# M&A Effect on Data Breaches in Hospitals: 2010-2022

Nan Clement

Updated frequently. Click here for the latest version.

**Abstract**

I study whether and how hospital mergers increase the probability of a data breach. Using proprietary hospital merger records and the archived data breach reporting from the Department of Health and Human Services from 2010 to 2022, I implement a stacked difference-in-differences estimation strategy to show that in the two-year window after hospital consolidation, incidents of data breaches in merger targets, buyers, and sellers more than double as compared to the pre-treated groups. The effect is robust to changes of the two-year window. The effect is also robust to the change in sample size due to the data availability of the control variables and the change in how standard errors are clustered. The signaling effect that reduces hackers' information asymmetry about the merging hospitals before the operational merger start causes an increase in hacking activities on hospitals, especially in recent years through ransomware attacks. The incompatibility of the two merging information systems causes an increase in hacking as well. Conversely, the complementary effect of organizational capital that improves internal risk control reduces the increase in data breaches. For example, mergers involving publicly traded hospitals can experience a decrease in data breaches during the time window. The truncated regression for the past five years shows that the data breach situation during mergers is getting worse because of soaring cases of hacking activities, even though the market's efforts to address misconduct breaches have increased.

First draft: February 2023. I would like to express my heartfelt gratitude to my advisors, Daniel Arce, Catherine Tucker, Anne Burton, and Anton Sobolev, for their invaluable guidance, unwavering support, and exceptional expertise throughout the entire dissertation process. I am deeply thankful to the participants in the following events: the 2022 WEIS rump session organized by Tyler Moore, Laura Brandimarte and Sadia Afroz, AEA-CSWEP online and SEA mentoring organized by Catherine Maclean, Orgül Öztürk, Melanie Guldi and Maya Rossin-Slater, the Texas Applied Microeconomics Student Workshop organized by Francisco Pardo Pajuelo, and the Cybersecurity Summer Institute at Georgia Tech organized by Nadiya Kostyuk. I am grateful to the reviewers of the 2023 WEIS for their positive and constructive feedback. Furthermore, I would like to extend my thanks to Avi Goldfarb and Catherine Tucker for their NBER Economics of Privacy Tutorial in Fall 2022. Any remaining mistakes or shortcomings in this work are solely my own responsibility.

# 1 Introduction

In 2022, healthcare data breaches in the US hit more than 40 million victims, violating their privacy rights. Nearly 600 hospitals spent multi-millions of dollars for ransom, lawsuits, incident response, and recovery in the year. More seriously, data breaches can be life-threatening emergencies for the entire hospital or, even worse, all the hospitals in a health system that share the information system infrastructure. For example, a newborn died nine months after being delivered in an Alabama hospital during a three-week ransomware IT meltdown in 2019. The mother alleges in a lawsuit that she was not informed of the cyberattack, which interrupted critical medical data availability leading to the death. A previous study shows that, in the long term, data breaches increase mortality rates and reduce healthcare quality (Choi and Johnson, 2019). Given these serious consequences, identifying risk factors for data breaches is crucial. I study whether, and how, hospital mergers increase the probability of a data breach. This paper is among the first empirical attempts to test what may be a reason that some hospitals have data breaches rather than others.

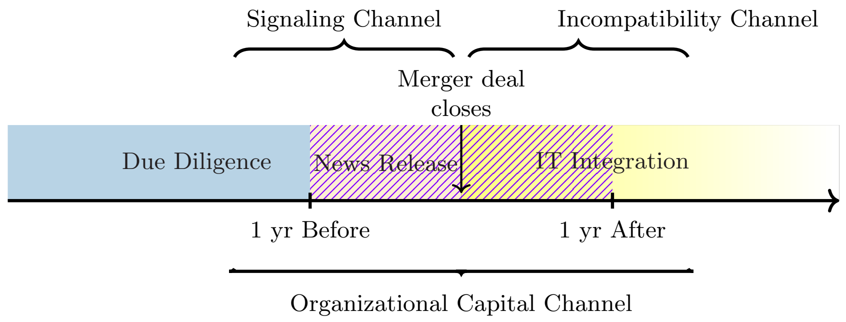


Figure 1: Merger Timeline and 2-year Window

*Notes:* The figure illustrates the two-year window. The Incompatibility Channel does not start until the merger deal closes. The cyber-attacks happen before are captured in the Signaling Channel. The main model assumes the Signaling Channel starts one year before the merger deal closes. Alternative assumptions are tested as well. Operational Capital Channel reflects the complimentary effects to IT security through out the process.

To achieve the goal, I use stacked difference-in-differences (Deshpande and Li, 2019) to document the result of changes in hospital cybersecurity risk factors during the process of mergers. I test whether hospital data breaches happen more often surrounding the two years when the hospital consolidation deal is closed, [one year before the merger deal closes, one year after the merger deal closes]. As shown in figure 1, the arrow points to the merger deal closure date in my observation. The closure date is when the merger deal is finalized and signed after years of investigation and negotiation. After the merger signing date, operational integration starts, including IT infrastructure integration, data migration, and cybersecurity protocols incorporation. The two-year window is the shaded area around the date. Section 3.3 provides more detailed background information on the merger timeline in figure 1. The stacked difference-in-differences estimation strategy holds mergers to be signed in two years or later as the control/pre-treated group. I test whether the hospital signs the deal on the "merger deal closes" date or the pre-treated group has more data breaches in the shaded two-year period.

To facilitate my research design, I use American hospital data, specifically proprietary hospital merger records and archived healthcare breach reporting data from the Office of Civil Rights. This data serves several important purposes. First, it provides accurate information on the exact dates of merger signings and data breach reports, which is essential for data building and analysis. These specific dates enable a granular analysis along the timeline. Second, the merger records include relevant information such as the hospital's size, market visibility, and profitability, factors that can influence its attractiveness as a target for cyberattacks. Third, the healthcare industry is the first in the US to mandate the reporting of data breaches. The Office for Civil Rights is responsible for monitoring and investigating hospitals' data breach reports, as required by section 13402(e)(4) of the HITECH Act. To ensure accuracy, I only use archived data from 2010 and up until 2022.

I begin by documenting that data breaches happen more during the two-year window. By examining the entirety of this period, I demonstrate that data breaches happen twice as often during this specific window. On average, the probability of a data breach for pre-merger deals is approximately 3%, while the data breach rate reaches 6% for the treated group. The increase in the mean occurs in the target hospitals for mergers, as well as among the buyers and sellers. Furthermore, I show that the gradual inclusion of control variables does not alter the magnitude of the effect.

My research design is subject to two concerns. The first relates to the identification assumptions underlying the difference-in-differences model. I justify the assumptions in several ways. First, by employing stacked difference-in-differences and using future mergers as control groups, I avoid using already treated cases as control in classic staggered treatment difference-in-differences analysis (Goodman-Bacon, 2021). Second, I employ an event study design focusing on mergers that occurred in 2018 and 2019. Through graphical analysis, I demonstrate that hospitals' data breach probabilities do not exhibit divergent trends prior to the treatment time, which is defined as one year before the merger deal is signed. Last, I provide evidence that the dynamic effects of the merger progressively increase as approaching the merger signing date.

The second concern pertains to the two-year window in my research design. It is possible that the effects of mergers on data breaches begin before one year prior to the signing of the merger deal or persist beyond the observed window. To address this concern, I present several pieces of evidence. First, I examine data from Google Trends regarding abnormal search patterns to provide supporting evidence that one year before merger deal is signed is a reasonable approximation to when the news is out. Hackers have been known to exploit Google Trends by taking advantage of unpredictable events like earthquakes to manipulate search results and promote malicious content (Bittner and Ullrich, 2023). Secondly, I extend the window symmetrically to include a four-year and six-year timeframe and present the corresponding results. Thirdly, I explore an asymmetric window, focusing on one year prior to the deal's signing and three years after the merger is completed, and demonstrate that it yields similar findings. The identification of the three-year window is based on Gaynor, Sacarny, Sadun, Syverson and Venkatesh (2021) finding that following the merger deal closes, the target hospitals initiated the installation of EMR from the acquirer's vendor, with modest progress initially that later accelerated, resulting in a third of the hospitals implementing the system within three years.

I then proceed to investigate the mechanisms underlying this effect and present four key findings. First, I observe that the increase in data breaches during mergers is primarily driven by a rise in hacking incidents rather than insider misconduct breaches. To examine this, I remove data breaches caused by hackers and demonstrate that although there is an increase in the mean, the results are no longer statistically significant when considering only misconduct breaches. To assess whether this pattern holds for both the buyers and the merger targets, I further stratify the breaches based on the involved parties and show that there is no significant effect on either group. The probability of insider misconduct data breaches for a pre-merger group is 2.7%. During the merger, it increases by around 30% but with significant variation. I interpret these findings as evidence that while insider misconduct may contribute to a higher occurrence of data breaches during mergers, it does not dominate the observed results.

My second finding about the mechanisms is that such an increase in hacking is due to two effects. Upon confirming that the consolidation period is associated with more data breaches, I introduce two mechanisms that explain how merger events can alter the outcome of the hospital-hacker interaction and empirically evaluate these mechanisms using the baseline model on hacker-triggered data breaches. The first mechanism accounts for the vast amount of information released about the target hospitals and the buyers, which reduces information asymmetry on the hackers' side. I refer to it as the "Signaling Channel." The second mechanism recognizes consolidating two different information systems generates more vulnerability on the hospitals' side. I refer to this as the "Incompatibility Channel." I identify the Signaling Channel using the year before the merger closing period when the public knows about the potential merger, but the deal is not yet signed. Before the deal is signed, it is impossible that operations have started to merge. Consequently, the year after the deal is signed identifies the Incompatibility Channel during the IT consolidation. In this way, I document a closer examination of cybersecurity risk changes along the merger timeline. The signaling channel accounts for a 1.98 percentage point increase in hacking data breaches during consolidations. Hacking data breaches owing to incompatibility increased by 1.62 percentage points in the year after the deal closes. For the pre-merger group, the probability of hacking is 0.52%, and for the treated group during the merger, the probability increases 5 times to 2.6%, similar to the observed probability in misconduct breaches. In detail, before the deal is signed, the probability of hacking for a pre-merger group is 0.14%, and it increases 10 times for the merging deals to 1.41%, and after the deal is signed, the probability of hacking for the pre-merger group is 0.38%, and it increases 3 times to 1.19%. These findings suggest that merger events reshape the hackers' behavior because the information structure is changed, and incompatibility increases vulnerability.

