M&A and Cybersecurity Risk: Empirical Evidence

Gabriele Lattanzio[ϕ]
(University of Melbourne)

Jérôme P. Taillard[∞]
(Babson College)

Abstract

We document that low cybersecurity risk firms are more likely to be involved in M&A transactions. Mergers are significantly less likely to be withdrawn if the target has a weak cybersecurity risk profile. Merger premium are higher for mergers involving low cybersecurity risk acquirers. Deals involving low cybersecurity risk firms yield superior post-merger operating performance and are less likely to trigger goodwill impairments. Announcement returns have also started to reflect cybersecurity risk in recent years. These findings offer novel evidence on the economic impact of cybersecurity risk on the market for corporate control.

Keywords: Mergers and Acquisitions; Cybersecurity Risk; M&A Withdrawal; Valuation.

JEL Classification: G30; G34; M15.

[ϕ] University of Melbourne, Faculty of Business and Economics, Barkley Street 198, 12.054, Melbourne, 3000., Australia. E-mail address: Gabriele.lattanzio@unimelb.edu.au
[∞] Babson College, Department of Finance, 231 Forest St, Babson Park, MA 02457, United States. E-mail address: jtaillard1@babson.edu

The authors thank Manuel Adelino, Emanuele Bajo, Simon Gervais, Laurie Krigman, Daniel Rabetti, and David T. Robinson, and seminar and conference participants at the University of Bologna, Babson College, Duke University, Durham University, European FMA 2022, World Finance Conference 2022, Global Finance Conference 2022, and AFFI 2022 for their insightful comments. All errors are ours.

Introduction

The 2021 Fortune 500 CEO survey documents that two thirds of the interviewed CEOs consider cybersecurity risk as their greatest concern, far exceeding the risks presented by political instability and climate change.[1] The implications of this new and rising source of risk are potentially more severe in the context of mergers and acquisitions (M&A). Indeed, M&A transactions offer sophisticated cyber terrorists a clear opportunity to target the firms involved (IBM, 2019). For instance, the process of data migration and integration related to an acquisition is complex and exposes valuable data to potential cyberattacks (Henningsson et al., 2018, Okafor, 2021),[2] and media coverage of large M&A deals can heighten these concerns by attracting the attention of cyber terrorists. Further, target firms may also carry with them undisclosed or otherwise unidentified cyber-related liabilities that will be transferred to the acquirer upon deal completion.[3] These factors can exacerbate cybersecurity concerns during all phases of a deal, from initial search, to post-merger integration. However, there is little empirical evidence of whether and how cybersecurity risk drives firms' decision to engage in M&A transactions, nor of its ultimate impact on mergers outcomes. Our study aims to fill this gap.

The importance of cybersecurity in the M&A process is exemplified by the threat posed by *past* cybersecurity weaknesses at the target firm, as highlighted by two recent cases. In 2017, the price tag of Verizon's acquisition of Yahoo's internet business was cut by $350 million after Yahoo disclosed three previously undisclosed massive data breaches compromising more than one billion customer accounts.[4] In another example, Marriott Hotels was fined $23.8 million for a data breach affecting the Starwood Hotels group that occurred in 2014, two years *prior* to its acquisition by Marriot Hotels. The fine was levied by the Information Commissioner's Office (ICO) in the U.K. where the breach affected seven million users.[5]

Building on these observations, we begin by investigating whether firms' cybersecurity exposure is a significant determinant of M&A involvement, either as an acquirer or a target. Using

[1] https://fortune.com/2021/05/21/fortune-500-ceo-survey-post-pandemic-profits-revenue-cybersecurity-risk/
[2] In 2019, the IBM Institute for Business Value (IBV) published a survey of 720 executives responsible for the M&A functions at acquirer organizations. More than 33% of them stated their firm experienced data breaches that can be attributed to M&A activity during integration.
[3] Similar to environmental liabilities under the Comprehensive Environmental Response, Compensation, and Liability Act, 42U.S.C. §§9601- 9675 ("CERCLA"), undisclosed and unidentified cybersecurity-related liabilities are transferred to the acquiring firm following the successful completion of the transaction.
[4] https://www.verizon.com/about/news/verizon-and-yahoo-amend-terms-definitive-agreement
[5] https://www.bbc.com/news/technology-54748843

text-based measures of cybersecurity risk developed in recent studies (Lattanzio and Ma, 2023, and Florackis et al., 2022), we show that low cybersecurity risk firms are significantly more likely to engage in M&A. These findings are consistent with the hypothesis that pre-existing cybersecurity-related liabilities and post-merger IT integration concerns might preclude firms with high cybersecurity risk from doing deals. Furthermore, we show that - conditional on being involved in an M&A transaction - firms with stronger cybersecurity profiles are more likely to merge. This result suggests that low cybersecurity risk firms display a strong preference for avoiding high cybersecurity risk targets.

Importantly, cybersecurity measures do not proxy for Corporate Social Responsibility (CSR) features of firms involved in M&A activity. It is plausible that cybersecurity risk exposure could be higher for firms displaying low levels of social engagement, and more generally lower ESG scores. For instance, firms with perceived poor corporate social responsibility (CSR) may be more likely the target of activists (e.g., see Goldman (2012)). These firms could also be more at risk because their governance structure is such that they were less likely to invest in their cybersecurity infrastructure in the first place (Lending et al., 2018). However, we show that cybersecurity risk measures exhibit almost no correlation with CSR ratings for the firms in our sample. Furthermore, our finding that low cybersecurity risk firms are significantly more likely to engage in M&A is robust to adding CSR ratings among our set of control variables.

Next, we examine how the cybersecurity profiles of two merging firms affect market reaction at merger announcement. We find no significant effects over the full sample period. However, we document that the market reacts more positively to merger announcements involving an acquirer with a low cybersecurity-risk profile in recent years and in periods of heightened cybersecurity concerns. This result is consistent with Florackis et al. (2022) and Lattanzio and Ma (2023) who find evidence of increasing investors' cybersecurity risk awareness over time.

In terms of the M&A process, we document that attempted mergers are significantly less likely to be withdrawn when the target has low cybersecurity risk. This result is indicative of the importance of cybersecurity risk to the likelihood of deal completion. It also highlights how the

due-diligence process is an essential step in assessing corporate cybersecurity risk in the M&A context.[6]

Finally, we show that the outcome of this evaluation process is reflected in the merger premium, which appears to be systematically higher for low cybersecurity acquirers. This finding is consistent with low cybersecurity acquirers being better able at capturing synergies from the deal by being better positioned to manage the challenging task of data migration and integration (Sarrazin and West, 2011). Consistent with this interpretation, we document that mergers involving low cybersecurity risk firms achieve higher post-merger operating performance and are less likely to incur goodwill write-offs over the three years following the deal completion.

Taken together, our evidence is consistent with cybersecurity risk posing a significant threat throughout the merger process, from the likelihood of being attempted in the first place, to the likelihood of being completed through to the post-merger integration phase.

Our study makes several contributions to the literature. First, this paper shed lights on how cybersecurity risk influences the market for corporate control. A growing literature has been investigating the real consequences of cybersecurity risk. Increased cybersecurity risk – and the growing threat emerging from the digitalization of the U.S. economy - has resulted in increased cost of capital (Havakhor, Rahman, and Zhang, 2021; Huang and Wang, 2021; Ashraf and Saunders, 2022, Jiang, Khanna, and Yang, 2021, Florackis, Louca, Michaely, and Weber, 2022, Binfarè, 2021), reduced returns on investments in R&D (Lattanzio and Ma, 2023, Ettredge et al., 2018), the destruction of reputational capital (Akey, Lewellen, Liskovich, and Schiller, 2021), and lower capital investments, profitability and lower executive compensation (Kamiya et al., 2020). While the majority of these studies focus on the implications of successful cyberattacks, we build on recent studies and exploit cyber-related disclosures for the population of U.S. publicly-traded firms to assess how *ex-ante* corporate cybersecurity risk exposure affects economic agents' behavior with regards to significant corporate transactions – namely mergers and acquisitions. To the best of our knowledge, this is the first comprehensive analysis examining how cybersecurity

[6] Our measure of cybersecurity risk exposure is based solely on publicly available information. We would thus expect it to serve only as an indicator of actual exposure. As such, a detailed due-diligence process is more likely to uncover any potential liability and/or any cybersecurity threats that could jeopardize a given deal.

concerns shape the behavior of both acquiring and target firms in the context of merger transactions.[7]

Second, our study contributes directly to the literature analyzing the determinants of M&A activity and sources of synergistic gains.[8] In particular, we complement previous studies by identifying and studying the implications of a previously overlooked source of risk – cybersecurity risk – on the likelihood of merger transactions and their successful completions.[9]

The remainder of the paper proceeds as follows. In section 1 we develop and present our hypothesis. Section 2 describes the data, provides summary statistics for the variable of interest, and outlines our empirical strategy. Section 3 discuss our main empirical results. Section 4 concludes.

1. Hypothesis Development

1.1. Corporate Cybersecurity Profile and M&A Market Participation

Cybersecurity poses unique challenges to corporations nowadays. The consequences of firms' exposure to this emerging source of risk are particularly prominent in the context of M&A transactions, as both buyers and sellers are exposed to a wide array of both internal and external cyber threats when executing deal terms (IBM, 2019). First, undisclosed and unidentified cybersecurity-related liabilities are transferred to acquiring firms following the successful completion of the transaction. Given that these liabilities are often not directly observable ex ante,

[7] Henningsson et al. (2018) offer a comprehensive literature review on the importance of information system integration processes in M&A transactions. While this related topic has been extensively investigated in the literature, available evidence is still largely based on case studies and industry specific analyses focusing on the outcome of these deals. As such, our study provides novel large sample evidence concerning the ex-ante consequences of cybersecurity risk exposure on large corporate investments.

[8] Recent studies identify many factors affecting firms' propensity to engage in M&A transactions. For instance, stock overvaluation (Shleifer and Vishny, 2003; Rhodes-Kropf and Viswanathan, 2004), economic, regulatory, and technological shocks (Harford, 2005; Mitchell and Mulherin, 1996) might initiate merger waves. Similarly, improved resource allocation and product differentiation (Lichtenberg and Siegel, 1987; Healy, Palepu, and Ruback, 1992; McGuckin and Nguyen, 1995; Maksimovic and Phillips, 2001; Schoar, 2002; Hoberg and Phillips, 2010; Maksimovic, Phillips, and Prabhala, 2011), interest tax shields (Devos, Kadapakkam, and Krishnamurthy, 2009; Fee, Hadlock, and Pierce, 2012), improvements in product quality (Sheen, 2014), to improvements in structured management practices (Bai, Jin, and Serfling, 2021), corporate culture similarities (Bereskin, Byuun, Officer, and Oh, 2018; Deng, Kang, and Low, 2013), similarity in political attitudes among employees (Duchin et al., 2021) and environmental concerns (Bai, Chu, Shen, and Wan, 2021), among others, have been documented as major drivers of synergistic gains in M&A transactions.

[9] Sun, Wei, and Xie (2020) analyze the impact of the passage of mandatory disclosure laws related to data breaches on M&A activity. Their analysis is performed at a more aggregated level using industry-level data. They find that more data-intensive industries see significantly more M&A activity after the enaction of such laws.

firms featuring weak cybersecurity profiles might (1) make for less desirable targets; and (2) be more reluctant to attempt an acquisition.

Second, the data and IT systems integration process that takes place in the aftermath of a successful M&A deal offers sophisticated cyber terrorists an opportunity to target the firms involved (IBM, 2019). During such a process, both customers' data (Kamyia et al., 2020) and trade secrets (Lattanzio and Ma, 2023) might be potentially misappropriated.

Third, the data migration and integration process through which merged firms consolidate their IT systems are challenging from an operational perspective. IT breaches as well as unexpected compatibility issues between the technological structures used by the merging firms might result in large economic and financial costs, which could undermine the realization of the synergistic gains expected from the deal.[10] Cybersecurity risk may thus not only affect firms' propensity to engage in M&A transactions, but also pressure interested acquirers to seek targets with low cybersecurity risk to reduce the likelihood of post-merger integration challenges.

As a result, we hypothesize that the likelihood of a firm to be involved in an M&A transaction – either as a target or as an acquirer - declines as its cybersecurity risk exposure increases. Relatedly, we posit that low cybersecurity risk acquirers are more likely to initiate a merger transaction with low cybersecurity risk targets. Expressed in null form:

H1: The likelihood of a firm becoming an acquirer (target) in a merger deal is negatively related to its cybersecurity risk exposure.

