 10% or more of the firm's annual revenue. Prior studies find that major customers benefit the supplier's operating performance, tax planning, and other performance metrics (Patatoukas, 2012; Cen et al., 2017; Irvine et al., 2016). However, relying on major customers can also have adverse effects. For example, firms with high customer concentration are likely to have cash flow volatility, structural risk, or financial distress. Also, Chen et al. (2021a) find that the dependence on major customers drives firms to invest less in radical innovation.

Additionally, the quality of information shared between suppliers and customers is critical in maintaining customer-supplier collaboration. Timely and credible information sharing between the two groups will bring many benefits, such as uncertainty reduction and resource management enhancement (Zhou & Benton Jr, 2007). Quality customer disclosures are associated with better supplier performance, efficiency, and greater trade credit extensions (Chen et al., 2019; Radhakrishnan et al., 2014; Nelson, 2018; Fei et al., 2023). On the other hand, reducing information quality will likely affect the customer-supplier relationship. For example, Bauer et al. (2018) finds that poor internal control quality increases the likelihood of subsequent customer-supplier relationship termination by reducing information quality.

Due to the nature of data availability and the SEC disclosure requirements, most studies focus on how a customer's properties affect suppliers (Chen et al., 2021b; Phua et al., 2018; Nelson & Schwartz, 2019; Hui et al., 2019). However, investigating supplier properties is important for a proper understanding of the supply chain and for managers to apply research in attracting and keeping major customers. Chen (2022) finds that customers react to a supplier's relationship-specific investments (RSI) by issuing more earnings forecasts. Raman and Shahrur (2008) provide evidence that customers respond to RSI with more accruals earnings management but that earnings management reduces the relationship length.

2.3 | Hypothesis development

We add to this literature by examining the importance of a supplier's cybersecurity disclosures. Berkman et al. (2018) demonstrates that markets value these disclosures. Customers likely value them for several reasons. First, cybersecurity protects the confidentiality of private information, ensures customers can access data on time, and ensures firms can provide accurate, reliable, and valid information (Gordon et al., 2006). Cyber incidents and attacks are costly to firms because they can result in litigation risk and regulatory costs Crosignani et al. (2023). They may also suffer other damages, such as reputation loss, business operations decline, and customer base decline (Mossburg et al., 2016). Thus, firms with high cybersecurity awareness tend to "adopt appropriate cybersecurity policies, implement effective threat detection, and ensure a proper and adequate response capability." (Berkman et al., 2018). Therefore, suppliers with high cybersecurity awareness are better positioned to prevent cyber incidents from occurring or minimize the costs associated with cyberattacks.

Second, as previous research discussed, cyber-related incidents are associated with financial distress. Kale and Meneghetti (2014) conclude that customers will be affected if suppliers experience financial distress. Also, suppliers may reduce their production quality when involved in financial distress. For example, Phillips and Sertsios (2013) finds that product quality declines when the firm is in financial distress, and the degree of quality decline is positively associated with the probability of bankruptcy. Hortaÿcsu et al. (2013) provide evidence that "a firm's financial difficulties can disrupt the provision of services and thus reduce the price a customer is willing to pay for the product." In short, customers prefer better supplier cybersecurity to both protect their own information and to ensure quality operations. We expect that the change in suppliers' cybersecurity awareness scores will promote the customer-supplier relationship because high cybersecurity awareness is associated with lower cyberattack risks and adverse effects related to cyberattacks. Thus, our first hypothesis states:

HYPOTHESIS 1. *Ceteris paribus, the change in suppliers' cybersecurity awareness is positively associated with the duration of the customer-supplier relationship.*

3 | RESEARCH DESIGN

3.1 | Sample selection

To be consistent with Berkman et al. (2018), we collect data from the Russell 3000 firms from 2011 to 2018. Our sample starts in 2012 because it is the first year following the SEC's initial guidance on cybersecurity disclosure. The sets of supplier-customer pairs are obtained from WRDS Supply Chain, which applies fuzzy-match strategies to match suppliers and principal customers in Compustat segment data (Cen et al., 2017). Firms are required to report their principal customers in their annual 10-K filings under ASC 280. Principal customers generally represent at least ten percent of a firm's total sales in a given year. Following prior literature, we exclude suppliers in the financial industry (SIC: 6000–6999). We obtain customer and supplier firm variables from Compustat. The cybersecurity awareness score is obtained from Berkman et al. (2018). All continuous variables are winsorized at the 1 and 99 percent levels to minimize the effects of outliers.

