

# Cybersecurity and merger outcomes

Yizhe Dong<sup>a\*</sup>, Haoyu Li<sup>b</sup>, Yue Liu<sup>a</sup>

<sup>a</sup> University of Edinburgh Business School, 29 Buccleuch Place, Edinburgh, EH8 9JS, UK

<sup>b</sup> Brunel Business School, Brunel University London, London, UB8 3PN, UK

05<sup>th</sup> Oct 2023

## Abstract

This paper explores the impact of target cybersecurity risk on merger outcomes. Using reported data breaches as a proxy for cybersecurity risk, we find strong evidence that the target data breach experience is negatively associated with the acquirer and combined entity announcement returns and long-run post-merger performance. We further show that the acquirer recognizes a greater goodwill impairment loss, takes longer to complete the transaction, and is more likely to experience a future data breach, when it purchases a data-breached firm. The value destruction effect is more pronounced in deals involving acquirers belonging to certain industries that are vulnerable to data breaches and have higher financial distress risk, but less pronounced in deals involving acquirers that hire top-tier due diligence advisors. We also find that acquirers' strategic considerations and prior data breach experience affect the probability of acquiring a data-breached target. Overall, the evidence indicates that cybersecurity risk reduces shareholder gains from mergers and acquisitions (M&As), which has important implications for policy and practice.

**Keywords:** Data breaches; Cybersecurity; Mergers and acquisitions; Performance.

**JEL classification:** G12 G14 G32 G34

---

\* Corresponding author. E-mail addresses: yizhe.dong@ed.ac.uk (Y. Dong), haoyu.li@brunel.ac.uk (H. Li), and Yue.Liu@ed.ac.uk (Y. Liu)

# Cybersecurity and merger outcomes

## Abstract

This paper explores the impact of target cybersecurity risk on merger outcomes. We find that the target data breach experience is negatively associated with the acquirer and combined entity announcement returns and long-run post-merger performance. We further show that the acquirer recognizes a greater goodwill impairment loss, takes longer to complete the transaction, and is more likely to experience a future data breach, when it purchases a data-breached firm. The value destruction effect is more pronounced in deals involving acquirers belonging to certain industries that are vulnerable to data breaches and have higher financial distress risk, but less pronounced in deals involving acquirers that hire top-tier due diligence advisors. We also find that acquirers' strategic considerations and prior data breach experience affect the probability of acquiring a data-breached target. Overall, the evidence indicates that cybersecurity risk reduces shareholder gains from M&As, which has important implications for policy and practice.

**Keywords:** Data breaches; Cybersecurity; Mergers and acquisitions; Performance.

**JEL classification:** G12 G14 G32 G34

## 1. Introduction

*“Surprisingly perhaps, many M&A practitioners have no clear sense of the overall magnitude of the risk they face from cyber attacks and data breaches.”*

- Financier Worldwide Magazine<sup>1</sup>

Over the past decade, the IT and cyber landscape has changed dramatically. Alongside remarkable technological advances that have boosted firm profits and created growth opportunities, there has also been a sharp increase in cybersecurity threats and incidents, resulting in substantial losses and some far-reaching consequences. As a result, cybersecurity risk has become a top concern for corporations, investors, and regulators. A global survey of CEOs conducted by PwC revealed that cybersecurity risk is ranked by CEOs as one of the top risks, even higher than health risks, macroeconomic volatility, climate change, and geopolitical conflict.<sup>2</sup> Many countries have realized the severity of the cybersecurity risk problem, and implemented numerous legislative and regulatory measures to address the issue. For example, in the U.S., the federal government, the Securities Exchange Commission (SEC), and the Federal Trade Commission (FTC) have promulgated several policies regarding cybersecurity issues<sup>3</sup>. In the European Union (EU), the General Data Protection Regulation (GDPR), enacted in 2018, includes detailed obligations and comprehensive guidelines for firms in the area of data protection and privacy. Accordingly, cybersecurity research, particularly on the economic effects of cybersecurity breaches, has also rapidly expanded.

Some previous studies have focused on the short-term economic impact of data breaches (e.g., Florackis et al., 2023; Foerderer and Schuetz, 2022; Jamilov et al., 2021; Malhotra and Malhotra, 2011). They generally report negative market reactions to firms' data breaches. Recently, more studies have documented the longer-term impacts of data breaches on firms' operations, performance, financial policy, and other strategies. For example, data breaches can increase the cost of capital of a firm (Huang and Wang, 2021; Florackis et al., 2023), reduce profitability and firm value (Ettredge et al., 2018), damage firms' reputations and customer trust and loyalty (Kshetri, 2018; Kamiya et al. 2021),

---

<sup>1</sup> “Cyber hygiene: identifying and defusing risks in M&A”, Cover story of Financier Worldwide Magazine, October 2021.

<sup>2</sup> 25th Annual Global CEO Survey – PwC: <https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2022.html>

<sup>3</sup> The legal acts and regulatory policies include “Statement and Guidance on Public Company Cybersecurity Disclosures”; “The Cybersecurity Information Sharing Act (CISA)”; “The Federal Information Security Modernization Act (FISMA)”; and “Section 5 of the FTC Act - Privacy and Security Enforcement”.

hamper firms' innovation and investment efficiency (He et al., 2020; Kamiya et al., 2021), and motivate firms to manipulate earnings (Xu et al., 2019).

A recent global survey by Forescout Technologies highlights the important role cybersecurity plays during mergers and acquisitions (M&As), one of the most important strategic business decisions. In the survey, 62% of respondents expressed that cybersecurity risk was their biggest post-M&A concern, and 81% of respondents indicated that organizations were placing more focus on a target's cybersecurity during an M&A deal than in the past.<sup>4</sup> Some anecdotal evidence also suggests that cybersecurity concerns are an important source of risk for M&A transactions and can cause huge losses if the parties concerned are not diligent in identifying, quantifying, and patching cybersecurity deficiencies before and after a deal. For example, FedEx acquired Bongo International in 2014 to enhance its portfolio of e-commerce businesses. It inherited Bongo's server and a problem arose years later. In 2018, FedEx confirmed that its inherited customer information had been exposed to a data breach, which highlights that cyber vulnerabilities can be inherited through transactions and destroy post-merger firm value. The 2017 acquisition of Yahoo by Verizon Communications Inc also exemplifies this concern. After Verizon discovered that Yahoo had experienced massive data breaches, it reduced the purchase price by \$350 million to reflect the economic damage and integration challenges caused by the data breaches.

Despite the growing importance of cybersecurity risk in firm decision making and performance, and ample anecdotal evidence of cybersecurity concerns in the context of M&As, there has been little empirical evidence in the literature as to whether cybersecurity risk is an important determinant of M&A success. Thus, in this paper, we seek to fill this void. Specifically, we mainly address the following questions: Does the target's data breach experience affect merger performance? If it does, through what potential channels does it influence the acquisition announcement returns? What are the possible motivations for an acquirer in buying a data-breached firm? Is the target's data breach a significant determinant of the forming of a merger pair between firms?

We conjecture that targets' past cybersecurity weaknesses (i.e., having experienced a data breach) are negatively related to post-merger performance. An important rationale for this prediction is that

---

<sup>4</sup> Forescout surveyed 2,700 IT decision makers and business decision makers to provide a better understanding of cybersecurity risk in the M&A lifecycle. See "The Role of Cybersecurity in M&A Diligence" at <https://www.forescout.com/merger-and-acquisition-cybersecurity-report/> for more details.

acquiring a firm with a poor cybersecurity posture may lead to more post-merger integration challenges being experienced, which will destroy the deal value and shareholder wealth. A data breach indicates a weakness in the information system and a lack of a strong cybersecurity culture (Huang and Wang, 2021). Acquiring a data-breached firm can result in cultural clashes and difficulties in integrating the information systems from the two firms, thereby potentially exposing the acquiring firm to cyber attacks and data breaches itself. Remediating the cybersecurity issues of the target firm can be a time-consuming and expensive process. The acquiring firm may have to invest in new technology, retrain employees, and perform extensive testing to ensure that the merged firms' systems are secure. This can result in higher integration costs and slower integration timelines. Data breaches can also lead to significant financial and legal costs, reputation damage, and stricter regulatory scrutiny, which have long-term implications for a firm's financial performance, competitiveness, and ability to innovate (He et al., 2020). These long-lasting impacts could undermine the realization of the synergies and growth opportunities that were anticipated to be gained from the deal, and tarnish investor confidence, resulting in a negative market reaction to the deal and poor post-merger performance.

To test our hypothesis, we use a large sample of 8,146 U.S. domestic acquisitions announced by public firms over 2006-2020. We construct three measures of a target's material cybersecurity risk based on reported data breach incidents<sup>5</sup>: (1) a dummy variable for whether the target had experienced a data breach before the M&A announcement; (2) the number of data breaches the target had previously experienced; (3) the total number of records exposed in the target's previous data breaches. Consistent with our predictions, we find that the target's data breach experience is negatively associated with the acquirer's announcement returns. This effect is statistically and economically significant for all three data breach measures. In economic terms, acquiring a data-breached target decreases the acquirer's five-day cumulative abnormal returns (CARs) by 1.4%. We also find a significant adverse impact of target data breaches on both the merger synergy (i.e. combined acquirer and target announcement returns) and the acquirer's post-merger operating performance (i.e. changes in the one-, two-, and three-year post-merger return on assets (ROA)). The evidence suggests that

---

<sup>5</sup> Data breach incidents are among the most costly and frequent types of cybersecurity incidents (Aldasoro et al., 2022) and widely used to measure firms' cybersecurity risk in the finance and information systems literature (e.g. He et al., 2020; Garg, 2020; Chen et al., 2022; Wang and Ngai, 2022).

targets' cybersecurity risk could be an important risk factor in M&A transactions, one that could lead to an unfavourable market reaction and poor performance during post-merger integration.

A potential concern in the interpretation of the results is that the data-breached targets are not randomly selected. Thus, our study employs two tests to address such potential endogeneity concerns. Specifically, we apply both propensity score matching (PSM) and entropy balancing to address the selection bias associated with certain observable firm and deal characteristics. Consistent with the baseline results, the estimation results based on the matched samples reveal a statistically significant and negative relation between the target data breaches and acquirer CARs. In addition, we use a quasi-experiment identification strategy based on a staggered difference-in-differences method to investigate whether the effect of target data breaches on the announcement returns is reinforced by the introduction of data breach notification laws that require affected firms to compulsorily notify their main stakeholders of any data breach. We find that the acquisition of a breached firm produces significantly lower announcement returns after the enactment of the notification laws. Overall, our results depict a causal relation between the targets' data breach incidents and acquirers' shareholder wealth losses.

We next explore several potential channels through which (or reasons why) targets' data breach experiences may reduce the value for acquirers. First, we use the acquirer goodwill write-off as a proxy for the shortfall in synergy generation and find a positive association between the goodwill impairment of the acquiring firm and the target's data breach. It indicates that a target's high cybersecurity risk could impede the materialization of the expected synergies during the post-acquisition period. Second, we find that an acquirer is more likely to experience a data breach after it purchases a data-breached firm, suggesting that the target's cybersecurity risk can be transferred into the system of the acquirer during the post-merger integration. Finally, we find that the time to completion between the M&A's initial announcement and the completion date is significantly longer in deals with data-breached targets, which could reflect the complexity and difficulty of these merger integrations.

In addition, we identify three conditions under which target data breaches are likely to inflict more harm on merger performance. Specifically, we find that the value destruction caused by acquiring a data-breached firm is more pronounced when the acquirer belongs to an industry vulnerable to cyber attacks, has higher financial distress risk, and does not hire the Big 4 due diligence advisors. Furthermore, we document that the impact of a target's data breach on merger performance also depends on the type and the elapsed time of the data breach incident.

This study documents that targets that have experienced data breaches can destroy acquirers' shareholder value. If the acquisitions do not create value for the acquirers, then why do they initiate such deals and what do they intend to achieve with this M&A activity? To answer these questions, we further examine the effects of targets' data breach experience on merger decisions. In logit regressions based on a sample of merging and matched non-merging firm pairs, we find that the likelihood of a merger is not significantly associated with the target's data breach experience. This result implies that the target's cybersecurity risk may not be seriously considered, and the devastating effects of a breach may be underestimated when acquirers make merger decisions. Although it seems that the target's cybersecurity risk is not a key determining factor in merger occurrence, we find that acquisitions are more likely to take place between two firms that have both experienced data breaches but operated at different levels within an industry's supply chain (i.e., vertical mergers). The evidence suggests that similar prior experiences and strategic considerations may motivate the acquirers to buy data-breached firms.

Our study makes several important contributions. First, this paper expands our knowledge of the role of cybersecurity in corporate strategic decision making and performance (see, e.g., survey by Walton et al., 2021). Several recent studies focus on how data breaches affect firms' financial policies (Garg, 2020; Boasiako and Keefe, 2021; Huang and Wang, 2021), governance (Lending et al., 2018; Banker and Feng, 2019; Ashraf, 2022), risk management (Kamiya et al., 2021), innovation (He et al., 2020), earnings management (Xu et al., 2019), equity value and financial performance (Tosun, 2021; Foerderer and Schuetz, 2022). To the best of our knowledge, our study is among the first in the literature to explore the role of cybersecurity risk in the context of M&As, and reveals that targets' data breach experiences significantly impact M&A decision making and performance.

Our findings also contribute to the information systems (IS) literature on information and cybersecurity. Previous IS research focuses on some organizational and environmental factors that influence the likelihood of data breaches, such as firms' location and industry affiliation (Sen and Borle, 2015), IT security investments (Angst et al., 2017), firms' social performance (D'Arcy et al., 2020), supply chain network features (Hu et al., 2022), and cybercrime regulation and information security enforcement (Png et al. 2008; Hui et al., 2017). We add to this literature by showing that data breach risk can spill over from the target to the buyer after an acquisition and suggesting that a firm's external growth strategy can influence its cybersecurity risk.

Furthermore, we offer insight on the role of financial intermediaries (e.g., advisors) in M&As. Several studies have investigated the value effect of financial advisors in M&As, with a particular focus on their informational role (e.g., Allen et al., 2004; Kisgen et al., 2009; Golubov et al., 2012; Chang et al., 2016). Our study highlights the role of due diligence advisors in deals with cybersecurity concerns. We reveal that hiring due diligence advisors can significantly mitigate the negative effect of a target's data breach risk on merger performance.

The rest of the paper proceeds as follows. Section 2 reviews the related literature and develops our hypothesis. Section 3 describes the data, the sample, and the research method. Section 4 presents and discusses the main results. Section 5 provides additional analyses. Finally, section 6 concludes.

## **2. Literature and Hypothesis Development**

### **2.1 The consequences of cybersecurity breaches**

Prior literature has highlighted that data breaches have a significant impact on firms from many perspectives (see Richardson et al., 2019; Walton et al., 2021; Crosignani et al., 2023). Similarly to other operational loss events, data breaches can cause financial losses for firms. Data breaches can result in significant direct costs, including payments for investigations of breaches, system remediation costs, costs of the compromised confidentiality of customers' personal information, legal fees and fines, and penalties from regulatory bodies (see, e.g., Campbell et al., 2003; Romanosky et al., 2014; Furnell et al., 2020).