H2: Attempted deals are more likely to involve two firms with low levels of cybersecurity risk.

An alternative hypothesis could posit that firms with strong cybersecurity risk profiles might be able to reap greater synergies from targeting firms with weak cybersecurity risk profiles. The premise in this case is that the acquirer could implement its cybersecurity best practices in the target firm's operations during the post-merger integration process, unlocking economic value (e.g., Wang and Xie, 2009). Conversely, a target with a strong cybersecurity profile might make for a more desirable target for an acquirer with a weaker profile. The target' s strengths and know-how in cybersecurity competences could indeed be transferred to the acquiring firm, similarly to any core competence that might be sought after by a potential suitor.

[10] Sarrazin and West (2011) estimate that the realization of about 45% of the expected benefits emerging from a M&A deal depends upon the successful successful completion of the information system integration process.

1.2. Cybersecurity Risk and the Market Reaction to Merger Announcement

Recent studies document that cybersecurity concerns are perceived as a material risk by investors, ultimately inducing a positive and significant effect on stock returns (Jamilov et al., 2021; Jiang, Khanna, and Yang, 2021; Florackis, Louca, Michaely, and Weber, 2022). The materiality of cybersecurity risk is further confirmed by investors' negative reaction to the occurrence and disclosure of successful data breaches results (He et al. 2019; Li et al. 2016; Amir et al. 2018; and Kamiya et al. 2020), despite both the economic severity and overall magnitude of these events still being a contentious issue (Richardson, Smith and Watson 2019; Hilary; Segal and Zhang 2019, Lattanzio and Roner, 2021).

Since M&A transactions expose both target and acquiring firms to material cybersecurity threats, one should thus expect the market to take a more favorable stance on deals where the merging parties feature a low cybersecurity risk profile.[11]To test this prediction, we investige cumulative abnormal returns (CAR) around merger announcements and test the following null hypothesis:

H3: The market reaction to mergers announcement is more favorable for deals involving low cybersecurity risk firms.

As before, an alternative hypothesis could posit that deals including an acquirer (target) with a strong cybersecurity risk profile and a target (acquirer) with a weak cybersecurity risk profile could see an overall more positive stock market reaction due to the potential for greater synergistic gains if the strong cybersecurity risk profile can be extended to the merged entity.

Note that hypothesis *H3* does not depend on markets prices fully incorporating cybersecurity risk exposure prior to deal announcement. Rather, it requires first that the cybersecurity profile of the combined firms is different than the cybersecurity profile of the two standalone firms. In that case, the merger announcement will convey novel information. Second, as long as market participants consider cybersecurity risk exposures as inputs into their assessment of the deal, we can expect this novel information to elicit a market reaction.

[11] As the cybersecurity profile of the merged entity is unlikely to be equal to a weighted average of the cybersecurity profiles of the two stand-alone firms, the merger announcement might indeed provide novel and material information on this dimension.

1.3. *Cybersecurity Risk and Merger Withdrawals*

Mergers and acquisitions are capital intensive investments whose economic and financial consequences are carefully scrutinized by investors, regulators, and other stakeholders (Jacobsen, 2014; Deng et al, 2013; Cunningham, Ederer, Ma, 2021; Arnold, 2020; among others). Furthermore, managers of the acquiring firm go through a detailed overview of the targets' financial and operating performance during the due diligence period, gaining access to private and confidential information that are not directly observable to outsiders (Wangerin, 2019). During this evaluation process, liabilities – either unknown or undisclosed – might be identified and the acquirer can develop a better understanding of the potential synergies of the deal and its willingness to go through with the deal. The quality of this cybersecurity due-diligence process could be a function of the acquirer's own cybersecurity-related profile.

The involvement of a large number of parties and the possibility of identifying material weaknesses in the target's technological infrastructure during the due diligence period might thus cause initiated deals to fail.[12] Supporting this contention, a recent survey by the law firm Freshfields Bruchkhaus Deringer documents that 83% of the surveyed CEOs stated that a deal could be abandoned if cybersecurity breaches are identified during the due diligence or mid-transactions phases.[13] We thus hypothesize that mergers involving low cybersecurity risk corporations should be significantly less likely to be terminated. That is, in null form:

H4: The likelihood of an initiated merger withdrawal is lower when the acquirer (target) firms involved feature low cybersecurity risk levels.

1.4. *Cybersecurity Risk and Deal Valuation*

As previously discussed, the process of data migration and IT system integration conducted in the immediate aftermath of the deal completion is complex and highly challenging (Henningsson et al., 2018). During the post-merger integration process, high-value data including customers' information and trade secrets are exposed to potential cyberattacks. Furthermore, unexpected compatibility issues might raise operational concerns, ultimately undermining the realization of the synergistic gains expected from the merger. This risk should be reflected in

[12] Recent analyses document that about 15% of initiated mergers are ultimately withdrawn (Liu, 2019; Madura, Ngo, and Viale, 2012).

[13] Freshfields Bruckhaus Deriger, 2015. Cybersecurity in M&A. Available at https://www.freshfields.com/4ac9b5/globalassets/campaign-landing/cyber-security/ma-cyber-security-report.pdf

takeover premiums. Specifically, the merger premium captures the synergies generated through the combination of the two businesses that accrue to target shareholders. As long as a portion of the synergies are captured by the target firm's shareholders, a lower cybersecurity risk profile of the target should result in greater realized synergies and hence a greater premium to be captured. In null terms:

H5A: Takeover premiums are higher for deals where the target has a low cybersecurity risk profile.

As the acquirer is ultimately the entity managing such a complicated process, we expect the premium to be increasing in the acquirers' cybersecurity profile as well. The reasoning echoes findings reported in Sarrazin and West (2011): as long as the target can capture some of the synergies generated by the deal (through a higher premium), an acquirer that has a stronger cybersecurity risk profile will be better able to generate synergies (e.g., fewer post-merger integration challenges) and that should ultimately result in a higher premium paid.

H5B: Takeover premiums are higher for deals where the acquirer has a low cybersecurity risk profile.[14]

1.5. *Cybersecurity Risk and Post-Deal Performance*

Do the aforementioned synergistic gains materialize after the successful completion of the merger? If this is the case, the post-merger performance of low cybersecurity risk consolidated firms should be systematically higher than that of their high risk counterparties. That is, in null terms:

H6A: Deals involving low cybersecurity risk corporations should result in higher post-merger accounting performance than those involving high cybersecurity risk firms.

Similarly, if corporations featuring a stronger cybersecurity risk profile are better equipped to navigate the process of data migration and IT system integration conducted in the aftermath of the deal completion as well as potential compatibility and technological issues, one would expect low

[14] Note that, as with hypothesis *H3* above, hypotheses *H5A* and *H5B* do not depend on markets prices fully incorporating cybersecurity risk exposure prior to announcement. Rather, they assume that on average, acquirers will offer a cybersecurity premium in their offers for low cybersecurity risk targets as target shareholders will recognize that the realization of synergy gains is more likely in such circumstances.

cybersecurity risk deals to be less likely to trigger material goodwill impairments. Goodwill is an accounting asset recognized at the merger closing date representing the value paid by the acquirer for the target in excess of the target's book value of net assets. That is, under current accounting rules (SFAS 141 and SFAS 142 and following updates), goodwill represents "the portion of the premium related to expected synergies". Importantly, the Financial Accounting Standards Board (FASB) mandates firms to test this accounting item for impairment on a yearly basis. The eventually resulting write-offs are generally interpreted as original misvaluations of (or unexpected declines in) the synergies originated from the deal itself (Gu and Lev, 2011). Consequently, in null form, we posit that:

H6B: Low cybersecurity risk deals are less likely to trigger a goodwill impairment than their high cybersecurity risk counterfactuals over the post-acquisition period.

2. Data and Summary Statistics

2.1. *Measuring Cybersecurity Risk*

Recent studies develop measures of firms' ex-ante exposure to cybersecurity risk based on their cybersecurity disclosure practices (Gordon et al., 2006; 2010; Lawrence et al., 2018; Ettredge et al., 2018; Florackis et al., 2022; Jamilov et al., 2021, Lattanzio and Ma, 2021).[15] In particular, these papers rely on textual analyses of firms' 10-Ks to assess a firm's cybersecurity profile. Despite using different approaches, the resulting scores exhibit comparable time-series and cross-industry distributions, and they have all been extensively validated by documenting that these proxies have economically material predictive power with respect to future occurrences of data breaches. For the purposes of this study, we use the Florackis, Louca, Michaely, and Weber (2022) cybersecurity score as our primary proxy. This score is built on the premise that firms that actually suffered from a cyberattack are more vulnerable to cybersecurity risk *ex-ante*. Under the assumption that this expectation is (at least partially) reflected in firms' disclosure, firms using similar words to describe their cybersecurity risk profile to those that actually suffer an attack should feature similarly high level of ex-ante cybersecurity risk exposure.

[15] Another stream of papers relies on cybersecurity breaches detected ex post (e.g., Hinz et al. (2015), Kamiya et al., 2020), Makridis (2022)). However, Francis, Hu, and Shohfi (2021) show that such an approach, which relies on newsworthy successful cyberattacks, can lead to sample selection issues. Alternatively, Liu and Makridis (2022) attempt to identify actual cybersecurity vulnerabilities through network scans.

The Florackis et al. (2022) cybersecurity measure is available for the period 2007-2018 for 44,972 firm-year observations and allows us to rank firms based on their ex-ante exposure to cybersecurity risk. As we are interested in identifying firms with low cybersecurity risk exposures, we define a *Low Cybersecurity Risk (Tercile, Quartile, or Quintile)*$_{i,t}$ indicator variable identifying firms included in the first tercile, quartile, or quintile of the Florackis et al. (2022) cybersecurity score distribution respectively.[16] All our results are robust to the use of the Lattanzio and Ma (2021) cybersecurity score. Their 10-K based measure of cybersecurity risk is available for the period 2001-2019 and features a 61% in-sample correlation with the Florackis et al. (2022) measure. To avoid redundancy, all results based on this alternative cybersecurity score are available in the Online Appendix.

2.2. *Merger and Acquisitions Data*

We construct our initial sample by gathering data for all announced U.S. mergers and acquisitions between 2007 and 2018 from the Thomson Reuters Financial Securities Data Company (SDC Platinum). Following the existing literature (Deng et al., 2013; Bena and Li, 2014; Bereskin et al., 2018; Bai et al., 2021), we include in our sample all attempted mergers involving U.S. acquirers and targets and we require that the acquiring firms control less than 50% of the shares of the target firms before the deal announcement, are seeking to own more than 50% of the target firm, and own more than 90% of the target firm after deal completion for the subsample of completed deals. We also filter out deals with a value lower than $1 million and for which either the acquirer or the target is not covered by Compustat/CRSP. This sample selection results in 607 deals between 2007 and 2018 for which full information are available.[17]

Building on the established methodology discussed in Bena and Li (2014), we further construct a control sample including pseudo acquirer-target pairs. In particular, for each actual merger included in our sample, pseudo deals are formed by matching each actual acquirer (target) with up to five matched pseudo-targets (pseudo-acquirers). The matching is executed based on the

[16] We are grateful to the authors for sharing their data. The tercile (quartile, and quintile) indicators are defined yearly using the full sample provided by the authors. We also recognize that Sustainalytics and KLD report potentially viable measures capturing firms' cybersecurity profile. In particular, Sustainalytics reports a score describing the quality of a firm's policy statement on data privacy (S_3_1_3) and KLD includes an indicator variable set equal to 1 if the firm has material privacy and data security concerns (PRO_con_G). However, the Sustainalytics variable is available for only approximately 150 firms per year over the period from 2009 to 2019, generating only 73 matches with our sample. Similarly, the KLD variable is only available for the period from 2015 to 2018, generating a negligible number of matches with our sample of M&A transactions.