My third finding is that ransomware attack happens significantly more through both Signaling Channel and the Incompatibility Channel, but increase even more through the Signaling Channel. This finding is important because ransomware attacks disrupt hospital operations and even cause death. For example, a tragic incident at Dusseldorf University Hospital in Germany, where a hospital turned away an ambulance due to a ransomware attack and a 78 years old patient on the way to another hospital, highlights the potential dangers and consequences of this specific kind of attack on healthcare institutions (Ralston, 2020). These findings indicate that the rise in data breaches during mergers can significantly decrease patients' well-being. Moreover, it is important to note that my results show that ransomware attacks are not solely caused by an increase in vulnerability resulting from incompatibility, but more by a change in the hackers' motivation and behaviors.

My fourth finding emphasizes the crucial role of organizational capital in reducing the risks of data breaches, especially in deals that involve a public buyer, a public target, or a non-financially distressed target hospital, where the surge in data breaches during the merger is mitigated as compared with those that do not have the comparative advantage of organizational capital. Especially for those deals involving a publicly traded target hospital, there is even a decrease in insider misconduct breaches during the two-year window.

Motivated by these findings, I next examine whether the market has effectively addressed the privacy protection issues that arise from hospital mergers, considering patients' increased awareness and bargaining power. I use truncated and stratified results to investigate this issue. The baseline regression result over the past five years shows that even though the efforts in mitigating the misconduct data breaches have increased, the surge in hacking activities overturned the efforts. Furthermore, an examination of private market funding deals can offer valuable insights into how professional investors, who often prioritize short-term profit-seeking objectives and respond rapidly to market fluctuations, respond to the increasing privacy awareness and bargaining power of patients, and the potential impact such responses may have on the data breaches during mergers. The analysis on professional investors shows that they are able to reduce data breaches before the merger signing date.

My contribution differs from previous studies in four key dimensions. First, the findings presented in this paper are among the first to empirically investigate what causes data breaches in some hospitals rather than others. Second, by comparing the results for different levels of organizational capital during the special transformation period of a merger, I verify its importance for information technology application change and effective risk control. Third, by documenting the changed results of hackers' behavior during the merging process, I partially reveal the preferences of malicious actors with respect to their reactions to market structure change in the healthcare market. Lastly, I contribute to the discussion of privacy protection and competition and recent literature on the effect of Private Equity (PE) on healthcare. The new results are well-timed both for the undergoing discussion of data breach disclosure policy at the federal and state level and around the world and for the antitrust regulation reforms that consider new evaluations for data-driven mergers.

My findings point to M&A as a fundamental reason for the rise in healthcare data breaches. Considering the rising cybersecurity costs for companies in recent years, the government should provide cybersecurity incident prevention warnings based on the hospital and health system size and market visibility. Best practice managing post-merger information system risk control deserves more policy attention from the healthcare and financial market authorities. Overall, my results suggest that new measures for cyber risk prevention during the merger process are needed to protect hospitals' data safety.

The remaining parts of this paper proceed as follows. Section 2 goes into detail in discussing the literature. In Section 3, the institutional context and summary statistics are presented, with particular emphasis on introducing the two types of data breaches. Section 4 discusses the methodology and critical assumptions. In section 5, 6, and 7, I present the main results and discussions on the mechanisms. Section 8 tests alternative assumptions on time windows before concluding in section 9.

# 2 Literature Review

## 2.1 Healthcare Security

Health data digitization brings direct benefits for medical record data holders, but a trade-off between privacy protection and "data-based technological process" exists (Acquisti, Taylor and Wagman, 2016). Information technology adoption improves healthcare quality and the healthcare ecosystem (Yuan, Li and Wu, 2021; Lin, Lin and Chen, 2019). As hospitals adopt information systems, data breaches also show up and negatively impact the welfare of patients (Kwon and Johnson, 2015b; Huang, Behara and Goo, 2014; Payne, Bates, Berner, Bernstam, Covvey, Frisse, Graf, Greenes, Hoffer, Kuperman et al., 2013). Notably, Choi and Johnson (2019) prove that data breaches increase the mortality rate. As private data accumulate exponentially, regulations catch up in attempting to protect it from malicious usage and ungraceful storage. A stream of literature has studied the trade-off between privacy protection laws and innovation in healthcare information system technology(Janakiraman, Park, M. Demirezen and Kumar, 2022; Miller and Tucker, 2018; Adjerid, Acquisti, Telang, Padman and Adler-Milstein, 2016; Miller and Tucker, 2011, 2009). As information technology adoption is beneficial and data breaches can be life-threatening and operationally disrupting, why are some hospitals rather than others attacked in the first place? I contribute to the discussion by switching the focus to the reasons behind cyber-attacks on hospitals, one of the hospitals' biggest concerns nowadays when utilizing digitization.

## 2.2 Market Competition and Privacy

The second body of literature addresses the relationship between privacy protection and market competition (Cecere, Le Guel, Lefrere, Tucker and Yin, 2022; Marthews and Tucker, 2019). Hospital mergers and acquisitions claim to reduce costs by achieving scope and scale economies. By contrast, I bring light to the potential cost of merging two information systems (Gaynor, Sacarny, Sadun, Syverson and Venkatesh, 2021). Market competition has an inverse effect on privacy protection because hospitals shift resources to more visible activities from data protection to compete (Gaynor, Hydari and Telang, 2012; Geer, Jardine and Leverett, 2020). Instead of focusing on the long-term merger synergies of mergers and their impact on privacy protection behavior, I contribute to the conversation by documenting the rise in data breaches that occur during mergers. By doing so, I show how changes in market structure can impact short-term privacy behaviors with potentially harmful consequences for patients.

The motivation to merge also evolves as technology progresses throughout time. Data-driven healthcare service evolves thanks to computation technology(Miller, 2022). In recent years, there has been a growing number of data-driven merger cases in the healthcare industry. "Data blocking" (Savage, Gaynor and Adler-Milstein, 2018) means health systems prevent the patients' data from transferring to providers outside their system. Such a data-blocking effect should induce data-driven mergers (Chen, Choe, Cong and Matsushima, 2022). The data-driven mergers in hospitals have a further impact on the hospital competition (De Corniere and Taylor, 2020), and data-driven mergers in healthcare attract authorities' attention (Wilde and Kendall, 2022). I participate in the conversation by providing evidence on how to fully account for the potential risks of the increasing data-driven mergers.

## 2.3 Economics of Digitization

American companies have better readiness for IT adoption and are most advanced in their digital transformation because of the intangible investment ties to the IT technology, namely the "organizational capital and organizational structure" (Goldfarb and Tucker, 2019; Brynjolfsson, Hitt and Yang, 2002) including business process redesign, co-invention of new products and business models, and investments in human capital. Previous research has demonstrated that US firms have a greater ability to utilize information and communication technologies (ICT) due to their superior organizational capital (Bloom, Sadun and Van Reenen, 2012). Organizational capital enables them to leverage technology more efficiently and effectively, and organizational capital and structure are critical factors in maximizing the benefits of ICT investments (Goldfarb and

Tucker, 2019; Bresnahan, Brynjolfsson and Hitt, 2002; Milgrom and Roberts, 1990; Garicano, 2010; Brynjolfsson, Rock and Syverson, 2021). However, given that hospitals have higher rates of IT adoption, it remains unclear what role organizational capital plays in IT productivity in the later stage of adoption. To address this gap, this study investigates the contribution of organizational capital to cybersecurity during mergers and acquisitions, particularly in the context of hospital IT transformation. I assess the impact of mergers on varying levels of organizational capital environments by stratifying deals involving publicly traded hospitals, bankrupt hospitals, or buyers with a female CEO. By doing so, this research contributes to the existing literature on the role of organizational capital in MA and sheds light on how different levels of organizational capital can impact cybersecurity outcomes in merger deals.

## 2.4 Economics of Cybersecurity and Privacy

The economics of cybersecurity literature dives deeper into the equilibrium of privacy protection behaviors by considering the malicious actors' motivations and strategies. The economic effects of a breach show up in terms of stock price reactions (Islam, Wang, Farah and Stafford, 2022; Kannan, Rees and Sridhar, 2007; Acquisti, Friedman and Telang, 2006; Campbell, Gordon, Loeb and Zhou, 2003) or credit financial resources reactions (Huang and Wang, 2021; Blascak and Toh, 2022), and has a long-term effect on competition (De Corniere and Taylor, 2020; Chen, Choe, Cong and Matsushima, 2022; Bonatti and Cisternas, 2020; Chen, Choe and Matsushima, 2020; Kwon and Johnson, 2015a; Acquisti and Varian, 2005). By contrast, I address how hackers react to M&A as a major market structure change and important financial source for innovation.

The literature assumes that a larger market share attracts more cyber attacks (O'Donnell, 2008; Garcia, Sun and Shen, 2014; Arce, 2018; Geer, Jardine and Leverett, 2020). My analysis provides new empirical evidence on the association between economic motivation and cybersecurity (Arce, 2022) by supporting this hypothesis. M&A, as an external shock on market share, signals to the hackers the potential financial benefit. At the same time, most healthcare providers are not public companies, and when they announce a potential acquisition, it signals to the market that they have the resources for expansion. For example, one interpretation of the news could be that if they have the cash to buy a new hospital, they have the cash to pay a ransom. Such evidence verifies the importance of economic motivation for successful cyber-attacks in the health industry and answers whether hackers indeed do a cost-benefit analysis. The results in this paper partially reveal the preference and the change in their strategic behavior when hackers face such a big information asymmetry reduction. Specifically, the extant literature focuses on the static view of the hospital-hacker interaction (Cavusoglu, Raghunathan and Yue, 2008), but my paper instead focuses on the timeline of the long merger process and how different stages of such process may change the results.

