Data Breaches (Hacking) and Trade Credit

Amanjot Singh
Assistant Professor of Finance
King's University College at the University of Western Ontario
Canada, N6A2M3
asing853@uwo.ca

Phone: +1 2262015119

Data Breaches (Hacking) and Trade Credit

Abstract

This study examines the relationship between data breaches (hacking) and trade credit for U.S. firms. Employing a staggered difference-in-differences approach, we observe that breached firms face shorter payable periods from suppliers than the control group. Data breaches increase the operational risks of breached firms. Suppliers associate high information risks with breached firms. Our findings remain robust to alternative specifications and are more pronounced for firms with (1) no IT expertise, (2) an increased number of stolen records, (3) internal control weakness, (4) low product market competition, and (5) less diversified business operations. Overall, our findings suggest that supplier firms become more prudent with the extension of trade credit after data breaches.

Keywords: Data hacking; Trade credit; Accounts payable

JEL Codes: G30; G32

1. Introduction

"…malicious cyberattacks designed to paralyze IT infrastructures can have devastating effects not only on the directly hit firms, but also on other firms through supply chain linkages…"

Crosignani et al. (2021)[1]

This study investigates the relationship between data breaches (hacking) and trade credit for U.S. firms. With the advent of information technology (IT), most firms spend heavily on the collection (in the region of 36 billion dollars), storage, processing, and analyses of data relating to their customers and employees (Columbus 2014; Huang and Wang 2021). These confidential datasets add to the competitive advantages of firms, helping them elucidate and analyze the intricacies of business operations. However, firms are becoming increasingly vulnerable to data breaches, which are associated with increased costs (Ponemon Institute 2017; Florakis et al. 2022).

The Colonial Pipeline was the target of a data hack in May 2021, and the company had to shut down its gasoline pipeline system in the U.S.[2]. This data breach impacted 45% of the fuel supply to the East Coast, leading to fuel shortages and increases in the price of gasoline across the region. In June 2021, Colonial Pipeline was further served a lawsuit by 11,000 gas stations over the data breach; this resulted in the complete halt of the company's operations, which subjected gas stations to revenue losses. Similarly, JBS, a global food supplier, became the target of a data hack, which resulted in a temporary shutdown of its operations across Australia, Canada, and the U.S.[3]. Between 2005 and 2016, over 7,000 cases of data breaches have been reported in the U.S., as per

[1] Matteo Crosignani, Marco Macchiavelli, and André F. Silva, "Cyberattacks and Supply Chain Disruptions," Federal Reserve Bank of New York Liberty Street Economics (accessed on January 3, 2022: https://libertystreeteconomics.newyorkfed.org/2021/06/cyberattacks-and-supply-chain-disruptions.html.

[2] For details, please refer to: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password (accessed on 2nd July 2021)

[3] For details, please refer to: https://www.bbc.com/news/world-us-canada-57318965 (accessed on January 3, 2022)

the database of the Privacy Rights Clearinghouse (PRC). Of these 7,000 cases, over 1,900 were due to external hacking-based data breaches. Thus, data breaches can influence the business operations of affected firms, thereby disrupting their cash flows.

If data breaches are expected to influence firms' operations, they may also be expected to impact stakeholders. The research on the impact of data breaches on breached firms' creditors is limited. Thus, the effect of data breaches on trade creditors, i.e., operational creditors, remains an empirical question. Recently, Huang and Wang (2021) posited that bankers pay additional attention to firms' data breaches. The authors reported the increased costs of bank loans for breached firms and argued that bankers flag breach-induced disruptions in cash flows and information risks. Therefore, this study investigates the relationship between hacking-based data breaches and the payable periods of the breached firms. Dissimilar to non-hacking-based data breaches, hacking-based ones are generally exogenous and are caused by an external party. This exogenous feature of data hacking can be employed to account for potential endogeneity concerns.

Trade credit facilitates improved monitoring of customers by their suppliers. Amid breach-induced disruptions in cash flows, it is essential to understand how hacking-based data breaches might influence the response of trade creditors. U.S. non-financial firms fund a significant proportion of the short-term funding requirements of their customers (D'Mello and Toscano 2020; Gyimah et al. 2020). Trade credit constitutes approximately 2.5 times the overall value of external public debt, three times bank loans, and 15 times commercial papers on an aggregate basis (Ng et al. 1999; Barrot 2016). Trade credit involves the informal extension of short-term credit from suppliers to customers. It involves short-term (inter-firm) lending as part of the overall supply chain. From the trade credit perspective, suppliers offer an upfront cash discount for making an immediate payment, or the customers are required to make full payments after a determined number of days.

This practice of availing an upfront cash discount versus a delay essentially indicates the extension of suppliers' trade credit to their customers.

Two competing hypotheses are related to trade creditors' response to hacking-based data breaches. First, supplier firms might be expected to extend an increased level of trade credit to breached firms because of the breach-induced disruptions in the cash flows of such firms. Trade creditors act as liquidity providers and even substitute for bank loans during challenging periods involving cash flow disruptions (Cunat 2007; Biais and Gollier 1997; Burkart and Ellingsen 2004). Firms' reliance on trade credit increases during uncertain times, as suppliers can potentially mitigate credit market imperfections leading to the redistribution of funds (Garcia-Appendini and Montoriol-Garriga 2013; Goto et al. 2015; Singh 2022a). Thus, suppliers might be expected to extend additional trade credit to breached firms.

Second, suppliers might be expected to reduce the extension of trade credit because of the increased operational and information risks of breached firms. Firms incur both direct and indirect costs because of data breaches. Direct costs are the costs that are associated with the identification and notification of a data breach. Further, breached firms undertake remedial measures, which eventually increase their total direct costs (Corbet and Gurdgiev 2019; Huang and Wang 2021). Thus, firms must improve their existing cybersecurity measures and rebuild their customer relationship. Legal obligations also fall into the purview of direct costs, which firms may have to incur because of data breaches.

Conversely, indirect costs include the loss of reputation, customer trust, and market share due to a data breach (Romanosky et al. 2014; Martin et al. 2017; Rosati et al. 2017; Gwebu et al. 2018; Huang and Wang 2021). The costs that are associated with data breaches can increase the volatility

of cash flows (or the operational risks) of breached firms (Kamiya et al. 2018). Trade creditors also rely on the financial statements of their customers, and hacking-based data breaches can potentially influence suppliers' perception of the information environment of their customer firms (Amir et al. 2018; Li et al. 2021). Therefore, suppliers might be expected to reduce the extension of trade credit to breached firms, resulting in reduced payable periods.

Employing a sample comprising U.S. firms from 2003 to 2019 and a staggered difference-in-differences approach, our findings reveal that breached firms face shorter payable periods than control firms from suppliers after data breaches. These reduced payable periods are attributed to a supply-side response since hacking-based data breaches do not influence sales growth, return-on-assets (ROA), and the receivable days of breached firms. However, hacking-based data breaches increase the cash flow volatility of breached firms, potentially accounting for the suppliers' negative reaction. It was also observed that breached firms with high analyst coverage, low forecast dispersion, and high institutional ownership in the year preceding the data breach face reduced payable periods from their suppliers. Further, firms with high analyst coverage, low forecast dispersion, and high institutional ownership are expected to have reduced concerns over their information environment (Boone and White 2015; Baghdadi et al. 2020; Jeon et al. 2021). Therefore, it surprises suppliers when firms with reduced concerns over their information environment suffer data breaches. Data breaches increase the information risks of such firms.