Table 1 reports results of our sample selection procedure. After merging with related financial data, we obtain 13,602 observations of supplier-customer segment data. Next, we require each supplier must have consecutive years of data. Thus, choice mitigates 9197 observations from our sample. Our final sample comprises 4405 observations, including 1469 unique suppliers and 1044 unique customers.

TABLE 1 Sample selection. This table reports the sample selection process, including total observation numbers at each level of selection.

Description	Observations
Observations available in Compustat database for 2010–2016 Less: missing variables	88,852
Subtotal	−34,619
Less: cannot be merged with supplier-customer segment data	40,631
Subtotal	13,602
Less: Suppliers miss consecutive years of data	9197
Final sample	4405

3.2 | Cybersecurity awareness measure

The cybersecurity awareness measure is based on a score (SCORE) from Berkman et al. (2018). Berkman et al. (2018) measures a firm's cybersecurity awareness by considering both the length of relevant disclosures and the relevance of the language used. A firm will have a higher SCORE if the language applied in the disclosure is more directly related to cybersecurity. They developed a dictionary based on the glossary of common cybersecurity terminology from the National Initiative for Cybersecurity Careers and Studies (NICCS) and supplemented it with cyber-related legislative Acts obtained from the Congressional Research Service. Next, they used that dictionary to check the language relevance.

Since disclosure is correlated with managers' disclosing strategy, Berkman et al. (2018) also considers the tone of cybersecurity disclosures in the analysis. They capture the positive (negative) tone using the word lists from Loughran and McDonald (2011). Neg Tone (Pos_Tone) is calculated as the negative (positive) words divided by the total number of words in a given 10-k disclosure.[2]

3.3 | Customer-supplier relationship measure

We focus on the duration of the customer-supplier relationship as an important result of the supplier's cybersecurity disclosures (Bauer et al., 2018). To measure the duration of the relationship, we use two measures: (1) the sales percentage to each major customer; and (2) the total sales change to a major customer, scaled by the prior year's sales to that customer. Additionally, we create dichotomous variables for whether these values

increase from year to year to eliminate measurement error when a supplier stops reporting major customers.[3] These measures capture the importance of the customer-supplier relationship to the supplier.

3.4 | Baseline models

To examine the association between the duration of the customer-supplier relationship and the change in cybersecurity awareness scores, we estimate the following regression, clustering standard errors by industry and year.

$$\begin{aligned} Duration_{i,t_{+1}} = {} & \alpha_0 + \alpha_1 Cyber_{i,t} + Disc_{i,t} \\ & + \Sigma_m \alpha_m SupplierCharacteristics_{i,t} \\ & + \Sigma_n \alpha_n CustomerCharacteristics_{i,t} \\ & + SupplierFE + YearFE + \epsilon_{i,t} \end{aligned} \quad (1)$$

The analysis is on the supplier-customer-year level. *Duration* is either the percentage change of sales to customer *i*, the total sales change to customer *i*, or an indicator variable for either increasing. Therefore, the dependent variable is one of four proxies: (1) Sale change, which is the change of customer purchase in year t_{+1}. (2) *percentchange*, which represents the percentage change of customer's purchase in year t_{+1}. (3) *salechangedum*, an indicator variable that equals one if *salechange* is positive. (4) *percentchangedum*, an indicator variable that equals one if *percentchange* is positive. *Cyber* is the change of SCORE provided by Berkman et al. (2018). *Disc* is an indicator variable that equals one if the supplier provides cybersecurity disclosure. We include vectors of variables to control for other factors that may affect supplier-customer relationship duration. Specifically, we include vectors for supplier and customer performance variables, general variables, and relationship variables.

The supplier and customer performance variables include return on assets (ROA) and market-to-book values. We control for firm size (size), leverage ratios, research and development expenditures (RD), and negative free cash flow (NegFCF) (Bauer et al., 2018). For the relationship variable, we control for supplier concentration (SuppCon). Appendix A defines all required variables.