Instead of the mismanagement issues raised by the lack of organizational capital, another interpretation of some of the serious data breaches from within the institution is insider cyber crime (Nykodym, Taylor and Vilela, 2005; Shaw, 2006; Greitzer, Moore, Cappelli, Andrews, Carroll and Hull, 2008; Georgiadou, Mouzakitis and Askounis, 2022). I contribute to this literature by analyzing this alternative interpretation.

### 2.5 Private Equity Funding's Effect on Hospital Mergers

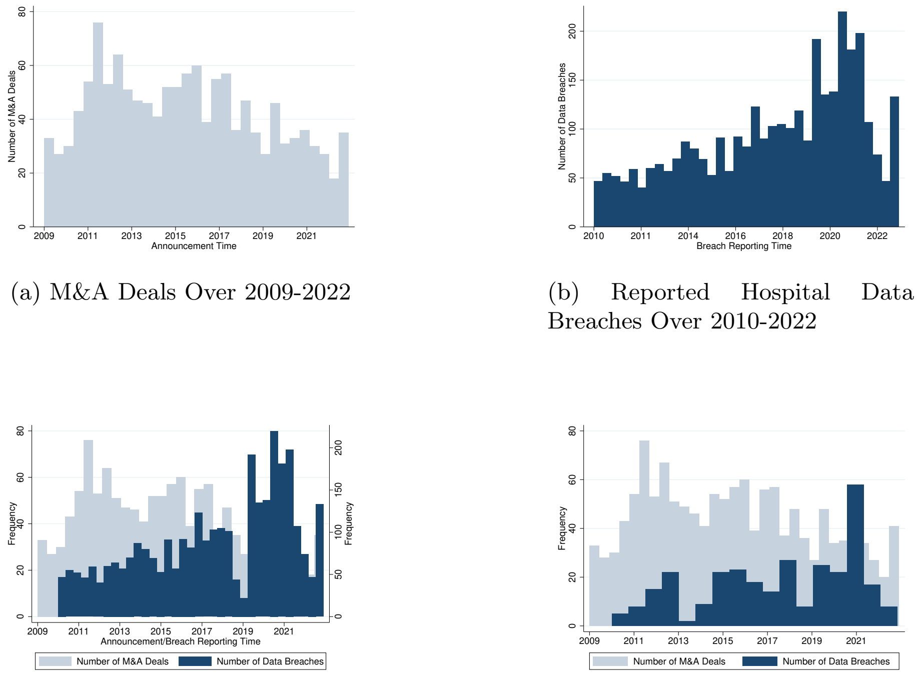
The healthcare industry has seen a significant increase in PE investment in the past decade, with an estimated $800 million dollars flooding into the sector (Scheffler, Alexander and Godwin, 2021). Nevertheless, the impact of such investment on the welfare of hospitals and patients has remained a subject of discussion in the PE literature (Bruch, Gondi and Song, 2020; Liu, 2021; Richards and Whaley, n.d.; Gao, Sevilir and Kim, 2021). While some scholars assert that PE investment generates employment opportunities and enhances profitability, others argue that these objectives may not be aligned with the priorities of hospitals and patients. These opposing views can be attributed to two policy deliberations centered on the commercialization of medical practice (Zhu, Hua and Polsky, 2020) and the potential for rent-seeking behavior (Gondi and Song, 2019).

To contribute to the discussion of the impact of commercialization, this paper focuses on the immediate implications of PE investment in healthcare, specifically highlighting the potential for private equity funding to improve cybersecurity outcomes compared to other investors. The central argument is that if private equity funding investors can effectively control data breaches, it is reasonable to have confidence that market forces can resolve this issue. Notably, in this scenario, private equity funding is not a healthcare provider and does not report data breaches, and the acquisition process involves zero incompatibility issues. Additionally, the signaling effects are minimal due to its positioning outside of the regulatory radar. This type of analysis presents a unique opportunity to examine the cybersecurity experiences of target hospitals internally.

## 3 Institutional Context and Data

### 3.1 Data Source

To answer the question of whether mergers cause more data breaches or not, I combine two data sets at the quarterly level. The first data set is the merger deals closed in 2009-2022 from the proprietary merger data platform. Graph 2a shows the number of hospital merger deals signed in each quarter. This data set is commonly used in the economics of health literature for accurate hospital merger information. The advantage of this data is that it has an accurate date when the merger deal is signed. At the same time, the merger records include relevant information such as the hospital's size, market visibility, and profitability. The second data set is the U.S. Department of Health and Human Services, Office of Civil Rights' archived healthcare breach reporting data for



(a) M&A Deals Over 2009-2022

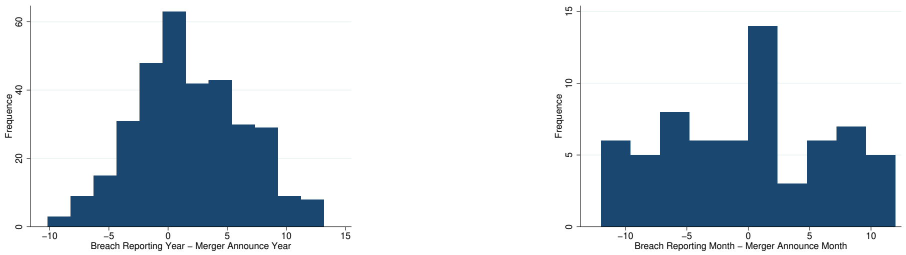
(b) Reported Hospital Data Breaches Over 2010-2022

(c) M&A Deals and Data Breaches Over 2009-2022 (all)

(d) M&A Deals and Data Breaches Over 2009-2022 (matched)

Figure 2: M&A Deals and Data Breaches Over 2009-2022

*Notes:* The figure shows the number of the mergers and reported data breaches in each quarter from 2009-2022. Data source: Proprietary merger information and DHHS 2009-2022.



(a) Breach Reporting Year - Merger Closing Year (matched)

(b) Whithin 1 year: Breach Reporting Month - Merger Closing Month (matched)

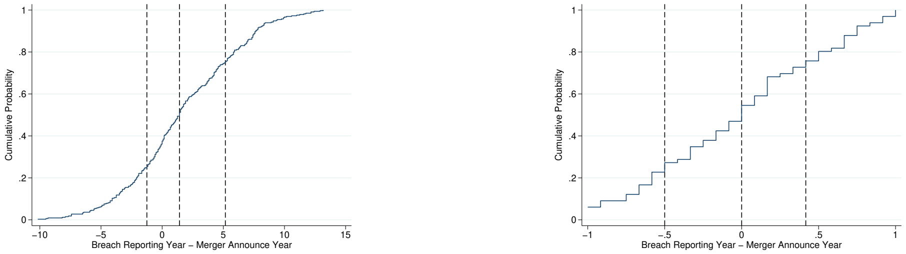
Figure 3: Time Difference: Breach Reporting Time Minus Merger Closing Time

*Notes:* The figure shows the histogram for the number of reported data breaches around the merger signing date. Data source: Proprietary merger information and DHHS 2010-2022.

2010-2022 (DHHS), as shown in figure 2b. The official reporting period began in 2009; however, there were only a limited number of reports during the ramp-on period with possible delays. Therefore, I remove them for accuracy. In the context of this study, the merger data under consideration spans the period from 2009 through to the end of 2022. Similarly, the data on data breaches covers the period from 2010 until the end of 2022. Notably, for mergers that took place in 2009, only the post-closure effect is analyzed, while for those in 2022, only the pre-merger signing effect is taken into account.

The combination of the two events over time is shown in figure 2c. The dark histograms are the number of breaches reported in each quarter, and the light color histograms are the number of mergers signed in each quarter. To find out which hospitals or health systems experience a merger reports data breach, I match the names of the target, the buyer, and the seller of each hospital merger deal to the reporting entity in the data breach database. In the last graph, figure 2d, the dark histogram is the number of such matched data breaches each month. It shows how many hospitals and health systems recorded in the merger data also report a data breach.

Such matching includes the data breaches that either happen before or after the merger closes. I plot the difference between the merger signing date and the breach reporting date in figure 4a. I limit my analysis of the merger impact to the data breach that happens within one year before or after the merger closure date, as in figure 4b. Note that both graphs are stewed distribution towards the post-merger period.



(a) Breach Reporting Year - Merger Closing Year (25 50 70 percentile)

(b) Whithin 1 year: Breach Reporting Month - Merger Closing Month (25 50 70 percentile)

Figure 4: Time Difference CDF: Breach Reporting Time Minus Merger Closing Time

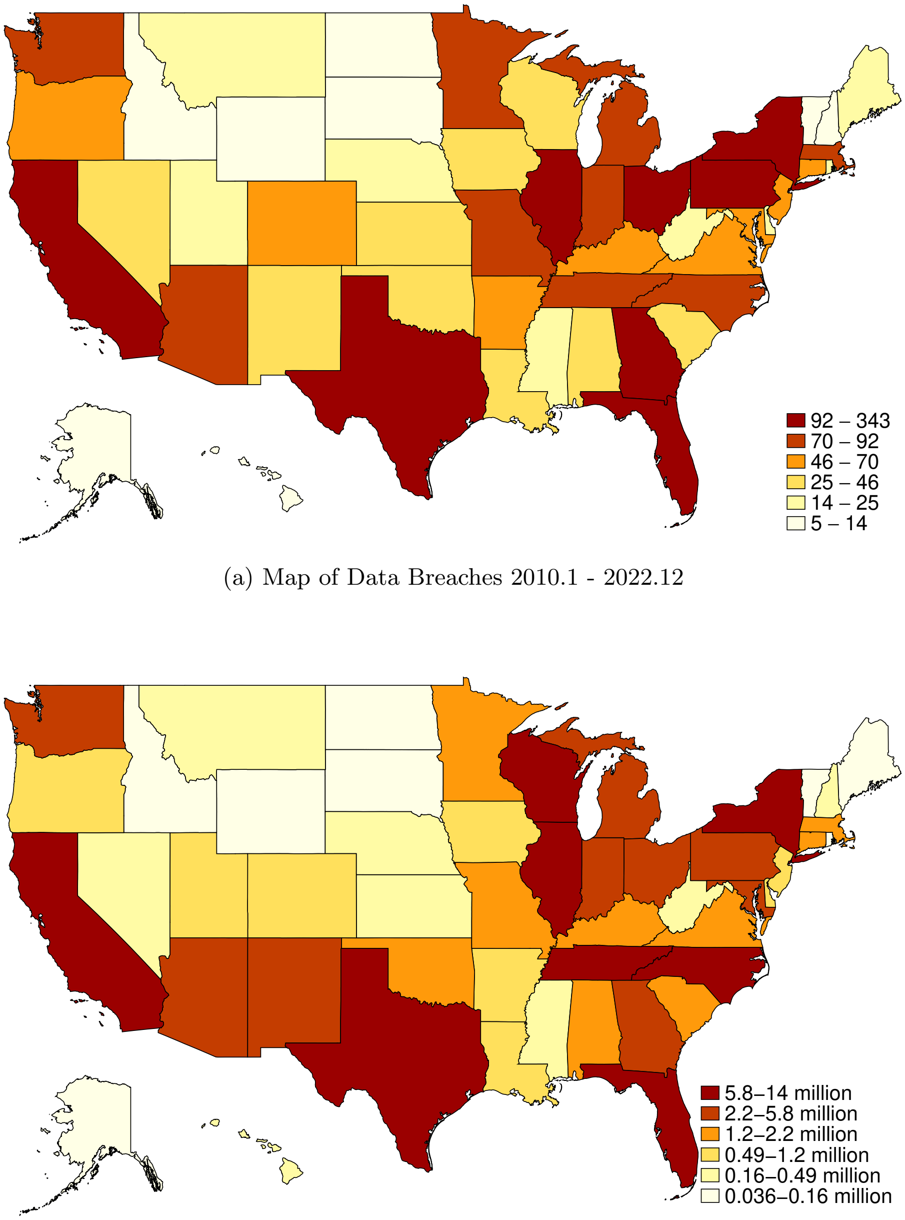
*Notes:* The figure shows the CDF for the number of reported data breaches around the merger signing date. Data source: Proprietary merger information and DHHS 2010-2022.