Besides the direct costs, firms could also suffer from indirect consequences of experiencing a data breach. Such incidents can change the perceptions of stakeholders including investors, customers, debt holders, and employees, regarding a firm. Investors may view a data breach as a sign of poor management and a lack of focus on security. Prior research generally finds a negative market reaction to data breach incidents (e.g., Amir et al., 2018; Li et al., 2020; Kamiya et al., 2021; Tosun, 2021). In particular, Avery (2021), Malhotra and Malhotra (2011), and Gordon et al. (2011) document that shareholders suffer significant wealth decreases over a short (1-3 days) as well as long (up to a few years) time window following a data breach disclosure. Some of those studies also find that the announcement time and type of a data breach can affect the market reaction (e.g., Foerderer and Schuetz, 2022; Martin et al., 2017). Another major impact of a data breach is reputational damage to

a firm, which leads to a loss of customer trust and confidence, and can take years to rebuild. Customers are likely to choose to purchase less or even stop purchasing from affected firms (Janakiraman et al., 2018; Huang and Wang, 2021). Kamiya et al. (2021) provide clear evidence that data-breached firms suffer significant reputational losses, measured by the excess of shareholder wealth losses over the out-of-pocket costs and sales growth, respectively. Makridis (2021) also finds firms experience a 5-9% decline in reputational intangible capital following large-scale data breaches. Moreover, banks are likely to perceive firms that have experienced a data breach as having higher default and information risks than non-breached firms. Huang and Wang (2021) use a propensity score matching with difference-in-differences (PSM-DID) approach to show that data breaches lead to greater increases in loan spreads, collateral required, and loan covenants for breached than non-breached firms.

Several recent studies document that cybersecurity breaches can also influence corporate financial and strategic decision making. He et al. (2020) show that firms' R&D spending, patents, and investment efficiency decrease significantly in the years following a data breach, suggesting that cybersecurity risk significantly impacts firms' future innovation strategies and investment decisions. Garg (2020) finds that firms significantly increase their cash holdings following a data breach. He further shows that the effect of a data breach can go beyond the firm that was attacked, with peer firms also raising their cash holdings as a precaution. Similarly, Ashraf (2022) provides empirical evidence of the role of peer data breach incidents on corporate governance, and shows that non-breached firms do take real actions to strengthen their internal controls so as to mitigate exposure to cybersecurity risk. Xu et al. (2019) investigate how data breaches impact corporate financial reporting. They show that data-breached firms are more likely to use real earnings management to manipulate earnings, which leads to worsened subsequent financial performance. Although the extant literature has identified a number of impacts of data breaches on firms, there is as yet a very limited understanding of the role cybersecurity risk plays, and its impact, in the context of M&As. Thus, we attempt to fill this gap in this paper.

## 2.2 Hypothesis development

Based on the above discussion on the potential consequences of a data breach, we expect that acquiring a target that has experienced a data breach has a negative effect on M&A outcomes, for the following four reasons. First, integrating the IT and data operating systems of two firms after a merger

or acquisition can be challenging, with employee, customer, and third-party data (Kamiya et al., 2021) usually needing to be fully or partially transferred from the target to the acquiring firm. The integration can be even more difficult and complex if the target has a poor information security posture and high cybersecurity risk. This can delay the integration process and increase IT and IS integration costs, which in turn decreases the value of the deal and any synergy gains.

Second, previous studies have documented the spillover effect of cybersecurity breaches (e.g., Wang, 2019; Walton et al., 2021; Islam et al., 2022). Thus, the target's cybersecurity risk is also likely to spill over onto the system of the acquiring firm if integration occurs and increases the likelihood of a data breach for the acquirer. Additionally, M&A activity brings major organizational changes to merging firms and a high chance of human and technology errors. Thus, an M&A, particularly when the deal involves a data-breached target, may provide fertile ground for cybercriminals. These effects are also confirmed by a North-American-based survey of 30 senior executives at corporate and PE firms.<sup>6</sup> The report shows that 40% of respondents said they encounter data security problems after an M&A transaction (Curran et al., 2016). Increased cyber risks and threats can lead to a loss of customer and employee trust and loyalty (Huang and Wang, 2021; Janakiraman et al., 2018), with negative impacts on the firm's revenue and employee productivity after the acquisition. Moreover, given the increased cybersecurity risk, the combined firm is likely to require more cyber insurance within its risk management practices (Florackis et al., 2023) and face higher insurance premiums, increasing its operating expenses. In addition, banks perceive breached firms as having higher credit and information risks, and therefore tend to offer less favourable loan terms (Huang and Wang, 2021). Those risks can also be transferred to the acquirers, with banks adjusting their loan terms to reflect the increased risks caused by the acquisition. Thus, debt financing costs, either for the transaction itself or for post-merger operations, are expected to increase when a firm acquires a data-breached firm. Similarly, external auditors view breached firms as likely to have higher financial reporting risk and to be more likely to engage in real earnings management, therefore requiring greater audit assessment efforts (Yen, et al., 2018; Xu, et al., 2019; Li et al., 2020). Thus, when an acquirer purchases a breached target, it may face increased audit fees. All these effects can reduce the potential synergies and cost savings of a merger.

---

<sup>6</sup> The survey was conducted by West Monroe Partners and Mergermarket in 2016.

Third, when an acquisition is made, the acquirer inherits not only the tangible assets of the target but also the intangibles (e.g. corporate reputation). The intangible assets of the target could be an important source for shareholder value creation in an acquisition (Masulis, et al., 2023). One of the most significant negative impacts of a data breach is that it can seriously damage a firm's reputation (Kamiya et al., 2021; Tosun, 2021). Acquiring a target with reputational concerns could tarnish the acquirer's reputation and public image (Fong et al., 2013). In such a case, investors, customers, and employees may raise concerns about the acquirer's post-merger reputation, in turn reducing the confidence of the capital markets regarding the future growth and success of the target and the merged entity.

Fourth, a data breach can result in significant legal consequences and regulatory penalties. Any unresolved legal issues are transferred to the acquirer when it buys a data-breached firm. The combined firm may face legal action from customers or other parties whose information was exposed during the target's data breach, which can increase the legal liabilities and costs of the combined firm and negatively impact its financial performance and growth. Additionally, after a data breach, a firm may attract regulatory attention. Thus, an M&A transaction involving a data-breached target may face more regulatory scrutiny, which can slow down the merger process and increase the associated risks and costs. With the above all taken together, we expect that the target's experience of a data breach is an important risk factor in an M&A transaction and formalize the above discussion with the following testable hypothesis:

***Hypothesis:*** *Acquiring a target that has experienced a data breach negatively affects merger performance.*

### **3. Data and Method**

#### **3.1 Sample**

Our sample of acquisitions is collected from the Thomson SDC database. We start with all completed domestic acquisitions in the United States from 2006 to 2020. 2006 is chosen as the start year because data breach information is available from 2005 and we need to have at least one year of data breach information prior to the mergers. Following the M&A literature, we apply several screening criteria to construct our sample. Specifically, we require that the deal value should be more

than one million dollars. The acquirer should be a public firm and the target either public, private, or a subsidiary firm. The acquirer should own less than 50% of the target's shares before the deal, and 100% after the deal. Our sample excludes privatizations, acquisitions of remaining interest, repurchases, exchange offers, self-tenders, recapitalizations, spinoffs, tender offers, and leveraged buyouts.

Our data breach measures are constructed using data breach information collected from Privacy Rights Clearinghouse. This database provides rich information on publicly known U.S. data breach events, including the event time, company name, location, number of records lost in the data breach, and the type of breach. To match the data breach events with our sample of acquisitions, we manually compare the names and locations of companies in our sample of acquisitions with those in Privacy Rights Clearinghouse. We also use the linking table provided by Rosati and Lynn (2021) to supplement the matched samples. Our final sample covers a total of 8,146 completed domestic acquisitions conducted by firms in the United States.

In further analysis, we also categorize data breach events into the following types based on how the information was exposed: *Bank card fraud* (fraud involving debit and credit cards, not carried out via hacking, such as skimming devices at point-of-service terminals); *Hack* (hacked by an outside party or infected by malware); *Stakeholder* (data breach caused by contractor or customer); *Lost* (physical loss of paper documents, portable devices, or stationary computers); and *Unknown* (reason for data breach unknown).

### 3.2 Empirical model

To examine the impact of the data breach experience on acquisition performance, we use the following baseline model, specified at the deal level:

$$CAR_{i,t} = \alpha_{i,t} + \beta \times Data\ breach_i + \lambda \times Firm_{level}\ Control_{i,t-1} + \mu \times Deal_{level}\ Control_{i,t-1} + Year\ FE + Industry\ FE + \varepsilon_{i,t}$$

The dependent variable is the acquirer's five-day cumulated abnormal return,  $CAR[-2, +2]$ , around the announcement of the acquisition. We use the capital asset pricing model to estimate the expected return, where the estimation window is  $[-241, -40]$  trading days, and the CRSP value-weighted index return is used as the proxy for the market return. We require the firm to have at least 100 active trading days in the estimation window. Moreover, we also use the market-value-weighted average  $CAR[-2, +2]$  of

the acquirer and the target as the measure of the synergies generated by the transaction. The weight is based on the acquirer's and the target's market value eleven days prior to the acquisition announcement (Masulis et al., 2007).

*Data breach* denotes our measure of the incidence of data breach events. In our study, we use the incidence of data breach events as an ex-post proxy for cyber security risk, following Hinz et al. (2015) and Kamiya et al. (2021). Specifically, we create three variables to measure the incidence of data breach events. The first measure, *If breach*, is a dummy variable which equals one if the firm experienced a publicly known data breach, between the start of the recording of such breaches in the database and the year before the acquisition, and zero otherwise. It measures the occurrence of data breaches. Some studies also suggest that the frequency and severity of data breaches can significantly affect the magnitude of the market response (e.g., Rosati et al., 2017). Therefore, we further construct the following two proxies to measure the frequency and severity of data breaches. *Count breach* is defined as the natural logarithm of one plus the number of documented data breach events up until the year before the acquisition. *Amount breach* is defined as the natural logarithm of one plus the number of records exposed in documented data breach events up until the year before the acquisition.

We also control for a set of firm characteristics that are revealed by literature to affect acquisition performance. *Acq. Ln Assets* is a measure of the acquirer's size, defined as the natural logarithm of the total assets of the acquiring firm. This variable is used to control for the size effect, as some studies suggest that the announcement returns for small acquirers are higher than those for large acquirers (e.g., Moeller et al., 2004; 2005). *Acq. Tobin's q* is included to control for the effect of the acquirer's growth opportunities on acquisition performance (Lang et al., 1991). It is defined as the market to book value of the acquirer's total assets. Prior studies also suggest that the availability of abundant free cash flows in a firm may encourage managers' empire building and lead them to conduct value-destructive acquisitions (Jensen, 1986). Consequently, the market tends to react negatively to such deals (Lang et al., 1991). Similarly, high leverage could force managers to consider an acquisition opportunity more carefully before making the final decision, resulting in a positive association between the acquirer's leverage and acquisition performance (Maloney et al., 1993). Hence, we control for the free cash flows (*Acq. Free cash flow*) and leverage (*Acq. Leverage*) of the acquirer. Information leakage during the pre-announcement period is another factor that could potentially affect deal performance. Thus, we follow John et al. (2015) to construct another control variable, *Acq. Stock price runoff*.

Furthermore, prior studies suggest that acquisition performance could be associated with some deal characteristics, such as payment method (e.g., Travlos, 1987; Chang, 1998; Moeller et al., 2004; Officer, et al., 2009), relative size of the transaction (e.g., Asquith et al., 1983; Alexandridis et al., 2013), industry (e.g., Kohers and Kohers, 2000; Cloudt et al., 2006), public status (e.g., Fuller et al., 2002; Faccio et al., 2006), and whether an acquisition is a diversifying deal (e.g., Amihud and Lev, 1981; Shleifer and Vishny, 1989; Morck et al., 1990). Therefore, we also include these deal characteristics in our regression models. In our study, we classify the targets into public firms, private firms, and subsidiaries of public firms. We control for *Public target* and *Private target*, which are two dummy variables that equal 1 if the target firm is a public or target firm, respectively. In the appendix we present details of all variables. Our model also includes year fixed effects and industry (2-digit SIC) fixed effects.

### 3.3 Descriptive statistics

Our sample of acquisitions is mostly evenly distributed over the years, although 2009 and 2020 experienced troughs due to the financial crisis and pandemic, respectively. The frequency of acquisitions by announcement year is presented in Table 1. Columns (1) and (2) show the deals in the full sample, while Columns (3) and (4), and Columns (5) and (6) present the subsets of deals with and without data-breached targets, respectively. The majority of targets had no data breach incidents before the acquisition (95.48%). Column (4) shows a time trend, with deals involving data-breached targets accounting for larger shares in more recent years than in the early stages of the sample period. Specifically, the percentage of target firms experiencing data breaches increased from 1.53% in 2006 to 6.51% in 2019. The increasing percentage of data-breached targets may be attributable to the soaring amount of data collected, disclosed, and used by firms. Lattanzio and Taillard (2022) also point out that the introduction of cybersecurity-related disclosure guidance by the SEC in 2011 led to a rapid increase in the amount of public information on cybersecurity.

[Insert Table 1 here]

The industry distribution of the acquisitions (based on the acquirers' Fama-French 12 industries) is presented in Table 2. As shown in Column (1), the finance industry (31.73%) and the business

equipment industry (17.47%) contribute nearly half of the U.S. domestic acquisitions. We then split the full sample into groups with (Columns (3) and (4)) and without (Columns (5) and (6)) data-breached targets. Column (4) shows a great variance in the likelihood of acquiring a data-breached target across industries. 10.74% of acquirers in the telecommunication industry buy data-breached targets, while only 1.35% of acquirers do so in the chemical products industry. The “data intensity” trait of telecommunication, finance, and retail businesses may help to explain those industries’ higher-than-average percentages of data-breached targets. That result is also consistent with prior studies reporting that the telecommunication, finance, wholesale, and retail industries are among those most vulnerable to cyber attacks (e.g., Romanosky, 2016; Kamiya et al., 2021).

[Insert Table 2 here]

Table 3 presents the descriptive statistics for the full sample in Columns (1) and (2) and for the subsamples with and without data-breached targets in Columns (3) and (4), and Columns (5) and (6), respectively. All continuous variables are winsorized at the 1st and 99th percentiles. The table shows that around 4.5% of U.S. domestic acquisitions involve data-breached targets. The targets on average experienced 0.129 data breach incidents, with 96,600 exposed records, before the acquisitions. Around 5.8% of acquirers in our sample have experienced a data breach incident, slightly higher than the percentage of targets. In the data-breached subsample, the targets have on average suffered 2.85 data breach incidents, with 2.8 million leaked records, before the acquisitions.

The results in Column (7) suggest that many acquirer and deal characteristics differ statistically between the two subsamples. For example, for deals with data-breached targets, 18.9% of the acquirers have also experienced data breaches, while in the deals without, only 5.18% of the acquirers have experienced such incidents. This result implies that two firms are more likely to combine if both of them have experienced data breaches. Additionally, we observe that, for the data-breached sample, on average, the acquirers have made 0.485 acquisitions in the prior five years that involved a data-breached target, while this figure is only 0.101 for the non-data-breached sample. This result suggests that those firms that acquire data-breached targets usually have more previous experience in acquisitions involving data-breached targets.

[Insert Table 3 here]

The statistics for the acquirer characteristics show that, on average, the total assets of the acquirers in our sample are \$8,907 million, with a *Tobin's q* of 1.808, *Leverage* of 19.7%, and *Free cash flow* of 2.3%. The market reaction to the acquirer's stock prior to the acquisition announcement [-210, -11] is 5.2%. The average write-off goodwill of the acquirer in the year after the acquisition is \$0.26 million. In terms of synergy and target wealth, on average, the acquisitions in our sample create 2.47% synergy for the shareholders of the acquirers and targets. The mean value of *Premium* is 33.688%, which is in line with Eckbo (2009). Regarding deal characteristics, we notice that 14.7% (54.7%) of targets are public (private) firms. Diversifying deals count for 29.9% of deals, and 30.6% (6.2%) of deals are completed with a 100% cash (stock) payment. The transaction value accounts for approximately 22.5% of the acquirer's market value, on average, and 2.4% of acquirers in our sample hire Big 4 due diligence advisors.