4 | RESULTS

4.1 | Descriptive statistics

Table 2 presents the sample descriptive statistics. Customer firms tend to have larger sizes and are more profitable than supplier firms, which is consistent with prior studies. 64.2% of our suppliers in our sample have cyber-related disclosures. For suppliers with cyber-related disclosures, 65.2% of them improved their cybersecurity awareness scores compared to the last year. It suggests that most suppliers value cybersecurity more and more over our sample period.

TABLE 2 Descriptive Statistics. This table summarizes the descriptive statistics for variables in the main analysis. All continuous variables are winsorized at the 1st and 99th percentile. All variables are defined in Appendix A.

Variables	*N*	Mean	p25	p50	p75	SD
Cyber	4405	0.65	0.00	1.00	1.00	0.48
Disc	4405	0.64	0.00	1.00	1.00	0.48
Sale change	4405	0.17	−0.09	0.03	0.20	0.72
Perc change	4405	−0.01	−0.02	0.00	0.01	0.12
Sale change Dum	4405	0.72	0.00	1.00	1.00	0.45
Perc change Dum	4405	0.62	0.00	1.00	1.00	0.49
Supplier:						
Size	4405	6.68	5.37	6.96	8.20	2.06
MB	4405	2.85	1.17	1.87	3.18	5.11
Lev	4405	0.30	0.03	0.28	0.49	0.26
RD	4,405	0.09	0.00	0.02	0.11	0.20
ROA	4405	−0.04	−0.02	0.02	0.06	1.27
NegFCF	4405	0.32	0.00	0.00	1.00	0.46
SuppCon	4405	0.02	0.00	0.00	0.01	0.06
Customer:						
CustSize	4405	10.29	9.16	10.43	11.73	1.88
CustLev	4405	0.25	0.13	0.22	0.33	0.19
CustROA	4405	0.04	0.02	0.05	0.08	0.22
CustMB	4405	3.18	1.38	2.27	3.39	4.17
Crush	2803	0.09	−0.51	−0.51	−0.06	0.45

4.2 | Customer relationship duration and cybersecurity awareness score change

Table 3 presents the results of estimating the association between the customer relationship duration and the cybersecurity awareness score change of suppliers. In all models, consistent with the prediction of H1, we find a positive and significant correlation between the two variables. Overall, customers tend to increase their purchases from suppliers whose cybersecurity awareness scores improves. These results indicate that customers value their suppliers' cybersecurity-related issues.

We also find that the indicator of having a cybersecurity disclosure (disc) is positively and significantly correlated with the customer relationship duration in columns 3 and 4. Economically, an increase in cybersecurity disclosure

TABLE 3 Customer relationship duration and cybersecurity awareness score change of suppliers. This table examines the relationship between customer relationships and the change in the cybersecurity awareness score of suppliers. All variables are defined in Appendix A. T-statistics are presented in parentheses. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$ (two-tailed tests).

	(1)	(2)	(3)	(4)
Dependent variable	**Sale change**	**Perc change**	**Sale change Dum**	**Perc change Dum**
Cyber	0.066***	0.006***	0.036*	0.051**
Disc	0.05	0.005	0.091***	0.070**
ROA	−0.255***	−0.006	−0.024	0.057
Lev	−0.073***	0.004	−0.040**	0.029
Size	−0.022**	0.003***	0.01	0.01
AD	−0.418***	0.026**	0.036	0.119*
MB	0.010***	0.000	0.008***	0.002
RD	0.307	−0.050**	0.014	−0.155*
SuppCon	−0.596***	−0.067*	−0.349	−0.411**
CustSize	−0.013**	0.000	−0.015**	0.009
CustLev	−0.051	−0.008	−0.041	−0.132**
CustROA	−0.028	0.000	0.230*	0.167
CustMB	0.003	0.001*	−0.001	−0.002
NegFCF	0.023	0.002	−0.035	0.02
Constant	0.406***	−0.035***	0.593***	0.369***
Year FE	Y	Y	Y	Y
Industry FE	Y	Y	Y	Y
Cluster by industry	Y	Y	Y	Y
Adjusted R^2	0.052	0.17	0.037	0.022
Observations	4405	4405	4405	4405

scores relates to a 3.6% increase in the odds of increasing sales to a major customer and is consistent with suppliers highly valuing these scores.