## 3.2 Section 3.2 Data Breaches

This section introduces the concept of data breaches and provides an overview of the data breach reporting entities. I present an examination of the overall data breach situation in US hospitals. Furthermore, I discuss two primary data breach categories, namely, insider misconduct and hacking. Insider misconduct data breaches are employee-related issues, including loss, theft, improper disposal, and impermissible insider access and disclosure that are not initiated by a malicious actor from outside the organization. In contrast, hacking involves data breaches caused by malicious actors, typically through techniques such as email phishing, malware, zero-day attacks, and ransomware attacks. Lastly, I explore two recent developments and their impact on the research question and design.

### 3.2.1 Overview

Figure 5a displays the number of data breach reports in each state over the past 13 years, while Figure 5b exhibits the number of individuals impacted by these breaches. My purpose is to investigate whether data breaches occur randomly across hospitals or whether some hospitals are more prone to such incidents. Although states with larger populations tend to have more hospitals, this does not necessarily imply that data breaches happen more or have a larger impact in larger states. For instance, Georgia has significantly fewer hospitals than Texas, yet the number of data breaches reported in each state is comparable. Similarly, North Carolina has a higher number of individual impacts than Ohio or Pennsylvania, which exhibit similar levels of impact as New Mexico.

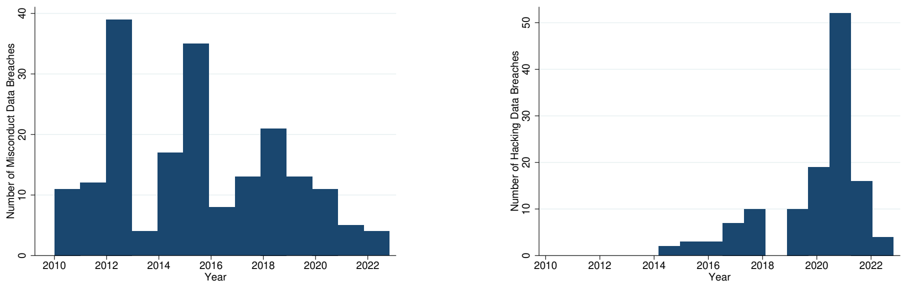


(a) Map of Data Breaches 2010.1 - 2022.12

(b) Map of individual impacted by Data Breaches 2010.1-2022.12

Figure 5: Maps

*Notes:* The figures show the geographic distribution of the number of data breach cases and individuals impacted. Data source: DHHS 2010-2022.



(a) Misconduct Data Breaches Over 2010-2022

(b) Hacking Data Breaches Over 2010-2022

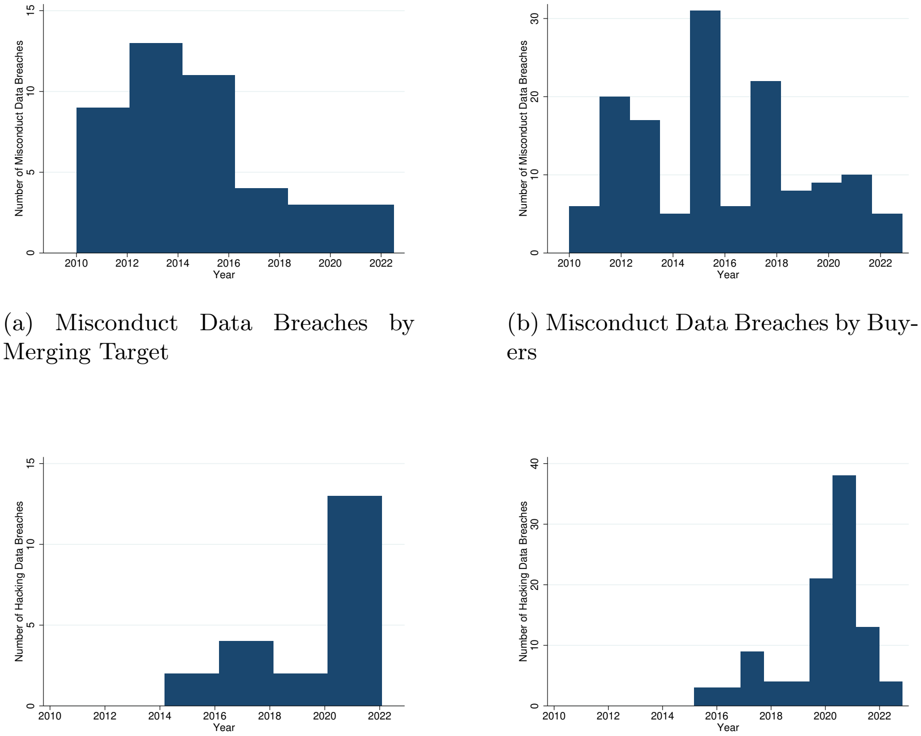
Figure 6: Two Categories of Data Breaches Over 2010-2022

*Notes:* The figures show the number of misconduct breaches and hacking data breaches over 2010-2022. The category of misconduct comprises instances of loss, theft, improper disposal, and impermissible employee access and disclosure, which could occur due to both fraudulent motives or accidents. Hacking incidents targeting hospitals are more frequently reported during mergers, with a higher incidence reported by buyers. Hacking is categorized into three types: general hacking, phishing, and ransomware. General hacking covers zero-day exploits, malware, and other non-phishing-triggered accidents. Data source: DHHS 2010-2022.

Consequently, it remains ambiguous from the map whether data breaches occur randomly across hospitals or whether specific risk factors dominate the probability of such incidents. Hence, it is worth exploring whether certain risk factors are associated with a higher probability of data breaches.

### 3.2.2 Types of Data Breaches

In order to comprehend the underlying causes of data breaches during mergers, I categorize data breaches into two types. Specifically, based on a Keyword Analysis in the "Web-description" column in the data breach report, I manually verify the types, whereby misplaced categories are corrected. For instance, data breaches that mention malware may be that the reporting entity ensured that forensic analysis excluded malware as a cause. Ultimately, I create two binary variables, namely, insider misconduct and hacking as shown in Figure 6. The category of misconduct comprises instances of loss, theft, improper disposal, and impermissible employee access and disclosure, which could occur due to both fraudulent motives or accidents. For instance, some cases may entail the sale of medical records by employees, while others may involve paper records mistakenly sent to the recycling center without proper shredding. Both motivated and non-motivated misconduct is indicative of management issues,



(a) Misconduct Data Breaches by Merging Target

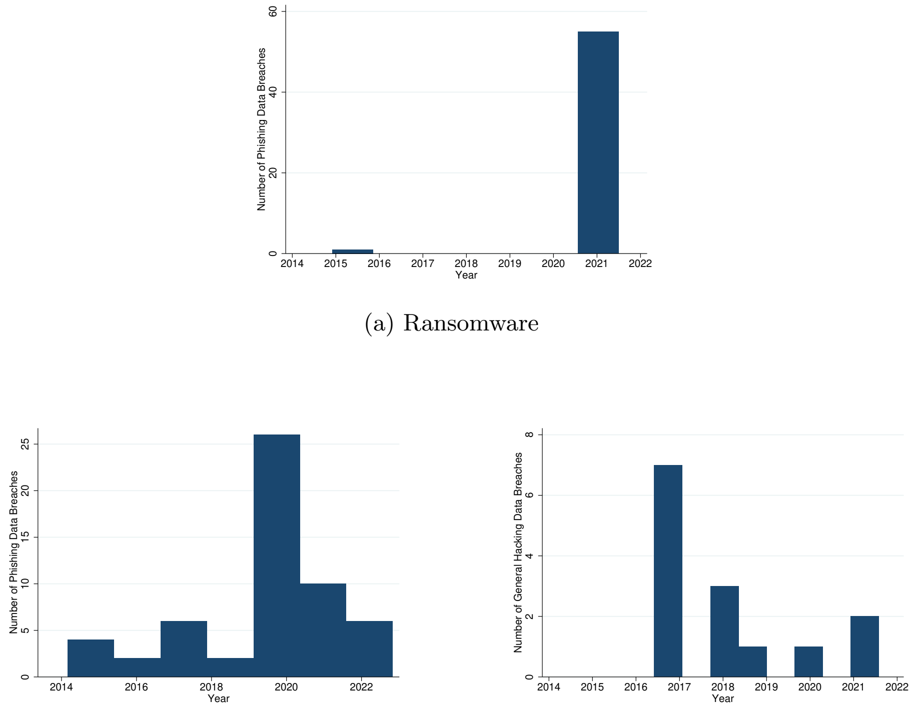
(b) Misconduct Data Breaches by Buyers

(c) Hacking Data Breaches by Merging Target

(d) Hacking Data Breaches by Buyers

Figure 7: Two Types of Data Breaches by Different Entities Over 2010-2022

*Notes:* The figure shows the number of misconduct breaches and hacking activities reported by different entities. Hacking incidents targeting hospitals are more frequently reported during mergers, with a higher incidence reported by buyers. Data source: DHHS 2010-2022.