### 3.4 Univariate analysis

We conduct a univariate analysis to compare acquirer performance for the full sample and subsamples based on whether or not the deal involves a data-breached target. The comparisons of *Acquirer CAR*, *Acquirer  $\Delta ROA$* , and *Acquirer  $\Delta Count breach$*  are presented in Table 4. The results show that both the mean and the median of *Acquirer CAR* for the full sample are positive. The values of *CAR*[-2, +2] over the 5-day event window, for the deals with data-breached targets, are significantly lower than those for the deals without data-breached targets. This result is consistent with our hypothesis that the market reacts less favourably to deals involving data-breached targets than to those not involving data-breached targets. We also find that *Acquirer  $\Delta Count breach$*  (i.e. the change in the number of acquirer data breach incidents between one (two, or three) year(s) prior to the deal announcement and one (two, or three) year(s) after deal completion) is significantly higher in the subsample of deals with data-breached targets than in the subsample of deals without data-breached targets. Specifically, the mean changes are 0.133 (from one year prior to one year after), 0.264 (from two years prior to two years after), and 0.302 (from three years prior to three years after), respectively, for the deals involving data-breached targets, while the respective mean changes are only 0, 0.001, and 0.007 for the deals not involving data-breached targets. These results indicate that merging with a data-breached target can increase the acquirer's data breach risk. Finally, we take the change in the ROA

as a measure of the operating performance of the merged firm. Again, we compare one (two, or three) year(s) pre-merger to one (two, or three) year(s) post-merger. We find that the mean values of  $\Delta ROA$  are more negative for the deals with data-breached targets than for those without data-breached targets.

[Insert Table 4 here]

## 4. Empirical Results

### 4.1 Acquirer announcement returns

To examine the effect of target cybersecurity risk on acquirer announcement performance, we run regressions of acquirer CAR on target data breach measures. The dependent variable is *Acquirer CAR*[-2, +2]. The main explanatory variables are the three data breach variables discussed previously: *Tar. If breach*, *Tar. Count breach*, and *Tar. Amount breach*. The baseline results are presented in Table 5. We report negative coefficients on all three measures of targets' data breaches, and the significance levels are 5% for *Tar. If breach* and *Tar. Count breach*, and 10% for *Tar. Amount breach*. The effect of a target's data breaches on an acquirer's short-term performance is also economically meaningful. For instance, all else being equal, the presence of the data-breached target reduces the five-day CAR of the acquirer by 1.4%, and a 10% increase in the number of data-breach events is associated with a 0.1% reduction in the five-day CAR of the acquirer (representing 7.5% of the mean value of *Acquirer CAR*[-2, +2]). In addition, considering that the between-group comparisons may not fully account for the unobserved differences between data-breached and non-breached target firms, we thus run a further regression analysis based on the subsample of data-breached target firms only. The last column of Table 5 reports the results. The coefficient on *Tar. Count breach* is significantly negative and its magnitude is much larger than that of the full sample. This further supports the findings from the full sample.

[Insert Table 5 here]

These results support our hypothesis that a target's data breach experience has a significant negative impact on the acquirer's announcement performance. This evidence reflects investors' concerns over the cybersecurity risk in target firms, given that intense data migration, sharing, and integration activities occur during and after an acquisition transaction (Kamiya et al., 2021; Lattanzio

and Ma, 2021). This process is particularly challenging when the target firm has high cybersecurity risk and could potentially decrease the value of any synergies involved in the deal. Investors' concerns can also result from the possibility of the target's cybersecurity risk spilling over onto the acquirer during the transaction or after the integration (Wang, 2019; Walton et al., 2021; Islam et al., 2022). Another important factor that could potentially lead to a negative market reaction is the reputational loss to the acquiring firm and additional legal costs or regulatory scrutiny it might face after buying a target that has experienced data breach incidents in the past.

#### 4.2 Propensity score matching (PSM) and entropy balancing

When examining the effect of data-breached targets on acquisition performance, the possibility that targets' data breach incidents are not randomly distributed but endogenously determined by certain firm and deal characteristics should be considered. Hence, it is important to test whether the effect on announcement returns still exists after controlling for differences in those characteristics. Therefore, in this section, we employ both the PSM and entropy balancing techniques to address the misspecification concerns and mitigate the selection bias.

To obtain the PSM control sample, we estimate a logit regression that includes 16 variables that potentially affect the likelihood of the presence of data-breached targets in M&As<sup>7</sup>. We use one-to-five nearest-neighbour matching (caliper=0.05, with replacement) based on the propensity score to match the sample deals with data-breached targets, resulting in a matched sample containing 1,144 M&As.<sup>8</sup> After we have built our matched sample, we proceed with OLS regressions using the new sample. The results based on the PSM sample are reported in Panels A and B of Table 6. Panel A of Table 6 presents the descriptive statistics for the PSM subsamples. It shows that the mean acquirer announcement return (*Acquirer CAR*[-2, +2]) is significantly higher in the subsample of deals that do not involve data-breached targets than in the subsample with data-breached targets. In addition, we find that the explanatory variables do not differ significantly between the treatment and control

---

<sup>7</sup> In addition to the variables used in our baseline model, we include four variables to more comprehensively capture observable firm and deal characteristics, *Horizontal*, *Vertical*, *Acq. If breach*, and *No. Acq. previous DB deals*, whose definitions are provided in the appendix.

<sup>8</sup> Our results are robust to different PSM specifications (e.g., calipers of 0.01 and 0.03, and ratios of 1:1 and 1:3).

samples after matching. The results of the regressions of *Acquirer CAR*[-2, +2] on the data breach variables are reported in Panel B of Table 6. The coefficients on all three measures of target data breaches (i.e. *Tar. If breach*, *Tar. Count breach* and *Tar. Amount breach*), in line with our baseline result, are negative and statistically significant to at least the 10% level.

In addition, to further improve the covariate balance between the treated and control samples, we employ the entropy balancing method to assemble a further matched sample. These results are reported in Panel C of Table 6. We find that both the sign and the significance of the coefficients on the target data breach variables are similar to those reported for the PSM analysis, except that the coefficient on *Tar. Ln Amount breach* is insignificantly different from zero. All the above findings alleviate the misspecification concerns and selection bias, to some extent it suggests that the endogeneity problem may not be a major concern in our analysis. The negative impact of the target's data breach experience on the acquirer's announcement performance is still statistically significant, even after controlling for differences in firm and deal characteristics using the PSM and entropy balancing matching methods.

[Insert Table 6 here]

#### 4.3 Staggered difference-in-differences

We further address the potential problems resulting from omitted variables, simultaneity, or measurement error, in our research context. For instance, there could be endogeneity issues that can lead to both more target data breach experiences and poor acquisition performance. To ameliorate this concern, we employ a staggered DID analysis based on the introduction of data breach notification laws, as an identification strategy. In the United States, Security Breach Notification Laws require all persons or entities in the 50 states and the District of Columbia to notify any resident whose personal information is involved in a data breach. The introduction of such laws can increase the disclosure of data breaches and additional costs associated with the incidents. As the laws were introduced at different points in time in different states, this provides an ideal setting for conducting a quasi-experimental evaluation of the effect of targets' data breach experience on M&A performance (Huang and Wang, 2021). The dates when the notification laws were introduced in each state are presented in Panel A of Table 7. The regression results showing the effects of the enactment of the data breach notification laws are presented in Panel B of Table 7. The dependent variable is still *Acquirer CAR*[-2, +2]. *Post* is a dummy variable which equals one if the acquisition announcement

date is after the enactment date in the state in which the target firm is incorporated, and otherwise zero. We report negative coefficients on the interaction terms between *Tar. If breach* and *Post*, and between *Tar. Count breach* and *Post*. They are significant at the 5% level. The results indicate that, after the enactment of the notification laws, the market reacts more negatively to the announcement of the acquisition of a data-breached target, which provides additional evidence in support of our baseline findings.

[Insert Table 7 here]

#### 4.4 Merger synergy

Previously, we have mainly focused on the wealth effect of M&As on the acquirer's shareholders and have found lower acquirer announcement returns on deals involving data-breached targets. In this section, we attempt to show whether the losses to the acquirer's shareholders are mainly caused by wealth transfers or by decreased shareholder synergies from the deal as a whole. To do so, we further examine the effect of the target's data breach experience on the overall shareholder synergies from the M&A. The overall synergies are measured by the market-value-weighted average of the acquirer's and the target's five-day cumulative abnormal returns around the acquisition announcement (i.e. *Combined CAR*[-2, +2]). The results are presented in Table 8. Across all specifications, the target data breach variables are consistently negative and significant to at least the 10% level. For example, a 10% increase in the number of target data breach incidents reduces the CAR of the combined entity by 0.26%, a reduction of 11% given the mean five-day combined CAR of 2.47%. The results suggest that acquiring a data-breached target results in a reduced synergy gain from the deal. Overall, the results in Table 8 are consistent with the arguments in section 2 that acquiring a firm with high cybersecurity risk can significantly decrease the value of any synergies gained through the acquisition.

[Insert Table 8 here]

#### 4.5 Post-merger operating performance

The negative announcement returns suggest that acquiring a data-breached target raises investors' concerns and leads to an unfavourable market reaction. It is possible, though, that the investors do not fully understand the value of the acquisition when it is announced, and the negative effect is temporary.

Thus, we extend our analysis to test whether the target's data breach experience influences the post-merger operating performance of the acquirer. Following Cai and Sevilir (2012) and Dong et al. (2021), the operating performance is measured by the change in the acquirer's industry-adjusted (2-digit SIC) ROA between the years prior to the merger and those subsequent to it. This could help us to understand whether the expected synergies are realized in the post-merger period. We argued in section 2 that the acquirer may face greater challenges integrating IT systems, more regulatory scrutiny, and increased legal costs after acquiring a data-breached target. Thus, we expect that, all else equal, deals with low-cyber-risk targets (i.e. non-data-breached targets) should experience better post-merger operating performance than those with high-cyber-risk targets (i.e. data-breached targets).

Table 9 presents the results from the regressions of the operational performance of the acquirer on the target's data breach experience. The dependent variable is *Acquirer  $\Delta$ ROA*, the change in the operating performance of the acquirer. It is calculated as the change in the industry-adjusted (2-digit SIC) ROA of the acquirer from one (two, or three) year(s) prior to the deal announcement to one (two, or three) year(s) after deal completion. We report significant negative coefficients on all three measures of the target's data breaches, over three different time horizons, suggesting that the target's cybersecurity risk can impair the acquirer's operating performance and impede the generation of synergies in the post-merger period. Taking the first two columns of Table 9 as an example, the results show that the presence of the data-breached target decreases the change in the acquirer's ROA from one year before the acquisition to one year afterwards by 1.1%; meanwhile, a 10% increase in the number of data breach events is associated with a 0.09% reduction in the change in the acquirer's ROA from one year before the acquisition to year afterwards, on average, indicating a 17% deterioration. We also notice that the coefficients on *Tar. If breach* and *Tar. Ln Count breach* are more negative and statistically significant for the shorter pre-/post- time window than for the longer one. For instance, when changing the time horizon from  $\pm 1$  year to  $\pm 3$  years, the coefficient on *Tar. If breach* changes from -0.011 (sig. at 1% level) to -0.007 (sig. at 10% level). The results may indicate that the negative effect on operating performance tends to diminish over time.

[Insert Table 9 here]

#### 4.6 Sources of the value destruction

Our analysis so far documents a negative relation between target data breach experience and M&A performance. Next, we explore some mechanisms/reasons through which targets' data breaches could impair the value of acquirers. The following three potential mechanisms are considered: goodwill write-off, acquirer data breach (spillover effect), and processing time.

##### *Goodwill write-offs*

According to the Statements of Financial Accounting Standards (SFAS), goodwill in M&As refers to an accounting asset calculated as the difference between the enterprise value and the book value of the target assets, representing the premium paid for the expected synergies from the deal. In previous studies, the goodwill write-off of acquiring firms has been used as a proxy for the decrease in post-acquisition synergies compared to the anticipated synergies at the time of the deal announcement (e.g., Gu and Lev, 2011). The Financial Accounting Standards Board (FASB) requires firms to assess goodwill impairment at least once a year. If significant goodwill write-offs occur from the acquirer's assets, it can result in substantial (paper) losses for the acquirer, as highlighted by Bereskin et al. (2018). Consequently, the potential for large goodwill write-offs in acquisitions raises significant concerns in the market and may result in poor merger performance. Therefore, in this section, we use the acquirer's goodwill write-off as a measure of the failure to produce synergies, to examine whether this is affected by the target firm's cybersecurity risk. We expect to observe greater goodwill write-offs in deals involving data-breached targets than in other deals.

The estimation results are presented in Table 10. The dependent variable is *Acquirer Ln goodwill write-off in year+1*, which is defined as the natural logarithm of the acquirer's goodwill write-off one year after the acquisition. We observe significantly positive coefficients for all three target data breach variables, showing that acquiring firms experience higher levels of goodwill impairment after acquisitions in which the target firms have a history of data breach incidents. Our findings indicate that a high level of cyber risk in the target firm is likely to cause the acquiring firm to fall short of realizing the anticipated synergies during the post-merger period, which may explain the unfavourable market reaction to such M&A announcements.

[Insert Table 10 here]

### *Acquirer cybersecurity risk (spillover effect)*

As we discussed previously, the cybersecurity risk of the target firm can spill over into the system of the acquiring firm during the M&A integration process, thereby increasing the acquirer's cybersecurity risk. Thus, in this section, we test whether acquiring a data-breached target affects the likelihood of a data breach for the acquirer, following the acquisition. To conduct this analysis, we regress the change in the number of acquirer data breach incidents, from before to after the deal, on the target's data breach experience. The dependent variable (*Acquirer  $\Delta$ Count breach*) is calculated as the difference between the number of acquirer data breach incidents recorded one (two, or three) year(s) prior to the deal announcement and that recorded one (two, or three) year(s) after the completion of the deal. In addition to the three measures of target data breach experience, we also include the acquirer's data breach experience (*Acq. Ln Count breach*) in the regression, as it may affect the change in the number of acquirer data breach incidents after the deal.

Table 11 presents the regression results. The coefficients on all three target data breach variables are positive and statistically significant across the different time horizons ( $\pm 1$  year,  $\pm 2$  years, and  $\pm 3$  years), indicating a significant increase in the number of acquirer data breach events following the acquisition of a target firm that has experienced a data breach. It is important to note that, as we extend the time horizon for comparison, the impact of the target's data breach experience on the change in the number of acquirer data breach incidents becomes even more pronounced. In summary, our findings strongly suggest that the cybersecurity risk associated with the target firm can indeed be transferred to the acquiring firm through the acquisition. This provides an additional explanation for the market's less favourable reaction to acquisitions involving data-breached targets.

[Insert Table 11 here]

### *The speed of deal completion*

The speed of deal completion is also considered an important component of merger integration (Feldman and Spratt, 2001; Berskin et al., 2018). Compared to acquisitions of non-data-breached targets, deals involving data-breached targets can be more complex and subject to greater uncertainties. Cybersecurity diligence may require more time and investment from the acquiring firm during the process. Both the acquirer and the market generally prefer a quicker merger completion as a prolonged process may increase transaction costs and uncertainty (Renneboog and Zhao, 2014). Therefore, we

further examine whether acquiring data-breached targets affects the speed of deal completion. We expect that additional risks and complexities introduced by data-breached targets could potentially slow down the deal process, leading to a longer duration between the announcement date and the effective date of completion. The dependent variable in Table 12 is the number of days between the announcement date and the effective date. The regression results reveal that all three measures of target data breaches are positively associated with the duration of deal completion. For example, on average, deals involving data-breached targets take approximately 11 days longer to process than other deals. Our findings suggest that acquiring data-breached targets may pose challenges in terms of due diligent assessment and merger integration, and is likely to result in value destruction in M&As.