These findings remain robust for alternative specifications and are more pronounced for firms with (1) no IT expertise, (2) many stolen records, (3) internal control weakness (ICW) reported under the Sarbanes–Oxley Act (SOX 302), (4) low product market competition, and (5) less diversified business operations in the year preceding the data breach. Information is highly valuable to firms operating in the less competitive business environment, i.e., low product market fluidity, and those

with a less diversified set of business operations (Berger and Hann 2007; Franco et al. 2016; Huang et al. 2017; Ryou et al. 2021). Such firms will be disadvantaged if their sensitive (internal) core business information is leaked to the public and available to competitors, which can attract future product market threats. Therefore, suppliers exhibit increased prudence after a data breach, and this prudence forces them to curtail the trade credit offerable to breached firms. Data breaches contain incremental evidence regarding firms' operational risks, information risks, IT expertise, ICW, product market competition, and diversification of business operations.

This study contributes to the growing body of literature on the possible implications of data breaches on corporate outcomes (Campbell et al. 2003; Cavusoglu et al. 2004; Bose and Leung 2014; Pirounias et al. 2014; Arcuri et al. 2017; Lending et al. 2018; Michel et al. 2020; Huang and Wang 2021; Florakis et al. 2022). The findings reported in this study reveal that hacking-based data breaches influence suppliers' perception of customer firms and that breached firms face reduced payable periods from their suppliers. Furthermore, this study contributes to the literature that examines the possible determinants of the trade credit policy of a firm (Smith 1987; Biais and Gollier 1997; Petersen and Rajan 1997; Ng et al. 1999; Burkart and Ellingsen 2004; Cunat 2007; Fabbri and Menichini 2010; Barrot 2016; Shang 2020; Gyimah et al. 2020; Singh 2022). Our results support that data breaches (hacking) also act as an essential determinant that can influence the trade credit offered by suppliers.

The remainder of this article is organized, as follows: Sections 2, 3, 4, and 5 discuss the literature review, empirical framework, empirical findings, and conclusion of the article, respectively.

2. Literature review

Trade creditors constitute an integral part of a firm's short-term financing requirements. Unlike other financial creditors, trade creditors facilitate the closer monitoring of customers by their suppliers. Suppliers act as liquidity providers during any disruption (Cunat 2007; Biais and Gollier 1997; Burkart and Ellingsen 2004). They can immediately impose sanctions by cutting their supplies if the customers default on their payments (Petersen and Rajan 1997). As a liquidity provider, suppliers might be expected to extend increased trade credit to breached firms. Suppliers can potentially mitigate credit market imperfections leading to the redistribution of funds during uncertain times (Garcia-Appendini and Montoriol-Garriga 2013; Goto et al. 2015; Singh 2022a). Conversely, trade creditors enjoy junior claims over their debt contracts (Zhang 2019). Therefore, suppliers might be expected to extend reduced trade credit to breached firms owing to the breach-induced disruptions in the cash flows, as well as increased information risk, of such firms.

While examining the credit risk implications of data breaches, Kamiya et al. (2018) reported that breached firms are subjected to increased cash flow volatility. Moreover, shareholders typically respond negatively to the announcement of data breaches (Campbell et al. 2003; Cavusoglu et al. 2004; Bose and Leung 2014; Pirounias et al. 2014; Arcuri et al. 2017; Tosun 2021). To elucidate shareholders' responses to data breaches, Michel et al. (2020) investigated the impact of data breaches on the stock returns of U.S. firms. The authors insisted that stock returns witness a negative abnormal return before the announcement of data breaches. A negative abnormal return potentially reflects information leakage that is restored during the post-announcement period.

Lending et al. (2018) examined the roles of the governance and social responsibility choices of firms in their becoming targets for data breaches. The authors posited that firms with strong

corporate governance and very high rankings in social responsibility are less likely to become targets. Breached firms also introduce changes in their corporate governance practices, following data breaches. The extant research on the impact of data breaches on the stakeholders of breached firms is limited. Breached firms' creditors are very vulnerable to breach-induced disruptions in cash flows and information risks. Huang and Wang (2021) reported that bankers respond negatively to data breaches and increase the cost of debt of such firms owing to these disruptions. Thus, this study examines the role of hacking-based data breaches in influencing the trade credit that is offered by supplier firms. Employing hacking-based data breaches as an exogenous shock, our findings indicate that data breaches (hacking) change suppliers' perceptions of breached firms. Payable periods decrease for breached firms because of their high cash flow volatility and increased information risks.

3. Empirical framework

The sample period ranges from 2003 to 2019. Data relating to firm-level data breaches is gathered from Privacy Rights Clearinghouse (PRC), a repository of public announcements on data breaches since 2005. This dataset has been widely employed by previous studies (Kamiya et al. 2018; Garg 2020). Following Garg's framework (2020), this study excludes the data breaches that impacted the government and military, medical and healthcare providers, educational institutions, financial firms, and non-profit organizations because of their unique financial structure. Only hacking-based data breaches between 2005 and 2016 are considered. This sample period (2005–2016) facilitates the comparison of the payable periods from three years before to three years after the data breach. Employing firm names as identifiers, this dataset was manually merged with the Compustat database, i.e., firm-level annual financial dataset.

Since data hacking is an exogenous event, i.e., an event caused by external actions, a staggered difference-in-differences regression approach is employed as part of the identification strategy. The staggered nature of hacking-based data breaches implicitly considers all non-breached firms as the control group at time *t*, even if they subsequently suffered a data breach (Bertrand and Mullainathan 2003). Further, since a hacking-based data breach is an exogenous shock, it is less likely to be caused by firms' payable periods, thus alleviating the reverse causality concerns. Thus, employing this staggered approach, the difference between the payable days for the breached firms before and after the breach are compared with that for the control group before and after the data breach. Further, firm and industry-by-year fixed effects (FEs) are appended to the regressions to account for the unobserved heterogeneous factors that are associated with a firm's data breach, as well its reliance on the trade credit offered by suppliers. These FEs also control the various demand-side factors that could be associated with a firm's reliance on trade credit (Gonçalves et al. 2018). The difference-in-differences regression is defined, as follows:

$$Payable\ Days_{it} = \alpha_i + \alpha_t + \beta_1.(Data\ Breach_i) \times (Post_{it}) + \gamma.Control_{it} + \varepsilon_{it}, \quad (1)$$

where *i* and *t* are subscripts representing the firm and year observations, respectively. α_i and α_t represent the firm and industry-by-year FEs, respectively. ε_{it} is the error term. *Payable Days*$_{it}$ represents the accounts payable as a proportion of the cost of goods sold multiplied by 360 days (Shang 2020). *Data Breach*$_i$ is an indicator variable with values 1 and 0 for hacking-based data-breached firm, *i*, and otherwise, respectively. *Post*$_{it}$ is an indicator variable with values 1 and 0 for the years after the data breach and otherwise, respectively. The employed firm and industry-by-year FEs subsume the individual effects of *Data Breach*$_i$ and *Post*$_{it}$ (Huang and Wang 2021). *Control*$_{it}$ includes a set of firm-level control variables. The following control variables are included in our regressions: firm size, sales growth, market-to-book ratio (M/B ratio), return-on-assets

(ROA), leverage, cash holdings, cash flow, research and development (R&D) expenditures, asset tangibility (property, plant & equipment; PPE), and the logarithm of firm age (Gonçalves et al. 2018; Shang 2020; Gyimah et al. 2020). All the variables are defined in the appendix (Table A1). The key coefficient of interest is (β_1), which indicates a differential shift (i.e., the direct effect) in the payable days of breached firms (post-hacking-based data breaches) compared with those of the control firms.