(a) Ransomware

(b) Phishing

(c) General Hacking

Figure 8: Three Types of Hacking Data Breaches Over 2014-2022

*Notes:* Hacking is categorized into three types: general hacking, phishing, and ransomware. General hacking covers zero-day exploits, malware, and other non-phishing-triggered accidents. Ransomware attacks are the main reason for the increase in data breaches. Data source: DHHS 2010-2022.

and a well-established risk control procedure can effectively reduce the likelihood of such incidents. As further shown in Figures 7a and 7b, misconduct data breaches both in merging targets and in buyers are less reported in the last five years.

Conversely, hacking incidents targeting hospitals are more frequently reported during mergers, with a higher incidence reported by buyers. Figures 8a, 8b, and 8c show that hacking is categorized into three types: general hacking, phishing, and ransomware. General hacking covers zero-day exploits, malware, and other non-phishing-triggered accidents. Note that there has been an increasing trend of ransomware incidents in recent years.

### 3.2.3 Latest Developments

The debate regarding the necessity of mandatory reporting of security incidents in the financial industry, including public companies and banks, and how to design such regulations at the federal level is ongoing worldwide. For instance, the Indian Computer Emergency Response Team (CERT-In) mandates notification within 6 hours following most cybersecurity incidents. In contrast, the current reporting regulation for US hospitals does not impose such a stringent deadline. Given that comprehensive forensic analysis of data breach incidents can be time-consuming, Federal Regulation Section 164.408 permits reporting the estimated number of affected individuals and cases under investigation. However, this does not imply that reporting is entirely delay-free. It is essential to acknowledge the possibility of reporting delays because the delay may lead to alternative interpretations of my results, as elaborated in the Dynamic Analysis section (see Section 6.4).

As hospitals experience a surge in data breaches, patients have become increasingly aware of the potential privacy violations and other harms associated with such incidents. This heightened awareness has resulted in an increase in lawsuits, as patients exercise their growing bargaining power to address the negative externality issue. In response, hospitals have implemented measures to deal with the rising awareness and bargaining power of patients. Simultaneously, the mergers and acquisition process has garnered greater cybersecurity measures from financial agencies, investors, and insurers. Two crucial questions arise: whether these additional efforts have resulted in an improvement in the data breach situation over the past five years compared to earlier and whether different investor groups, such as private equity or real estate investment trusts, have been able to achieve varying levels of success in improving the situation. Essentially, the question is whether the market has been able to achieve a Coasian Solution to address the data breach challenges associated with mergers. Section 7 provides a detailed analysis of this question.

## 3.3 Hospital Mergers

The last section introduces the background of hospital mergers and mainly focuses on explaining why it is important that data breaches before merger closures are included as merger-causing breaches in the analysis. Here, mergers include all mergers and acquisitions in the health industry with hospitals involved. It can be that two hospitals merged into one, or it can be that a health system bought a new hospital either from another health system. It can also be a health system bought by another health system that controls several hospitals.

After I show the data breaches and mergers' data, one possible question about the matchings I have in figure 4b is, why would breaches report before a merger is done count as merger-causing data breaches? The first reason is that although I observe a merger deal signing date, the merger is a long process that involves many stages, as shown in figure 1. After the initial invitation to merge, buyers perform investigations of the target hospitals, including IT due diligence investigation, before submitting the pre-merger notification to the Department of Justice and Federal Trade Commission and notifying the local Department of Healthcare. The internal decision will be reached, and negotiation of the price will start as well as the due diligence check. More importantly, once the deal gains approval from the antitrust authorities, the intention to merge information is disclosed to the general public through various channels such as media outlets or investor communication letters. After the merger deal is signed, the operational merger starts, including the Electronic Medical Record (EMR) systems integration and new management structure, IT protocols, and risk control method implementation.

Notice also that hospital mergers with a minimum value involve parties with a minimum size needing to report to the Department of Justice (DOJ) and Federal Trade Commission (FTC) as a pre-merger notification. The reporting threshold is adjusted on timely bases. Local Departments of Health, work unions, and local health activists will also actively follow the potential merger. At the same time, many hospitals are public companies. Significant events like mergers are required to be communicated with investors. At the same time, before the merger deal is finalized, management and IT teams will need to focus their attention on supporting the lengthy merging processes. This will require a significant amount of time and effort. The attention of these teams will be divided between these tasks and their usual responsibilities.

In short, the impact of the merger on operations begins well before the signing date and a vast amount of information about the potential merger becomes available to the general public before the merger deal closure date. The general public includes hackers.

### 3.4 Control Variables

Table 1 presents summary statistics for numerical variables. The first column shows the mean and standard errors for various variables for the full sample. The second column is only for the matched samples. The sample size is reduced in both cases because of the availability of the numerical variables in my data. Note that breached hospitals have higher bed counts, revenue, and EBITDA but involve fewer public companies and report lower price/revenue ratios. In this case, the public status of the target hospitals and the buyers, the target revenue, and EBITDA are included in the baseline model introduced in the following section. The last part of section 4.2 explains the contribution of the control variables.

## 4 Empirical Strategy

### 4.1 Baseline Model

I implement stacked difference-in-differences in Deshpande and Li (2019), focusing on the effect of the timing of the merger for the baseline causal design. With

Table 1: SUMMARY STATISTICS

| | (1)<br>Full Sample | (2)<br>Breached Hospitals |
|---|---|---|
| Public Target Hospital | 0.1568 | 0.1009 |
| | (0.3638) | (0.3019) |
| Target Hospital Bed Count(100) | 2.8500 | 3.7499 |
| | (8.1376) | (8.4948) |
| Target Hospital Revenue (million) | 275.7176 | 454.3875 |
| | (758.0346) | (1241.4964) |
| Target Hospital EBITDA(million) | 21.5235 | 42.1907 |
| | (77.4465) | (114.8471) |
| Public Buyers | 0.0977 | 0.0092 |
| | (0.2971) | (0.0956) |
| Health System Buyer | 0.5125 | 0.6376 |
| | (0.5001) | (0.4818) |
| Private Equity Buyer | 0.0261 | 0.0000 |
| | (0.1596) | (0.0000) |
| REIT Buyer | 0.0170 | 0.0046 |
| | (0.1295) | (0.0677) |
| Price of the Deal (million) | 261.3694 | 204.5854 |
| | (688.9149) | (214.0004) |
| Price/Revenue | 0.7793 | 0.6931 |
| | (0.8997) | (0.4936) |
| Price/EBITDA | 7.4123 | 9.1141 |
| | (24.3818) | (10.3377) |
| Observations | 880 | 218 |

a "clean" control group for each staggered treatment, the stacked difference-in-differences method is one of the solutions developed in the past five years combating the biases from the negative weighting in the two-way fixed effect estimators for staggered treatment (see Baker, Larcker and Wang (2022); Goodman-Bacon (2021); Athey and Imbens (2022); De Chaisemartin and d'Haultfoeuille (2022); Borusyak, Jaravel and Spiess (2021); Butts and Gardner (2021)). The stacked difference-in-differences prevent using already-treated units as a comparison to newly treated units. Plus, merger activity is not a perfect treatment since the merger process creates selection bias. It means that the target hospital that got merged must have some qualities that cause it to be picked for a merger. The selection issue could bias the data breach probability comparison between the merging hospitals and non-merging hospitals. Relatively, the timing of a merger is effectively random, and such randomized timing is another reason I use it as the treatment.

In detail, all the merger deals are treated groups in the sub-sample, and a set of control groups is created for each sub-sample. The control groups include all the pre-treated hospitals that will encounter a merger deal at least two years later than the treatment group's merger signing date. For example, for a treated deal that happens on July 31st, 2010, all the mergers signed on or after July 31st, 2012, will form pre-treated groups/control groups. In other words, for every two-year window, the target, buyer, and seller involved in the deal are in the treated group. For each treated deal that closed on time t, the control/pre-treated group is all the merger deals that will close in time [t+2years, T]. For each merger, the created data set is with one treated group and all the controls. Then the data sets are stacked into one data set for regression. As I stack all the treated and pre-treated groups together, I can compare the probability of a data breach in the treated group during their merging process with the likelihood of a data breach in the pre-treated group in the same period.

The period is picked as a two-year window for each deal, including the year before and the year after the treated group's merger signing date, and the two-year window is the shaded area in figure 1. Since the controls are the deals to be signed in at least two years, the gap in time guarantees that no hospital in the control group is treated in the two-year window I build to observe data breaches. The controls are not contaminated by the treatment. Additionally, the dynamic analysis results in section 6.4 underpin the sufficiency of the two-year window. The effects of the timing of the mergers are estimated in the following equation:

$$Breached_{i,m,t} = \gamma Treated_{i,m} + \sum_{\tau} D^{\tau}_{m,t} + \sum_{\tau} \beta_{\tau}(Treated_{i,m} * D^{\tau}_{m,t}) + \alpha X_m + \lambda_i + \iota_t + \epsilon_{i,m,t} \tag{1}$$

Where $Breached_{i,m,t}$ is a binary result indicating whether any hospital $i$ in deal $m$ has reported a data breach at quarter $t$ or not. $Treated_{i,m}$ is the indicator variable for current deal $m$. Timing difference indicator $D^{\tau}_{m,t}$ equals one if quarter $t$ is $\tau$ quarters after (or before, both positive) the quarter of the deal where $\tau \in [-4, 4]$. Only data breaches that happened within one year before and after the treated groups' merger closure date are recorded as one in the binary dependent variable. $X_m$ includes the control variables. The target hospitals' bed counts, revenue, and EBITDA indicate the size of the deal. The state and the listing status of the acquirers and targets infer the impact of the deal. Additionally, I include the hospital and time-fixed effects. The coefficients of interest are the $\beta_\tau$s. $\beta_\tau$ is the difference between cyber attacks on treated and pre-treated hospitals in merger deals $\tau$ quarters after the deal. The standard errors are clustered at the deal level.