[Insert Table 12 here]

## 5. Further Analyses

### 5.1 Cross-sectional analyses

In this section, we conduct cross-sectional analyses to provide further evidence on the impact channels. Prior research suggests that certain firm and industry characteristics, such as firms' financial conditions and industry affiliations, may be associated with both the likelihood and the effects of data breach incidents (e.g., Sen and Borle, 2015; Kopp et al., 2017; Kamiya et al., 2021; Eisenbach et al., 2022). Additionally, previous studies emphasize the significance of financial advisors in M&A transactions and document that acquisition deals are more likely to be completed successfully and yield better performance when top-tier advisors are hired (e.g., Golubov et al., 2012; Lawrence et al., 2021). Hence, we seek to shed light on the firm and deal characteristics that shape the relationship between the target's data breach experience and the acquirer's returns.

First, we examine the effect of targets' data breach experience across different industries. It is widely recognized that cybersecurity risks and associated costs vary significantly across industries (Florackis et al., 2023; Huang and Wang, 2021). Certain industries are more vulnerable to data breaches due to their heavy reliance on information technology and the increased sensitivity of their customers to leakages of personal information. Hence, we hypothesize that the negative effect of the target's data breach experience on the acquirer's returns is influenced by industry affiliation. To test this hypothesis, we construct a dummy variable, *Vulnerable industry*, that equals one if both acquirer

and target belong to vulnerable industries, and zero otherwise. Consistent with Huang and Wang (2021), we define the following industries as vulnerable: health (Fama-French code 11), personal services (33), business services (34), computer (35), electronic equipment (36), and transportation (40). We include this variable and its interactions with three measures of target data breaches, and present the estimation results in Columns (1)-(3) of Table 13. The results show that the coefficients on the interactions between *Tar. If breach* and *Tar. Count breach*, respectively, and *Vulnerable industry*, are significantly negative. This suggests that the negative effect of the target's data breach experience on the acquirer's announcement returns is more pronounced in industries that are vulnerable to cybersecurity attacks.

Second, we examine whether the effect of the target's data breach experience on the acquirer's announcement returns is amplified when the acquirer faces high insolvency or bankruptcy risks. Acquiring a data-breached target can introduce additional risks and potentially increase costs during the post-merger phase, which can put a strain on the acquirer's financial health. The impact could be particularly severe if the acquiring firm already has high insolvency risk. In this study, we use Altman's *Z-score* to measure the financial health and insolvency risk of a firm and include it, along with its interactions with the target data breach variables, in our empirical model (Altman, 1968). The results are presented in Columns (4)-(6) of Table 13. We find significantly negative coefficients for all three interaction terms. These results suggest that acquiring a data-breached target leads to even greater losses in shareholder value for the acquirer when its financial condition is more vulnerable prior to the acquisition.

The value of financial due diligence advisors in M&A transactions is widely recognized. These advisors, particularly top-tier advisors, can bring valuable expertise, analysis, and risk mitigation capabilities to M&A transactions. Therefore, we expect that the negative impact of the target's data breach experience on the acquirer's returns could be moderated by a due diligence assessment conducted by top-tier advisors. We consider the Big 4 accounting and professional services firms (i.e., PricewaterhouseCoopers, KPMG LLP, Ernst & Young LLP, and Deloitte & Touche LLP) to be top-tier due diligence advisors. Among the acquirers in our sample, 284 of them hired due diligence advisors, and a majority (68%) opted for Big 4<sup>9</sup>. For our analysis, we construct a dummy variable,

---

<sup>9</sup> Our results are robust to using a dummy variable indicating whether the acquirer hired a due diligence advisor (regardless

*Acq. Big 4 DD*, which takes a value of one if the acquirer hires one of the Big 4 as its due diligence advisor, and zero otherwise. In line with our expectations, the results presented in Columns (7)-(9) of Table 13 show that the coefficients on the interactions between *Acq. Big 4 DD* and the three target data breach measures are all statistically significant and positive. These findings indicate that the top-tier due diligence advisors are more adept at conducting proper due diligence and cyber assessments, thereby mitigating the negative impact of the target's data breach risk on the acquirer's announcement performance.

[Insert Table 13 here]

## 5.2 Why do acquirers bid for data-breached targets?

### *Data breach experience and the likelihood of being a target*

Our findings indicate that target firms with a history of data breaches have a significant negative impact on acquirers' deal performance, resulting in a decline in their shareholder value. A pertinent question thus arises: does a firm's history of data breaches discourage potential acquirers from initiating a bid? To address this question, we perform a logit regression analysis of acquisition propensity, as presented in Table 14. Our sample comprises all firms in the Compustat universe from 2006 to 2020. The dependent variable, *Acquisition*, takes a value of one if a firm was successfully acquired by another firm in a given year, and zero otherwise. We define *If Breach* as a dummy variable that equals one if a firm experienced any data breach incidents from the beginning of the sample period but before the announcement of the acquisition (shown in Column (1)), in the two years prior to the announcement of the acquisition (shown in Column (2)), or in the five years prior to the announcement of the acquisition (shown in Column (3)), and zero otherwise. *Count Breach* is defined as the number of data breach incidents that a firm experienced from the beginning of the sample period to before the announcement of the acquisition (or in the two or five years prior to the announcement of the acquisition). The coefficients on *If Breach* and *Count Breach* are all insignificant across the different time horizons, indicating that the likelihood of an acquisition is not significantly associated with the target's data breach experience. This suggests that acquiring firms may not consider the target's history of data breach incidents a significant threat when they make an M&A decision. By disregarding the

---

of whether the advisor was Big 4 or not).

importance of the target's data breach history and cybersecurity posture, acquiring firms may overlook critical cybersecurity vulnerabilities, which can ultimately lead to adverse consequences in the acquisition process.

[Insert Table 14 here]

### *The strategic motive to merge*

Strategic and competitive considerations are often viewed as pivotal factors in M&A decisions (Nilssen and Sørsgard, 1998; Bernile and Lyandres, 2019). To achieve some long-term strategic objectives, acquiring firms may proceed with acquisitions despite being aware of the potentially high risks involved in the deals (Dong et al., 2021). These objectives may include enhancing bargaining power in the product market, eliminating future competition, product or service diversification, cost savings, access to new markets, supply chain integration, and capitalizing on growth opportunities. It is important to note that the strategic motives behind different types of acquisitions can vary, which may impact the selection of data-breached targets. To examine this conjecture, we construct three variables that capture the types of acquisitions. The first, *Horizontal*, is a dummy variable that equals one if the acquirer and target share the same NAIC (North American Industry Classification) industry code, and zero otherwise. The second, *Vertical*, is a dummy variable that equals one if the acquirer and target operate in different stages of the value chain, and zero otherwise. We define a vertical relationship between the industries of the acquirer and target based on the 2012 U.S. input-output industry-pair table, based on whether one industry exceeds the 5% threshold of either selling to or purchasing from the other industry. The final variable, *Unrelated*, is a dummy variable that equals one if the acquisition is neither a horizontal nor a vertical deal, and zero otherwise. We perform separate regressions of the target data breach measure (*Tar. If breach*) on the different types of acquisitions, in order to investigate this relationship.

Table 15 presents the results of our analysis. We find that the coefficient for *Horizontal* is significantly negative, while that for *Vertical* is significantly positive. These findings indicate that acquirers are less likely to target companies that have experienced data breaches in horizontal acquisitions compared to vertical acquisitions. This distinction may be attributable to the differing motives behind these two types of deals. Vertical acquisitions are commonly driven by the objectives of gaining greater control over the supply chain and enhancing coordination between different stages

of production. Such objectives may motivate acquirers to acquire companies that have experienced data breaches, with cybersecurity risks being of secondary concern. On the other hand, horizontal acquisitions are often aimed at achieving economies of scale and expanding market share. In such cases, the cybersecurity risk associated a data-breached target could significantly impact the acquirer's ability to create value through the deal. As a result, acquirers in horizontal deals will tend to be more concerned about any data breach incidents that have affected their targets.

It is commonly believed that the main driver of vertical acquisitions is the aim of generating synergies by increasing power and gaining more control of the supply chain. Thus, strategic considerations may motivate an acquirer to buy a data-breached target, with cybersecurity risk only a secondary consideration. However, synergy gains in horizontal deals are more related to achieving economies of scale and increasing market share. Here, the target's cyber risk could have a significant impact on the acquirer's ability to create value through those channels. Therefore, acquirers in horizontal deals are likely to be more concerned about targets' data breaches. Regarding the *Unrelatedness* variable, we report a positive but statistically insignificant coefficient. This suggests there is no significant relationship between unrelated acquisitions and the selection of data-breached targets in our analysis. Overall, our findings highlight the different impacts of strategic considerations and motives on the likelihood of acquiring companies that have experienced a data breach in horizontal and vertical acquisitions.

[Insert Table 15 here]

### 5.3 Additional analysis

#### *Elapsed time of data breach incidents*

To further explore the relationship between target's data breach experience and deal performance, we conduct additional analysis to investigate whether this relationship varies over time. Previous studies on investor attention have highlighted significant temporal variations in attention levels. For example, Da et al. (2011) find a substantial increase in investor attention during the week of an IPO announcement, but attention levels returning to the pre-announcement level after the IPO. Similarly, Vozlyublennaya (2014) find the impact of investor attention on the returns and volatility of market indices to be relatively short-lived and to depend on the elapsed time. In our specific context of data

breach incidents, it is likely that, as time elapses following the breach incident, investor attention and concern regarding the incident weaken. Therefore, we expect the impact of a data breach incident on acquisition announcement performance to diminish over time.

To test the time effect, we examine the timing of targets' data breach incidents by considering five different time lags: Year [-1], Year [-2], Year [-3], Year [-4], and Year [-5]. These time lags represent data breach events occurring one, two, three, four, and five years prior to the acquisition, respectively. We regress acquirer announcement performance (*Acquirer CAR*[-2, +2]) on target data breach experience (*Tar. If breach*, *Tar. Count breach*, and *Tar. Amount breach*) for each of the five time lags. The results are presented in Table 16. We find that, although the coefficients are negative for all five time lags, the negative associations between acquirer's announcement performance and the target data breach measures are only significant for all of those measures for Year [-1]. For Year [-2], only *Tar. If breach* and *Tar. Count breach* show significant relationships; and for Year [-3], only *Tar. If breach* has a significant relationship. These findings indicate that the negative impact of target data breach events tends to diminish over time. It appears that the effect may primarily be driven by data breaches that occurred within the two years prior to the announcement, as they have a more pronounced influence on acquirer announcement performance.

[Insert Table 16 here]

### *Types of data breaches*

Several studies suggest that the type of data breach can influence the market's, the company's, and its stakeholders' responses to the announcement of data breaches (e.g., Rosati et al., 2017; Huang and Wang, 2021; Nikkhah and Grover, 2022). While data breaches in general can impose costs on firms, the significance and magnitude of these costs, as well as their overall impact, may vary across different types of events (Charette et al., 1997). To further explore the potentially differential impacts of different types of data breaches on the acquirer's announcement returns, we classify the targets' data breach incidents into five categories: *Bank card fraud*, *Hack*, *Stakeholder*, *Lost*, and *Unknown*. The number of cases for each category of data breach is 33 in *Bank card fraud*, 103 in *Hack*, 93 in *Stakeholder*, 207 in *Lost*, and 47 in *Unknown*.<sup>10</sup> We then conduct separate regression analyses,

---

<sup>10</sup> The total number is 483 which is higher than the total number of acquisitions with data-breach targets. This is because a

regressing *Acquirer CAR*[-2, +2] on the *Tar. Count breach* variable associated with each category. The results are presented in Table 17. Across all categories, we find that the coefficients on *Tar. Count breach* are negative, indicating a negative relationship between the extent of the target's data breach and the acquirer's announcement return. However, statistical significance is observed only for the *Hack* and *Lost* types of incidents. These results suggest that the impact of a target's data breach on the acquirer's announcement performance is contingent upon the specific type of data breach incident, and the negative effect is most pronounced for targets that have security vulnerabilities and subjective faults. These findings underscore the importance of considering the specific characteristics and implications of different types of data breaches in order to understand their effects on acquirers' announcement performance.

[Insert Table 17 here]

## 6. Conclusions

The rise in cyber attacks has led to increased attention being paid to cybersecurity risk among market participants. While previous studies have examined the impact of cybersecurity risk on firms' general operations and performance, its potential influence on M&As, which are highly significant corporate events, has received limited research attention. In this study, we use a large sample of U.S. acquisitions and corporate data breach incidents to examine the impact of the target's cybersecurity risk on acquisition performance.

Our findings provide compelling evidence that the target's data breach experience has a significant negative impact on the acquirer's announcement returns and post-merger operational performance. We identify potential channels through which targets' data breach experience can erode acquirers' shareholder value, including overpayment, goodwill impairment, the spillover of cybersecurity risk from data-breached targets to acquirers, and the speed of deal completion. Moreover, we observe that the negative impact of target data breaches on acquirer announcement returns is more pronounced in industries vulnerable to cyber attacks, for financially distressed acquirers, and when acquirers do not hire top-tier due diligence advisors. Furthermore, we find that an acquirer's prior data breach

---

data-breach target may have multiple categories of historical data breach cases.

experience and certain strategic considerations may motivate acquirers to buy target firms that have experienced a data breach. Finally, our analysis reveals that the impact of targets' data breaches on acquirers' announcement returns can vary based on the time that has elapsed since the breach incident and the type of data breach.

In summary, our study highlights the significant impact of cybersecurity risk on M&As. It emphasizes the need for careful consideration of cybersecurity risk in the assessment and execution of M&A transactions. These findings have important implications for corporate managers, policymakers, and investors. Corporate managers should recognize cybersecurity risk as a critical factor in the M&A decision-making process. They should prioritize thorough due diligence assessments of target firms' cybersecurity practices and their history of data breaches. This should include evaluating their cybersecurity infrastructure, protocols, and response capabilities. By doing so, managers can better assess the potential risks and mitigate any negative impacts on the acquiring company's performance. In addition, investors should integrate cybersecurity risk assessments into their investment decisions and consider the long-term implications of data breach incidents for the financial performance and value of the companies in which they invest. By incorporating cybersecurity risk analysis, investors can make informed investment choices and proactively manage potential risks. Our research should also be of interest to policymakers considering implementing or strengthening disclosure requirements regarding firms' cybersecurity practices and history of data breaches. Our findings also suggest that policymakers should take on a vital role, namely fostering collaboration and information sharing between government agencies, industry associations, and companies. This could effectively address cybersecurity risks, not only in M&A transactions, but also in other types of transactions, promoting a more resilient business environment.