4. Findings

Out of 8,743 Compustat firms, firm names were employed as identifiers to manually match the obtained data to 116 firms that had witnessed hacking-based data breaches. These 116 firms are distributed belonging to different industries across Fama–French's 12 industry classifications, including non-durable consumers, durable consumers, manufacturing, energy, business equipment, telecommunication, healthcare, wholesale, and retail, and excluding the utility and financial sectors.

Table 1 presents the descriptive statistics of the variables from 2003 to 2019. Averagely, the sample firms have 115 payable days. This indicates that the firms require 115 days to pay bills to their suppliers on an average. The aim is to examine the relationship between hacking-based data breaches and the payable days for breached firms employing the staggered difference-in-differences regression specification. Since data hacking is an exogenous shock, we consider the staggered nature of hacking-based data breaches as the identification strategy. The total firm-year observations are 63,127, and all the continuous variables are winsorized at the 1% and 99% levels.

[Insert Table 1]

Firm leverage, cash holdings, R&D expenditures, and PPE account for ~32%, 23%, 8%, and 24% of the total assets, respectively. Table 2 reports the univariate correlation coefficients of the employed variables. Although the correlation coefficients indicate that the payable days and other control variables are associated, the various firm and industry-year-level characteristics might affect the relationship between hacking-based data breaches and payable days. Thus, a multivariate regression setting employing the staggering nature of hacking-based data breaches as an exogenous external shock and high-dimensional FEs (Equation (1)) is adopted for the analyses.

[Insert Table 2]

Table 3 presents the baseline regression results between the hacking-based data breaches and trade credit. Column (1) includes only *Data Breach*Post* as the variable of interest along with the firm and industry-by-year FEs. The t-statistics (standard errors clustered by industries) are reported in parentheses. The coefficient for *Data Breach*Post* is negative and statistically significant, indicating that the breached firms face shorter payable periods from their suppliers after the data breach compared with the control group. In column (2), other control variables are included with the variable of interest, i.e., *Data Breach*Post.* The coefficient of *Data Breach*Post* remain negative and statistically significant even after the control variables are included. Regarding the economic magnitude, the payable days decrease by 17.5% (−20.11/115) of the sample average payable days for the breached firms compared with those of the control group. Consistent with the results of Shang (2020), these results indicate that firm leverage and the M/B ratio are positively related to the payable days, while ROA and PPE are negatively related to the payable days.[4]

[Insert Table 3]

[4] Our findings remain qualitatively similar after the inclusion of receivable days as a control variable.

To address the issues of the pre-event effects between the breached and non-breached firms, the relationship between the hacking-based data breaches and trade credit is examined from three years before the breach to three years after (Column (3)). Thus, *Pre-Breach 3yrs* and *Post-Breach 3yrs* are appended in the regression specification. *Pre-Breach 3yrs* is an indicator variable with values 1 and 0 for three years before the data breach and otherwise, respectively. *Post-Breach 3yrs* is an indicator variable with values 1 and 0 for the three years after the data breach and otherwise, respectively. The coefficient of *Post-Breach 3yrs* is negative and statistically significant, indicating that the payable days decrease after the data breach with no observed effect three years before the data breach. Particularly, this test demonstrates that there is no evidence of a decrease in the payable periods before the data breach, further confirming that the hacking-based data breaches are indeed exogenous, and that reverse causality is less of a concern.

4.1 Operational performance

The mechanisms through which hacking-based data breaches negatively affect the suppliers' payable days are also explored. Therefore, this section examines the operational performances of the breached and non-breached firms. The operational performances regarding the cash flow volatility, ROA, sales growth, and receivable days are measured (Huang and Wang 2021). Table 4 presents the regression results of these operational performances employing the operational performance variables as the dependent variables in the staggered difference-in-differences regression setting. Except for cash flow volatility[5], the findings indicate that no statistically significant relationship is observed between hacking-based data breaches and other operational performance measures. Regarding the cash flow volatility, the coefficient of *Data Breach*Post* is

[5] Our findings remain consistent after employing the cash flow volatility of the past five years.

positive and statistically significant, indicating increased cash flow volatility for the breached firms compared with those of the control group after the data breach. This finding demonstrates that breach-induced cash flow volatility potentially influences suppliers' decision to offer trade credit to breached firms.

[Insert Table 4]

This reduction in payable days could be a demand-side effect. Since hacking-based data breaches might cause reputational and revenue losses for breached firms, such firms might decrease their demand for payable days following a decrease in their sales (Huang and Wang 2021). Conversely, these findings do not support the latter effect because sales growth, ROA, and receivable days are not significantly affected by hacking-based data breaches. If this change in the payable days was due to the demand-side factors, its impact on the sales growth, ROA, and receivable days might be expected. Thus, suppliers are concerned with the cash flow volatility of breached firms, which provokes a negative reaction in the form of reduced payable days to breached firms.

4.2 Information environment

Since trade creditors rely on the financial statements and overall information environment of firms (Li et al. 2021); data breaches can indicate a weakness in the information environment of firms (Amir et al. 2018; Huang and Wang 2021). Considering that breached firms exhibit high information risks, suppliers' trust in the information provided by such firms correspondingly decreases. Thus, firms' pre-data-breach information environment can also affect suppliers' decisions to extend their trade credit after the data breach. Therefore, unlike Huang and Wang (2021), we examine the role of suppliers' perception of the information environment based on breached firms' pre-data-breach information environment in influencing the payable days of

breached firms and compared with those of the control group. When firms are unexpectedly hit by data breaches, suppliers are taken by surprise and respond negatively.

To capture suppliers' perception of the information environment, three different measures of the information environment of firms, i.e., analyst coverage, analyst forecast dispersion, and institutional ownership are considered. Firms with high analyst coverage, low forecast dispersion, and high institutional ownership exhibit reduced concerns about the information environment (Boone and White 2015; Baghdadi et al. 2020; Jeon et al. 2021). Shorter payable periods are expected for firms that exhibited lesser concerns over the information environment in the year before the data breach. For such firms, data breaches constitute a surprise element for the suppliers who might react negatively because they associate breached firms with high information risks. Table 5 reports the results for the data breaches and the information environment of firms.

High is an indicator variable with values 1 and 0 for breached firms that exhibited above-the-median values for the analyst coverage, forecast dispersion, and institutional ownership in the year before the data breach and otherwise, respectively. The triple interaction term is introduced into the regression Equation (1) to elucidate the relationship between hacking-based data breaches and the information environment of firms.