4.3 | Customer relationship duration and cybersecurity awareness score change of suppliers with cox model

It is possible that suppliers still have relationships with their customers but do not report their information in their financial reports because the customer relationship falls below the 10% threshold. Thus, to better estimate the customer-supplier relationship duration, we applied a Cox proportional hazard model. To use the Cox model, we set a failure variable equal to one when the purchase from a customer does not increase, which includes the disappearance of a customer from the database. We measure the time to failure beginning the year the supplier' discloses the cybersecurity reports.

Table 4 presents estimations of the Cox Hazard model. Consistent with the results in Table 3, suppliers with a dropped score in cybersecurity awareness are less likely to experience sales increases from their main customers. The hazard ratios imply that decreased cybersecurity scores increase the risk of falling sales from one year to the next by a factor of 1.371 (sale change dum) or 1.395 (perc change dum).

TABLE 4 Customer relationship duration and cybersecurity awareness score change of suppliers with Cox model. This Table examines the relationship between customer relationships and cybersecurity awareness score change of suppliers with Cox models. T-statistics are presented in parentheses. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$(two-tailed tests).

	(1)	(2)
	Sale change Dum	**Perc change Dum**
Cyber	−1.371***	−1.395***
	(0.145)	(0.156)
Disc	−0.799***	−0.747***
	(0.184)	(0.208)
Controls	Y	Y
Observations	3522	3150

4.4 | Cross-sectional results

We explore cross-sectional variations in the importance of a supplier's cybersecurity disclosure to a customer. A firm's

TABLE 5 Customer relationship duration, cybersecurity awareness score change, and stock crush. This table reports the estimates of Equation (1) augmented with interaction terms for crush and cyber. All variables are defined in Appendix A. T-statistics are presented in parentheses. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$(two-tailed tests).

	(1)	(2)	(3)	(4)
Dependent variable	**Sale change**	**Perc change**	**Sale change Dum**	**Perc change Dum**
Cyber	0.021	0.002	−1.480***	−1.639***
	(0.029)	(0.002)	(0.169)	(0.169)
Crush	0.050	0.000	0.024	0.001
	(0.003)	(0.000)	(0.013)	(0.027)
Cyber*Crush	0.012*	0.001***	−0.236***	−0.217***
	(0.006)	(0.001)	(0.026)	(0.031)
Disc	0.041	0.006	−1.147***	−0.217***
	(0.028)	(0.010)	(0.016)	(0.032)
Control	Y	Y	Y	Y
Adjusted R^2	0.052	0.17		
Observations	2803	2803	2013	2013
χ^2			173	224

stock-market crash risk is associated with both traders' inability to incorporate bad news into stock prices and management's reluctance to share bad news (Hong & Stein, 2003; Jin and Myers, 2006; Kim et al., 2016). In the event of a cyberattack, sharing all relevant information with a customer in a timely manner will mitigate the negative results along a supply chain. Suppliers with greater crash risk may be less likely to share relevant information in a timely manner. Having better cybersecurity awareness and policies mitigates this risk for customers. Therefore, we expect the previous results to be more important when considering a firm's crash risk.

We augment Equation (1) by interacting a firm's crash risk, *Crush*, with *Cyber*. Table 5 presents the results of our estimations. Columns 1 and 2 present OLS regression with the continuous dependent variables. The interaction term is positive and statistically significant in both models, consistent with customers placing a higher value on these disclosures when a supplier is slow to reveal bad news. Columns 3 and 4 present our dichotomous dependent variables with the interaction term. We use the Cox Hazard model for this estimation. The negative coefficient indicates that relationships are less likely to fail when a firm has a positive change in cybersecurity disclosure quality. The effect is particularly strong when the supplier has a higher stock-price crash risk. Overall, the cross-sectional test provides further confirmation of our main results.

5 | CONCLUSION

This paper investigates the effect of a firm's cybersecurity-related disclosure quality on its ability to maintain relationships with major customers. We find that cyber disclosure quality is positively related to the likelihood of both maintaining a relationship with a major customer and increasing sales to the customer if the relationship is maintained. We interpret these results as evidence that the customer values a firm's cybersecurity awareness and is more likely to interact with customers who have high cybersecurity awareness. Additionally, we find that the relationship is particularly important for firms with high stock-price crash risk, consistent with cybersecurity awareness helping to mitigate other risks.