## References

- Ahern, K.R., 2012. Bargaining power and industry dependence in mergers. *Journal of Financial Economics*, 103(3), pp.530-550.
- Ahern, K.R. and Harford, J., 2014. The importance of industry links in merger waves. *The Journal of Finance*, 69(2), pp.527-576.
- Aldasoro, I., Gambacorta, L., Giudici, P. and Leach, T., 2022. The drivers of cyber risk. *Journal of Financial Stability*, 60, p.100989.
- Alexandridis, G., Fuller, K.P., Terhaar, L. and Travlos, N.G., 2013. Deal size, acquisition premia and shareholder gains. *Journal of Corporate Finance*, 20, pp.1-13.
- Allen, L., Jagtiani, J., Peristiani, S. and Saunders, A., 2004. The role of bank advisors in mergers and acquisitions. *Journal of Money, Credit and Banking*, pp.197-224.
- Altman, E.I., 1968. Financial ratios, discriminant analysis and the prediction of corporate bankruptcy. *The Journal of Finance*, 23(4), pp.589-609.
- Amihud, Y. and Lev, B., 1981. Risk reduction as a managerial motive for conglomerate mergers. *The Bell Journal of Economics*, pp.605-617.
- Amir, E., Levi, S. and Livne, T., 2018. Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, 23(3), pp.1177-1206.
- Angst, C.M., Block, E.S., D'Arcy, J. and Kelley, K., 2017. When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly*, 41(3), pp.893-A8.
- Ashraf, M., 2022. The role of peer events in corporate governance: Evidence from data breaches. *The Accounting Review*, 97(2), pp.1-24.
- Asquith, P., Bruner, R.F. and Mullins Jr, D.W., 1983. The gains to bidding firms from merger. *Journal of Financial Economics*, 11(1-4), pp.121-139.
- Avery, A., 2021. After the disclosure: measuring the short-term and long-term impacts of data breach disclosures on the financial performance of organizations. *Information and Computer Security*, 29(3), pp.500-525.
- Banker, R.D. and Feng, C., 2019. The impact of information security breach incidents on CIO turnover. *Journal of Information Systems*, 33(3), pp.309-329.
- Barkema, H.G. and Schijven, M., 2008. How do firms learn to make acquisitions? A review of past research and an agenda for the future. *Journal of Management*, 34(3), pp.594-634.
- Bereskin, F., Byun, S. K., Officer, M. S., & Oh, J. M., 2018. The effect of cultural similarity on mergers and acquisitions: Evidence from corporate social responsibility. *Journal of Financial and Quantitative Analysis*, 53(5), pp. 1995-2039.
- Bernile, G. and Lyandres, E., 2019. The effects of horizontal merger operating efficiencies on rivals, customers, and suppliers. *Review of Finance*, 23(1), pp.117-160.
- Billett, M.T. and Qian, Y., 2008. Are overconfident CEOs born or made? Evidence of self-attribution bias from frequent acquirers. *Management Science*, 54(6), pp.1037-1051.
- Boasiako, K.A. and Keefe, M.O.C., 2021. Data breaches and corporate liquidity management. *European Financial Management*, 27(3), pp.528-551.
- Cai, Y. and Sevilir, M., 2012. Board connections and M&A transactions. *Journal of Financial Economics*, 103(2), pp.327-349.

- Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L., 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer security*, 11(3), pp.431-448.
- Charette, R.N., Adams, K.M. and White, M.B., 1997. Managing risk in software maintenance. *IEEE Software*, 14(3), pp.43-50.
- Chang, S., 1998. Takeovers of privately held targets, methods of payment, and bidder returns. *The Journal of Finance*, 53(2), pp.773-784.
- Chang, X., Shekhar, C., Tam, L.H. and Yao, J., 2016. The information role of advisors in mergers and acquisitions: Evidence from acquirers hiring targets' ex-advisors. *Journal of Banking & Finance*, 70, pp.247-264.
- Chen, J., Henry, E. and Jiang, X., 2022. Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. *Journal of Business Ethics*, pp.1-26.
- Cloodt, M., Hagedoorn, J. and Van Kranenburg, H., 2006. Mergers and acquisitions: Their effect on the innovative performance of companies in high-tech industries. *Research Policy*, 35(5), pp.642-654.
- Crosignani, M., Macchiavelli, M. and Silva, A.F., 2023. Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics*, 147(2), pp.432-448.
- Curran, Sean, Paul Cotter, Matt Sondag, and John Stiffler, Testing the Defenses: Cybersecurity Due Diligence in Mergers and Acquisitions, West Monroe Partners (July 12, 2016), <https://www.westmonroepartners.com/Insights/Newsletters/Best-of-the-West-July-2016/MA-Security-Survey>.
- Da, Z., Engelberg, J. and Gao, P., 2011. In search of attention. *The Journal of Finance*, 66(5), pp.1461-1499.
- D'Arcy, J., Adjerid, I., Angst, C.M. and Glavas, A., 2020. Too good to be true: Firm social performance and the risk of data breach. *Information Systems Research*, 31(4), pp.1200-1223.
- de La Bruslerie, H., 2013. Crossing takeover premiums and mix of payment: An empirical test of contractual setting in M&A transactions. *Journal of Banking & Finance*, 37(6), pp.2106-2123.
- Dikova, D., Sahib, P.R. and Van Witteloostuijn, A., 2010. Cross-border acquisition abandonment and completion: The effect of institutional differences and organizational learning in the international business service industry, 1981–2001. *Journal of International Business Studies*, 41(2), pp.223-245.
- Dong, Y., Li, C. and Li, H., 2021. Customer concentration and M&A performance. *Journal of Corporate Finance*, 69, p.102021.
- Eckbo, B. E., 2009. Bidding strategies and takeover premiums: A review. *Journal of Corporate Finance*, 15(1), 149-178.
- Eisenbach, T.M., Kovner, A. and Lee, M.J., 2022. Cyber risk and the US financial system: A pre-mortem analysis. *Journal of Financial Economics*, 145(3), pp.802-826.
- Ettredge, M., Guo, F. and Li, Y., 2018. Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, 37(6), pp.564-585.
- Faccio, M., McConnell, J.J. and Stolin, D., 2006. Returns to acquirers of listed and unlisted targets. *Journal of Financial and Quantitative Analysis*, 41(1), pp.197-220.
- Feldman, M.L. and Spratt, M.F., 2001. *Five Frogs on a Log: A CEO's Field Guide to Accelerating the Transition in Mergers, Acquisitions & Gut Wrenching Change*. John Wiley & Sons.

- Florackis, C., Louca, C., Michaely, R. and Weber, M., 2023. Cybersecurity risk. *The Review of Financial Studies*, 36(1), pp.351-407.
- Foerderer, J. and Schuetz, S.W., 2022. Data breach announcements and stock market reactions: a matter of timing? *Management Science*, 68(10), pp.7298-7322.
- Fong, C.M., Lee, C.L. and Du, Y., 2013. Target reputation transferability, consumer animosity, and cross-border acquisition success: A comparison between China and Taiwan. *International Business Review*, 22(1), pp.174-186.
- Fuller, K., Netter, J. and Stegemoller, M., 2002. What do returns to acquiring firms tell us? Evidence from firms that make many acquisitions. *The Journal of Finance*, 57(4), pp.1763-1793.
- Furnell, S., Heyburn, H., Whitehead, A. and Shah, J.N., 2020. Understanding the full cost of cyber security breaches. *Computer Fraud & Security*, 2020(12), pp.6-12.
- Garg, P., 2020. Cybersecurity breaches and cash holdings: Spillover effect. *Financial Management*, 49(2), pp.503-519.
- Golubov, A., Petmezas, D., & Travlos, N. G. (2012). When it pays to pay your investment banker: New evidence on the role of financial advisors in M&As. *The Journal of Finance*, 67(1), 271-311.
- Gordon, L.A., Loeb, M., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, 19, pp. 33–56.
- Gu, F. and Lev, B., 2011. Overpriced shares, ill-advised acquisitions, and goodwill impairment. *The Accounting Review*, 86(6), pp.1995-2022.
- Haislip, J., Kolev, K., Pinsker, R. and Steffen, T., 2019. The economic cost of cybersecurity breaches: A broad-based analysis. In *Workshop on the Economics of Information Security (WEIS)*, pp. 1-37.
- Hayward, M.L., 2002. When do firms learn from their acquisition experience? Evidence from 1990 to 1995. *Strategic Management Journal*, 23(1), pp.21-39.
- He, C.Z., Frost, T. and Pinsker, R.E., 2020. The impact of reported cybersecurity breaches on firm innovation. *Journal of Information Systems*, 34(2), pp.187-209.
- Hinz, O., Nofer, M., Schiereck, D. and Trillig, J., 2015. The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management*, 52(3), pp.337-347.
- Hu, K., Levi, R., Yahalom, R. and Zerhouni, E.G., 2022. Supply Chain Characteristics as Predictors of Cyber Risk: A Machine-Learning Assessment. *arXiv preprint arXiv:2210.15785*.
- Hu, N., Li, L., Li, H. and Wang, X., 2020. Do mega-mergers create value? The acquisition experience and mega-deal outcomes. *Journal of Empirical Finance*, 55, pp.119-142.
- Huang, H. H., & Wang, C. (2021). Do banks price firms' data breaches? *The Accounting Review*, 96(3), 261-286.
- Hui, K.L., Kim, S.H. and Wang, Q.H., 2017. Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. *Mis Quarterly*, 41(2), p.497.
- Islam, M.S., Wang, T., Farah, N. and Stafford, T., 2022. The spillover effect of focal firms' cybersecurity breaches on rivals and the role of the CIO: Evidence from stock trading volume. *Journal of Accounting and Public Policy*, 41(2), p.106916.
- Jamilov, R., Rey, H. and Tahoun, A., 2021. *The anatomy of cyber risk* (No. w28906). National Bureau of Economic Research.
- Janakiraman, R., Lim, J.H. and Rishika, R., 2018. The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, 82(2), pp.85-105.

- Jensen, M.C., 1986. Agency costs of free cash flow, corporate finance, and takeovers. *The American Economic Review*, 76(2), pp.323-329.
- John, K., Knyazeva, A. and Knyazeva, D., 2015. Employee rights and acquisitions. *Journal of Financial Economics*, 118(1), pp.49-69.
- Kamiya, S., Kang, J.K., Kim, J., Milidonis, A. and Stulz, R.M., 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, 139(3), pp.719-749.
- Kisgen, D.J. and Song, W., 2009. Are fairness opinions fair? The case of mergers and acquisitions. *Journal of Financial Economics*, 91(2), pp.179-207.
- Kohers, N. and Kohers, T., 2000. The value creation potential of high-tech mergers. *Financial Analysts Journal*, 56(3), pp.40-51.
- Kopp, E., Kaffenberger, L. and Wilson, C., 2017. *Cyber risk, market failures, and financial stability*. International Monetary Fund.
- Kshetri, N. 2018. The economics of cyber-insurance. *IT Professional*, 20 (6): 9–14.
- Lang, L.H., Stulz, R. and Walkling, R.A., 1991. A test of the free cash flow hypothesis: The case of bidder returns. *Journal of Financial Economics*, 29(2), pp.315-335.
- Lattanzio, G. and Ma, Y., 2021. Corporate innovation in the cyber age. *SMU Cox School of Business Research Paper*, (20-04).
- Lattanzio, G. and Taillard, J., 2022. M&A and Cybersecurity Risk: Empirical Evidence. Available at SSRN 4170093.
- Lawrence, E.R., Raithatha, M. and Rodriguez, I., 2021. The effect of cultural and institutional factors on initiation, completion, and duration of cross-border acquisitions. *Journal of Corporate Finance*, 68, p.101950.
- Lending, C., Minnick, K. and Schorno, P.J., 2018. Corporate governance, social responsibility, and data breaches. *Financial Review*, 53(2), pp.413-455.
- Li, H., No, W.G. and Boritz, J.E., 2020. Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice & Theory*, 39(1), pp.151-171.
- Loughran, T. and Ritter, J., 2004. Why has IPO underpricing changed over time? *Financial Management*, 33(3), pp.5-37.
- Makridis, C.A., 2021. Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018. *Journal of Cybersecurity*, 7(1), p.tyab021.
- Malhotra, A. and Kubowicz Malhotra, C., 2011. Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research*, 14(1), pp.44-59.
- Maloney, M.T., McCormick, R.E. and Mitchell, M.L., 1993. Managerial decision making and capital structure. *Journal of Business*, 66(2), pp.189-217.
- Martin, K.D., Borah, A. and Palmatier, R.W., 2017. Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), pp.36-58.
- Masulis, R.W., Reza, S.W. and Guo, R., 2023. The sources of value creation in acquisitions of intangible assets. *Journal of Banking & Finance*, p.106879.
- Masulis, R. W., Wang, C. and Xie, F., 2007. Corporate governance and acquirer returns. *The Journal of Finance*, 62(4), 1851-1889.
- Moeller, S.B., Schlingemann, F.P. and Stulz, R.M., 2004. Firm size and the gains from acquisitions. *Journal of Financial Economics*, 73(2), pp.201-228.
- Moeller, S.B., Schlingemann, F.P. and Stulz, R.M., 2005. Wealth destruction on a massive scale? A

- study of acquiring-firm returns in the recent merger wave. *The Journal of Finance*, 60(2), pp.757-782.
- Morck, R., Shleifer, A. and Vishny, R.W., 1990. Do managerial objectives drive bad acquisitions?. *The Journal of Finance*, 45(1), pp.31-48.
- Nikkhah, H.R. and Grover, V., 2022. An empirical investigation of company response to data breaches. *MIS Quarterly*, 46(4), pp.2163-2196.
- Nilssen, T. and Sørsgard, L., 1998. Sequential horizontal mergers. *European Economic Review*, 42(9), pp.1683-1702.
- Officer, M.S., Poulsen, A.B. and Stegemoller, M., 2009. Target-firm information asymmetry and acquirer returns. *Review of Finance*, 13(3), pp.467-493.
- Png, I.P., Wang, C.Y. and Wang, Q.H., 2008. The deterrent and displacement effects of information security enforcement: International evidence. *Journal of Management Information Systems*, 25(2), pp.125-144.
- Renneboog, L. and Zhao, Y., 2014. Director networks and takeovers. *Journal of Corporate Finance*, 28, pp.218-234.
- Richardson, V.J., Smith, R.E. and Watson, M.W., 2019. Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems*, 33(3), pp.227-265.
- Romanosky, S., 2016. Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2), pp.121-135.
- Romanosky, S., Hoffman, D. and Acquisti, A., 2014. Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies*, 11(1), pp.74-104.
- Rosati, P. and Lynn, T., 2021. A dataset for accounting, finance and economics research on US data breaches. *Data in Brief*, 35, p.106924.
- Rosati, P., Cummins, M., Deeney, P., Gogolin, F., Van der Werff, L. and Lynn, T., 2017. The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis*, 49, pp.146-154.
- Sen, R. and Borle, S., 2015. Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, 32(2), pp.314-341.
- Shleifer, A. and Vishny, R.W., 1989. Management entrenchment: The case of manager-specific investments. *Journal of Financial Economics*, 25(1), pp.123-139.
- Travlos, N.G., 1987. Corporate takeover bids, methods of payment, and bidding firms' stock returns. *The Journal of Finance*, 42(4), pp.943-963.
- Tosun, O.K., 2021. Cyber-attacks and stock market activity. *International Review of Financial Analysis*, 76, p.101795.
- Vozlyublennaiia, N., 2014. Investor attention, index performance, and return predictability. *Journal of Banking & Finance*, 41, pp.17-35.
- Walton, S., Wheeler, P.R., Zhang, Y. and Zhao, X., 2021. An integrative review and analysis of cybersecurity research: Current state and future directions. *Journal of Information Systems*, 35(1), pp.155-186.
- Wang, S.S., 2019. Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal*, 57, p.101173.
- Wang, Q. and Ngai, E.W., 2022. Firm diversity and data breach risk: A longitudinal study. *The Journal of Strategic Information Systems*, 31(4), p.101743.
- Xu, H., Guo, S., Haislip, J.Z. and Pinsker, R.E., 2019. Earnings management in firms with data security

breaches. *Journal of Information Systems*, 33(3), pp.267-284.