[Insert Table 5]

The coefficient of *High Analyst Coverage*Data Breach*Post* is negative and statistically significant for firms with above-median analyst coverage in the year preceding the data breach. A negative and statistically significant coefficient is also observed for firms with high institutional ownership in the year preceding the data breach, i.e., *High Institutional Ownership*Data Breach*Post*. This implies that the differential effect of hacking-based data breaches is pronounced

for firms with high analyst coverage and high institutional ownership. In both cases, the direct effect of hacking-based data breaches (*Data Breach*Post*) for firms with low analyst coverage and low institutional ownership is not statistically distinguishable from zero. However, the sum of the two coefficients, i.e., *Data Breach*Post + High Analyst Coverage*Data Breach*Post* for high analyst coverage, and *Data Breach*Post + High Institutional Ownership*Data Breach*Post* for high institutional ownership, is negative and statistically significant, suggesting that the negative implications of hacking-based data breaches are noticeable for firms with high analyst coverage and high institutional ownership.

The appended interaction term for high forecast dispersion is not statistically significant, indicating that the differential effect of hacking-based data breaches for firms with high forecast dispersion is not statistically distinguishable from breached firms with low forecast dispersion. However, the direct effect of the hacking-based data breaches (*Data Breach*Post*) remains negative and statistically significant for firms with low forecast dispersion, and the sum of the two coefficients, i.e., *Data Breach*Post + High Forecast Dispersion*Data Breach*Post,* is also negative and statistically significant, confirming that the negative implications of hacking-based data breaches exist across both high and low forecast dispersion groups. However, the magnitude of the direct effect of hacking-based data breaches (*Data Breach*Post*) is almost 50 percent bigger than the sum of the two coefficients, suggesting that the negative implications of hacking-based data breaches are more pronounced for firms with low forecast dispersion.

Overall, these findings indicate that the firms that exhibited lesser concerns over the information environment in the year preceding the data breach face reduced payable days from their suppliers. Since suppliers are taken by surprise, they reduce their extension of trade credit because they perceive such firms to exhibit high information risks after the data breach.

4.3 IT expertise, number of stolen records, and internal control weakness

Following Huang and Wang (2021), we explore the role of IT expertise, the number of stolen records and ICW reported under the Sarbanes–Oxley Act (SOX 302) while elucidating the relationship between hacking-based data breaches and trade credit. A negative response is expected from the suppliers for firms with no in-house IT expertise in the year preceding the data breach. This is because the presence of in-house IT experts, such as chief information officers, chief security officers, or any other officer responsible for information- or security-related issues, indicates that firms were keen to protect their data from external threats. Thus, reduced payable periods are expected for firms with no IT experts in the year preceding the data breach. Further, the role of the number of actual stolen records is examined. Firms with many stolen records are more vulnerable to the negative implications of data breaches.

Firms with a material risk in their internal controls, i.e., firms with material ICW reported under SOX 302, are also more susceptible to the negative implications of data breaches (Huang and Wang 2021). Internal controls assume an imperative role in the restoration of lost data, as well as identification and prevention of data breaches in a firm. Therefore, we expect relatively reduced payable periods for firms with a material ICW reported under SOX 302 in the year preceding the data breach.

Table 6 presents the results of the IT expertise, the number of stolen records, and ICW reported under SOX 302. The triple interaction term is introduced in Equation (1) based on the firm's IT expertise, number of stolen records, and ICW reported under SOX 302 in the year preceding the data breach. *IT Expert* is an indicator variable with values 1 and 0 for breached firms that exhibited IT expertise in the year preceding that of the data breach and otherwise, respectively. *Large*

Records Stolen is an indicator variable with values 1 and 0 for breached firms with many stolen records based on the above-median values and otherwise, respectively. Similarly, *ICW* is an indicator variable with values 1 and 0 for breached firms that exhibited ICW, as reported under SOX 302, in the year before the data breach and otherwise, respectively.

For firms with IT expertise, no negative response is expected from suppliers since such expertise indicates the firm's desire to protect its data from external threats. Furthermore, such firms are expected to quickly regain control over breached information through their in-house IT experts. Our results demonstrate that the coefficient of *IT Expert*Data Breach*Post* is positive but statistically insignificant for firms with an in-house IT expertise and the sum of the two coefficients, i.e., *Data Breach*Post + IT Expert*Data Breach*Post*, is negative and statistically indistinguishable from zero. However, the direct effect of the hacking-based data breaches (*Data Breach*Post*) remains negative and statistically significant for firms with no in-house IT expertise, implying that the negative implications of hacking-based data breaches are pronounced for firms with no IT expertise in the year preceding the data breach. Firms without IT expertise are more vulnerable to the overarching implications of data breaches.

[Insert Table 6]

We also observe that firms with many stolen records are subject to negative implications regarding reduced payable periods from their suppliers. The direct effect of hacking-based data breaches (*Data Breach*Post*) is not statistically distinguishable from zero for firms with fewer records stolen. However, the coefficient of *Large Records Stolen*Data Breach*Post* is negative and statistically significant and the sum of the two coefficients, i.e., *Data Breach*Post + Large Records Stolen*Data Breach*Post* is also negative and statistically significant, indicating that the

negative implications of hacking-based data breaches are noticeable for firms with many stolen records. Firms with many stolen records are highly vulnerable to breach-induced disruptions in cash flows and information risks.

For the ICW, the direct effect of hacking-based data breaches (*Data Breach*Post*) is negative and statistically significant, suggesting that firms with no material ICW reported under SOX 302 experience reduced payable periods from their suppliers after the data breach. Although the coefficient of *ICW*Data Breach*Post* is not statistically significant, the sum of the two coefficients, i.e., *Data Breach*Post + ICW*Data Breach*Post*, is negative and statistically significant, indicating that firms with material ICW reported under SOX 302 also witness reduced payable periods from their suppliers after the data breach. However, the negative implications of hacking-based data breaches are more pronounced for firms with material ICW reported under SOX 302 in the year preceding the data breach.

Overall, our findings suggest that firms with (a) no IT expertise, (2) many records stolen, and (3) material ICW reported under SOX 302 in the year preceding the data breach experience a pronounced effect of hacking-based data breaches. Supplier firms become more prudent with the extension of trade credit after data breaches for such firms.

4.4 Product market fluidity and firm diversification

Prior studies like Fabbri and Klapper (2008), Dass et al. (2015), Gonçalves et al. (2018), and Singh (2022) have documented a significant relationship between the product market competition and the trade credit policy of a firm. Therefore, we also examine the role of product market competition and firm diversification to explain the negative relationship between hacking-based data breaches and trade credit. Information is more valuable to firms operating in a less competitive business

environment; thus, such firms would be disadvantaged if sensitive internal information is revealed to the public, which can attract future competitors in the product market space (Huang et al. 2017; Ryou et al. 2021). Therefore, this negative response from suppliers is expected to appear more for firms exhibiting low product market competition in the year preceding the data breach. Regarding product market competition, product market fluidity, as developed by Hoberg et al. (2014), is employed as a measure of product market competition. This fluidity measure is based on the firm's product text descriptions, capturing a change in the firm's product space owing to the changes made by the competitors in the firm's product markets. *Low Fluidity* is an indicator variable with values 1 and 0 for breached firms that exhibited below-the-median values for product market fluidity in the year preceding the data breach and otherwise, respectively. Firms with low product market fluidity tend to operate in a low competitive environment.