These results can be applied by regulators, firm management, and academics. The SEC has provided guidance on reporting cybersecurity risks. These disclosures are useful to investors but also help firms make decisions along the supply chain. This additional benefit can be considered when considering disclosure requirements. Firms that wish to attract major customers can use these results to understand the importance of cybersecurity to their larger customers.

Finally, we contribute to the academic literature by providing evidence that cybersecurity is valued by stakeholders outside of the market (Berkman et al., 2018). We add to the literature in finance and accounting that has investigated the supply chain by examining the upstream effects of a firm's disclosure choices. While most studies examine the effects of a customer on a supplier, we have identified a setting in which the supplier's characteristics can be studied (Radhakrishnan et al., 2014; Chen et al., 2019; Chiu et al., 2019; Chen, 2022). Further analysis of upstream effects will enrich the accounting literature and supplement management's ability to attract major customers and maintain relationships.

ACKNOWLEDGMENTS

The authors thank the Woody L. Hunt College of Business for generous funding and Dr. Jonathan Jona for providing data. Data are available from sources listed in the document. This is an original manuscript that has been produced consistent with Wiley's Publication Ethics Guidelines. The manuscript is not under consideration for publication at any other venue. All errors are our own.

DATA AVAILABILITY STATEMENT

The author has provided the required Data Availability Statement, and if applicable, included functional and accurate links to said data therein.

ORCID

Aaron Nelson https://orcid.org/0000-0002-7731-6463

ENDNOTES

[1] See McMillan (2017) for more details on the NotPetya attack.

[2] We thank the authors for sharing their data. See Berkman et al. (2018) for more details on the measure.

[3] If a supplier stops disclosing a major customer, we consider that a 100% reduction in sales. However, the customer may have simply slipped below the 10% of sales threshold for disclosure.

REFERENCES

American Institute of Certified Public Accountants (AICPA). (2018), "Cybersecurity risk management reporting fact sheet", available at https://www.aicpa-cima.com/resources/download/why-use-the-aicpas-cybersecurity-risk-management-reporting-framework

Amir, E., Shai, L., & Tsafrir, L. (2018). Do firms underreport information on cyberattacks? Evidence from capital markets. *Review of Accounting Studies*, *23*(3), 1177–1206.

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

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

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508–526.

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

Chen, C. X., Jiang, W., & Yao, W. (2022). Do major customers help or hurt innovation? The effects of customer-base concentration on radical and incremental innovation. Available at SSRN: https://ssrn.com/abstract=3902729

Chen, K. (2022). Suppliers' relationship-specific investments and customers' management forecasts. *Advances in Accounting*, *59*, 100626.

Chen, T., Levy, H., Martin, X., & Shalev, R. (2021). Buying products from whom you know: Personal connections and information asymmetry in supply chain relationships. *Review of Accounting Studies*, *26*(4), 1492–1531.

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

Cisco, C. (2017). Annual Cybersecurity Report, 2017.

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

Fei, X., Xu, H., & Zhang, J. (2023). Linguistic attributes and trade credit: Evidence from textual analysis of earnings conference calls. *Journal of Corporate Accounting & Finance*, *34*(1), 119–136.

Gordon, L A., Loeb, M P., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, *25*(5), 503–530.

Haapamĺaki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, *34*(7), 808–834.

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

Hong, H., & Stein, J. C. (2003). Differences of opinion, short-sales constraints, and market crashes. *The Review of Financial Studies*, *16*(2), 487–525.

Hortaÿcsu, A., Matvos, G., Syverson, C., & Venkataraman, S. (2013). Indirect costs of financial distress in durable goods industries: The case of auto manufacturers. *The Review of Financial Studies*, *26*(5), 1248–1290.

Irvine, P. J., Park, S. S., & Yıldızhan, C. (2016). Customer-base concentration, profitability, and the relationship life cycle. *The Accounting Review*, *91*(3), 883–906.

Kale, J. R., & Meneghetti, C. (2014). Supplier/customer considerations in corporate financial decisions. *IIMB management review*, *26*(3), 149–155.

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

Loughran, T., & McDonald, B. (2011). When is a liability not a liability? Textual analysis, dictionaries, and 10-Ks. *The Journal of finance*, *66*(1), 35–65.

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

McMillan, R. (2017). Cyberattack Launched for Pain, Not Profit, Experts Say.