## 4.2 Difference-in-Differences Assumptions

In this section, I discuss the validity of the method by going through the three main assumptions of the difference-in-differences method: the Stable Unit Treatment Value Assumption (SUTVA), the Exogenous Treatment Assumption, and the Parallel Trend Assumption. Then I present the reasons for picking the control variables.

SUTVA requires that the outcome of a unit only depends on its own treatment. I fulfill the assumption since I use all future merging hospitals as the control. On average, one control hospital's cyber risk does not depend on the other hospitals' treatment. Without this assumption, the results on hacking may contain a positive bias. This is because if hackers only have limited resources to target hospitals, the data breach possibility of one hospital may be driven down by another hospital's treatment. A result without such potential bias may require a different strategy, for example, network difference-in-differences.

The treatment, in this case, is the timing of the mergers. Although the mergers may not be random, the control groups are the hospitals that also experience mergers, and the timing of the merger closure is not predictable. The current data I use cannot facilitate a statistical test on whether the mergers' timing can be predicted. Still, the deal closure timing depends on many moving factors, such as the efficiency of the legal and financial agents, the complication of the due diligence check, or the hospitals' financial situation. One way to guarantee the assumption is to use a further delayed control group. For example, instead of using mergers that happen two years or later in the future, as I picked for the baseline model, I can perform a robustness check, including the mergers only three years later. The downside of using more conservative control groups is that my treatment group will be squeezed earlier on the timeline, and the causal effect I test will be less up-to-date.

The parallel trend assumption is that both the treated hospitals and the pre-treated hospitals have the same time trend of the probability of data breaches. Gaps in the current literature do not allow me to specify the time trend of probability or probability distribution of a data breach if it is not entirely random, so it is currently impossible to directly test the parallel trend assumption. Since I use the pre-treated hospitals experiencing mergers in the future, it is easier to assume that the pre-treated groups would have a more similar time trend of the probability of data breaches than all the other hospitals as a whole. In the immediate next step, I will work on finding out whether I can use Rambachan and Roth (2023) to test the parallel trend sensitivity. Another control group used in hospital mergers studies is the synthetic hospitals with similar market power. In the future, I can perform a robustness check on such control groups, but the current data I have cannot work in such a way, and more importantly, the treatment effect will be the merger rather than the timing of the merger event in such a robustness check.

The controls further enhance the robustness of the assumptions. Deal fixed effects eliminate persistent unobserved selection biases. I further control the public status of the buyers and the targets. This is because of the governance requirements of risk controls, the difference in public information available, and the difference in financial structure. Especially in the Signaling Channel analysis, general information availability matters a lot. I then control the target hospital revenue and EBITDA. This is for two reasons. On one hand, targeting larger or more profitable hospitals may have been more rewarding. On the other hand, the target hospitals that are of different sizes and profitability must get various resources and attention from the potential acquirers, the legal, financial service, and information technology vendors for both the merger investigation stage and the execution of the operation merger stage. They are essential confounders that may impact the time trend of data breaches.

# 5 Impacts of Mergers

Table 2 displays the baseline outcomes for the effect of mergers on data breaches reported in the two-year window [one year before, one year after merger closure] from 2010 to 2022, with various control combinations. Hospitals that go through mergers are twice as likely to experience a data breach relative to the pre-treated group. Specifically, Column 7 corresponds to Equation 1, which includes all control variables. I observe a large positive effect, 4.20 percentage points, on data breach probability from the merger signing date, and it is statistically significant at the 5% level. As elaborated below, such an increase ranges from 3.61 to 4.24 percentage points with other control selections. Columns 1 to 6 pertain to individual control variables. These alternative outcomes are shown for a larger sample size (columns 1, 3, and 5) due to the availability of data on control variables and for a constant sample size (columns 2, 4, and 6). On average, hospitals encounter twice as many data breaches during the merger closure period. Despite their substantial effects, the point estimate uncertainty is also noteworthy.

I underscore this by displaying the treatment effect individually for target buyers, acquirers, and sellers next. The impact of the size, profitability, and market visibility is uncertain. The subsequent section addresses the impact of these controls.

Table 3 presents the results of separated regressions to investigate which party - the buyers, sellers, or target hospitals - reported data breaches. The initial columns exclude all breaches that happened to the buyers or sellers. Target hospitals in a merger have more than double the chances of being attacked

Table 2: EFFECT OF M&A ON DATA BREACHES

| | (1) | (2) | (3) | (4) | (5) | (6) | (7) |
|---|---|---|---|---|---|---|---|
| Does M&A cause data breaches? | 0.0361*** | 0.0416*** | 0.0422*** | 0.0417*** | 0.0424*** | 0.0420*** | 0.0420*** |
| | (0.0117) | (0.0157) | (0.0150) | (0.0157) | (0.0157) | (0.0158) | (0.0158) |
| Public Acquirer | -0.0626** | 0.0387* | 0.1584 | 0.8762*** | -0.1871** | 0.0448*** | 0.6044*** |
| | (0.0255) | (0.0218) | (0.1355) | (0.2813) | (0.0860) | (0.0095) | (0.1634) |
| Public Target | -0.0588** | 0.2095** | 0.0082 | 0.4645*** | 0.1884 | -0.0977* | 0.1764** |
| | (0.0248) | (0.0942) | (0.1017) | (0.0835) | (0.1303) | (0.0565) | (0.0744) |
| Target Hospital's Bed Count | -0.0134* | -0.0409* | -0.0210 | -0.0305* | -0.0293 | 0.0134 | 0.0021 |
| | (0.0079) | (0.0242) | (0.0131) | (0.0163) | (0.0255) | (0.0108) | (0.0017) |
| Target Hospital's Revenue | | | 0.0002 | 0.0010*** | | | 0.0007*** |
| | | | (0.0002) | (0.0003) | | | (0.0002) |
| Target Hospital's EBITDA | | | | | 0.0001 | -0.0127*** | -0.0084*** |
| | | | | | (0.0049) | (0.0026) | (0.0017) |
| $N$ | 673847 | 500832 | 524154 | 500832 | 504388 | 500832 | 500832 |
| $R^2$ | 0.2430 | 0.2347 | 0.2383 | 0.2347 | 0.2357 | 0.2372 | 0.2372 |
| Mean of Data Breach on Pre-treated % Effect | 2.68 | 3.22 | 3.20 | 3.22 | 3.24 | 3.22 | 3.22 |
| Mean of Data Breach on Treated % Effect | 4.97 | 6.06 | 5.85 | 6.06 | 6.11 | 6.06 | 6.06 |
| Mean of Data Breach on Pre-treated Targets % Effect | 1.96 | 2.32 | 2.31 | 2.34 | 2.32 | 2.33 | 2.33 |
| Mean of Data Breach on Treated Targets % Effect | 4.48 | 5.65 | 6.02 | 5.38 | 5.53 | 5.25 | 5.50 |
| Mean of Data Breach on Pre-treated Seller % Effect | 1.35 | 1.78 | 1.66 | 1.81 | 1.80 | 1.68 | 1.66 |
| Mean of Data Breach on Treated % Effect Seller | 7.10 | 9.03 | 7.79 | 9.35 | 9.09 | 9.86 | 10.14 |
| Mean of Data Breach on Pre-treated Acquirer % Effect | 1.94 | 2.39 | 2.38 | 2.36 | 2.40 | 2.36 | 2.40 |
| Mean of Data Breach on Treated Acquirer % Effect | 4.79 | 5.93 | 5.84 | 5.62 | 6.14 | 6.32 | 6.15 |

Note: The table shows the effect of M&A on data breaches using different sets of controls as estimated from the main model. The main variable of interest is a binary dummy, $Treated_{i,m}$, which equals 1 if a data breach was reported by the buyer, target, or seller for deal $m$ within the time period $[t-a, t+a]$. Date $t$ is when deal $m$ is signed, and $a \in [0, 4]$ quarters. The treated groups are the hospitals that participate in the deal $m$. The control group includes hospitals involved in a merger to be signed at least two years after $t$. All the regressions include a full set of hospital-year fixed effects. The table also reports the baseline mean outcome for the treated and the control groups. Standard errors clustered at the deal level are displayed in parentheses.

Table 3: BUYERS, SELLERS, AND TARGETS BREACHES SEPARATELY

| | Targets | Buyers | Sellers |
|---|---|---|---|
| Does M&A cause data breaches? | 0.0132 | 0.0329*** | 0.0035 |
| | (0.0123) | (0.0094) | (0.0048) |
| Acquirer Public Company | -0.0699*** | -0.0157*** | 0.0031** |
| | (0.0170) | (0.0045) | (0.0013) |
| Target Public Company | -0.3168*** | 0.0028*** | -0.0071 |
| | (0.0758) | (0.0008) | (0.0069) |
| Target Hospital Bed Count | 1.3366 | -0.0001 | -0.00009 |
| | (1.0759) | (0.0001) | (0.0017) |
| Target Hospital Revenue | | 0.9900*** | 0.1046 |
| | | (0.2821) | (0.1452) |
| Target Hospital EBITDA | -0.1090*** | -0.1184*** | -1.2509 |
| | (0.0225) | (0.0337) | (1.7356) |
| $N$ | 387061 | 457008 | 375803 |
| $R^2$ | 0.2868 | 0.2617 | 0.1767 |
| Mean on Pre-treated % Effect | 0.88 | 1.84 | 0.51 |
| Mean on Treated % Effect | 2.46 | 4.14 | 0.82 |

Note: The table shows the effect of M&A on data breaches in the targets, buyers, and sellers separately. The main variable of interest is a binary dummy, $Treated_{i,m}$, which equals 1 if a data breach was reported by the buyer, target, or seller (separately) for deal $m$ within the time period $[t-a, t+a]$. Date $t$ is when deal $m$ is signed, and $a \in [0,4]$ quarters. The treated groups are the hospitals that participate in the deal $m$. The control group includes hospitals involved in a merger to be signed at least two years after $t$. All the regressions include a full set of hospital-year fixed effects. The table also reports the baseline mean outcome for the treated and the control groups. Standard errors clustered at the deal level are displayed in parentheses.