Similarly, information is highly valuable for firms with a less diversified set of business operations across the different business segments (Berger and Hann 2007; Franco et al. 2016). Such firms would be disadvantaged if their sensitive internal information (pertaining to core business operations) is leaked into the market, which can negatively influence the competitive advantage of breached firms. Thus, this negative response from suppliers is expected to appear for firms with a less diversified set of operations based on their number of business segments. *Focused Firms* is an indicator variable with values 1 and 0 for breached firms exhibiting only one business segment in the year preceding the data breach and otherwise, respectively. Firms with only one business segment are categorized as "focused" firms.

[Insert Table 7]

Table 7 presents the regression results of firms' product market fluidity and diversification. The triple interaction terms are introduced to capture the roles of product market competition and firm diversification. In both cases, the direct effect of hacking-based data breaches (*Data Breach*Post*) is negative and statistically significant for firms with high product market competition and a diversified set of business operations (i.e., firms with multiple business segments). However, the coefficients of *Low Fluidity*Data Breach*Post* and *Focused Firms*Data Breach*Post* are negative but statistically insignificant and the sum of the two coefficients, i.e., *Data Breach*Post + Low Fluidity*Data Breach*Post* for firms with low product market competition, and *Data Breach*Post + Focused Firms*Data Breach*Post* for firms with only one business segment are negative and statistically significant. This suggests that payable periods decrease for firms with both high and low product market competition and single and multiple business segments. However, the negative implications of hacking-based data breaches are more pronounced for firms with low product market fluidity and single business segment experience. Put differently, firms operating under a low competitive environment with a valuable set of sensitive internal information that can attract future competition in the product market space experience reduced payable periods from their suppliers after a data breach. Such firms are disadvantaged if their internal information becomes public and available to competitors.

4.5 Robustness

The robustness of the findings are explored in two different aspects. First, the control group is considered via the propensity score matching (PSM) approach. It is arguable that hacking-based data-breached firms are fundamentally different from non-breached firms. These findings might exhibit a selection bias. To address this concern, a PSM model is employed to determine the matched control group. Thus, the matched control firms are determined from the same 2-digit SIC

codes and the year of the data breach by using firm size, ROA, leverage, cash flow volatility, PPE, Altman's Z-score, and M/B ratio as matching factors via the probit model. These firm-level characteristics account for some of the observable fundamental differences across our sample firms (Custodio et al. 2013; Boubaker et al. 2018).

The data for 90 breached and 90 control firms are collected without replacement. Table 8 presents the results of the PSM model. Panel A reveals that the treatment (breached firms) and the control firms (non-breached firms) are statistically indistinguishable in terms of firm size, profitability (ROA), total debt (leverage), cash flow volatility, asset tangibility (PPE), default risk (Altman's Z-score), and growth opportunities (M/B ratio). The breached and non-breached firms exhibit similar firm-level characteristics, indicating that the variable, *Data Breach*Post*, captures the change in the payable days after accounting for the observable differences between the breached and non-breached firms.

[Insert Table 8]

Panel B reveals that a negative relationship persists between hacking-based data breaches and trade credit. The coefficient of *Data Breach*Post* is negative and statistically significant. Thus, the main finding is robust to the PSM analysis that controls some observable differences between the breached and non-breached firms. The breached firms face shorter payable periods from their suppliers after the data breach.

Second, it could be argued that even non-hacking-based data breaches could generate a similar negative reaction from suppliers probably because hacking- and non-hacking-based data breaches can cause breach-induced disruptions in business operations. To address this concern, the non-hacking-based data breaches in Table A2 (reported in the appendix) are considered, after which

the regression in Equation (1) is re-estimated. According to PRC, non-hacking-based data breaches generally include frauds involving debit and credit cards, insider data breaches, physical data breaches, portable-device data breaches, stationary computer loss, and unintended disclosures.

After excluding hacking-based data breaches, it was observed that 231 firms experienced non-hacking-based data breaches during the sample period. Thus, the regression Equation (1) is rerun based on these non-hacking-based data breaches. The results reveal that the coefficient of *Non-Hack Data Breach*Post* is negative but statistically insignificant, indicating that the firms that experience non-hacking-based data breaches do not observe a significantly negative reaction from their suppliers. This finding indicates that the suppliers consider hacking-based data breaches more serious, considering their influence as an exogenous external threat compared with non-hacking-based data breaches.

5. Conclusion

Over time, firms have become vulnerable to data breaches with high associating costs. Therefore, this study examined the relationship between the hacking-based data breaches and trade credit for U.S. firms. Dissimilar to non-hacking-based data breaches, hacking-based ones are truly exogenous. Therefore, a staggered difference-in-differences approach is employed. Our findings reveal that firms face shorter payable periods from suppliers after hacking-based data breaches relative to the control group. Both operational and information risks act as potential mechanisms through which data breaches influence the payable periods. Suppliers consider breached firms to have a high information risk. These findings remain robust to alternative specifications and are more pronounced for firms with (1) no IT expertise, (2) increased number of stolen records, (3) ICW reported under SOX 302, (4) low product market competition, and (5) less diversified

business operations in the year preceding the data breach. Suppliers become more prudent with their extension of trade credit after data breaches. These findings report another facet related to the implications of data breaches for trade credit financing. Data breaches contain incremental evidence of firms' operational risks, information risks, IT expertise, ICW, product market threats, and diversification of business operations.

References

Amir, E., S. Levi, and T. Livne. 2018. "Do Firms Underreport Information on Cyber-Attacks? Evidence From Capital Markets." *Review of Accounting Studies, 23* (3), 1177–1206.

Arcuri, M. C., M. Brogi, and G. Gandolfi. 2017. "How Does Cyber Crime Affect Firms? The Effect of Information Security Breaches on Stock Returns." *In ITASEC* (pp. 175–193).

Baghdadi, G. A., L. H. Nguyen, and E. J. Podolski. 2020. "Board Co-option and Default Risk." *Journal of Corporate Finance, 64*, 101703.

Barrot, J. 2016. "Trade Credit and Industry Dynamics: Evidence from Trucking Firms." *Journal of Finance. 71* (5), 1975–2016.

Berger, P. G., and R. N. Hann. 2007. "Segment Profitability and the Proprietary and Agency Costs of Disclosure." *The Accounting Review, 82* (4), 869–906.

Bertrand, M., and S. Mullainathan. 2003. "Enjoying the Quiet Life? Corporate Governance and Managerial Preferences." *Journal of Political Economy, 111* (5), 1043–1075.

Biais, B., and C. Gollier. 1997. "Trade Credit and Credit Rationing." *Review of Financial Studies, 10* (4), 903–937.

Boone, Audra L., and Joshua T. White. 2015. "The effect of institutional ownership on firm transparency and information production." *Journal of Financial Economics, 117*(3), 508-533.

Bose, I., and A. C. M. Leung. 2014. “Do Phishing Alerts Impact Global Corporations? A Firm Value Analysis.” *Decision Support Systems, 64*, 67–78.

Boubaker, S., W. Saffar, and S. Sassi. 2018. “Product Market Competition and Debt Choice.” *Journal of Corporate Finance, 49*, 204–224.

Burkart, M., and T. Ellingsen. 2004. “In-Kind Finance: A Theory of Trade Credit.” *American Economic Review, 94* (3), 569–590.

Campbell, K., L. A. Gordon, M. P. Loeb, and L. Zhou. 2003. “The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market”. *Journal of Computer Security, 11* (3), 431–448.

Cavusoglu, H., B. Mishra, and S. Raghunathan. 2004. “The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers”. *International Journal of Electronic Commerce, 9* (1), 70–104.