[17] The Online Appendix reports all our tests based on the Lattanzio and Ma (2021) cybersecurity risk measure. Importantly, since their measure is available for 39,033 firm-year observations for the period 2001-2019, the relevant sample expands to include 964 mergers when we use their alternative cybersecurity proxy.

actual target (acquirer)'s characteristics including industry-year (SIC3 digit), firm size (log of total assets), and book-to-market ratio as in Bena and Li (2014).[18] That is, for each deal announced in year *t* we identify up to ten firm-pairs, that includes up to five actual acquirer – pseudo-targets pairs and up to five pseudo acquirer – actual target pairs.[19] Similarly to previous studies, there are several deals for which we are unable to find 10 matching pseudo pairs. Our control sample includes 4,251 pseudo mergers, including 1,609 unique pseudo acquirers and 1,573 unique pseudo targets; that is, each actual deal is matched to an average of 7 pseudo mergers.

2.3. Dependent Variables and Other Control Variables

Our tests are related to six key outcomes related to the M&A process: (1) likelihood of being active in the M&A market; (2) likelihood of being a merger pair; (3) market reaction to the merger announcement; (4) likelihood of an initiated merger being withdrawn; (5) determinants of the merger premium; (6) post-merger performance.

For the first set of tests (likelihood of being active in the M&A market), our dependent variable are $Actual\ Acquirer_{i,t}$ *(Actual Target* $_{i,t}$*),* an indicator variable set equal to one if firm *i* is the acquirer (target) in an M&A transaction at time *t*, zero otherwise. For the analysis assessing the likelihood of being a merger pair, the dependent variable, $Actual\ Merger_{d,t}$, is an indicator variable set equal to one for the combination of firms (acquirer-target pair) that initiates a merger transaction in year *t*, zero otherwise.

Our dependent variables for tests on short-term market reactions at announcement are the acquirer, target, and combined stock's cumulative abnormal returns (CAR) estimated around the announcement date. CARs are estimated over a three-day windows using Fama-French four-factor model where the market factor is based on CRSP value-weighted returns, and the remaining three factors include: small-minus-big (SMB), high-minus-low (HML), and momentum (MOM). The

[18] As discussed in Bereskin et al. (2018), these matching criteria are intended to control for time, industry, firm size, growth opportunities, and overvaluation. These factors have indeed been shown to drive M&A deals (see, for instance, Andrade, Mitchell, and Stafford, 2001; Shleifer and Vishny, 2003; Rhodes-Kropf and Viswanathan, 2004; Harford, 2005; and Rhodes-Kropf and Robinson, 2008). Similarly, by matching on industry, size, and book-to-market this methodology also mitigates concerns related to the heterogeneity in firms' strategic commitment towards cybersecurity investments (Kamiya et al., 2020; Lattanzio and Ma, 2021; Dhyne; Konings, Van den bosch, and Vanormelingen, 2021).

[19] Pseudo acquirers and pseudo targets are selected so that they are neither an acquiring firm, nor a target firm in the three years preceding the deal.

parameters of the four-factor model are estimated over the window [-300,-101] relative to the corresponding event's date.

For the tests assessing the likelihood of the merger being withdrawn, our dependent variable, $Withdrawn_{d,t}$ is an indicator variable set equal to 1 if the deal is withdrawn, zero if it is successfully completed. Finally, our last array of tests uses $Merger\ Premium_{d,t}$ as our dependent variable, defined as the ratio between the target final equity valuation relatively to its market capitalization as observed 4 weeks prior to the initial offer.

With respect to evaluating acquirers' post-merger performance, we use two different dependent variables. First, following extant literature (Wang and Xie (2009), Custodio (2014), Qian and Zhu (2018), among others), we use return on assets (ROA) as a measure of profitability. ROA has the advantage of being unaffected by changes in capital structure or by the presence of unusual and non- recurring items, and it has been shown in simulations to be superior to any other commonly use proxy in detecting abnormal operating performance (Barber and Lyon (1996)). Second, we construct an indicator variable set equal to 1 if the acquirer report a goodwill impairment over the three years from the completion of the acquisition, zero otherwise.[20]

We complete our sample by including a set of (1) firm-level controls – including Firm Size, Tobin's Q, Cash Holdings, Leverage, R&D to Sales, ROA, as well as governance controls including % Institutional Ownership and a dummy indicator for staggered board,[21] and the 3-digit SIC code Herfindahl–Hirschman Index – and (2) deal-level controls – including whether the deal is a tender offer, an indicator variable identifying horizontal acquisitions, an indicator variable for whether the deal was fully paid for in cash, and an indicator flagging withdrawn mergers. All variables are defined in the Appendix.

2.4. Summary Statistics

Table 1 presents summary statistics. Panel A (Panel B) of Table 1 reports descriptive statistics for actual acquirers and targets, as well as for unique pseudo acquirers and targets.[22] Consistent with cybersecurity risk negatively affecting firms' M&A activity, the documented

[20] No acquisition included in our sample was completed using pooling accounting.
[21] We are grateful to Matthew Serfling for sharing his staggered board data from Guernsey, Guo, Liu, and Serfling (2022) on his website: https://sites.google.com/utk.edu/matthew-serfling/data.
[22] All continuous variables are winsorized at the 1% level.

univariate statistics strongly suggest that low cybersecurity risk firms are significantly more likely to be involved in a merger transaction than their more exposed peers. Looking at firm characteristics, acquiring firms are significantly larger, have a substantially higher profitability, measured in terms of ROA, and have higher market valuation multiples (Tobin's Q) than both targets and pseudo acquirers (Harford, Jenter, and Li, 2011; Bena and Li, 2014; Bereskin et al., 2018).[23]

With respect to the characteristics of the deal included in our sample, Panel C of Table 1 documents that about 18% are tender offer, 86% are horizontal acquisitions, 67% are all cash deals, and 24% of the selected deals are ultimately withdrawn.

Finally, Table 1, Panel D (Column 1) provides the time-series distribution of our deal announcements, which matches relatively well to that of the U.S. domestic M&A market over the last two decades (Lattanzio, Megginson, and Sanati, 2021). As previously mentioned, all the findings reported in this study are robust to the use of the Lattanzio and Ma (2021) cybersecurity score. This alternative 10-K based measure of cybersecurity risk is available for the period 2001-2019 and features a 61% in-sample correlation with the Florackis et al. (2022) measure. In order to avoid redundancy, we report all our estimates based on this alternative cybersecurity score in the Online Appendix. However, Table 1, Panel D (Column 2) provides the complete time-series distribution of the 964 mergers included in this alternative sample. The two time-series follow similar trends, which provides internal consistency between the estimates reported in this paper and the robustness tests available in the Online Appendix.

Overall, our sample is comparable to those used in other studies such as Bena and Li (2014), Moeller, Schlingemann, and Stulz (2004), Lee, Mauer, and Xu (2018), and Bereskin et al. (2018).

[Table 1 About Here]

3. Empirical Results

3.1. *Cybersecurity Risk and Merger Activity*

We begin our analysis by testing whether cybersecurity risk negatively impacts firms' M&A activity (*H1).* If this is the case, we expect firms with low cybersecurity risk exposures to

[23] The statistical differences between the actual and pseudo acquirers and targets are similar those reported in Bena and Li (2014) and Bereskin et al. (2018), validating the execution of our matching procedure.

be more likely to take part in a merger either as a target or as an acquiring firm. In order to operationalize this test, we estimate the following linear probability model on our sample of actual acquirers (targets) and pseudo acquirers (pseudo targets):[24]

$$Actual\ Acquirer_{i,t} = \alpha + \beta_1 Low\ Cybersecurity\ Risk_{i,t-1} + \beta_2 Acquirer\ Controls_{i,t-1} + Year\ FE_t + Industry\ FE_i + \varepsilon_{i,t} \quad (1)$$

$$Actual\ Target_{i,t} = \alpha + \beta_1 Low\ Cybersecurity\ Risk_{i,t-1} + \beta_2 Target\ Controls_{i,t-1} + Year\ FE_t + Industry\ FE_i + \varepsilon_{i,t} \quad (2)$$

Where *Acquirer (Target) Controls*$_{i,t-1}$ include firm size, cash holdings, institutional ownership, a staggered board indicator, leverage, the HHI index measured at the 3-digit SIC level, Tobin's Q and ROA.

Column (1) to Column (4) of Table 2 reports our estimates for Model (1). Consistent with our prediction (*H1*), firms with low exposure to cybersecurity risks are systematically more likely to be active acquirers. The effect is robust to defining our low cybersecurity indicator based on tercile (Column (2)), quartile (Column (3)), and Quintile (Column (4)) of the distribution of our cybersecurity risk exposure measure. The stability of the coefficient supports the assertion that the identified effect is unlikely to be driven by a handful of outliers. Similar results emerge when focusing on targets. Column (5) to Column (8) in Table 2 reports our estimates for Model (2). Low cybersecurity risk firms are significantly more likely to become targets in the M&A market.

Taken together, these estimates support our first hypothesis (H1) by documenting that firms' cybersecurity profile is a significant determinant of both (1) the decision to initiate an M&A transaction (acquirer), as well as (2) the probability of being selected as a potential target. These results are consistent with managers being concerned about potential cybersecurity weaknesses threatening the successful completion of an M&A transaction.

[Table 2 About Here]

Recent studies document that corporate culture, as well as environmental, social and governance (ESG) considerations are important determinants of M&A activity (Deng et al., 2013;

[24] The use of a linear probability model is dictated by the presence of high dimensional fixed effects. Estimating the model via a logit leads to estimating marginal effects only for the subset of data that is non-homogenous within the grouped data. As such, with high dimensional fixed effects, results can be substantially distorted (Beck, 2019).

Bereskin et al., 2018; Bai et al., 2021). Further, it is possible that cybersecurity risk exposure might be higher for firms displaying low levels of social engagement, and more generally lower ESG scores. For instance, firms with perceived poor corporate social responsibility (CSR) may be more likely the target of activists (e.g., see Goldman (2012)). These firms could also be more at risk because their governance structure is such that they were less likely to invest in their cybersecurity infrastructure in the first place (Lending et al., 2018). Overall, it is possible that our cybersecurity risk measure could be correlated with overall ESG measures in our sample firms.

To control for this confounding possibility, we begin by assessing the correlation between our indicators of low cybersecurity risk exposure with the CSR ratings obtained from KLD Research and Analytics. Table 3, Panel A, reports our estimates that highlight a lack of strong correlation between these two measures. To further assess the possibility of a confounding effect between CSR exposure and our cybersecurity risk exposure measure, we include the KLD net score in our multivariate regressions estimated in Table 2. These tests, reported in Panel B of Table 3 are consistent with our previous results. Namely, even after controlling for CSR exposure, firms with low cybersecurity risk exposure are still significantly more likely to become acquirers (Column (1)), or targets (Column (2)). Evidence from Table 3 supports the hypothesis that greater cybersecurity risk exposure reduces a firm's ability to participate in the market for corporate control.

[Table 3 About Here]

3.2. *Cybersecurity Risk and the Likelihood of Merger Pairs*

The relevance of cybersecurity risk as a determinant of corporate M&A activity raises the possibility that cybersecurity risk affects not only firms' propensity to initiate (or be targeted in) these transactions, but also the ultimate acquirer-target matching process. To test for this possibility, we modify our empirical specification to test whether corporations are more likely to merge with counterparties that have a similar cybersecurity risk profile. Using our sample of actual and pseudo mergers following the Bena and Li (2014) procedure, we estimate the following regression model:

$$
\begin{aligned}
Actual\ Merger_{d,t} \\
&= \alpha + \beta_1 Low\ Cybersecurity\ Risk\ Pair_{i,t-1} \\
&+ \beta_3 Acquirer\ Controls_{i,t-1} + \beta_4 Target\ Controls_{i,t-1} + Deal\ FE \\
&+ Year\ FE + Acquirer\ Industry\ FE + Target\ Industry\ FE + \varepsilon_{i,t}
\end{aligned} \tag{3}
$$

Table 4 reports our estimates, whereby "Low Cybersecurity Risk Pair" is defined as both acquiring and target firms being in the lower tercile (respectively quartile and quintile) in terms of their cybersecurity risk profile. Across these different specifications, we identify robust evidence supporting our second hypothesis (*H2*). That is, deals involving two low exposure cybersecurity corporations are significantly more likely to occur than those involving different profiles in terms of cybersecurity exposure. The effect is robust to controlling for a wide-array of target and acquirer controls, as well as to using higher dimensional fixed effects capturing year, industry of both the acquirer and target firm, and deal fixed effects.[25]

[Table 4 About Here]

3.3. *Cybersecurity Risk and Market Reactions to Merger Announcements*

Next, we assess whether and how investors take into consideration targets and acquirers' cybersecurity profile when reacting to merger announcements (*H3*). Following Li and Prabhala (2007), we tackle this question by studying cumulative abnormal returns (CAR) estimated around initial deal announcements. To operationalize this empirical analysis, we estimate the following regression model on the sample of 782 deals for which abnormal returns can be computed:

$$
\begin{aligned}
CAR_{i,t} = \alpha &+ \beta_1 Low\ Cybersecurity\ Risk\ Acquirer_{i,t-1} \\
&+ \beta_2 Low\ Cybersecurity\ Risk\ Target + \beta_3 Acquirer\ Controls_{i,t-1} \\
&+ \beta_4 Target\ Controls_{i,t-1} + \beta_4 Deal\ Controls_d + Year\ FE \\
&+ Acquirer\ Industry\ FE + Target\ Industry\ FE + \varepsilon_{i,t}
\end{aligned} \tag{4}
$$

$CAR_{i,t}$ represents cumulative abnormal returns computed over the 3-day window surrounding the announcement date for acquirers (Columns (1) – (3)), targets (Columns (4) – (6)), and the combination of the two (Columns (7) – (9)). Combined returns are value-weighted returns,

[25] Similarly to the approached proposed in Bena and Li (2014), deal fixed effects absorb any common variations shared by firms included in the (up to) eleven firm-pairs representing the actual deal; namely up to five pseudo acquirer – actual target pairs, and up to five actual acquirer – pseudo target pairs.

where weights are assigned based on the market capitalization of the merging parties.[26] The specifications includes the same wide array of targets and acquirers level controls discussed in the previous section, and a variety of deal-level characteristics including the method of payment (All Cash), whether the announcement is related to a tender offer (Tender Offer), and whether the acquirer and target operate in the same industry (Same Industry).