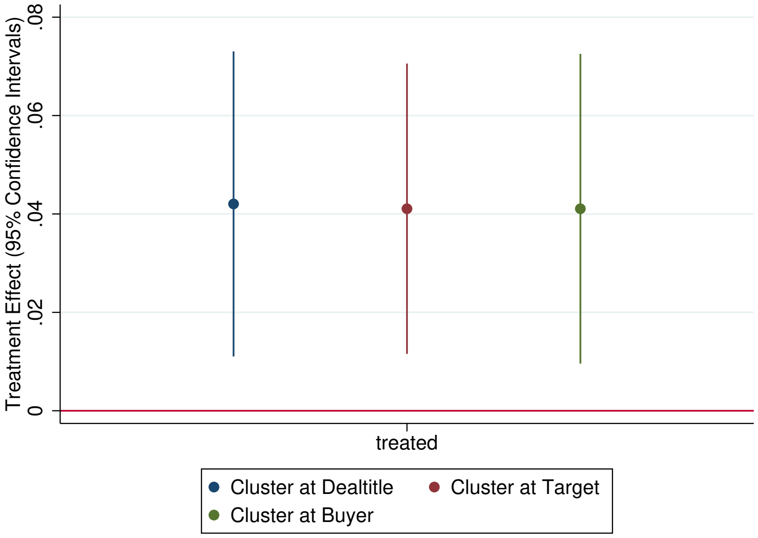


Figure 9: Standard Errors are Clustered at Different Levels

*Notes:*

compared to those that will merge two years or later, but the regression result is not significant. The effect is even bigger for buyers and significantly smaller for sellers. Notably, public buyers experience significantly fewer data breaches.

Last but not least, the analysis so far clusters standard error at the merger deal level, assuming that all the target hospitals engage in the same merger deal share certain unobserved characteristics that could lead to correlation in the error terms that I have not explained about the probability of data breach ("areg" function adopts cluster-robust standard errors proposed by Cameron, Gelbach and Miller (2011), assuming that the errors are homoscedastic within clusters but potentially heteroscedastic between clusters). Another alternative assumption is that there are unobserved characteristics related to the target hospital or the buyer included in the error term. Figure 9 demonstrates that employing such alternative clustering methods does not significantly change the estimation results.

# 6 Evidence on Channels of the Mergers' Effect on Data Breaches

To understand the channels that augment data breaches, I conduct a separate analysis in four stages. First, I isolate the impact of misconduct data breaches and hacking/non-misconduct data breaches as outlined in section 3.2.2. Con-

Table 4: EFFECT OF M&A ON MISCONDUCT BREACHES

| | (1) | (2) | (3) | (4) |
|---|---|---|---|---|
| Treatment Effect | 0.0057 | 0.0057 | 0.0060 | 0.0060 |
| | (0.0070) | (0.0070) | (0.0071) | (0.0071) |
| Public Acquirer | 0.0388$^{*}$ | 0.8746$^{***}$ | 0.0449$^{***}$ | 0.6032$^{***}$ |
| | (0.0218) | (0.2827) | (0.0096) | (0.1657) |
| Public Target | 0.2089$^{**}$ | 0.4634$^{***}$ | -0.0977$^{*}$ | 0.1758$^{**}$ |
| | (0.0942) | (0.0838) | (0.0564) | (0.0754) |
| Target Hospital's Bed Count | -4.0804$^{*}$ | -3.0450$^{*}$ | 1.3366 | 0.2134 |
| | (2.4216) | (1.6327) | (1.0753) | (0.1761) |
| Target Hospital's Revenue | | 0.9951$^{***}$ | | 0.6671$^{***}$ |
| | | (0.3424) | | (0.2026) |
| Target Hospital's EBITDA | | | -1.2681$^{***}$ | -0.8427$^{***}$ |
| | | | (0.2613) | (0.1755) |
| $N$ | 500832 | 500832 | 500832 | 500832 |
| $R^2$ | 0.2493 | 0.2494 | 0.2524 | 0.2524 |
| Mean on Nontreated % Effect | 2.70 | 2.70 | 2.70 | 2.70 |
| Mean on Treated % Effect | 3.46 | 3.46 | 3.46 | 3.46 |

Note: The table shows the effect of M&A on misconduct data breaches with different sets of controls. The explanatory variable of main interest is a dummy $Treated_{i,m}$ that equals 1 for the hospital $i$ to be involved in deal $m$ and reported a data breach in $[t-a, t+a]$. Date $t$ is when deal $m$ is signed, and $a \in [0, 4]$ quarters. The control group includes hospitals involved in a merger to be signed at least two years after $t$. All the regressions include a full set of hospital-year fixed effects. The table also reports the baseline mean outcome for the treated and the control groups. Standard errors clustered at the deal level are displayed in parentheses.

cerning hacking activities, I examine the Signaling Channel and the Incompatibility Channel separately. Second, I analyze a specific type of hacking activity, the ransomware attack, and show that on average, ransomware attack happens even more through the Signaling Channel. Third, an event study is used to test the pre-trend and show the dynamic effects. Fourth, I compare the regression outcomes on varying levels of organizational capital.

## 6.1 Insider Misconduct Breaches

In this section, I present the main regression on misconduct data breaches, including loss, theft, improper disposal, and impermissible employee access and disclosure. Tables 4, 5, and 6 suggest an increase in misconduct breaches during the two-year period, but no statistically significant treatment effect is observed. These findings indicate that, counter-intuitively, the impact on insider misconduct breaches is not significant. In this way, the large increase in data breaches is mainly due to the increase of hacking activities during mergers.

Table 5: EFFECT OF M&A ON MISCONDUCT BREACHES ON TARGETS

| | (1) | (2) | (3) | (4) |
|---|---|---|---|---|
| Treatment Effect | 0.0002 | 0.0003 | 0.0003 | 0.0003 |
| | (0.0048) | (0.0048) | (0.0048) | (0.0048) |
| Public Acquirer | 0.0367* | 0.8722*** | 0.0428*** | 0.6009*** |
| | (0.0218) | (0.2829) | (0.0096) | (0.1661) |
| Public Target | 0.2088** | 0.4632*** | -0.0977* | 0.1757** |
| | (0.0941) | (0.0839) | (0.0564) | (0.0756) |
| Target Hospital's Bed Count | -4.0789* | -3.0438* | 1.3367 | 0.2138 |
| | (2.4215) | (1.6334) | (1.0751) | (0.1765) |
| Target Hospital's Revenue | | 0.9948*** | | 0.6669*** |
| | | (0.3427) | | (0.2031) |
| Target Hospital's EBITDA | | | -1.2678*** | -0.8425*** |
| | | | (0.2615) | (0.1759) |
| $N$ | 500832 | 500832 | 500832 | 500832 |
| $R^2$ | 0.2484 | 0.2487 | 0.2487 | 0.2488 |
| Mean on Nontreated % Effect | 0.67 | 0.67 | 0.67 | 0.67 |
| Mean on Treated % Effect | 1.30 | 1.30 | 1.30 | 1.30 |

Note: The table shows the effect of M&A on misconduct data breaches reported by target hospitals with different sets of controls. The explanatory variable of main interest is a dummy $Treated_{i,m}$ that equals 1 for the hospital $i$ to be involved in deal $m$ and reported a data breach in $[t-a, t+a]$. Date $t$ is when deal $m$ is signed, and $a \in [0, 4]$ quarters. The control group includes hospitals involved in a merger to be signed at least two years after $t$. All the regressions include a full set of hospital-year fixed effects. The table also reports the baseline mean outcome for the treated and the control groups. Standard errors clustered at the deal level are displayed in parentheses.

Table 6: EFFECT OF M&A ON MISCONDUCT BREACHES ON BUYERS

| | (1) | (2) | (3) | (4) |
|---|---|---|---|---|
| Treatment Effect | 0.0049 | 0.0049 | 0.0049 | 0.0049 |
| | (0.0043) | (0.0043) | (0.0043) | (0.0043) |
| Public Acquirer | -0.1328 | 2.1957 | -0.1187 | 1.6620 |
| | (0.1530) | (2.7660) | (0.1504) | (3.4972) |
| Public Target | 0.7626 | 1.4716 | 0.0308 | 0.9031 |
| | (0.7695) | (1.3799) | (0.2619) | (1.6499) |
| Target Hospital's Bed Count | -1.3437 | -1.0552 | -0.0508 | -0.4091 |
| | (1.6161) | (1.5125) | (0.8273) | (0.4939) |
| Target Hospital's Revenue | | 0.2772 | | 0.2128 |
| | | (0.3437) | | (0.4311) |
| Target Hospital's EBITDA | | | -0.3037 | -0.1680 |
| | | | (0.2911) | (0.3663) |
| $N$ | 5000832 | 500832 | 500832 | 500832 |
| $R^2$ | 0.2694 | 0.2694 | 0.2693 | 0.2693 |
| Mean on Nontreated % Effect | 1.58 | 1.58 | 1.58 | 1.58 |
| Mean on Treated % Effect | 1.73 | 1.73 | 1.73 | 1.73 |

Note: The table shows the effect of M&A on misconduct data breaches reported by buyers with different sets of controls. The explanatory variable of main interest is a dummy $Treated_{i,m}$ that equals 1 for the hospital $i$ to be involved in deal $m$ and reported a data breach in $[t-a, t+a]$. Date $t$ is when deal $m$ is signed, and $a \in [0,4]$ quarters. The control group includes hospitals involved in a merger to be signed at least two years after $t$. All the regressions include a full set of hospital-year fixed effects. The table also reports the baseline mean outcome for the treated and the control groups. Standard errors clustered at the deal level are displayed in parentheses.