Yen, J.C., Lim, J.H., Wang, T. and Hsu, C., 2018. The impact of audit firms' characteristics on audit fees following information security breaches. *Journal of Accounting and Public Policy*, 37(6), pp.489-507.

## Tables:

**Table 1.** Number of acquisitions by year

This table presents our sample distribution by year. Our sample covers a total number of 8,146 completed domestic acquisitions in the United States between 2006 and 2020.

Year	Full sample		With data-breach target		Without data-breach target	
	Number	%	Number	%	Number	%
	(1)	(2)	(3)	(4)	(5)	(6)
2006	784	9.62	12	1.53	772	98.47
2007	700	8.59	15	2.14	685	97.86
2008	462	5.67	20	4.33	442	95.67
2009	327	4.01	17	5.20	310	94.80
2010	470	5.77	14	2.98	456	97.02
2011	507	6.22	25	4.93	482	95.07
2012	580	7.12	31	5.34	549	94.66
2013	556	6.83	24	4.32	532	95.68
2014	667	8.19	22	3.30	645	96.70
2015	624	7.66	41	6.57	583	93.43
2016	515	6.32	33	6.41	482	93.59
2017	566	6.95	38	6.71	528	93.29
2018	571	7.01	32	5.60	539	94.40
2019	430	5.28	28	6.51	402	93.49
2020	387	4.75	16	4.13	371	95.87
Total	8146	100	368	4.52	7778	95.48

**Table 2.** Number of acquisitions by industry

This table presents our sample distribution by acquirer industry. The industry classification is based on Fama-French 12 industries.

Acq. Fama-French 12 industries	Full sample		With data-breach target		Without data-breach target	
	Number	%	Number	%	Number	%
	(1)	(2)	(3)	(4)	(5)	(6)
1 Nondurables	251	3.08	10	3.98	241	96.02
2 Durables	122	1.50	5	4.10	117	95.90
3 Manufacturing	708	8.69	28	3.95	680	96.05
4 Oil, gas, & coal	312	3.83	13	4.17	299	95.83
5 Chemical products	148	1.82	2	1.35	146	98.65
6 Business equipment	1423	17.47	52	3.65	1371	96.35
7 Telecommunication	242	2.97	26	10.74	216	89.26
8 Utilities	182	2.23	9	4.95	173	95.05
9 Wholesale & retail	468	5.75	25	5.34	443	94.66
10 Health care	767	9.42	20	2.61	747	97.39
11 Finance	2585	31.73	148	5.73	2437	94.27
12 Other	938	11.51	30	3.20	908	96.80
Total	8146	100	368	4.52	7778	95.48

**Table 3.** Descriptive statistics

This table reports the descriptive statistics for all variables. The variables are presented in four categories: Target data breach, acquirer data breach, acquirer characteristics, synergy and target wealth, and deal characteristics. The definitions of all variables are presented in the Appendix.

Variables	Full sample		With data-breached target		Without data-breached target		Diff.
	Mean	Sd.	Mean	Sd.	Mean	Sd.	T-test
	(1)	(2)	(3)	(4)	(5)	(6)	(7) =(3)-(5)
<i>Targets</i>							
If breach	0.045	0.208	1.000	0.000	0.000	0.000	-
Count breach	0.129	0.901	2.850	3.196	0.000	0.000	-
Amount breach	96600	3774292	2830000	20269739	0.000	0.000	-
<i>Acquirers</i>							
If breach	0.058	0.233	0.189	0.392	0.0518	0.222	0.137***
Count breach	0.165	0.962	0.775	2.389	0.139	0.836	0.637***
Amount breach	252991	5958283	930271	10097594	223108	5706204	707162
<i>Acquirer characteristics</i>							
Assets (\$m)	8907	24522	23587	44512	8213	22926	15374***
Tobin's q	1.808	1.052	1.703	0.949	1.813	1.056	-0.11**
Leverage	0.197	0.162	0.230	0.161	0.195	0.162	0.035***
Free cash flow	0.023	0.097	0.029	0.030	0.023	0.098	0.006*
Stock price runup	0.052	0.398	0.070	0.336	0.052	0.400	0.018
Goodwill write off (\$m)	0.260	9.564	0.073	0.726	0.267	9.730	-0.193
<i>Synergy and Target wealth</i>							
Combined CAR[-2, +2]	2.47%	0.072	1.51%	0.071	2.52%	0.072	-1.01%
Premium (%)	33.688	31.779	33.399	21.698	33.703	32.229	-0.303
$\Delta$ \$Target CAR	0.043	0.064	0.059	0.058	0.043	0.064	0.017*
<i>Deal characteristics</i>							
Public target	0.147	0.354	0.185	0.389	0.145	0.352	0.040**
Private target	0.547	0.498	0.133	0.340	0.566	0.496	-0.433***
High tech	0.157	0.364	0.128	0.334	0.159	0.365	-0.031*
Diversify	0.299	0.458	0.340	0.474	0.297	0.457	0.043*
Relative deal size	0.225	0.591	0.352	0.816	0.218	0.577	0.134***
All-cash deal	0.306	0.461	0.318	0.466	0.305	0.461	0.013
All-stock deal	0.062	0.242	0.054	0.227	0.063	0.242	-0.009
If Acq. Big 4 DD	0.024	0.153	0.033	0.178	0.024	0.152	0.009
Horizontal	0.444	0.497	0.393	0.489	0.446	0.497	-0.053**
Vertical	0.101	0.301	0.134	0.341	0.099	0.299	0.035*
Unrelated	0.455	0.498	0.473	0.500	0.454	0.498	0.019
Days between ann. and eff.	61.058	98.188	93.245	107.233	58.907	95.530	34.338***

**Table 4.** Univariate analysis

Panel A of this table compares the means and medians of *Acquirer CAR*, *Acquirer  $\Delta$ ROA*, and *Acquirer  $\Delta$ Count breach* between the two subsamples of deals: deals with data-breached targets and deals without data-breached targets. The definitions of all variables are presented in the appendix. The two-sample t-test and the two-sample Wilcoxon rank-sum (Mann-Whitney) test are used to test the significance of the mean difference and median difference, respectively. The *t*-stat and *z*-stat are reported in parentheses. \*\*\*, \*\*, and \* indicate significance at the 1, 5, and 10% level, respectively.

Panel A: Comparison between target firms with/without data-breach											
	Full sample			With data-breached target			Without data-breached target			<i>t</i> -Value	<i>z</i> -Value
	Mean	Median	Sd.	Mean	Median	Sd.	Mean	Median	Sd.	( <i>t</i> -test)	(Wilcoxon test)
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
<i>Acquirer CAR</i>											
[-1, +1] day	1.32%	0.57%	0.088	0.82%	0.13%	0.075	1.35%	0.59%	0.089	1.307	2.084**
[-2, +2] day	1.33%	0.57%	0.093	0.49%	0.01%	0.086	1.37%	0.59%	0.094	1.894*	1.980**
[-3, +3] day	1.34%	0.54%	0.098	0.62%	0.42%	0.092	1.38%	0.55%	0.099	1.535	1.285
<i>Acquirer <math>\Delta</math>ROA</i>											
[-1, +1] year	-0.54%	-0.22%	0.081	-1.06%	-0.41%	0.059	-0.51%	-0.21%	0.081	1.471	0.989
[-2, +2] year	-0.22%	-0.12%	0.074	-0.81%	-0.18%	0.057	-0.19%	-0.11%	0.075	1.699*	0.751
[-3, +3] year	-0.03%	-0.06%	0.074	-0.57%	-0.13%	0.055	0.05%	-0.05%	0.075	1.701*	0.650
<i>Acquirer <math>\Delta</math>Count breach</i>											
[-1, +1] year	0.006	0.000	0.293	0.133	0.000	0.713	0.000	0.000	0.256	3.573***	6.839***
[-2, +2] year	0.013	0.000	0.459	0.264	0.000	1.221	0.001	0.000	0.383	4.114***	7.783***
[-3, +3] year	0.020	0.000	0.564	0.302	0.000	1.534	0.007	0.000	0.467	3.682***	7.420***

**Table 5.** Acquirer's cumulative abnormal return

This table presents the results from the regressions of the acquirer's cumulative abnormal return on the target's data breach experience. The dependent variable is *Acquirer CAR*[-2, +2]. It is the five-day cumulative abnormal return for the acquirer around the acquisition announcement, calculated using the CAPM. *Tar. If breach* is defined as a dummy variable which equals 1 if the target experienced publicly known data breach events and otherwise 0. *Tar. Count breach* is defined as the natural logarithm of one plus the number of historical data breach events experienced by the target. *Tar. Amount breach* is defined as the natural logarithm of one plus the number of records exposed in the target's historical data breach events. Columns (1)-(3) report the results for full sample; Column (4) reports the results within the subsample with data-breach targets. The definitions of all variables are presented in the appendix. All regressions control for calendar year fixed effects and industry fixed effects. *p*-values based on standard errors adjusted for firm clustering are reported in parentheses. \*\*\*, \*\*, and \* indicate significance at the 1, 5, and 10% levels, respectively.

	Acquirer CAR[-2, +2]			
	Full sample			Within data-breach targets
	(1)	(2)	(3)	(4)
Tar. If breach	-0.014** (0.016)			
Tar. Count breach		-0.011** (0.034)		-0.023** (0.046)
Tar. Amount breach			-0.001* (0.098)	
Acq. Ln Assets	-0.004*** (0.000)	-0.004*** (0.000)	-0.004*** (0.000)	-0.003 (0.303)
Acq. Tobin's q	0.004** (0.035)	0.004** (0.035)	0.004** (0.031)	-0.007 (0.196)
Acq. Leverage	0.024* (0.061)	0.023* (0.063)	0.025** (0.047)	-0.009 (0.812)
Acq. Free cash flow	0.003 (0.894)	0.003 (0.900)	0.003 (0.905)	0.111 (0.294)
Acq. Stock price runup	-0.024*** (0.000)	-0.024*** (0.000)	-0.024*** (0.000)	-0.022 (0.277)
Public target	-0.039*** (0.000)	-0.039*** (0.000)	-0.039*** (0.000)	-0.057*** (0.002)
Non-private target	-0.008*** (0.000)	-0.008*** (0.000)	-0.008*** (0.001)	-0.002 (0.863)
High tech	0.003 (0.434)	0.003 (0.418)	0.002 (0.564)	0.023 (0.280)
Diversify	-0.004 (0.176)	-0.003 (0.187)	-0.004 (0.136)	-0.006 (0.619)
Relative deal size	0.049*** (0.000)	0.049*** (0.000)	0.049*** (0.000)	0.021 (0.128)
All-cash deal	0.003 (0.152)	0.003 (0.156)	0.003 (0.186)	-0.001 (0.922)
All-stock deal	0.001 (0.903)	0.001 (0.902)	0.0001 (0.991)	0.021 (0.347)
Constant	0.027* (0.088)	0.027* (0.088)	0.027* (0.094)	-0.065 (0.159)
Year FE	YES	YES	YES	YES
Industry FE	YES	YES	YES	YES
Obs.	8,146	8,146	8,053	328
R <sup>2</sup>	0.145	0.145	0.146	0.240

**Table 6.** Propensity score matching and entropy balancing

The propensity score matching and entropy balancing methods are employed in the regressions presented in this table. In Panels A and B, the descriptive statistics for the PSM subsamples and the regression results based on PSM are presented. In Panel B, the dependent variable is *Acquirer CAR*[-2, +2]. It is the five-day cumulative abnormal return for the acquirer around the acquisition announcement, calculated using the CAPM. *Tar. If breach* is defined as a dummy variable which equals 1 if the target experienced publicly known data breach events and otherwise 0. *Tar. Count breach* is defined as the natural logarithm of one plus the number of historical data breach events experienced by the target. *Tar. Amount breach* is defined as the natural logarithm of one plus the number of records exposed in the target's historical data breach events. In Panel C, the regression results based on the entropy balancing approach are presented. The definitions of all variables are presented in the appendix. All regressions control for calendar year fixed effects and industry fixed effects. *p*-values based on standard errors adjusted for firm clustering are reported in parentheses. \*\*\*, \*\*, and \* indicate significance at the 1, 5, and 10% levels, respectively.

Panel A: Descriptive statistics for propensity-score matched subsamples (MR=1:5, caliper=0.05)			
	Targets with data breach means (N= 263)	Targets without data breach means (N= 881)	Difference in means ( <i>T</i> -test)
<i>Dependent variable:</i>			
Acquirer CAR[-2, +2]	0.002	0.018	0.016**
<i>Explanatory variables:</i>			
Acq. Ln Assets	8.436	8.133	-0.303
Acq. Tobin's <i>q</i>	1.729	1.762	0.033
Acq. Leverage	0.228	0.219	-0.009
Acq. Free cash flow	0.026	0.025	-0.001
Acq. Stock price runup	0.071	0.080	0.008
Public target	0.183	0.202	0.020
Private target	0.110	0.148	0.037
High tech	0.118	0.141	0.023
Diversify	0.342	0.319	-0.023
Relative deal size	0.316	0.285	-0.031
All-cash deal	0.335	0.341	0.006
All-stock deal	0.061	0.069	0.008
Panel B: Regression for sample matched by propensity score			
	Acquirer CAR[-2, +2]		
	(1)	(2)	(3)
Tar. If breach	-0.020** (0.031)		
Tar. Count breach		-0.017** (0.047)	
Tar. Amount breach			-0.002* (0.077)
Control variables	YES	YES	YES
Year FE	YES	YES	YES
Industry FE	YES	YES	YES
Obs.	1,144	1,144	1,144
R <sup>2</sup>	0.369	0.370	0.368
Panel C: Regression for sample matched by entropy balancing			
	Acquirer CAR[-2, +2]		
	(1)	(2)	(3)
Tar. If breach	-0.019** (0.032)		
Tar. Count breach		-0.019** (0.035)	
Tar. Amount breach			-0.001 (0.106)
Control variables	YES	YES	YES
Year FE	YES	YES	YES
Industry FE	YES	YES	YES
Obs.	8,146	8,146	8,053
R <sup>2</sup>	0.319	0.321	0.302

**Table 7. Staggered difference-in-differences**

This table presents the analysis based on the staggered difference-in-differences (DID) method, following Huang and Wang (2021). Panel A presents the dates when the notification laws were introduced in each state for the first time. Panel B presents the regression results from the DID analysis. It shows the effect of the introduction of the notification laws. The dependent variable is *Acquirer CAR*[-2, +2]. It is the five-day cumulative abnormal return for the acquirer around the acquisition announcement, calculated using the CAPM. *Post* is a dummy variable which equals 1 if the acquisition announcement date is after the effective date of the law in the state in which the target firm is incorporated, and otherwise 0. *Tar. If breach* is defined as a dummy variable which equals 1 if the target experienced publicly known data breach events and otherwise 0. *Tar. Count breach* is defined as the natural logarithm of one plus the number of historical data breach events experienced by the target. *Tar. Amount breach* is defined as the natural logarithm of one plus the number of records exposed in the target's historical data breach events. The definitions of all variables are presented in the appendix. All regressions control for calendar year fixed effects and industry fixed effects. *p*-values based on standard errors adjusted for firm clustering are reported in parentheses. \*\*\*, \*\*, and \* indicate significance at the 1, 5, and 10% level, respectively.