We find no statistically significance evidence that the market prices cybersecurity risk at the time of a merger announcement when estimating this model over the full period.[27] One potential explanation for the lack of statistical significance is related to the general awareness (as well as the availability of reliable public information) regarding corporate exposure to cybersecurity risk was much more limited in the early part of our sample (i.e., early 2000s). To wit, firms' cyber-related disclosure increased exponentially in quantity and quality following the publication of the CF Disclosure Guidance: Topic No. 2 Cybersecurity in 2011, a document requiring companies to include material information related to cybersecurity risk in their SEC regulatory filings (see Lattanzio and Ma, 2021). We thus hypothesize that investors' relative lack of awareness combined with generally less reliable measures of cybersecurity risk exposures characterizing the early years of our sample might have limited investors' capacity to price this source of risk early on.

In order to test for this possibility, we augment model (4) with an interaction term between the selected low cybersecurity risk indicators and a Post SEC Guidance dummy to assess whether the increase in cybersecurity disclosure that followed the release of this document has contributed to investors' attempts to price this economic dimension in M&A transactions. As documented in Table 5, Column (1), Column (4), and Column (7), we find a significant positive effect of low cybersecurity risk on the combined CAR post SEC Guidance.

[Table 5 About Here]

As cybersecurity related disclosure increases, investors seem to take into account the available information in evaluating merger announcements. In particular, we document that this effect appears to be driven by the cybersecurity risk profile of the acquiring firm, rather than that of the target. We interpret this result as suggestive that investors pay particular attention to the

[26] Assigning weights based on book value of assets yield comparable results.
[27] As shown in Table OA.X, in the Online Appendix, this finding holds for a wide range of indicators of low cybersecurity risk exposure across targets, acquirers, and the combined returns.

acquirers' ability to (1) assess the targets' cybersecurity risk profile during the due diligence period and (2) to capture potential synergies from the deal by being better able to successfully manage the complicated process of data migration and integration. Such an assessment would be consistent with recent survey evidence documenting that the due-diligence period is crucial in assessing the existence of material cybersecurity weaknesses affecting the target firm, thus emphasizing the active role of the acquiring firm in the early stages of the acquisition process (Forescout, 2021).

We explore these results further with two additional tests. First, we repeat our analysis by interacting the low cybersecurity risk indicators with a dummy set equal to one if the merger was announced after the passage of the Cybersecurity Information Sharing Act of 2015 (CISA). This regulation was signed into law on December 18, 2015 and it includes two main components. First, it authorizes companies to monitor and implement defensive measures on their own information systems to counter cyberattacks. Second, it provides firms with a certain degree of protections to encourage them to voluntarily share information concerning "cyber threat indicators" and "defensive measures" with the federal government, state and local governments, and other companies and private entities.[28] As the passage of the CISA increases investors' awareness of cybersecurity issues and improves both the quantity and quality of publicly available cybersecurity related information, we expect to identify a stronger market reaction to merger announcements over the post-regulation period. As shown in Table 5, Column (2), Column (5), and Column (8), we find this to be the case. In particular, both the statistical and economic significance of the effects are higher than those estimated for the post SEC disclosure guidance period. These results point once again to the increased awareness of investors over time of the impact of cybersecurity risk in M&A deals.

Second, we follow Florackis et al. (2022) and create a measure of attention towards cybersecurity risk by analyzing search volume index (SVI) in Google. SVI measures the intensity on search topics over a given timeframe and is widely used as a proxy for investor attention (Drake, Roulstone and Thornck, 2012; Da, Engelberg, and Gao, 2011; Florackis et al., 2022). Following the extant literature, we use the following relevant topics to build the SVI measure: hacker, data breach, cyberattack, cyber insurance, cybersecurity, cyber security regulation, hacking. We use this yearly measure to capture the time-varying attention intensity directed towards this rising

[28] These protections include protections from liability, non-waiver of privilege, and protections from FOIA disclosure.

source of risk. The resulting variable is interacted with our low cybersecurity risk indicators, allowing us to assess whether the market reaction to merger announcements is more pronounced in periods of high attention to cybersecurity risk. As documented in Table 5, Column (3), Column (6), and Column (9), these tests provide further support for a positive impact of low cybersecurity risk profile of the acquirer on merger announcement returns in times of heightened attention towards cybersecurity risk.

3.4. *Cybersecurity Risk and Probability of Deal Completion*

So far, our empirical findings echoes anecdotal evidence suggesting that the due-diligence process represents a crucial stage for interested acquirers to identify and evaluate undisclosed, or otherwise unknown cybersecurity-related weaknesses of target firms. A recent survey by the NYSE Governance Services (2017) finds that acquiring company are likely to withdraw from a deal if the target' cybersecurity profile is too weak. In particular, 85% of the 276 directors and officer of public companies stated that the identification of major security vulnerabilities in the target during the due diligence process were "very likely" to negatively affect the outcome of the attempted transaction.

Our sample includes 145 withdrawn mergers, representing about 24% of our initial sample. This proportion is in line with recent studies showing to between 15% and 20% of the attempted mergers are ultimately withdrawn (Officer, 2003; Bereskin et al, 2018).[29] We estimate the following linear probability model to test for the possibility that the merging parties' cybersecurity risk profiles materially impact the likelihood of withdrawal of these attempted M&A transactions (H4):

$$
\begin{aligned}
Withdrawn_{d,t} &= \alpha + \beta_1 Low\ Cybersecurity\ Risk\ Acquirer_{i,t-1} \\
&+ \beta_2 Low\ Cybersecurity\ Risk\ Target + \beta_3 Acquirer\ Controls_{i,t-1} \\
&+ \beta_4 Target\ Controls_{j,t-1} + Year\ FE + Acquirer\ Industry\ FE \\
&+ Target\ Industry\ FE + \varepsilon_{i,t}
\end{aligned}
\qquad (5)
$$

[29] This frequency includes deals withdrawn for either regulatory reasons (Savor and Lu, 2009) and idiosyncratic factors such as cultural incompatibility (McMains, 2014; Bereskin et al., 2018), the emergence of agency conflicts (Masulis et al., 2009; Ambrose and Megginson, 1992; Jensen, 1988), behavioral considerations (Roll, 1986), changes in the target's financial and economic conditions during the merger negotiation (Weston et al., 2004), among others.

Where withdrawn is a dummy set equal to 1 if the attempted deal is ultimately withdrawn, zero if it is successful. This specification includes the same target and acquirer level controls used in our previous estimations, as well as calendar year and both acquirer and target industry fixed effects. Results are reported in Table 6.

[Table 6 About Here]

Our estimates provide strong support for hypothesis (H4). Namely, mergers involving targets with low cybersecurity risk firms are significantly less likely to fail during the due-diligence period. This finding is consistent with acquiring firms carefully assessing the existence of material IT weaknesses during the due diligence process and being ultimately more likely to withdraw their bid in light of greater cybersecurity exposure.

3.5. *Cybersecurity Risk and Merger Premium*

Next, we assess whether merging firms' cybersecurity profile is ultimately reflected in the merger premium paid. In particular, we hypothesize that mergers involving low cybersecurity targets and (or) acquirers will ultimately be completed at a higher premium (respectively H5A and H5B). In order to operationalize this test, we estimate the following regression model:

$$\begin{aligned} Premium_{d,t} = {} & \alpha + \beta_1 Low\ Cybersecurity\ Risk\ Acquirer_{i,t-1} \\ & + \beta_2 Low\ Cybersecurity\ Risk\ Target + \beta_3 Acquirer\ Controls_{i,t-1} \\ & + \beta_4 Target\ Controls_{j,t-1} + \beta_5 Deal\ Controls_d + Year\ FE \\ & + Acquirer\ Industry\ FE + Target\ Industry\ FE + \varepsilon_{i,t} \end{aligned} \quad (5)$$

As discussed in Appendix Table A in the appendix, we define the merger premium as the difference between the final deal valuation and the market value of the target, as observed 4 weeks prior to its announcement.[30] The model includes the target, acquirer, and deal level controls used in previous analyses, as well as calendar year and both acquirer and target industry fixed effects. Table 7 reports our estimates.

[Table 7 About Here]

Our results do not support H5A, however they do provide support for H5B. Namely, we observe that mergers involving low cybersecurity risk acquirers are completed at higher relative valuations. These findings are consistent with low cybersecurity risk acquirers being better able to

[30] Similar results are identified if we measure the merger premium as the difference between the final deal valuation and the market value of the target, as observed 1 weeks prior to its announcement.

successfully conduct the integration process during which high-value data including customers' information and trade secrets are exposed to potential cyberattacks; and hence have an increased willingness to pay a premium for the target. It is also consistent with their superior ability to handle unexpected technological compatibility issues that might undermine the realization of the synergistic gains expected from the merger.

3.6. *Cybersecurity Risk and Post-Merger Performance*

If deals involving low cybersecurity risk are more likely to yield the synergistic gains expected from the merger, we should observe superior post-merger performance in such cases (*H6A*). To test this hypothesis, we begin by analyzing the post-merger performance of completed M&A transactions conditional on the merging firms' cybersecurity profile at the time of the merger. That is, we estimate the following regression model over the seven years surrounding the M&A completion:

$$\begin{aligned} ROA_{i,t} = {} & \alpha + Post_t + \beta_1 Post_t \; x \; Low\ Cybersecurity\ Risk\ Target_{i,t} \\ & + \beta_2 Post_t \; x \; Low\ Cybersecurity\ Risk\ Acquirer_{i,t} + Firm\ Controls \\ & + Firm\ FE + \ Year\ FE + \varepsilon_{i,t} \end{aligned} \qquad (6)$$

The dependent variable, *ROA*, is defined as the acquirer's ratio of operating income before depreciation to total assets. The indicator *Post* equals one for the post-merger time period, zero otherwise. The interaction term is the coefficient of interest, as it allows for the identification of potential differences in performance related to the cybersecurity risk profile of the merging firms. The model includes controls for firm size, cash holdings, institutional ownership, a staggered board indicator, leverage, the HHI index measured at the 3-digit SIC level, Tobin's Q and ROA, as well as year and firm fixed effects.[31] Table 8 reports our estimates.

[Table 8 About Here]

Our results provide support for H6A by documenting that mergers involving low cybersecurity risk firms systematically outperform their peers over the post-merger period. That is, low cybersecurity risk firms appear to be better equipped to complete successfully the integration process. This result is also consistent with our findings in support of *H5B*. Namely, we show that acquirers with a low cybersecurity risk profile are better able to extract synergies in the

[31] Notably, the use of firm-level fixed effects absorbs targets and acquirers' indicators of cybersecurity risk, which are thus dropped from the model due to collinearity concerns.

post-merger window, which is consistent with their willingness to pay a relatively higher premium upfront.