Mossburg, E., Gelinne, J., & Calzada, H. (2016). Beneath the surface of a cyberattack: A deeper look at business impacts.

Nelson, A. (2018). The Effect of a Major Customer's Information Quality on Its Supplier's Investment Decisions. PhD dissertation, The Ohio State University.

Nelson, A., & Schwartz, A. (2019). Trickle-Down Overconfidence: The Impact of Customer Overconfidence on Supplier Firms. *Available at SSRN 3467793*.

Patatoukas, P. N. (2012). Customer-base concentration: Implications for firm performance and capital markets: 2011 American accounting association competitive manuscript award winner. *The Accounting Review*, *87*(2), 363–392.

Phillips, G., & Sertsios, G. (2013). How do firm financial conditions affect product quality and pricing? *Management Science*, *59*(8), 1764–1782.

Phua, K., Tham, T. M, & Wei, C. (2018). Are overconfident CEOs better leaders? Evidence from stakeholder commitments. *Journal of Financial Economics*, *127*(3), 519–545.

Radhakrishnan, S., Wang, Z., & Zhang, Y. (2014). Customers' capital market information quality and suppliers' performance. *Production and Operations Management*, *23*(10), 1690–1705.

Raman, K., & Shahrur, H. (2008). Relationship-specific investments and earnings management: Evidence on corporate suppliers and customers. *The Accounting Review*, *83*(4), 1041–1081.

Richardson, V. J., Smith, R. E., & Weidenmier Watson, M. (2019). Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems*, *33*(3), 227–265.

Securities and Exchange Commission. (2011). CF disclosure guidance: Topic No. 2 cybersecurity. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Shumsky, T. (2016). Corporate judgment call: When to disclose you've been hacked. *The Wall Street Journal*, *2016*, https://www.wsj.com/articles/corporate-judgment-call-when-to-disclose-youve-been-hacked-1474320689

Zhou, H., & WC, B. Jr (2007). Supply chain practice and information sharing. *Journal of Operations Management*, *25*(6), 1348–1365.

How to cite this article: Nelson, A., & Wang, S. (2024). The importance of cybersecurity disclosures in customer relationships. *Journal of Corporate Accounting & Finance*, *35*, 66–74. https://doi.org/10.1002/jcaf.22695

APPENDIX A
Variable Definitions

Variable name	Definition
Sale change	The change of sales to the major customer; the difference between sales to a major customer in year $t+1$ and t, scaled by sales to the major customer in year t
Perc change	The percent change of sales to the major customer; the difference between the ratio of sales to a major customer in year $t+1$ to total sales of the supplier and the ratio of sales to the major customer in year t to total sales of the supplier
Sale Change Dum	An indicator equals one if sale change is greater than one, and zero otherwise
Perc change Dum	An indicator equals one if perc change is greater than one, and zero otherwise
Cyber	Raw scores for cyber disclosure extensiveness, provided by Berkman et al. (2018)
Disc	An indicator variable equals one if the supplier firm has cybersecurity disclosure
ROA	Return on assets in year $t+1$; income before extraordinary items (*ib*) in year $t+1$ divided by average total assets (*at*) in year $t+1$
Lev	Total long-term debt divided by total assets of the supplier firm
Size	Natural log value of total assets of supplier firm
AD	Advertisement expenses scaled by the total assets
MB	The market value of equity divided by the book value of equity of the supplier
RD	Supplier research and development expense (*xrd*) scaled by total assets (*at*)
SuppCon	Customer concentration; sales to a specific major customer (*salecs*) divided by total supplier sales
CustSize	Natural log value of total assets of the customer firm
CustLev	Total long-term debt divided by total assets of the customer firm
CustROA	Return on assets in year t+1 for the customer firm; income before extraordinary items (*ib*) in year $t+1$ divided by average total assets (*at*) in year $t+1$
CustMB	The market value of equity divided by the book value of equity of the customer
NegFCF	Indicator variable equal to one if supplier (customer) free cash flow (*oancf-capx*) is negative, zero otherwise
Crush	The negative skewness of firm-specific weekly returns over the fiscal year. For firm j in time Ω, crush is computed as follows: $\frac{n(n-1)^{3/2}\sum W_j^3}{(n-1)(n-2)\sum(W_j^2)^{3/2}}$ where W is a firm-specific weekly return