Columbus, L. 2014. “The Year Big Data Adoption Goes Mainstream in the Enterprise.” Forbes (January 12). Available at: https://www.forbes.com/sites/louiscolumbus/2014/01/12/2014-the-year-big-data-adoption-goes-mainstream-in-the-enterprise/#1aad46da2055

Corbet, S., and Gurdgiev, C. 2019. “What the hack: Systematic risk contagion from cyber events”. *International Review of Financial Analysis*, *65*, 101386.

Cunat, V. M. 2007. “Trade Credit: Suppliers as Debt Collectors and Insurance Providers.” *Review of Financial Studies, 20*(2), 491–527.

Custodio, C., M. A. Ferreira, and L. Laureano. 2013. “Why are US Firms Using More Short-Term Debt?” *Journal of Financial Economics, 108* (1), 182–212.

Dass, N., Kale, J. R., and Nanda, V. 2015. “Trade credit, relationship-specific investment, and product market power”. *Review of Finance*, *19*(5), 1867-1923.

D'Mello, R., and F. Toscano. 2020. “Economic Policy Uncertainty and Short-Term Financing: The Case of Trade Credit.” *Journal of Corporate Finance, 64*, 101686.

Fabbri, D., and Klapper, L. F. 2008. “Market power and the matching of trade credit terms”. World Bank Policy research working paper, (4754).

Fabbri, D., and A. M. C. Menichini. 2010. “Trade Credit, Collateral Liquidation, and Borrowing Constraints.” *Journal of Financial Economics*, *96*, 413–432.

Florakis, C., Louca, C., Michaely, R., and Weber, M. 2022. “Cybersecurity Risk.” *Review of Financial Studies*. Forthcoming.

Franco, F., O. Urcan, and F. P. Vasvari. 2016. “Corporate Diversification and the Cost of Debt: The Role of Segment Disclosures.” *The Accounting Review*, *91*(4), 1139–1165.

Garcia-Appendini, E., and Montoriol-Garriga, J. 2013. “Firms as liquidity providers: Evidence from the 2007–2008 financial crisis”. *Journal of Financial Economics, 109*(1), 272-291.

Garg, P. 2020. “Data Breaches and Cash Holdings: Spillover Effect.” *Financial Management, 49* (2), 503–519.

Gonçalves, A. B., R. F. Schiozer, and H. H. Sheng. 2018. “Trade Credit and Product Market Power During a Financial Crisis.” *Journal of Corporate Finance, 49*, 308–323.

Goto, S., Xiao, G., and Xu, Y. 2015. “As told by the supplier: Trade credit and the cross section of stock returns”. *Journal of Banking and Finance, 60,* 296-309.

Gwebu, K. L., J. Wang, and L. Wang. 2018. “The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management.” *Journal of Management Information Systems*, *35* (2), 683–714.

Gyimah, D., Machokoto, M., and Sikochi, A. S. 2020. “Peer influence on trade credit”. *Journal of Corporate Finance, 64,* 101685.

Hoberg, G., G. Phillips, and N. Prabhala. 2014. “Product Market Threats, Payouts, and Financial Flexibility.” *Journal of Finance*, *69* (1), 293–324.

Huang, Y., R. Jennings, and Y. Yu. 2017. “Product Market Competition and Managerial Disclosure of Earnings Forecasts: Evidence From Import Tariff Rate Reductions.” *The Accounting Review*, *92* (3), 185–207.

Huang, H. H., and C. Wang. 2021. “Do Banks Price Firms' Data breaches?” *The Accounting Review, 96* (3), 261–286.

Jeon, Y., T. H. McCurdy, and X. Zhao. 2021. “News as Sources of Jumps in Stock Returns: Evidence From 21 Million News Articles for 9000 Companies.” *Journal of Financial Economics*. Forthcoming.

Kamiya, S., J. K. Kang, J. Kim, A. Milidonis, and R. M. Stulz. 2018. “What is the Impact of Successful Cyberattacks on Target Firms?” (No. w24409). National Bureau of Economic Research.

Lending, C., K. Minnick, and P. J. Schorno. 2018. “Corporate Governance, Social Responsibility, and Data Breaches.” *Financial Review, 53* (2), 413–455.

Li, X., J. Ng, and W. Saffar. 2021. “Financial Reporting and Trade Credit: Evidence From Mandatory IFRS Adoption.” *Contemporary Accounting Research, 38* (1), 96–128.

Martin, K. D., A. Borah, and R. W. Palmatier. 2017. “Data Privacy: Effects on Customer and Firm Performance.” *Journal of Marketing, 81* (1), 36–58.

Michel, A., J. Oded, and I. Shaked. 2020. “Do Security Breaches Matter? The Shareholder Puzzle.” *European Financial Management, 26* (2), 288–315.

Ng, C. K., J. K. Smith, and R. L. Smith. 1999. “Evidence on the Determinants of Credit Terms Used in Interfirm Trade.” *Journal of Finance, 54* (3), 1109–1129.

Petersen, M. A., and R. G. Rajan. 1997. “Trade Credit: Theories and Evidence.” *Review of Financial Studies, 10* (3), 661–691.

Pirounias, S., D. Mermigas, and C. Patsakis. 2014. “The Relation Between Information Security Events and Firm Market Value, Empirical Evidence on Recent Disclosures: An Extension of the GLZ Study.” *Journal of Information Security and Applications, 19* (4–5), 257–271.

Ponemon Institute. 2017. “2017 Cost of Data Breach Study: United States.” Traverse City, MI: Ponemon Institute LLC.

Romanosky, S., D. Hoffman, and A. Acquisti. 2014. “Empirical Analysis of Data Breach Litigation.” *Journal of Empirical Legal Studies, 11* (1), 74–104.

Rosati, P., M. Cummins, P. Deeney, F. Gogolin, L. Van der Werff, and T. Lynn. 2017. “The Effect of Data Breach Announcements Beyond the Stock Price: Empirical Evidence on Market Activity.” *International Review of Financial Analysis, 49,* 146–154.

Ryou, J. W., A. Tsang, and K. T. Wang. 2021. “Product Market Competition and Voluntary Corporate Social Responsibility Disclosures.” *Contemporary Accounting Research*. Forthcoming.

Shang, C. 2020. “Trade Credit and Stock Liquidity.” *Journal of Corporate Finance, 62,* 101586.

Singh, A. 2022a. “Does trade credit financing matter for stock returns in times of crisis? Evidence from the COVID-19 stock market crisis”. *Applied Economics*, Forthcoming.

Singh, A. 2022. “Hedge fund activism and trade credit”. *Global Finance Journal*, Forthcoming.

Smith, J. K. 1987. “Trade Credit and Informational Asymmetry.” *Journal of Finance, 42* (4), 863–872.

Tosun, O. K. 2021. “Cyber-attacks and stock market activity”. *International Review of Financial Analysis, 76,* 101795.

Zhang, Z. 2019. “Bank Interventions and Trade Credit: Evidence From Debt Covenant Violations.” *Journal of Financial and Quantitative Analysis, 54* (5), 2179–2207.