An alternative way to examine post-merger performance of the acquiring firm is by studying the likelihood of a goodwill write-off over the post-merger period. According to current accounting rules (SFAS 141 and 142), this accounting item must be tested for impairment on a yearly basis. Since a goodwill impairment can be interpreted as the result of material misvaluation of expected synergies or unexpected decline in synergies (Gu and Lev, 2011), one should expect goodwill impairment to be less likely to occur for mergers involving low cybersecurity risk corporations (H6B).

To test this hypothesis, we estimate a linear probability model examining the likelihood of a goodwill write-off over the three years following the merger completion.

$$\begin{aligned} Goodwill\ Impairment_{f,t} &= \alpha + \beta_1 Low\ Cybersecurity\ Risk\ Target_{i,t} \\ &+ \beta_2\ Low\ Cybersecurity\ Risk\ Acquirer_{i,t} + Deal\ Controls \\ &+ Firm\ Controls + Industry\ FE + \ Year\ FE + \varepsilon_{i,t} \end{aligned} \quad (7)$$

As documented in Table 9, we find strong support for our hypothesis. In particular, we identify a significant negative association between the cybersecurity risk profile of both target and acquiring firms and post-acquisition goodwill write-offs. This result is consistent with post-merger integration being considerably more successful when the involved firms feature a strong cybersecurity profile.[32]

[Table 9 About Here]

The findings reported in this section provide strong support for the hypothesis that cybersecurity risk has material implications for deal synergies and the merged entity's ability to capture the expected improvements in operating performance over the post-merger period. In particular, mergers involving low cybersecurity risk firms are significantly more likely to exhibit

[32] A note of caution should be expressed with respect to these findings. To avoid a significant reduction in sample, we also include deals involving acquirers that engaged in other acquisitions over the 7 years surrounding the studied deal. Consequently, it is possible that the identified goodwill impairments might be related to a different M&A transaction. However, this confounding factor would result in inflated estimates for the standard errors, ultimately biasing towards finding no results. Furthermore, unreported results confirm that dropping "serial acquirers" (i.e., acquirers engaging in multiple M&A deals over the three years preceding the studied transaction) from our sample does not materially affect our findings.

material improvements in ROA and are significantly less likely to recognize goodwill impairments in the years following deal completion.

4. Conclusions

Recent survey evidence documents that managing cybersecurity risk has become one of the greatest concerns for CEOs. To our knowledge, this is the first study attempting to assess the impact of this significant and growing source of risk on mergers and acquisitions (M&A) related activities in the U.S. Our evidence is consistent with the proposition that cybersecurity risk poses a significant threat throughout the merger process, from the likelihood of being attempted in the first place to the likelihood of being completed through to the post-merger integration phase.

Overall, our findings suggest that cybersecurity risk is a critical risk factor affecting (1) a firm's propensity to engage in M&A transactions, (2) the matching process in the M&A market, (3) the likelihood of successful completion of deals, (4) both investors' ex-ante and ex-post pricing of M&A deals, as well as (5) the post-merger operating performance. These novel findings have important implications for both regulators and shareholders concerned about the potential impact of cybersecurity risk on M&A transactions.

Reference

Akey, P., Lewellen, S., Liskovich, I., Schiller, C., 2021. Hacking Corporate Reputations. Rotman School of Management Working Paper No. 3143740.

Ambrose, B. W., Megginson, W. L., 1992. The role of asset structure, ownership structure, and takeover defenses in determining acquisition likelihood. *Journal of Financial and Quantitative Analysis*, 27 (4), 575-589.

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

Andrade, G., Mitchell, M., and Stafford, E., 2001. New Evidence and Perspectives on Mergers. *Journal of Economic Perspectives*, 15 (2), p. 103-120.

Arnold, D., 2020. Mergers and Acquisitions, Local Labor Market Concentration, and Worker Outcomes. Working Paper.

Ashraf, M., Sunder, J., 2022. Can Shareholders Benefit From Consumer Protection Disclosure Mandates? Evidence from Data Breach Disclosure Laws and the Cost of Equity. Working Paper.

Bai, J., Chu, Y., Shen, C., Wan, C., 2021. Managing Climate Change Risks: Sea Level Rise and Mergers Acquisitions. Working Paper.

Bai, J., Jin, W., Serfling, M., 2021. Management Practices and Mergers and Acquisitions. *Management Science,* 68 (3), p. 2141-2165.

Beck, Nathaniel, 2019. Estimating Grouped Data Models with a Binary-Dependent Variable and Fixed Effects via a Logit versus a Linear Probability Model: The Impact of Dropped Units. *Political Analysis*, 28 (1), p. 139-145.

Bena, J., Li, K., 2014. Corporate Innovations and Mergers and Acquisitions. *The Journal of Finance*, 69, p. 1923-1960.

Bereskin, F. L., Byun, S. K., Officer, M., Oh, J-M., 2018. *Journal of Financial and Quantitative Analysis*, 53 (5), p. 1995-2039.

Binfare', M., 2021. The Real Effects of Operational Risk: Evidence from Data Breaches. Working Paper.

Cunningham, C., Ederer, F., Ma, S., 2021. Killer Acquisitions. *Journal of Political Economy*, p. 649-702.

Da, Z., Engelberg, J., and Gao, P., 2011. In Search of Attention. *The Journal of Finance*, 66 (5), p. 1461-1499.

Deng, X., Kang, J., Low, B. S., 2013. Corporate Social Responsibility and Stakeholder Value Maximization: Evidence from Mergers. *Journal of Financial Economics*, 110 (1), p. 87-109.

Devos, E., Kadapakkam, P. R., and Krishnamurthy, S., 2009. How do mergers create value? A comparison of taxes, market power, and efficiency improvements as explanations for synergies. *The Review of Financial Studies*, 22(3), p. 1179-1211.

Dhyne, E., Konings, J., Van den Bosch, J., and Vanormelingen, S., 2021. The Return on Information Technology: Who Benefits Most? *Information System Research,* 31(1), p. 194-211.

Drake, M.S., Roulstone, D.T., Thornock, J.R., 2012. Investor Information Demand: Evidence from Google Searches around Earnings Announcements. *Journal of Accounting Research,* 50, p. 1001-1040.

Duchin, R., Farroukh, A. El-K. Harford, J., Patel, T., 2021, Political Attitudes, Partisanship, and Merger Activity. Working Paper.

Ettredge, M., Guo, F., Li, Y., 2018. Trade Secrets and Cyber Security Breaches. *Journal of Accounting and Public Policy*, 37(6), p. 564-585.

Fee, C. E., Hadlock, C. J., and Pierce, J. R., 2012. What happens in acquisitions?: Evidence from brand ownership changes and advertising investment. *Journal of Corporate Finance*, 18(3), p. 584-597.

Florackis, C., Louca, C., Michaely, R., Weber, M., 2022. Cybersecurity Risk. *Review of Financial Studies, Forthcoming.*

Francis, B. Hu, W., and Shohfi, T., 2021, Ex-Intrusion Corporate Cyber-Risk: Evidence from Internet Protocol Networks. *Journal of Operational Risk*, 16 (3), p. 47-71.

Goldman, D., 2012. 'Hacktivists' stole 58% of thieved data in 2011. CNN Money. http://money.cnn.com/2012/03/22/technology/hacktivists-verizon-data-breach-report

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

Gu, F., Lev. B., 2011. Overpriced Shares, Ill-Advised Acquisitions, and Goodwill Impairment. *The Accounting Review*, 86, p. 23-48.

Guernsey, S., F. Guo, T. Liu, M. Serfling, 2022. Classified boards: Endangered species or hiding in plain sight? Working Paper.

Harford, J., 2005. What drives merger waves?. *Journal of Financial Economics*, 77(3), p. 529- 560.

Harford, J., Jenter, D., and Li, K., 2011. Institutional cross-holdings and their effect on acquisition decisions. *Journal of Financial Economics*, 99 (1), p. 27-39.

Havakhor, T., Rahman, M., Zhang, T., 2021. Disclosure of Cybersecurity Investments and the Cost of Capital. Working Paper.

Healy, P. M., Palepu, K. G., and Ruback, R. S, 1992. Does corporate performance improve after mergers?. *Journal of Financial Economics*, 31(2), p. 135-175.

Hilary, G., Segal, B., Zhang, M. H., 2016. Cyber-Risk Disclosure: Who Cares? Working Paper.

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

Hoberg, G., and Phillips, G., 2010. Product market synergies and competition in mergers and acquisitions: A text-based analysis. *The Review of Financial Studies*, 23 (10), p. 3773- 3811.

Huang, H. H., & Wang, C., 2020. Do Banks Price Firms' Data Breaches? Do banks price firms' data breaches? *The Accounting Review*, 96 (3), p. 261-286.

Kamiya, S., Kang, J., Kim, J., Milidonis, A., Stulz, R., 2020. Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms. *Journal of Financial Economics*, 139 (3), p. 719-749.

Jacobsen, S., 2014. The death of the deal: Are withdrawn acquisition deals informative of CEO quality? *Journal of Financial Economics,* p. 54-83.

Jamilov, R., Rey, H., Tahoun, A., 2021. The Anatomy of Cyber Risk. Working Paper.

Jensen, M.C., 1988. Takeovers: their causes and consequences. *Journal of Economic Perspectives*, 2 (1), 21-48.

Jiang, H., Khanna, N., Yang, Q., 2021. The Cyber Risk Premium. Working Paper.

Lattanzio, G., Ma, Y., 2022. Corporate Innovation in the Cyber Age. Working Paper.

Lattanzio, G., Megginson, W.L., Sanati, A., 2022. Dissecting the Listing Gap: Mergers, Private Equity, or Regulation? Working Paper.

Lattanzio, G., Roner, C., 2022. Reputational Risk, Cyber-Insurance and the Market Value of Breached Firms. Working Paper.

Lawrence, A., Minutti-Meza, M., Vyas, D., 2018. Is Operational Control Risk Informative of Financial Reporting Deficiency? *AUDITING: A Journal of Practice & Theory*, 37(1), p. 139-165.

Lee, K.H., Mauer, D.C., and Xu, E.Q., 2018. Human capital relatedness and mergers and acquisitions. *Journal of Financial Economics*, 129 (1), p. 111-135.

Lending, C., Minnick., K., and Schorno, P.J., 2018. Corporate governance, social responsibility and data breaches, *Financial Review*, 53, p. 413-455.

Li, K., and Prabhala, N.R., 2007. Self-Selection Models in Corporate Finance. *Handbook of Empirical Corporate Finance*, 1, p. 37-86.

Li, H., No, W. G., & Boritz, J. E., 2016. Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice & Theory*, August 1, 2016.

Lichtenberg, F. R., Sieger, D., 1987. Productivity and Changes in Ownership of Manufacturing Plants. *Brookings Papers on Economic Activity,* (3), p. 643-683.

Liu, T., C. Makridis, 2021. Abnormal Returns and Dispersion in Cybersecurity Exposure. Working Paper.

Liu, Y., 2019. Shareholder wealth effects of M&A withdrawals. *Review of Quantitative Finance and Accounting, 52*, p. 681-716.

Madura, J., Ngo, T., and Viale, A., 2012. Why do merger premiums vary across industries and over time? *The Quarterly Review of Economics and Finance,* 52 (1), p. 49-62.

Makridis, C., D.R. Desai, 2021. Identifying Critical Infrastructure in a World with Network Cybersecurity Risk. Working Paper.

Maksimovic, V., and Phillips, G., 2001. The market for corporate assets: Who engages in mergers and asset sales and are there efficiency gains? *The Journal of Finance*, 56 (6), p. 2019-2065.

Maksimovic, V., Phillips, G., and Prabhala, N. R., 2011. Post-merger restructuring and the boundaries of the firm. *Journal of Financial Economics*, 102 (2), p. 317-343.

Masulis, R.W., Wang, C., Xie, F., 2009. Agency problems at dual-class companies. *Journal of Finance*, 64 (4), 1697-1727.

McGuckin, R. H., and Nguyen, S. V., 1995. On productivity and plant ownership change: New evidence from the longitudinal research database. *The RAND Journal of Economics*, p. 257-276.

Mitchell, M. L., and Mulherin, J. H., 1996. The impact of industry shocks on takeover and restructuring activity. *Journal of Financial Economics*, 41 (2), p. 193-229.