Panel A: Effective date of the first data breach notification laws in each state					
Alabama	2018-06-01	Kentucky	2014-07-15	Ohio	2006-02-28
Alaska	2009-07-01	Louisiana	2006-01-01	Oklahoma	2008-11-01
Arizona	2006-12-31	Maine	2006-01-31	Oregon	2007-10-01
Arkansas	2005-08-12	Maryland	2008-01-01	Pennsylvania	2006-06-20
California	2003-07-01	Massachusetts	2007-10-31	Rhode Island	2016-07-02
Colorado	2006-09-01	Michigan	2007-07-02	South Carolina	2009-07-01
Connecticut	2006-01-01	Minnesota	2006-01-01	South Dakota	2018-07-01
Delaware	2005-06-28	Mississippi	2011-07-01	Tennessee	2005-07-01
District of Columbia	2007-07-01	Missouri	2009-08-28	Texas	2009-04-01
Florida	2014-07-01	Montana	2006-03-01	Utah	2007-01-01
Georgia	2005-05-05	Nebraska	2006-04-10	Vermont	2012-05-08
Hawaii	2007-01-01	Nevada	2005-10-01	Virginia	2008-07-01
Idaho	2006-07-01	New Hampshire	2007-01-01	Washington	2005-07-24
Illinois	2006-06-27	New Jersey	2006-01-01	West Virginia	2008-06-06
Indiana	2006-07-01	New Mexico	2017-06-16	Wisconsin	2006-03-31
Iowa	2008-07-01	New York	2005-12-07	Wyoming	2007-07-01
Kansas	2007-01-01	North Carolina	2005-12-31		
Alabama	2018-06-01	North Dakota	2005-06-01		
Panel B: Regression results from DID					
	Acquirer CAR[-2, +2]				
	(1)	(2)	(3)		
Tar. If breach	0.001 (0.959)				
Tar. If breach * Post	-0.033** (0.040)				
Tar. Count breach		-0.001 (0.915)			
Tar. Count breach * Post		-0.030** (0.043)			
Tar. Amount breach			-0.001 (0.592)		
Tar. Amount breach * Post			-0.002 (0.198)		
Post	0.002 (0.873)	0.002 (0.875)	0.002 (0.836)		
Controls	YES	YES	YES		
Year FE	YES	YES	YES		
Industry FE	YES	YES	YES		
Obs.	1,470	1,470	1,436		
R <sup>2</sup>	0.242	0.245	0.245		

**Table 8.** Combined cumulative abnormal return

This table presents the results from the regressions of the combined cumulative abnormal return of the acquirer and the target on the target's data breach experience. The dependent variable is *Combined CAR*[-2, +2], defined as the market-value-weighted average of the acquirer's and the target's CAR (-2, +2). *Tar. If breach* is defined as a dummy variable which equals 1 if the target experienced publicly known data breach events and otherwise 0. *Tar. Count breach* is defined as the natural logarithm of one plus the number of historical data breach events experienced by the target. *Tar. Amount breach* is defined as the natural logarithm of one plus the number of records exposed in the target's historical data breach events. The definitions of all variables are presented in the appendix. All regressions control for calendar year fixed effects and industry fixed effects. *p*-values based on standard errors adjusted for firm clustering are reported in parentheses. \*\*\*, \*\*, and \* indicate significance at the 1, 5, and 10% level, respectively.

	Combined CAR[-2, +2]		
	(1)	(2)	(3)
Tar. If breach	-0.021* (0.090)		
Tar. Count breach		-0.026** (0.012)	
Tar. Amount breach			-0.003*** (0.006)
Acq. log Assets	0.001 (0.677)	0.001 (0.580)	0.001 (0.650)
Acq. Tobin's q	-0.001 (0.716)	-0.001 (0.722)	-0.001 (0.775)
Acq. Leverage	0.023 (0.356)	0.024 (0.338)	0.023 (0.345)
Acq. Free cash flow	0.024 (0.336)	0.023 (0.364)	0.023 (0.358)
Acq. Stock price runup	-0.022 (0.236)	-0.022 (0.243)	-0.022 (0.246)
High tech	-0.015 (0.221)	-0.014 (0.229)	-0.014 (0.223)
Diversify	-0.015 (0.111)	-0.015 (0.119)	-0.014 (0.127)
Relative deal size	-0.002 (0.874)	-0.002 (0.868)	-0.003 (0.745)
All-cash deal	0.025*** (0.003)	0.025*** (0.003)	0.023*** (0.006)
All-stock deal	0.009 (0.287)	0.009 (0.273)	0.008 (0.326)
Constant	0.001 (0.956)	-0.001 (0.950)	0.001 (0.964)
Year FE	YES	YES	YES
Industry FE	YES	YES	YES
Obs.	849	849	832
R <sup>2</sup>	0.164	0.167	0.172

**Table 9.** Acquirer's operational performance

This table presents the results from the regressions of the operational performance of the acquirer on the target's data breach experience. The dependent variable is *Acquirer ΔROA*, the measure of the operational performance of the acquirer. It is calculated as the change in the ROA of the acquirer from one (two, three) year(s) prior to deal announcement to one (two, three) year(s) after deal completion. *Tar. If breach* is defined as a dummy variable which equals 1 if the target experienced publicly known data breach events and otherwise 0. *Tar. Count breach* is defined as the natural logarithm of one plus the number of historical data breach events experienced by the target. *Tar. Amount breach* is defined as the natural logarithm of one plus the number of records exposed in the target's historical data breach events. The definitions of all variables are presented in the appendix. All regressions control for calendar year fixed effects and industry fixed effects. *p*-values based on standard errors adjusted for firm clustering are reported in parentheses. \*\*\*, \*\*, and \* indicate significance at the 1, 5, and 10% levels, respectively.

	Acquirer ΔROA								
	± 1 year			± 2 years			± 3 years		
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Tar. If breach	-0.011*** (0.003)			-0.008** (0.017)			-0.007* (0.068)		
Tar. Count breach		-0.009*** (0.005)			-0.007** (0.019)			-0.006* (0.051)	
Tar. Amount breach			-0.001*** (0.007)			-0.001** (0.022)			-0.001* (0.073)
Constant	YES	YES	YES	YES	YES	YES	YES	YES	YES
Controls	YES	YES	YES	YES	YES	YES	YES	YES	YES
Year FE	YES	YES	YES	YES	YES	YES	YES	YES	YES
Industry FE	YES	YES	YES	YES	YES	YES	YES	YES	YES
Obs.	6,307	6,307	6,243	6,213	6,213	6,150	5,876	5,876	5,817
R <sup>2</sup>	0.231	0.232	0.232	0.201	0.201	0.200	0.155	0.156	0.155

**Table 10. Goodwill write-off**

This table presents the results from the regressions of acquirer's goodwill write-off on target's data breach experience, using the sample of deals with public targets. The dependent variable is *Acquirer goodwill write-off*, which is defined as the natural logarithm of the acquirer's goodwill write-off one year after the acquisition. *Tar. If breach* is defined as a dummy variable which equals 1 if the target experienced publicly known data breach events and otherwise 0. *Tar. Count breach* is defined as the natural logarithm of one plus the number of historical data breach events experienced by the target. *Tar. Amount breach* is defined as the natural logarithm of one plus the number of records exposed in the target's historical data breach events. The definitions of all variables are presented in the appendix. All regressions control for calendar year fixed effects and industry fixed effects. *p*-values based on standard errors adjusted for firm clustering are reported in parentheses. \*\*\*, \*\*, and \* indicate significance at the 1, 5, and 10% levels, respectively.

	Acquirer goodwill write-off		
	(1)	(2)	(3)
Tar. If breach	0.045*** (0.004)		
Tar. Count breach		0.061*** (0.000)	
Tar. Amount breach			0.005*** (0.002)
Controls	YES	YES	YES
Year FE	YES	YES	YES
Industry FE	YES	YES	YES
Obs.	1,174	1,174	1,174
R <sup>2</sup>	0.024	0.037	0.026

**Table 11.** Acquirers' data breaches

This table presents the results from the regressions of the change in the acquirer's data breach experience after deal completion on the target's data breach experience. The dependent variable is *Acquirer  $\Delta$ Count breach*, which is defined as the change in the number of acquirer data breach events from one (two, three) year(s) prior to deal announcement to one (two, three) year(s) after deal completion. *Tar. If breach* is defined as a dummy variable which equals 1 if the target experienced publicly known data breach events and otherwise 0. *Tar. Count breach* is defined as the natural logarithm of one plus the number of historical data breach events experienced by the target. *Tar. Amount breach* is defined as the natural logarithm of one plus the number of records exposed in the target's historical data breach events. *Acq. Count breach* is defined as the natural logarithm of one plus the number of data breach events experienced by the acquirer. The definitions of all variables are presented in the appendix. All regressions control for calendar year fixed effects and industry fixed effects. *p*-values based on standard errors adjusted for firm clustering are reported in parentheses. \*\*\*, \*\*, and \* indicate significance at the 1, 5, and 10% level, respectively.

	Acquirer $\Delta$ Count breach								
	$\pm 1$ year			$\pm 2$ years			$\pm 3$ years		
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Tar. If breach	0.156*** (0.000)			0.323*** (0.000)			0.414*** (0.000)		
Tar. Count breach		0.129*** (0.000)			0.258*** (0.000)			0.355*** (0.000)	
Tar. Amount breach			0.019*** (0.000)			0.035*** (0.000)			0.045*** (0.000)
Controls	YES	YES	YES	YES	YES	YES	YES	YES	YES
Year FE	YES	YES	YES	YES	YES	YES	YES	YES	YES
Industry FE	YES	YES	YES	YES	YES	YES	YES	YES	YES
Obs.	8,149	8,149	8,056	7,762	7,762	7,676	7,332	7,332	7,256
R <sup>2</sup>	0.065	0.066	0.067	0.111	0.112	0.113	0.140	0.144	0.143

**Table 12.** Days between announcement date and effective date

This table presents the results from the regressions of processing time on target's data breach experience. The dependent variable is *Days between announcement and effective dates*. *Tar. If breach* is defined as a dummy variable which equals 1 if the target experienced publicly known data breach events and otherwise 0. *Tar. Count breach* is defined as the natural logarithm of one plus the number of historical data breach events experienced by the target. *Tar. Amount breach* is defined as the natural logarithm of one plus the number of records exposed in the target's historical data breach events. The definitions of all variables are presented in the appendix. All regressions control for calendar year fixed effects and industry fixed effects. *p*-values based on standard errors adjusted for firm clustering are reported in parentheses. \*\*\*, \*\*, and \* indicate significance at the 1, 5, and 10% levels, respectively.

	Days between announcement and effective dates		
	(1)	(2)	(3)
Tar. If breach	10.590** (0.027)		
Tar. Count breach		8.983** (0.035)	
Tar. Amount breach			1.468** (0.011)
Acq. log Assets	8.243*** (0.000)	8.235*** (0.000)	8.235*** (0.000)
Acq. Tobin's q	1.860* (0.059)	1.872* (0.057)	1.865* (0.060)
Acq. Leverage	-24.108*** (0.003)	-23.932*** (0.003)	-23.877*** (0.003)
Acq. Free cash flow	-18.862* (0.064)	-18.736* (0.066)	-18.703* (0.066)
Acq. Stock price runup	7.272*** (0.006)	7.316*** (0.006)	7.131*** (0.007)
High tech	48.535*** (0.000)	48.718*** (0.000)	48.503*** (0.000)
Diversify	-10.272*** (0.00001)	-10.235*** (0.00001)	-10.087*** (0.00001)
Relative deal size	-9.510** (0.013)	-9.603** (0.012)	-9.343** (0.015)
All-cash deal	-13.444*** (0.00000)	-13.506*** (0.00000)	-13.503*** (0.00000)
All-stock deal	29.264*** (0.000)	29.212*** (0.000)	29.020*** (0.000)
Constant	24.909** (0.038)	24.688** (0.040)	24.854** (0.039)
Year FE	YES	YES	YES
Industry FE	YES	YES	YES
Obs.	8,146	8,146	8,053
R <sup>2</sup>	0.311	0.311	0.309

**Table 13.** Cross-sectional analyses

This table presents the results of the heterogeneity tests regarding industries, acquirers' financial positions, and the hire of due diligence advisors. Specifically, we examine the effects of the interactions between the target's data breach experience and three important industry, firm, and deal characteristics: *Vulnerable industry*, *Z-score*, and *If Acq. Big 4 DD*. The dependent variable is Acquirer CAR[-2, +2]. *Vulnerable industry* is a dummy variable which equals 1 if both the acquirer and the target are from industries vulnerable to data breaches and otherwise 0. Following Huang and Wang (2021), the following industries are classified as vulnerable: health (Fama-French code 11), personal services (33), business services (34), computer (35), electronic equipment (36), and transportation (40). *Z-score* is the Altman Z-score (Altman, 1968) of the acquirer. It is calculated as  $(1.2 * \text{working capital} + 1.4 * \text{retained earnings} + 3.3 * \text{income before extraordinary items} + 0.999 * \text{sales}) / \text{total assets}$ . *If Acq. Big 4 DD* is defined as a dummy variable which equals 1 if the acquirer hires one of the Big 4 (i.e. PricewaterhouseCoopers, KPMG LLP, Ernst & Young LLP, or Deloitte & Touche LLP) as its due diligence advisor and otherwise 0. In the table, the variable labelled 'Interaction' is representing either *Vulnerable industry*, *Z-score*, or *If Acq. Big 4 DD*. *Tar. If breach* is defined as a dummy variable which equals 1 if the target experienced publicly known data breach events and otherwise 0. *Tar. Count breach* is defined as the natural logarithm of one plus the number of historical data breach events experienced by the target. *Tar. Amount breach* is defined as the natural logarithm of one plus the number of records exposed in the target's historical data breach events. The definitions of all variables are presented in the appendix. All regressions control for calendar year fixed effects and industry fixed effects. *p*-values based on standard errors adjusted for firm clustering are reported in parentheses. \*\*\*, \*\*, and \* indicate significance at the 1, 5, and 10% levels, respectively.

Interaction=	Acquirer CAR[-2, +2]								
	Vulnerable industry			Z-score			If Acquirer Big 4 DD		
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Tar. If breach	-0.006 (0.268)			-0.017** (0.033)			-0.015*** (0.006)		
Tar. If breach * Interaction	-0.038** (0.024)			0.006* (0.072)			0.063** (0.049)		
Tar. Count breach		-0.004 (0.257)			-0.014** (0.037)			-0.011*** (0.006)	
Tar. Count breach * Interaction		-0.046** (0.037)			0.004** (0.041)			0.071* (0.052)	
Tar. Amount breach			-0.001 (0.341)			-0.002* (0.060)			-0.001** (0.033)
Tar. Amount breach * Interaction			-0.003 (0.210)			0.001** (0.042)			0.007** (0.045)
Interaction	-0.002 (0.710)	-0.001 (0.791)	-0.002 (0.674)	-0.002 (0.187)	-0.002 (0.173)	-0.002 (0.178)	-0.018*** (0.008)	-0.018*** (0.008)	-0.018*** (0.008)
Controls	YES	YES	YES	YES	YES	YES	YES	YES	YES
Year FE	YES	YES	YES	YES	YES	YES	YES	YES	YES
Industry FE	YES	YES	YES	YES	YES	YES	YES	YES	YES
Obs.	8,146	8,146	8,053	8,105	8,105	8,019	8,146	8,146	8,053
R <sup>2</sup>	0.146	0.147	0.146	0.148	0.149	0.150	0.154	0.154	0.153

**Table 14.** Firms' data breach experience and the likelihood of being a target

This table presents the regression analysis for acquisition propensity. The dependent variable is *Acquisition*, which equals 1 if a firm was successfully acquired by another firm in a given year and otherwise 0. *If Breach* is defined as a dummy variable which equals 1 if a firm experienced data breach incidents in the years before the announcement of the acquisition (shown in Column (1)), in the two years prior to the announcement of the acquisition (shown in Column (2)), or in the three years prior to the announcement of the acquisition (shown in Column (3)), and otherwise 0. *Count Breach* is defined as the number of historical data breach incidents experienced by the target in the years before the announcement of the acquisition (shown in Column (4)), in the two years prior to the announcement of the acquisition (shown in Column (5)), or in the three years prior to the announcement of the acquisition (shown in Column (6)). The definitions of all variables are presented in the appendix. All regressions control for calendar year fixed effects and industry fixed effects. *p*-values based on standard errors adjusted for firm clustering are reported in parentheses. \*\*\*, \*\*, and \* indicate significance at the 1, 5, and 10% levels, respectively.