Table 1: Descriptive Statistics

Variables	Mean	S.D.	P25	P50	P75
Payable Days	115.3028	334.2885	24.6710	43.2915	74.5890
Firm Size	5.5901	2.6210	3.8745	5.7181	7.4051
Leverage	0.3248	0.6663	0.0128	0.1834	0.3722
Cash Holdings	0.2264	0.2353	0.0457	0.1369	0.3362
Sales Growth	0.2329	0.9011	−0.0447	0.0720	0.2292
M/B ratio	3.0709	5.7543	1.1627	1.6353	2.6756
ROA	−0.0993	0.7530	−0.0273	0.0884	0.1486
Cash Flow	−0.0533	0.4720	−0.0261	0.0657	0.1234
R&D	0.0752	0.1652	0.0000	0.0060	0.0782
PPE	0.2377	0.2374	0.0564	0.1468	0.3487
Log(Firm Age)	2.5366	0.8738	1.9459	2.6391	3.1781

Note: This table reports the descriptive statistics of our variables ranging from the payable days; firm size; leverage; cash holdings; sales growth; market-to-book ratio (M/B); return on assets (ROA); cash flow; research and development (R&D); and plant, property, and equipment (PPE) to firm age. All the variables are defined in the appendix.

Table 2: Correlation

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
(1) Payable Days	1										
(2) Firm Size	−0.2498	1									
(3) Leverage	0.3175	−0.2722	1								
(4) Cash Holdings	0.0476	−0.257	−0.1317	1							
(5) Sales Growth	0.0731	−0.11	0.017	0.1076	1						
(6) M/B ratio	0.3664	−0.423	0.6128	0.1341	0.1099	1					
(7) ROA	−0.3992	0.5093	−0.5956	−0.1429	−0.0959	−0.7394	1				
(8) Cash Flow	−0.3641	0.5047	−0.5511	−0.1773	−0.1022	−0.6603	0.8967	1			
(9) R&D	0.1724	−0.341	0.1715	0.4149	0.0873	0.3332	−0.4711	−0.5363	1		
(10) PPE	−0.0221	0.2204	0.0709	−0.4066	−0.0279	−0.1038	0.1035	0.1355	−0.2355	1	
(11) Log(Firm Age)	−0.1058	0.2531	−0.0615	−0.2125	−0.1756	−0.1479	0.1689	0.1687	−0.1207	0.0289	1

Note: This table reports the correlation coefficients of our variables ranging from the payable days, firm size, leverage, cash holdings, sales growth, M/B, ROA, cash flow, R&D, and PPE to firm age. All the variables are defined in the appendix.

Table 3: Baseline Regression

Variables	**(1)**	**(2)**	**(3)**
	Payable Days	**Payable Days**	**Payable Days**
*Data Breach*Post*	−18.65***	−20.11***	
	(−2.89)	(−2.62)	
Pre-Breach 3yrs			0.602
			(0.20)
Post-Breach 3yrs			−18.11**
			(−2.56)
Firm Size		−10.15*	−10.15*
		(−1.90)	(−1.90)
Leverage		43.57***	43.57***
		(4.19)	(4.19)
Cash Holdings		−0.864	−0.889
		(−0.05)	(−0.05)
Sales Growth		−5.045	−5.045
		(−1.11)	(−1.11)
M/B		3.862**	3.860**
		(2.24)	(2.24)
ROA		−27.71*	−27.71*
		(−1.81)	(−1.81)
Cash Flow		−5.738	−5.748
		(−0.33)	(−0.33)
R&D		2.598	2.611
		(0.09)	(0.09)
PPE		−47.40*	−47.40*
		(−1.68)	(−1.68)
Log(Firm Age)		−1.371	−1.248
		(−0.14)	(−0.12)
Observations	63,127	63,127	63,127
Firm FEs	Yes	Yes	Yes
Industry-by-Year FEs	Yes	Yes	Yes
Adjusted R^2	0.53	0.54	0.54

Note: This table reports the baseline regression results. Column (1) includes only *Data Breach* as the variable of interest, (2) includes control variables and *Data Breach*, and (3) considers three years each before and after the data breaches. *Data Breach* is an indicator variable with values 1 and 0 for hacking-based data-breached firms and otherwise, respectively. *Post* is an indicator variable with values 1 and 0 for the years after the breach and otherwise, respectively. *Pre-Breach 3yrs* is an indicator variable with values 1 and 0 for the three years before the data breach and otherwise, respectively. *Post-Breach 3yrs* is an indicator variable with values 1 and 0 for the three years after the data breach and otherwise, respectively. All the variables are defined in the appendix. The t-statistics (standard errors clustered by industries) are reported in parentheses. ***, **, and * indicate the significances at the 1%, 5%, and 10% levels, respectively.

Table 4: Operational Performances

Variables	Cash Flow Volatility	ROAs	Sales Growth	Receivable Days
*Data Breach*Post*	49.75**	0.00226	−0.00247	0.188
	(2.25)	(0.28)	(−0.09)	(0.08)
Controls	Yes	Yes	Yes	Yes
Firm FEs	Yes	Yes	Yes	Yes
Industry-by-Year FEs	Yes	Yes	Yes	Yes
Observations	63,127	63,127	63,127	63,127
Adjusted R^2	0.79	0.89	0.14	0.61

Note: This table presents the results of the firm performance and data breaches. Cash flow volatility, ROAs, sales growth, and receivable days are considered as the measures of firm performance. *Data Breach* is an indicator variable with values 1 and 0 for hacking-based data-breached firms and otherwise, respectively. *Post* is an indicator variable with values 1 and 0 for the years after the data breach and otherwise, respectively. The t-statistics (standard errors clustered by industries) are reported in parentheses. ***, **, and * indicate the significances at the 1%, 5%, and 10% levels, respectively.

Table 5: Information Risks

Variables	**Analyst Coverage**	**Forecast Dispersion**	**Institutional Ownership**
	Payable Days	**Payable Days**	**Payable Days**
*Data Breach*Post*	−4.050	−24.29**	−3.372
	(−0.73)	(−2.27)	(−0.68)
*High Analyst Coverage*Data Breach*Post*	−31.59**		
	(−2.56)		
*High Forecast Dispersion*Data Breach*Post*		11.79	
		(0.93)	
*High Institutional Ownership*Data Breach*Post*			−34.96***
			(−2.73)
Controls	Yes	Yes	Yes
Firm FEs	Yes	Yes	Yes
Industry-by-Year FEs	Yes	Yes	Yes
Observations	63,127	63,127	63,127
Adjusted R^2	0.54	0.54	0.54
*Data Breach*Post + High Analyst Coverage*Data Breach*Post*	-35.64*** [8.73]		
*Data Breach*Post + High Forecast Dispersion*Data Breach*Post*		-12.5* [3.24]	
*Data Breach*Post + High Institutional Ownership*Data Breach*Post*			-38.33*** [9.03]

Note: This table presents the results for the payable days after considering the role of firms' information risk. The information environment is measured based on the analyst coverage, forecast dispersion, and institutional ownership. *Data Breach* is an indicator variable with values 1 and 0 for the hacking-based data-breached firms and otherwise, respectively. *Post* is an indicator variable with values 1 and 0 for the years after the data breach and otherwise, respectively. *High* is an indicator variable for breached firms with values 1 and 0 for the above-median values of the respective measures in the year before the data breach and otherwise, respectively. The t-statistics (standard errors clustered by the industries) are reported in parentheses. F-test is reported in the square brackets. ***, **, and * indicate the significances at the 1%, 5%, and 10% levels, respectively.