Moeller, S.B., Schlingemann, F., and Stulz, R., 2004. Firm size and the gains from acquisitions. *Journal of Financial Economics*, 73 (2), p. 201-228.

Richardson, V., J., Smith, R., E., Watson, M., W., 2019. Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches. *Journal of Information Systems* 33 (3), p. 227-265.

Rhodes-Kropf, M., and Robinson, D.T., 2008. The Market for Mergers and the Boundaries of the Firm. *The Journal of Finance*, 63, p. 1169-1211.

Rhodes-Kropf, M., and Viswanathan, S., 2004. Market valuation and merger waves. *The Journal of Finance*, 59 (6), p. 2685-2718.

Roll, R., 1986. The hubris hypothesis of corporate takeovers. *Journal of Business*, 59, 197-216.

Schoar, A., 2002. Effects of corporate diversification on productivity. *The Journal of Finance*, 57 (6), 2379-2403.

Seru, A., 2014. Firm Boundaries Matter: Evidence From Conglomerates and R&D Activity. *Journal of Financial Economics*, 111, p. 381-405.

Sheen, A., 2014. The real product-market impact of mergers. *The Journal of Finance*, 69(6), p. 2651-2688.

Shleifer, A., and Vishny, R. W., 2003. Stock market-driven acquisitions. *Journal of Financial Economics*, 70(3), p. 295-311.

Sun, Y., Wei, L., Xie, W., 2020. Data Security and Merger Waves. Working Paper.

Wang, C., Xie, F., 2009. Corporate Governance Transfer and Synergistic Gains from Mergers and Acquisitions. *Review of Financial Studies*, 22, 829–858.

Wangerin, D., 2019. M&A Due Diligence, Post-Acquisition Performance, and Financial Reporting for Business Combinations. *Contemporary Accounting Research*, 36, p. 2344-2378.

Weston, J., Mitchell, M. L., Mulherin, J.H., 2004. *Takeovers, Restructuring and Corporate Governance*, 4 edition. New Jersey: Pearson Prentice Hall.

Table I

Summary Statistics

Panel A reports summary statistics of the acquirers and the target firms included in the sample. Pseudo acquirers and pseudo targets are selected for each deal by pairing the actual acquirers and targets with up to five matches following the industry-year matched approach presented in Bena and Li (2014). Panel B reports deal characteristics for the transactions included in the sample. Panel C reports the time-series distribution of the selected M&A deals. Definitions of the variables are provided in the Appendix. All continuous variables are winsorized at the 1% on both tails. *, ** and *** denote significance at the 10%, 5%, and 1% level, respectively.

Panel A: Summary Statistics Acquirers

	Actual Acquirers			Unique Pseudo Acquirers				
Cybersecurity Risk								
	N	Frequency		N	Frequency		Delta	P-value
Low Cybersecurity Risk (Tercile)	583	0.3464		1609	0.2218		0.1246	0.0000
Low Cybersecurity Risk (Quartile)	583	0.3670		1609	0.2361		0.1308	0.0000
Low Cybersecurity Risk (Quintile)	583	0.4065		1609	0.2647		0.1417	0.0000
Firms Characteristics								
	N	Mean	St. Dev.	N	Mean	St. Dev.	Delta	P-value
Assets	583	7.5036	2.0445	1609	7.1110	2.2668	0.3925	0.0002
Tobin's Q	583	1.6575	2.1090	1609	1.5070	3.8648	0.1505	0.3755
Cash	583	0.1558	0.1485	1609	0.1313	0.1526	0.0244	0.0009
% Institutional Ownership	583	0.6303	0.3272	1609	0.3495	0.3781	0.2808	0.0000
Leverage	583	0.2440	0.2127	1609	0.2505	0.2127	-0.0065	0.5294
R&D to Sales	583	0.1164	0.6113	1609	0.1641	0.8924	-0.0476	0.2351
HHI (SIC3)	583	0.1222	0.1118	1609	0.1239	0.1120	-0.0017	0.7406
ROA	583	0.1073	0.1136	1609	0.0461	0.4196	0.0611	0.0011
Staggered Board	583	0.3785	0.4852	1609	0.2731	0.4456	0.1053	0.0000

Panel B: Summary Statistics Targets								
	Actual Targets			Unique Pseudo Targets				
Cybersecurity Risk								
	N	Frequency		N	Frequency		Delta	P-Value
Low Cybersecurity Risk (Tercile)	607	0.3770		1573	0.2534		0.1235	0.0000
Low Cybersecurity Risk (Quartile)	607	0.3918		1573	0.2692		0.1225	0.0000
Low Cybersecurity Risk (Tercile)	607	0.3582		1573	0.2656		0.0937	0.0000
Firms Characteristics								
	N	Mean	St. Dev.	N	Mean	St. Dev.	Delta	P-Value
Assets	607	6.7394	2.1919	1573	6.5401	2.4775	0.1930	0.0818
Tobin's Q	607	1.9845	1.2528	1573	1.3905	2.1485	0.5939	0.0010
Cash	607	0.1658	0.1678	1573	0.1458	0.1740	0.0199	0.0015
% Institutional Ownership	607	0.6129	0.3379	1573	0.3463	0.3768	0.0488	0.0023
Leverage	607	0.2919	0.7663	1573	0.2648	0.4750	0.0158	0.0158
R&D to Sales	607	0.1431	0.7045	1573	0.1705	0.9150	-0.0270	0.5105
HHI (SIC3)	607	0.1260	0.0030	1573	0.1235	0.1144	-0.0030	0.5920
ROA	607	0.0446	0.3822	1573	0.0136	0.4416	0.0309	0.1285
Staggered Board	607	0.3976	0.4896	1573	0.3896	0.4496	0.0080	0.7346
Panel C: Deal Characteristics								
	N	Frequency						
Tender Offer	607	0.1838						
Horizontal Acquisition	607	0.8591						
All Cash Deal	607	0.6690						
Withdrawn	607	0.2402						

Panel D: Time-Series of M&A Deals

	Florackis et al. (2022) Sample		Lattanzio and Ma (2021) Sample	
Year	Number of Deals	% of the Sample	Number of Deals	% of the Sample
2001			65	6.74%
2002			66	6.85%
2003			50	5.19%
2004			56	5.81%
2005			57	5.91%
2006			50	5.19%
2007	44	7.25%	43	4.46%
2008	45	7.41%	45	4.67%
2009	45	7.41%	45	4.67%
2010	34	5.60%	32	3.32%
2011	35	5.77%	33	3.42%
2012	52	8.57%	52	5.39%
2013	72	11.86%	70	7.26%
2014	88	14.50%	85	8.82%
2015	73	12.03%	67	6.95%
2016	48	7.91%	48	4.98%
2017	36	5.93%	32	3.32%
2018	35	5.77%	33	3.42%
2019			35	3.63%
Total	607	100.00%	964	100.00%

Table II

Cybersecurity Risk and Likelihood of Being Involved in an M&A Transaction

Table 2 reports the results from linear probability models assessing the likelihood of being an actual (as opposed to pseudo) acquirer or target as a function of firms' Cybersecurity Risk and other control variables. The dependent variable is an indicator variable set equal to one if the observation is an "actual" acquirer (Column (1) to (4)) or target (Column (5) to (8)), 0 if the observation is a pseudo acquirer (target). The matched sample is built following Bena and Li (2014) and it contains for each actual acquirer (target) up to five pseudo controls matched within SIC3 industry code - year, and upon a propensity score based on size and Tobin's Q. The sample period is from 2007 to 2018. Cybersecurity Risk is defined as in Florackis et al. (2022). All variables are defined in the Appendix. Standard errors are clustered at the actual deal level acquirer (Column (1) to (4)) or target (Column (5) to (8)) SIC3 industry code and are reported in parentheses. All specifications include fiscal year and industry fixed effect. Control variables are winsorized at the 1% level on both tails. *, **, and *** indicates statistical significance at the 10%, 5%, and 1% level, respectively.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Variable	Acquirer				Target			
Low Cybersecurity Risk (Tercile)	0.132***	0.101***			0.126***	0.093***		
	(0.026)	(0.019)			(0.026)	(0.022)		
Low Cybersecurity Risk (Quartile)			0.059**				0.085***	
			(0.022)				(0.021)	
Low Cybersecurity Risk (Quintile)				0.084***				0.095***
				(0.021)				(0.020)
Firm Size		0.027***	0.024***	0.026***		0.012**	0.012**	0.012**
		(0.003)	(0.003)	(0.003)		(0.004)	(0.004)	(0.004)
Cash Holdings		0.254***	0.239***	0.246***		0.168***	0.170***	0.169***
		(0.080)	(0.076)	(0.079)		(0.048)	(0.048)	(0.048)
% Institutional Ownership		0.354***	0.357***	0.359***		0.379***	0.380***	0.381***
		(0.019)	(0.018)	(0.019)		(0.020)	(0.019)	(0.019)
Staggered Board		0.075***	0.083***	0.078***		0.096***	0.097***	0.098***

		(0.018)	(0.019)	(0.018)		(0.017)	(0.018)	(0.018)
Leverage		-0.012	-0.011	-0.011		-0.001	-0.001**	-0.001**
		(0.031)	(0.032)	(0.032)		(0.001)	(0.000)	(0.000)
R&D to Sales		-0.017***	-0.016***	-0.016***		-0.003	-0.003	-0.003
		(0.004)	(0.004)	(0.004)		(0.005)	(0.005)	(0.005)
HHI (SIC3)		0.022	0.025	0.024		-0.003	-0.002	-0.004
		(0.057)	(0.063)	(0.059)		(0.060)	(0.061)	(0.0059)
Tobin's Q		0.017***	0.016***	0.017***		0.014***	0.014***	0.014***
		(0.003)	(0.003)	(0.003)		(0.004)	(0.004)	(0.004)
ROA		0.111***	0.114***	0.112***		0.096***	0.097***	0.098***
		(0.034)	(0.033)	(0.034)		(0.020)	(0.018)	(0.018)
Constant	0.226***	-0.034	-0.003	-0.024	0.236***	0.091***	0.095**	0.094***
	(0.008)	(0.035)	(0.003)	(0.035)	(0.009)	(0.029)	(0.031)	(0.030)
Year Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acquirer Industry Fixed Effects	Yes	Yes	Yes	Yes	No	No	No	No
Target Industry Fixed Effects	No	No	No	No	Yes	Yes	Yes	Yes
R-squared	0.051	0.078	0.078	0.078	0.036	0.049	0.049	0.049
Observations	2192	2096	2096	2096	2180	2074	2074	2074

Table III

Cybersecurity Risk, CSR engagements, and Likelihood of being involved in an M&A

Panel A reports pairwise correlation between firms' cybersecurity score and corporate social responsibility performance, measured using the KLD net score. Panel B replicates the results reported in the linear probability models estimated in Table II after controlling for the KLD Net Score. All variables are defined in the Appendix. *,**, and *** indicates statistical significance at the 10%, 5%, and 1% level, respectively.

Panel A: Pairwise correlations between corporate environmental performance and cybersecurity risk

Acquirers

	Low Cybersecurity Risk (Tercile)	Low Cybersecurity Risk (Quartile)	Low Cybersecurity Risk (Quintile)	KLD Net Score
Low Cybersecurity Risk (Tercile)	1			
Low Cybersecurity Risk (Quartile)	0.9697	1		
Low Cybersecurity Risk (Quintile)	0.9647	0.9585	1	
KLD Net Score	-0.0486	-0.0681	-0.0712	1

Targets

	Low Cybersecurity Risk (Tercile)	Low Cybersecurity Risk (Quartile)	Low Cybersecurity Risk (Quintile)	KLD Net Score
Low Cybersecurity Risk (Tercile)	1			
Low Cybersecurity Risk (Quartile)	0.929	1		
Low Cybersecurity Risk (Quintile)	0.8988	0.9634	1	
KLD Net Score	-0.0566	-0.0680	-0.0710	1

Panel B: Likelihood of being involved in an M&A		
Variable	(1) Acquirer	(2) Target
Low Cybersecurity Risk (Tercile)	0.099***	0.093***
	(0.019)	(0.021)
KLD Net Score	-0.098***	-0.018
	(0.035)	(0.056)
Firm Size	0.026***	0.012**
	(0.003)	(0.004)
Cash Holdings	0.250***	0.168***
	(0.080)	(0.048)
% Institutional Ownership	0.355***	0.379***
	(0.019)	(0.020)
Staggered Board	0.073***	0.073
	(0.018)	(0.018)
Leverage	-0.011	-0.001**
	(0.032)	(0.000)
R&D to Sales	-0.017***	-0.003
	(0.004)	(0.005)
HHI (SIC3)	0.026	-0.003
	(0.053)	(0.006)
Tobin's Q	0.016***	0.014***
	(0.003)	(0.004)
ROA	0.112***	0.096***
	(0.034)	(0.020)
Acquirer Industry Fixed Effects	Yes	No
Target Industry Fixed Effects	No	Yes
Year Fixed Effects	Yes	Yes
Observations	2096	2074
R-squared	0.080	0.049

Table IV
Merger Pairs and Cybersecurity Risk

Table 4 reports the results from linear probability models estimating the likelihood of an observation being an actual (as opposed to pseudo) merger as a function of the paired Cybersecurity Risk profile of the acquirer-target pairing and other control variables. The dependent variable is an indicator variable set equal to one if the observation is an "actual" merger deal, 0 if the observation is a pseudo firm-pair generated from the control group. The matched sample is built following Bena and Li (2014). All variables are defined in the Appendix. Standard errors are clustered at the deal level and reported in parentheses. All specifications include deal, year, acquirer, and target fixed-effects. Control variables are winsorized at the 1% level on both tails. *,**, and *** indicates statistical significance at the 10%, 5%, and 1% level, respectively.