	Acquisition (If a firm was a target)					
	History	2-year	5-year	History	2-year	5-year
	(1)	(2)	(3)	(4)	(5)	(6)
If Breach	0.110 (0.482)	0.045 (0.859)	0.044 (0.816)			
Count Breach				0.043 (0.770)	-0.045 (0.876)	-0.026 (0.894)
Ln Assets	-0.053*** (0.002)	-0.051*** (0.003)	-0.051*** (0.003)	-0.052*** (0.003)	-0.050*** (0.003)	-0.050*** (0.003)
Tobin's q	-0.064*** (0.007)	-0.063*** (0.007)	-0.063*** (0.007)	-0.064*** (0.007)	-0.063*** (0.007)	-0.063*** (0.007)
Leverage	-0.381** (0.039)	-0.385** (0.037)	-0.385** (0.037)	-0.384** (0.037)	-0.386** (0.036)	-0.386** (0.036)
Free cash flow	0.334** (0.036)	0.331** (0.038)	0.331** (0.038)	0.332** (0.037)	0.330** (0.039)	0.330** (0.039)
Earnings per share	-0.061*** (0.001)	-0.060*** (0.001)	-0.060*** (0.001)	-0.061*** (0.000)	-0.060*** (0.000)	-0.060*** (0.000)
Working capital	-0.588*** (0.002)	-0.591*** (0.002)	-0.590*** (0.002)	-0.590*** (0.0002)	-0.591*** (0.0002)	-0.591*** (0.0002)
Constant	-3.566*** (0.000)	-3.580*** (0.000)	-3.578*** (0.000)	-3.575*** (0.000)	-3.585*** (0.000)	-3.585*** (0.000)
Year FE	YES	YES	YES	YES	YES	YES
Industry FE	YES	YES	YES	YES	YES	YES
Obs.	74,245	74,245	74,245	74,245	74,245	74,245
Pseudo R <sup>2</sup>	0.025	0.025	0.025	0.025	0.025	0.025

**Table 15.** Horizontal/vertical acquisition and the choice of data-breached targets

This table examines the association between types of acquisitions and choosing data-breached targets. The dependent variable is *Tar. If breach*. It is defined as a dummy variable which equals 1 if the target experienced data breach events before the acquisition, and otherwise 0. *Horizontal* is defined as a dummy variable which equals 1 if the acquirer and target share the same NAIC industry code, and otherwise 0. *Vertical* is defined as a dummy variable which equals 1 if the acquisition is defined as a vertical merger, based on the acquirer and target, using the 2012 U.S. input-output industry-pair table, and otherwise 0. If the industries of the acquirer and the target exceed the 5% threshold of selling to or purchasing from each other, these two industries are defined as having a vertical relationship. *Unrelated* is defined as a dummy variable which equals 1 if the acquisition is neither a horizontal nor a vertical deal, and otherwise 0. The definitions of all variables are presented in the appendix. All regressions control for calendar year fixed effects and industry fixed effects. *p*-values based on standard errors adjusted for firm clustering are reported in parentheses. \*\*\*, \*\*, and \* indicate significance at the 1, 5, and 10% level, respectively.

	Tar. If breach		
	(1)	(2)	(3)
Horizontal	-0.317** (0.015)		
Vertical		0.323* (0.060)	
Unrelated			0.168 (0.193)
Acq. Ln Assets	0.281*** (0.000)	0.280*** (0.000)	0.287*** (0.000)
Acq. Tobin's q	0.134* (0.080)	0.143* (0.058)	0.132* (0.086)
Acq. Leverage	0.314 (0.398)	0.320 (0.384)	0.280 (0.451)
Acq. Free cash flow	0.613 (0.413)	0.655 (0.375)	0.640 (0.395)
Acq. Stock price runup	0.461** (0.023)	0.441** (0.030)	0.451** (0.026)
Public target	-0.831*** (0.000)	-0.880*** (0.000)	-0.867*** (0.000)
Private target	-2.226*** (0.000)	-2.234*** (0.000)	-2.231*** (0.000)
High tech	-0.262 (0.289)	-0.303 (0.225)	-0.286 (0.249)
Relative deal size	0.338*** (0.000)	0.332*** (0.000)	0.340*** (0.000)
All-cash deal	-0.055 (0.678)	-0.047 (0.719)	-0.056 (0.675)
All-stock deal	-0.289 (0.278)	-0.313 (0.240)	-0.312 (0.241)
Constant	-6.125*** (0.000)	-6.277*** (0.000)	-6.359*** (0.000)
Year FE	YES	YES	YES
Industry FE	YES	YES	YES
Obs.	8,108	8,108	8,108
Pseudo R <sup>2</sup>	0.171	0.170	0.170

**Table 16. Elapsed time since data breach incidents**

This table examines the time effect of the target's data breaches on the acquirer's announcement performance. We consider the time since the target experienced a data breach event using five time periods: Year [-1], Year [-2], Year [-3], Year [-4], and Year [-5], representing that data breach events occurred one, two, three, four, and five years prior to the acquisition, respectively. The dependent variable is *Acquirer CAR*[-2, +2]. It is the five-day cumulative abnormal return of the acquirer around the acquisition announcement, calculated using the CAPM. *Tar. If breach* is defined as a dummy variable which equals 1 if the target experienced data breach events in Year [-1], Year [-2], Year [-3], Year [-4], or Year [-5], and otherwise 0. *Tar. Count breach* is defined as the natural logarithm of one plus the number of data breach events experienced by the target in Year [-1], Year [-2], Year [-3], Year [-4], or Year [-5]. *Tar. Amount breach* is defined as the natural logarithm of one plus the number of records exposed in data breach events experienced by the target in Year [-1], Year [-2], Year [-3], Year [-4], or Year [-5]. The definitions of all variables are presented in the appendix. All regressions control for calendar year fixed effects and industry fixed effects. *p*-values based on standard errors adjusted for firm clustering are reported in parentheses. \*\*\*, \*\*, and \* indicate significance at the 1, 5, and 10% level, respectively.

Data breach in	Acquirer CAR[-2, +2]														
	Year [-1]			Year [-2]			Year [-3]			Year [-4]			Year [-5]		
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)
Tar. If breach	-0.020**			-0.025**			-0.017*			-0.007			-0.022		
	(0.027)			(0.018)			(0.076)			(0.545)			(0.170)		
Tar. Count breach		-0.017*			-0.033**			-0.014			-0.020			-0.029	
		(0.067)			(0.012)			(0.139)			(0.292)			(0.261)	
Tar. Amount breach			-0.002**			-0.002			-0.001			-0.002			-0.004
			(0.033)			(0.256)			(0.601)			(0.245)			(0.115)
Constant	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Controls	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Year FE	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Industry FE	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Obs.	8,146	8,146	8,146	8,146	8,146	8,146	8,146	8,146	8,146	8,146	8,146	8,146	8,146	8,146	8,146
R <sup>2</sup>	0.145	0.144	0.145	0.145	0.145	0.146	0.145	0.144	0.146	0.144	0.144	0.146	0.145	0.145	0.147

**Table 17.** Types of data breaches

This table presents the results from the regressions of the acquirer's cumulative abnormal return on the target's data breach experience using subsamples of deals based on five types of data breach events: bank card fraud, hack, stakeholder, lost, and unknown. The dependent variable is *Acquirer CAR*[-2, +2]. It is the five-day cumulative abnormal return of the acquirer around the acquisition announcement, calculated using the CAPM. *Tar. Count breach* is defined as the natural logarithm of one plus the number of historical data breach events experienced by the target. The definitions of all variables are presented in the appendix. All regressions control for calendar year fixed effects and industry fixed effects. *p*-values based on standard errors adjusted for firm clustering are reported in parentheses. \*\*\*, \*\*, and \* indicate significance at the 1, 5, and 10% level, respectively.

Type of data breach:	Acquirer CAR[-2, +2]				
	Bank card fraud	Hack	Stakeholder	Lost	Unknown
	(1)	(2)	(3)	(4)	(5)
Tar. Count breach	-0.005 (0.813)	-0.023** (0.036)	-0.018 (0.230)	-0.013* (0.055)	-0.050 (0.105)
Constant	YES	YES	YES	YES	YES
Controls	YES	YES	YES	YES	YES
Year FE	YES	YES	YES	YES	YES
Industry FE	YES	YES	YES	YES	YES
Obs.	8,146	8,146	8,146	8,146	8,146
R <sup>2</sup>	0.144	0.145	0.145	0.145	0.145

## Appendix

### Dependent variables

CAR[-2, +2]	Five-day cumulative abnormal return around the acquisition announcement, calculated using the market model. The market model parameters are estimated over the period (-241, -41), with the CRSP value-weighted return as the market index. Source: CRSP.
Combined CAR[-2, +2]	The market-value-weighted average of the acquirer's and the target's CAR[-2, +2]. Source: CRSP.
Premium	The offer price divided by the target's stock price four weeks prior to the announcement of the acquisition minus 1 (%). Source: SDC
$\Delta ROA$	The change in industry-adjusted (2-digit SIC) ROA from one (two, three) year(s) prior to deal announcement to one (two, three) year(s) after deal completion. E.g., suppose year 0 is the year of transaction. $\Delta ROA$ $(\pm 3 \text{ years}) = \frac{1}{3} \sum_{year=1}^3 ROA_{year} - \frac{1}{3} \sum_{year=-3}^{-1} ROA_{year}$
$\Delta \$Target \text{ CAR}$	The relative gain for the target, measured as the difference in dollar gains between the target and the acquirer, scaled by the sum of the acquirer's and the target's market values 50 days prior to the announcement date (Ahern, 2012; Cai and Sevilir, 2012): $\Delta \$Target \text{ CAR} = \frac{Target \text{ MV} \times T\text{CAR} - Acquirer \text{ MV} \times A\text{CAR}}{Acquirer \text{ MV} + Target \text{ MV}}$
Acquirer goodwill write-off	The natural logarithm of the acquirer's goodwill write-off one year after the acquisition.
Acquisition	A dummy variable which equals 1 if a firm was successfully acquired by another firm in a given year and otherwise 0.
<b>Data breach measures</b>	
Tar. If breach	A dummy variable which equals 1 if the target experienced publicly known data breach events and otherwise 0. Source: Privacy Rights Clearinghouse.
Tar. Count breach	The number of data breach events. It is defined as the natural logarithm of one plus the number of historical data breach events experienced by the target. Source: Privacy Rights Clearinghouse.
Tar. Amount breach	The number of records exposed in data breach events. It is defined as the natural logarithm of one plus the number of records exposed in the target's historical data breach events. Source: Privacy Rights Clearinghouse.
Acquirer $\Delta Count \text{ breach}$	The change in the number of data breach cases experienced by the acquirer, from one (two, three) year(s) prior to deal announcement to one (two, three) year(s) after deal completion. E.g., suppose year 0 is the year of the transaction, then $\Delta Count \text{ breach} (\pm 3 \text{ years}) = \sum_{year=1}^3 Count \text{ breach}_{year} - \sum_{year=-3}^{-1} Count \text{ breach}_{year}$

No. Acq. previous DB deals	The number of previous acquisition deals with a data-breach target made by the acquirer in the last five years.
If Breach	A dummy variable which equals 1 if the target experienced data breach events in any years before the announcement of the acquisition, in the two years prior to the announcement of the acquisition, or in the three years prior to the announcement of the acquisition, and otherwise 0. in the year
Count Breach	The number of data breach events in any years before the announcement of the acquisition, in the two years prior to the announcement of the acquisition, or in the three years prior to the announcement of the acquisition.

Firm characteristics	
Firm size	Natural logarithm of the book value of total assets (item6). Source: Compustat.
Tobin's Q	The ratio of the market value of assets to the book value of assets, (item6-item60+item25*item199)/item6. Acquirer characteristic. Source: Compustat.
Leverage	The ratio of the book value of debts (item34+item9) to the market value of total assets (item6-item60+item25*item199). Source: Compustat.
Free cash flow	Operating income before depreciation (item13) – interest expenses (item15) – income taxes (item16) – capital expenditures (item128), scaled by the book value of total assets (item6). Source: Compustat.
Stock price runup	The buy-and-hold abnormal return (BHAR) during the period (–210, –11). The market index is the CRSP value-weighted return. Source: CRSP.
Vulnerable industry	A dummy variable which equals 1 if both acquirer and target are from vulnerable industries and otherwise 0. Following Huang and Wang (2021), the following industries are classified as vulnerable: health (Fama-French code 11), personal services (33), business services (34), computer (35), electronic equipment (36), and transportation (40).
Z-score	The Altman Z-score (Altman, 1968) of the acquirer, which is calculated as $(1.2 * \text{working capital} + 1.4 * \text{retained earnings} + 3.3 * \text{income before extraordinary items} + 0.999 * \text{sales}) / \text{total assets}$ .

Transaction characteristics	
Public target	A dummy variable which equals 1 if the target firm is a public firm. Source: SDC.
Private target	A dummy variable which equals 1 if the target firm is a private firm. Source: SDC.
High tech	A dummy variable which equals 1 if the acquirer and target are both from high-tech industries, as defined by Loughran and Ritter (2004), and otherwise 0. Loughran and Ritter (2004) define tech stocks as those in SIC codes 3571, 3572, 3575, 3577, 3578 (computer hardware), 3661, 3663, 3669 (communications equipment), 3671, 3672, 3674, 3675, 3677, 3678, 3679 (electronics), 3812 (navigation equipment), 3823, 3825, 3826, 3827, 3829 (measuring and

	controlling devices), 3841, 3845 (medical instruments), 4812, 4813 (telephone equipment), 4899 (communications services), and 7371, 7372, 7373, 7374, 7375, 7378, 7379 (software). Source: Compustat.
Diversify	A dummy variable which equals 1 if the acquirer and target do not have the same two digits at the start of their SIC codes and 0 otherwise. Source: SDC.
Relative deal size	The ratio of the transaction value to the acquirer's market value of equity as defined above. Source: SDC.
All-cash deal	A dummy variable which equals 1 for fully cash-financed deals, and otherwise 0. Source: SDC.
All-stock deal	A dummy variable which equals 1 for fully stock-financed deals, and otherwise 0. Source: SDC.
Horizontal	A dummy variable which equals 1 if the acquirer and target share the same NAIC industry code, and otherwise 0 (Ahern and Harford, 2014).
Vertical	A dummy variable which equals 1 if the acquisition is defined as a vertical merger using the 2012 U.S. input-output industry-pair table, and otherwise 0. A vertical relationship between the industries of the acquirer and target is based on whether one industry exceeds the 5% threshold of either selling to or purchasing from the other industry. (Ahern and Harford, 2014).
Unrelated	A dummy variable which equals 1 if the acquisition is neither a horizontal nor a vertical deal, and otherwise 0.
If Acq. Big 4 DD	A dummy variable which equals 1 if the acquirer hires PricewaterhouseCoopers, KPMG LLP, Ernst & Young LLP, or Deloitte & Touche LLP as its due diligence advisor, and otherwise 0.

---