Table 6: IT Expertise, Stolen Records, and ICW

Variables	IT Expert	Records Stolen	Internal control Weakness
	Payable Days	Payable Days	Payable Days
*Data Breach*Post*	−20.50**	−6.972	−20.09**
	(−2.57)	(−1.46)	(−2.57)
*IT Expert*Data Breach*Post*	12.00		
	(0.93)		
*Large Records Stolen*Data Breach*Post*		−32.73**	
		(−2.36)	
*ICW*Data Breach*Post*			−1.247
			(−0.10)
Controls	Yes	Yes	Yes
Firm FEs	Yes	Yes	Yes
Industry-by-Year FEs	Yes	Yes	Yes
Observations	63,127	63,127	63,127
Adjusted R^2	0.54	0.54	0.54
*Data Breach*Post + IT Expert*Data Breach*Post*	-8.5 [0.93]		
*Data Breach*Post + Large Records Stolen*Data Breach*Post*		-39.70*** [7.93]	
*Data Breach*Post + ICW*Data Breach*Post*			-21.34** [4.68]

Note: This table reports the regression results after considering the role of IT expertise, stolen records, and ICW reported under SOX 302. *Data Breach* is an indicator variable with values 1 and 0 for data-hacking-breached firms and otherwise, respectively. *Post* is an indicator variable with values 1 and 0 for the years after the data breach and otherwise, respectively. *IT Expert* is an indicator variable with values 1 and 0 for breached firms that had a chief information officer, chief security officer, or any officer dedicated to information or security in the year before the data breach and otherwise, respectively. *Large Records Stolen* is an indicator variable with values 1 and 0 for breached firms that had a large number of records stolen based on the above-median values and otherwise, respectively. *ICW* is an indicator variable with values 1 and 0 for breached firms that exhibited an ICW reported under SOX 302 in the year before the data breach and otherwise, respectively. The t-statistics (standard errors clustered by industries) are reported in parentheses. F-test is reported in the square brackets. ***, **, and * indicate the significance at the 1%, 5%, and 10% levels, respectively.

Table 7: Product Market Competition and Firm Diversification

Variables	**Product Market Fluidity**	**Diversification**
	Payable Days	**Payable Days**
*Data Breach*Post*	−17.72**	−16.30**
	(−2.18)	(−2.08)
*Low Fluidity*Data Breach*Post*	−6.798	
	(−0.42)	
*Focused Firms*Data Breach*Post*		−13.26
		(−0.72)
Controls	Yes	Yes
Firm FEs	Yes	Yes
Industry-by-Year FEs	Yes	Yes
Observations	63,127	63,127
Adjusted R^2	0.54	0.54
*Data Breach*Post + Low Fluidity*Data Breach*Post*	-24.52* [2.80]	
*Data Breach*Post + Focused Firms*Data Breach*Post*		-29.56* [3.12]

Note: This table presents the results of payable days after considering the roles of product market fluidity and firm diversification. *Data Breach* is an indicator variable with values 1 and 0 for data-hacking-breached firms and otherwise, respectively. *Post* is an indicator variable with values 1 and 0 for the years after the data breach and otherwise, respectively. *Low Fluidity* is an indicator variable with values 1 and 0 for breached firms that had below-the-median values for product market fluidity in the year before the data breach and otherwise, respectively. *Focused Firms* is an indicator variable with values 1 and 0 for breached firms that had only one business segment in the year before the data breach and otherwise, respectively. The t-statistics (standard errors clustered by industries) are reported in parentheses. F-test is reported in the square brackets. ***, **, and * indicate the significance at the 1%, 5%, and 10% levels, respectively.

Table 8: PSM Model

Panel A: Treatment V/S Control Firms

Variable	Treatment	Control	Difference	t-statistics
Firm Size	8.1049	7.9735	0.1314	0.34
ROA	0.1237	0.1139	0.0097	0.39
Leverage	0.2226	0.2212	0.0014	0.04
Cash Flow Volatility	222.40	168.91	53.49	0.75
PPE	0.2033	0.2231	−0.0197	−0.47
Altman's Z-Score	1.0748	1.8651	−0.7903	−1.54
M/B	2.0415	1.6842	0.3573	1.40

Panel B: Regression Results

Variables	Payable Days
*Data Breach*Post*	−15.08**
	(−2.11)
Controls	Yes
Firm FEs	Yes
Industry-by-Year FEs	Yes
Observations	1,137
Adjusted R^2	0.90

Note: This table presents the results for payable days after considering the PSM approach. The treatment firms (data-hacking-breached firms) are matched with the control group. Panel A reports the average firm-level differences between the treatment and control firms. Panel B reports the regression results of the matched samples. *Data Breach* is an indicator variable with values of 1 and 0 for data-hacking-breached firms and otherwise, respectively. *Post* is an indicator variable with values of 1 and 0 for the years after the data breach and otherwise, respectively. All the variables are defined in the appendix. The t-statistics (standard errors clustered by industries) are reported in parentheses. ***, **, and * indicate the significances at the 1%, 5%, and 10% levels, respectively.

Appendix A

Table A1: Variable Definitions

Variables	Definitions
Payable Days	Accounts payable divided by the cost of goods sold and multiplied by 360
Firm Size	The natural logarithm of the book value of total assets
Leverage	Total of short-term and long-term debt divided by the total assets
Cash Holdings	Cash and short-term investments divided by the total assets
Sales Growth	Growth rate of sales on year-on-year basis
M/B ratio	Market value of assets to the book value of total assets
ROA	Earnings before interest, tax, depreciation, and amortization divided by the total assets
Cash Flow	Operating cash flows divided by the total assets
R&D	Research and development expenditures divided by the total assets
PPE	Net property, plant, and equipment divided by the total assets
Firm Age	Number of years between data availability and the recorded year in the Compustat
Cash Flow Volatility	Standard deviation of operating cash flows during the past three years
Receivable Days	Trade receivables divided by sales and multiplied by 360
Analyst Coverage	Number of analysts following a particular firm
Forecast Dispersion	Standard deviation of analysts' earnings forecasts divided by the absolute values of mean earnings forecast
Institutional Ownership	Institutional ownership as a percentage of market capitalization
Internal Control Weakness	Indicator variable taking the value 1 for firms that had internal control weakness reported under SOX 302, and 0 otherwise
IT Expert	Indicator variable taking the value 1 for firms that had a chief information officer, or chief security officer, or any officer dedicated to information or security, and 0 otherwise
Market Fluidity	Measure of product market threats developed by Hoberg et al. (2014)

Note: This table provides definitions of variables employed in the paper.

Table A2: Non-Hack Data Breaches

Variables	Payable Days
*Non-Hack Data Breach*Post*	−16.04
	(−1.53)
Controls	Yes
Firm FEs	Yes
Industry-by-Year FEs	Yes
Observations	62,010
Adjusted R^2	0.54

Note: This table presents the results of the payable days after considering only non-hacking-based data breaches. *Non-Hack Data Breach* is an indicator variable with values of 1 and 0 for non-hacking-based breached firms and otherwise, respectively. *Post* is an indicator variable with values of 1 and 0 for the years after the non-hacking-based data breach and otherwise, respectively. The t-statistics (standard errors clustered by industries) are reported in parentheses. ***, **, and * indicate the significances at the 1%, 5%, and 10% levels, respectively.