Variable	(1)	(2)	(3)	(4)	(5)	(6)
	Actual Merger					
Low CyberSecurity Risk Pair (Tercile)	0.171***	0.171***				
	(0.012)	(0.013)				
Low CyberSecurity Risk Pair (Quartile)			0.038***	0.040***		
			(0.007)	(0.008)		
Low CyberSecurity Risk Pair (Quintile)					0.165***	0.160***
					(0.015)	(0.020)
Acquirer Controls						
Firm Size		0.021***		0.019***		0.020***
		(0.003)		(0.003)		(0.003)
Cash Holdings		0.122***		0.123***		0.113***
		(0.033)		(0.033)		(0.034)
% Institutional Ownership		0.121***		0.130***		0.129***
		(0.010)		(0.008)		(0.009)
Staggered Board		0.028***		0.034***		0.031***
		(0.009)		(0.009)		(0.009)
Leverage		0.000		0.003		0.002
		(0.001)		(0.010)		(0.010)
R&D to Sales		-0.011**		-0.010*		-0.012**
		(0.005)		(0.004)		(0.005)
Tobin's Q		0.007***		0.007***		0.007***
		(0.002)		(0.002)		(0.002)
ROA		0.069***		0.073***		0.067***
		(0.020)		(0.021)		(0.021)
Target Controls						
Firm Size		0.008***		0.006***		0.007***
		(0.002)		(0.002)		(0.002)
Cash Holdings		0.102***		0.113***		0.107***

		(0.003)		(0.031)		(0.030)
% Institutional Ownership		0.118***		0.120***		0.117***
		(0.011)		(0.010)		(0.010)
Staggered Board		0.041***		0.054***		0.047***
		(0.009)		(0.009)		(0.009)
Leverage		-0.000**		-0.001***		-0.001*
		(0.000)		(0.000)		(0.000)
R&D to Sales		-0.006*		-0.006*		-0.007*
		(0.004)		(0.003)		(0.004)
Tobin's Q		0.008***		0.008***		0.008***
		(0.002)		(0.002)		(0.002)
ROA		0.048***		0.056***		0.050***
		(0.013)		(0.013)		(0.013)
Constant	0.094***	-0.194***	0.111***	-0.166***	0.103***	-0.177***
	(0.002)	(0.038)	(0.002)	(0.038)	(0.015)	(0.039)
Deal Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes
Year Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes
Acquirer Industry Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes
Target Industry Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes
Observations	4858	4496	4858	4496	4858	4496
R-Squared	0.051	0.067	0.026	0.043	0.043	0.059

Table V
Market Reaction to Deal Announcement Over Time

This table reports linear regression models estimated via OLS of Cumulative Abnormal Return (CAR) estimated around merger announcements for the actual deals for which returns data are available in CRSP. The dependent variable is CAR, the 3-day cumulative abnormal announcement return for the acquirer (Column (1), (2), and (3)), the target (Column (4), (5), and (6)) and for a value-weighted portfolio of the acquirer and the target centered on the deal announcement date (Column (7), (8), and (9)). We introduce three variables (Post 2010, Post 2015, and Google SVI search) to identify periods of heightened concerns for cybersecurity risk. All variables are defined in the Appendix. All models include both target and acquirer industry (3-digits SIC code) fixed effects, and calendar year fixed effects. Standard errors are clustered at the target and acquirer industry level and calendar year. *, **, and *** refer to significance at the 10%, 5%, and 1% level, respectively.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Variable	Acquirer CAR			Target CAR			Combined CAR		
Acquirer Low Cybersecurity Risk (Tercile)	-0.010	-0.015	-0.026	-0.014	0.001	-0.004	-0.018*	-0.010*	-0.004
	(0.019)	(0.030)	(0.095)	(0.016)	(0.011)	(0.032)	(0.008)	(0.005)	(0.006)
Target Low Cybersecurity Risk (Tercile)	0.013	0.011	-0.025	-0.015	-0.004	-0.077**	0.007	-0.003	0.002
	(0.050)	(0.025)	(0.086)	(0.020)	(0.010)	(0.034)	(0.005)	(0.005)	(0.070)
Acquirer Low Cybersecurity Risk (Tercile) x Post 2010	0.013			0.013			0.029**		
	(0.024)			(0.008)			(0.012)		
Target Low Cybersecurity Risk (Tercile) x Post 2010	-0.003			0.003			-0.009		
	(0.034)			(0.013)			(0.012)		
Acquirer Low Cybersecurity Risk (Tercile) x Post 2015		-0.013			0.030***			0.036***	
		(0.019)			(0.007)			(0.014)	
Target Low Cybersecurity Risk (Tercile) x Post 2015		0.037			0.006			-0.002	
		(0.035)			(0.012)			(0.016)	

Acquirer Low Cybersecurity Risk (Tercile) x Google SVI Search			0.001			0.003**			0.004**
			(0.003)			(0.001)			(0.001)
Target Low Cybersecurity Risk (Tercile) x Google SVI Search			0.005			0.001			0.009
			(0.004)			(0.002)			(0.030)
Deal Controls									
All Cash	0.102	0.106	0.112	0.010	0.010	0.025	0.067*	0.068*	0.079*
	(0.080)	(0.082)	(0.087)	(0.028)	(0.029)	(0.031)	(0.036)	(0.037)	(0.002)
Tender Offer	-0.228*	-0.228*	0.000	-0.096***	-0.095***	0.000	-0.093**	-0.087**	-0.089**
	(0.117)	(0.122)	(0.000)	(0.030)	(0.031)	(0.000)	(0.047)	(0.044)	(0.037)
Same Industry	0.003	0.001	-0.015	0.005	0.005	-0.015	-0.004	-0.005	-0.019
	(0.033)	(0.032)	(0.032)	(0.017)	(0.016)	(0.016)	(0.026)	(0.026)	(0.023)
Acquirer Controls									
Firm Size	0.069***	0.068***	0.074***	-0.006	-0.006	-0.007	-0.007	-0.007*	-0.004
	(0.005)	(0.005)	(0.007)	(0.003)	(0.003)	(0.004)	(0.004)	(0.004)	(0.004)
Cash Holdings	0.002	-0.004	0.063	-0.030	-0.029	-0.076**	0.000	0.001	0.008
	0.069***	0.068***	0.074***	-0.006	-0.006	-0.007	(0.035)	(0.033)	(0.025)
% Institutional Ownership	0.009	0.010	0.010	-0.004	-0.004	-0.006	0.007	0.006	-0.003
	(0.016)	(0.016)	(0.019)	(0.009)	(0.010)	(0.010)	(0.012)	(0.012)	(0.014)
Staggered Board	-0.002	-0.002	-0.020	-0.012	-0.012	-0.016**	-0.016	-0.016*	-0.023**
	(0.021)	(0.021)	(0.024)	(0.007)	(0.007)	(0.006)	(0.009)	(0.009)	(0.010)
Leverage	-0.067*	-0.064*	-0.047	-0.016	-0.015	-0.012	-0.047**	-0.040**	-0.042**
	(0.037)	(0.036)	(0.046)	(0.014)	(0.014)	(0.019)	(0.019)	(0.018)	(0.019)
R&D to Sales	0.022*	0.022*	0.032***	-0.003	-0.003	-0.005	0.024**	0.025**	0.030***
	(0.011)	(0.011)	(0.008)	(0.004)	(0.004)	(0.003)	(0.010)	(0.010)	(0.009)
Tobin's Q	0.015**	0.015**	0.019*	-0.003	-0.003	-0.001	0.003	0.002	0.005**
	(0.006)	(0.006)	(0.010)	(0.004)	(0.004)	(0.004)	(0.002)	(0.002)	(0.002)
ROA	-0.029	-0.027	-0.053	0.001	0.002	-0.018	0.022	0.018	-0.006
	(0.061)	(0.063)	(0.103)	(0.022)	(0.022)	(0.032)	(0.038)	(0.040)	(0.005)

Target Controls									
Firm Size	-0.079***	-0.078***	-0.085***	0.002	0.002	0.003	0.002	0.002	-0.002
	(0.006)	(0.005)	(0.007)	(0.003)	(0.003)	(0.003)	(0.004)	(0.003)	(0.005)
Cash Holdings	0.076	0.079	-0.012	0.015	0.016	0.054**	0.011	0.014	-0.024
	(0.080)	(0.078)	(0.072)	(0.025)	(0.024)	(0.023)	(0.037)	(0.036)	(0.022)
% Institutional Ownership	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.001
	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.001)	(0.001)
Staggered Board	0.002	0.003	0.013	0.008	0.008	0.010	0.019*	-0.016*	0.021*
	(0.025)	(0.024)	(0.026)	(0.005)	(0.005)	(0.006)	(0.009)	(0.009)	(0.010)
Leverage	0.080	0.076	0.062	0.021	0.022	0.019	0.053***	0.052***	0.054**
	(0.049)	(0.047)	(0.053)	(0.014)	(0.013)	(0.016)	(0.017)	(0.017)	(0.018)
R&D to Sales	0.020***	0.020***	0.015	-0.003	-0.004	0.003	0.002	0.002	0.003
	(0.006)	(0.006)	(0.011)	(0.003)	(0.002)	(0.002)	(0.002)	(0.002)	(0.003)
Tobin's Q	-0.021**	-0.021**	-0.023**	0.002	0.002	-0.000	-0.006	-0.005	-0.007**
	(0.008)	(0.008)	(0.009)	(0.003)	(0.003)	(0.004)	(0.004)	(0.003)	(0.002)
ROA	0.042	0.039	0.090	-0.008	-0.010	0.012	-0.009	-0.009	0.027
	(0.064)	(0.067)	(0.105)	(0.012)	(0.013)	(0.035)	(0.040)	(0.042)	(0.060)
Constant	-0.082***	-0.081***	-0.090***	0.002	0.002	0.002	0.006	0.064***	0.069***
	(0.007)	(0.007)	(0.009)	(0.003)	(0.003)	(0.003)	(0.003)	(0.018)	(0.018)
Year Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acquirer Industry Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Target Industry Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
R-squared	0.556	0.555	0.558	0.165	0.167	0.165	0.237	0.182	0.195
Observations	508	508	508	493	493	493	482	482	482

Table VI
Likelihood of Merger Withdrawal

This table reports estimates from a logit model aimed at assessing the likelihood of an announced deal being completed. The dependent variable is an indicator variable that equals one if the deal is completed, 0 otherwise. All variables are defined in the Appendix. *, **, and *** refer to significance at the 10%, 5%, and 1% level, respectively.

Variable	(1)	(2)	(3)	(4)	(5)	(6)
	Withdrawn M&A Transaction					
Acquirer Low Cybersecurity Risk (Tercile)	0.057	0.029				
	(0.165)	(0.189)				
Target Low Cybersecurity Risk (Tercile)	-0.420**	-0.386**				
	(0.166)	(0.190)				
Acquirer Low Cybersecurity Risk (Quartile)			0.165	0.066		
			(0.215)	(0.243)		
Target Low Cybersecurity Risk (Quartile)			-0.404**	-0405**		
			(0.218)	(0.247)		
Acquirer Low Cybersecurity Risk (Quintile)					0.274	0.176
					(0.221)	(0.253)
Target Low Cybersecurity Risk (Quintile)					-0.496**	-0.473*
					(0.228)	(0.262)
Acquirer Controls						
Firm Size		-0.432***		-0.427***		-0.427***
		(0.092)		(0.092)		(0.092)
Cash Holdings		-0.789		-0.804		-0.801
		(0.850)		(0.848)		(0.848)
% Institutional Ownership		0.745***		0.744***		0.744***
		(0.281)		(0.279)		(0.279)

Staggered Board		0.101		0.109		0.116
		(0.217)		(0.217)		(0.217)
Leverage		0.718*		0.707*		0.712*
		(0.411)		(0.411)		(0.411)
R&D to Sales		0.372		0.373		0.373
		(0.235)		(0.235)		(0.235)
HHI (SIC3)		0.776		0.951		0.968
		(1.676)		(1.635)		(1.638)
Tobin's Q		-0.118		-0.116		-0.116
		(0.093)		(0.093)		(0.093)
ROA		0.003		0.021		0.010
		(0.772)		(0.772)		(0.772)
Target Controls						
Firm Size		0.485***		0.480***		0.479***
		(0.091)		(0.091)		(0.091)
Cash Holdings		0.014		0.009		-0.003
		(0.834)		(0.833)		(0.832)
% Institutional Ownership		0.732***		0.732***		0.745***
		(0.268)		(0.268)		(0.271)
Staggered Board		-0.164		-0.170		-0.170
		(0.214)		(0.214)		(0.213)
Leverage		-0.984**		-0.983**		-0.988**
		(0.433)		(0.433)		(0.434)
R&D to Sales		-0.283		-0.287		-0.286
		(0.300)		(0.303)		(0.302)
HHI (SIC3)		0.091		-0.064		-0.103
		(1.694)		(1.653)		(1.656)
Tobin's Q		0.156**		0.156**		0.156**
		(0.075)		(0.075)		(0.075)
ROA		0.068		0.045		0.048
		(0.659)		(0.658)		(0.659)
Observations	607	508	607	508	607	508

Table VII
Paid Premium

This table reports estimates from a linear regression model assessing the association between the premium paid and firms' cybersecurity risk profile. The dependent variable is the difference ratio of the deal valuation to the target's market capitalization as observed four weeks before the deal completion. All models include both target and acquirer industry (3-digits SIC code) fixed effects and calendar year fixed effects. Standard errors are clustered at the target and acquirer industry and year. All variables are defined in the Appendix. *, **, and *** refer to significance at the 10%, 5%, and 1% level, respectively.

	(1)	(2)	(3)	(4)	(5)	(6)
Variable			Merger Premium			
Acquirer Low Cybersecurity Risk (Tercile)	2.843***	2.901**				
	(0.843)	(1.370)				
Target Low Cybersecurity Risk (Tercile)	-4.400	-3.024				
	(3.289)	(3.031)				
Acquirer Low Cybersecurity Risk (Quartile)			3.309***	4.110***		
			(1.098)	(1.420)		
Target Low Cybersecurity Risk (Quartile)			-0.896	-1.659		
			(0.808)	(1.253)		
Acquirer Low Cybersecurity Risk (Quintile)					3.510***	4.231**

			(1.018)	(1.522)
Target Low Cybersecurity Risk (Quintile)			-0.990	-1.765
			(0.961)	(1.468)
Deal Controls				
All Cash	12.059	12.459		11.803
	(10.682)	(10.917)		(10.436)
Tender Offer	48.659***	46.807***		51.970***
	(12.354)	(12.370)		(10.542)
Same Industry	-13.272	-11.886		-15.477
	(8.424)	(9.163)		(9.862)
Acquirer Controls				
Firm Size	3.782**	3.767**		3.919**
	(1.410)	(1.488)		(1.483)
Cash Holdings	13.493	12.475		14.131
	(14.469)	(15.053)		(14.636)
% Institutional Ownership	0.497***	0.505***		0.497***
	(0.315)	(0.299)		(0.300)
Staggered Board	4.525	4.295		4.211

	(3.596)	(3.524)	(3.789)
Leverage	-3.520	-4.868	-4.398
	(9.730)	(9.673)	(9.806)
R&D to Sales	-2.630	-2.310	-2.480
	(2.003)	(2.123)	(2.252)
HHI (SIC3)	-13.743	-15.553	-12.120
	(26.486)	(27.205)	(31.744)
Tobin's Q	0.520	0.525	0.379
	(1.638)	(1.543)	(1.636)
ROA	3.841	6.034	1.521
	(23.840)	(23.932)	(20.974)
Target Controls			
Firm Size	-4.738***	-4.595***	-4.737***
	(1.230)	(1.275)	(1.391)
Cash Holdings	-5.054	-6.498	-7.302
	(13.138)	(14.220)	(12.782)
% Institutional Ownership	0.697***	0.689***	0.652***
	(0.156)	(0.163)	(0.181)
Staggered Board	-1.831	-1.578	-1.791
	(4.487)	(4.272)	(4.727)

Leverage		11.566		12.667		11.727
		(10.417)		(10.115)		(10.291)
R&D to Sales		-0.417		-0.634		-0.655
		(1.018)		(0.959)		(0.848)
HHI (SIC3)		5.809		10.664		5.162
		(23.610)		(24.368)		(24.664)
Tobin's Q		-3.117***		-3.007***		-2.706***
		(0.491)		(0.576)		(0.671)
ROA		10.280		8.571		9.376
		(14.352)		(14.127)		(14.365)
Year Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes
Acquirer Industry Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes
Target Industry Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes
R-squared	0.169	0.237	0.171	0.240	0.171	0.240
Observations	419	384	419	384	419	384

Table VIII
Post-Acquisition Performance

This table reports estimates from a linear regression model assessing the association between acquirers' post-merger performance and deals' cybersecurity risk profile. The dependent variable is the ratio of operating income before depreciation to total assets (ROA). Post is a dummy set equal to one for the three years following the deal, zero otherwise. The model is estimated over the six years surrounding the event. All models include firm fixed effects and calendar year fixed effects. Standard errors are clustered at the year level. All variables are defined in the Appendix. *, **, and *** refer to significance at the 10%, 5%, and 1% level, respectively.

	(1)	(2)	(3)
Variable		ROA	
Low Cybersecurity Risk Acquirer (Tercile) x Post	0.010*		
	(0.006)		
Low Cybersecurity Risk Target (Tercile) x Post	0.000		
	(0.012)		
Low Cybersecurity Risk Acquirer (Quartile) x Post		0.017*	
		(0.007)	
Low Cybersecurity Risk Target (Quartile) x Post		0.001	
		(0.021)	
Low Cybersecurity Risk Acquirer (Quintile) x Post			0.017*
			(0.008)
Low Cybersecurity Risk Target (Quintile) x Post			-0.001
			(0.019)
Additional Controls	Yes	Yes	Yes
Year Fixed Effects	Yes	Yes	Yes
Firm Fixed Effects	Yes	Yes	Yes
Observations	2,304	2,304	2,304
R-squared	0.791	0.792	0.792

Table IX
Post-Acquisition Performance

This table reports estimates from a linear regression model assessing the association between the likelihood of post-merger goodwill impairment and the deal's cybersecurity risk profile. The dependent variable is a dummy set equal to one if the acquirer recognizes a goodwill write-off over the three years following the deal, zero otherwise. All models include industry (3-digits SIC code) fixed effects and calendar year fixed effects. Standard errors are clustered at the industry and year level. All variables are defined in the Appendix. *, **, and *** refer to significance at the 10%, 5%, and 1% level, respectively.

	(1)	(2)	(3)
Variable	Goodwill Impairment		
Low Cybersecurity Risk Acquirer (Tercile)	-0.098**		
	(0.042)		
Low Cybersecurity Risk Target (Tercile)	0.201		
	(0.277)		
Low Cybersecurity Risk Acquirer (Quartile)		-0.081*	
		(0.036)	
Low Cybersecurity Risk Target (Quartile)		-0.139**	
		(0.053)	
Low Cybersecurity Risk Acquirer (Quintile)			-0.084*
			(0.044)
Low Cybersecurity Risk Target (Quintile)			-0.135**
			(0.060)
Additional Controls	Yes	Yes	Yes
Year Fixed Effects	Yes	Yes	Yes
Industry Fixed Effects	Yes	Yes	Yes
Observations	464	464	464
R-squared	0.270	0.266	0.268

Appendix Table A
Variable Definitions

Variable	Definition
Cybersecurity Risk	
Low Cybersecurity Risk (Tercile)	An indicator variable set equal to 1 if the firm-year observation belongs to the lowest tercile of the industry-year distribution of the Florackis et al. (2022) cybersecurity risk measure.
Low Cybersecurity Risk (Quartile)	An indicator variable set equal to 1 if the firm-year observation belongs to the lowest quartile of the industry-year distribution of the Florackis et al. (2022) cybersecurity risk measure.
Low Cybersecurity Risk (Quintile)	An indicator variable set equal to 1 if the firm-year observation belongs to the lowest quintile of the industry-year distribution of the Florackis et al. (2022) cybersecurity risk measure.
Low Cybersecurity Risk Pair (Tercile)	An indicator variable set equal to 1 if the both the target and acquirer of an actual or pseudo merger belong to the lowest tercile of the industry-year distribution of the Florackis et al. (2022) cybersecurity risk measure.
Low Cybersecurity Risk Pair (Quartile)	An indicator variable set equal to 1 if the both the target and acquirer of an actual or pseudo merger belong to the lowest quartile of the industry-year distribution of the Florackis et al. (2022) cybersecurity risk measure.
Low Cybersecurity Risk Pair (Quintile)	An indicator variable set equal to 1 if the both the target and acquirer of an actual or pseudo merger belong to the lowest quintile of the industry-year distribution of the Florackis et al. (2022) cybersecurity risk measure.
Deal Characteristics	
Due Diligence Period	The number of days between the deal announcement and its completion or withdrawal.
Premium	The difference between the deal valuation and the market value of the target as observed four weeks prior to its completion.
Tender Offer	An indicator variable set equal to 1 if the deal is initiated via a tender offer, 0 otherwise.
Horizontal acquisition	An indicator variable set equal to 1 if both the target and the acquiring firm belong to the same SIC 3 digits industry, 0 otherwise
All Cash Deal	An indicator variable set equal to 1 if the deal is fully paid in cash, 0 otherwise.
Withdrawn	An indicator variable set equal to 1 if the deal is withdrawn, 0 if it is completed.

Firms Characteristics	
Assets	The book value of assets adjusted for inflation using 2009 dollars. We use the natural logarithm of this variable.
Tobin's Q	Market value of outstanding equity plus the book value of debt minus the firm's current assets divided by the sum of the book value of property, plant, and equipment, and the replacement cost of intangible capital (the sum of the firm's externally purchased and internally created intangible capital). Calculation follows Peters and Taylor (2017). Measure and source data is available on WRDS.
Cash	Cash and short-term investments scaled by the book value of assets. Calculated from Compustat using che / at.
% Institutional Ownership	% of shares hold by institutional investors as disclosed in end-of-the-year 13F forms.
Staggered board	Staggered board is indicator variable developed in Guernsey et al. (2022) and named cbi. The indicator is set equal to 1 if a firm has a classified board, and 0 otherwise. "This variable is based on our manual corrections and the date when a (de)classified board is fully implemented (i.e., when all board members are subject to annual elections or all board members have staggered terms). This variable typically takes a value of 1 a couple of years after when cbv equals 1. We recommend using this variable in situations such as when examining the relation between classified boards and firm outcomes (e.g., M&A decisions or shareholder value), as the relevant period is when all directors can be replaced at the annual meeting (i.e., a fully declassified board) that creates disciplining incentives."
Leverage	Book leverage. Calculated from Compustat using (dltt + dlc) / at.
R&D to Sales	The ratio of R&D expenditure to total sales. Calculated from Compustat using xrd / sale.
HHI (SIC3)	The Herfindahl–Hirschman Index, computed using the Compustat universe of firms and based on 3-digits SIC industries
ROA	Return on assets. Calculated from Compustat using oibdp / at.
KLD Net Score	A score computed as the difference between the total sum of strengths and concerns for firm i in year t. Data are from the KLD dataset.