## 6.2 Hacking: Signaling and Incompatibility Channels

In this section, I remove all the insider misconduct data breaches and investigate hacking activities in the two years surrounding the merger deal closure date separately. A hospital merger is an event that can change the behavior of hackers targeting hospitals. On one hand, mergers can signal potential increases in financial benefits of a successful hacking to encourage more efforts from hackers. On the other hand, the process of operational integration increases vulnerability when all the data, access rights, and keys are transferred. Forensic analysis to investigate the real reason can be costly and lengthy, and since it is not possible to directly observe all the hackers' decisions, it is hard to separate the two reasons. Nevertheless, all data breaches that happen before the closing of the deal can never come from the merging of the two information systems. Information operation mergers should not start before the deal is signed. In this way, I can simply remove all the hacking activities after the signing date to remove incompatibility-triggered hacking activities with no false negative problem to identify the Signaling Channel in section 6.2.2. Results for the Incompatibility Channel are in section 6.2.3.

### 6.2.1 Hacking Activities Around Merger Signing Date

Before analyzing the two hacking channels, I present the result of the main regression on hacking activities. Table 7 reveals that hacking activities are reported more frequently during the two-year treatment window, and the result is statistically significant. The average probability of hacking activities in the treated group is 2.6%, which is comparable to the probability of misconduct breaches in the pre-treated group as shown in table 4. This represents a fivefold increase from the pre-treated group mean of 0.52%.

### 6.2.2 Signaling Channel

The result for the pre-signing Signaling Channel is in table 8. The Signaling Channel accounts for an increase of 1.98 percentage points in data breaches during consolidations. It means that for the hospitals for which a merger deal is impending within a year, there is more than a ten times chance that a data breach will happen compared with the hospitals that will sign a merger deal much later. Note also that the control effects look similar to table 3 where public visibility does not have a clear outcome. I analyze publicly traded hospitals in section 6.5.1.

There are multiple interpretations of the significant increase in hacking activities through pre-signing Signaling Channels. Firstly, it is speculated that the increase is not a result of more hacking, but rather due to compliance reasons and pressure from the legal department prior to finalizing the merger deal. This leads to an increase in the reporting of hacking incidents rather than the actual occurrence of hacks. Three results are presented to address this speculation. The first result indicates that over one-third of the reported increase can be attributed to ransomware attacks, which are difficult to conceal compared

Table 7: EFFECT OF M&A ON HACKINGS

| | (1) | (1) | (1) | (1) |
|---|---|---|---|---|
| Treatment Effect | $0.0359^{**}$ | $0.0359^{**}$ | $0.0360^{**}$ | $0.0360^{**}$ |
| | (0.0140) | (0.0140) | (0.0141) | (0.0141) |
| Public Acquirer | -0.0001 | 0.0016 | -0.0001 | 0.0012 |
| | (0.0001) | (0.0016) | (0.0001) | (0.0024) |
| Public Target | 0.0006 | $0.0011^{*}$ | .0000224 | 0.0007 |
| | (0.0004) | (0.0006) | (0.0002) | (0.0011) |
| Target Hospital's Bed Count | -0.0001 | -0.0001 | -0.0000 | -.0000298 |
| | (0.0001) | (0.0001) | (0.0001) | (.0000275) |
| Target Hospital's Revenue | | 2.02e-06 | | 1.55e-06 |
| | | (1.95e-06) | | (2.90e-06 ) |
| Target Hospital's EBITDA | | | $-.0000221^{*}$ | -.0000123 |
| | | | (.0000123) | (.0000249) |
| $N$ | 500832 | 500832 | 500832 | 500832 |
| $R^2$ | 0.1792 | 0.1792 | 0.1792 | 0.1792 |
| Mean on Nontreated % Effect | 0.52 | 0.52 | 0.52 | 0.52 |
| Mean on Treated % Effect | 2.60 | 2.60 | 2.60 | 2.60 |

Note: The table shows the effect of M&A on hacking activities with different sets of controls. The explanatory variable of main interest is a dummy $Treated_{i,m}$ that equals 1 for the hospital $i$ to be involved in deal $m$ and reported a data breach in $[t-a, t+a]$. Date $t$ is when deal $m$ is signed, and $a \in [0, 4]$ quarters. The control group includes hospitals involved in a merger to be signed at least two years after $t$. All the regressions include a full set of hospital-year fixed effects. The table also reports the baseline mean outcome for the treated and the control groups. Standard errors clustered at the deal level are displayed in parentheses.

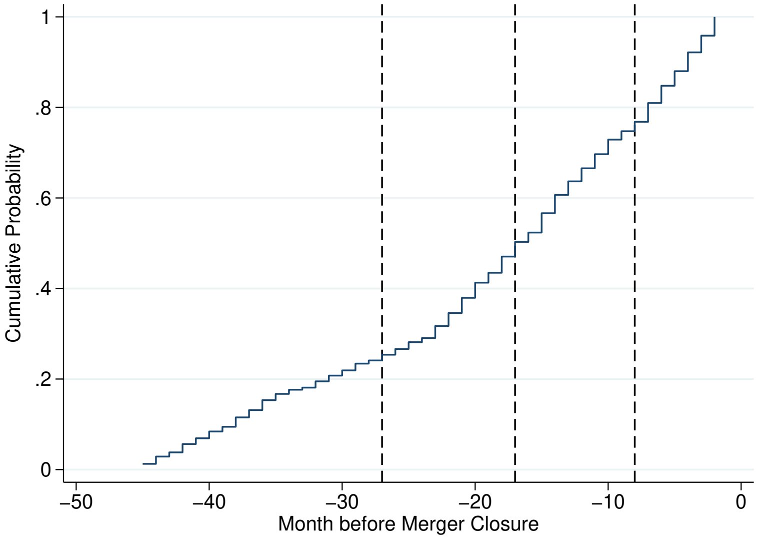


Figure 10: Google Trends: CDF of the Peak Growth Rate

*Notes:* This figure shows the CDF of when the largest Google search growth rate happens relative to the merger closure date. The $25^{th}$ percentile suggests that in some cases the peak activity can occur as far back as 27 months before the merger closing date, while the $75^{th}$ percentile suggests a peak as close as 8 months before the merger signing date. The median suggests a peak of 17 months. Data source: Google Trends called “pytrends” (Unofficial API for Google Trends) package on Python 2005-2022.

Table 8: EFFECT OF M&A ON HACKINGS: SIGNALING CHANNEL

| | (1) | (2) | (3) | (4) |
|---|---|---|---|---|
| Treatment Effect | 0.0198$^{**}$ | 0.0198$^{**}$ | 0.0198$^{**}$ | 0.0198$^{**}$ |
| | (0.0092) | (0.0092) | (0.0092) | (0.0092) |
| Public Acquirer | -0.0001 | 0.0009 | -.0000476 | 0.0007 |
| | (.0000471) | (0.0009) | (.000049) | (0.0013) |
| Public Target | 0.0003 | 0.0006$^{*}$ | .0000124 | 0.0004 |
| | (0.0002) | (0.0003) | (0.0001) | (0.0006) |
| Target Hospital's Bed Count | -0.0005 | -0.0004 | -.0000204 | -0.0002 |
| | (0.0005) | (0.0005) | (0.0003) | (0.0002) |
| Target Hospital's Revenue | | 0.0001 | | 0.0001 |
| | | (0.0001) | | (0.0002) |
| Target Hospital's EBITDA | | | -0.0012 | -0.0007 |
| | | | (0.0007) | (0.0014) |
| $N$ | 500832 | 500832 | 500832 | 500832 |
| $R^2$ | 0.1219 | 0.1219 | 0.1219 | 0.1219 |
| Mean on Nontreated % Effect | 0.14 | 0.14 | 0.14 | 0.14 |
| Mean on Treated % Effect | 1.41 | 1.41 | 1.41 | 1.41 |

Note: The table shows the effect of M&A on pre-signing hacking activities with different sets of controls. The explanatory variable of main interest is a dummy $Treated_{i,m}$ that equals 1 for the hospital $i$ to be involved in deal $m$ and reported a data breach in $[t-a, t+a]$. Date $t$ is when deal $m$ is signed, and $a \in [0,4]$ quarters. The control group includes hospitals involved in a merger to be signed at least two years after $t$. All the regressions include a full set of hospital-year fixed effects. The table also reports the baseline mean outcome for the treated and the control groups. Standard errors clustered at the deal level are displayed in parentheses.

to insider misconduct breaches or small-scale misconfigurations (as discussed in section 6.3). The second result is based on the findings from the past five years (section 7), which demonstrate a significant decrease in insider misconduct during the pre-signing window. Therefore, it is unlikely that the reports are accumulated solely due to compliance reasons before the merger deal closes. The third result, obtained from dynamic analysis in section 6.4, reveals neither a sudden surge in data breach reports approaching the merger signing date nor a sudden decrease afterward.

It is challenging to separately account for all the changes in the hackers' and the hospitals' motivation and behavior listed below, however, among the various alternative interpretations, the reduction of information asymmetry explanation complements most of the rest. From a defense perspective, it is possible that the merging buyers and targets experience organizational chaos. For instance, the CTO of the merging target may be less motivated to address problems if they anticipate being replaced during the merger. Additionally, third parties can contribute to increased vulnerability. For example, when a financial service audits a firm's IT, it provides hackers with an opportunity to socially engineer and steal credentials. Considering these potential vulnerabilities, hackers may be more motivated to attack the hospital for several reasons. First, the merging buyer may be financially stronger. Second, a merged hospital presents an attractive target, as it provides access to two entities through a single attack. Third, increased media coverage may expose more information about the merger, attracting hackers. Fourth, hackers may have learned from past experiences that the negotiation and investigation phase of a merger presents opportune moments for attacks, leading them to make more attempts. Other reasons for increased hacking activity include competitors hiring hackers or hacktivists opposing the merger deal. Hackers utilize news and information for their hacking activities, as shown by Moore and Clayton (2009), who demonstrated hackers' use of Google to identify potential targets. To determine when the merger deal gains public attention, an analysis of search score growth rates using Google Trends is conducted, particularly focusing on the period leading up to the merger signing date.

Another reason for analyzing Google Trends data is that the treatment period does not necessarily begin one year before the signing date as assumed in the main analysis. Through data examination, it is determined that the mean of the highest growth rate in Google searches indicates a peak in search activity approximately 18 months prior to the merger signing date, while the median suggests a peak around 17 months. Figure 10 illustrates that the $25^{th}$ percentile suggests instances where peak activity can occur as early as 27 months before the merger closing date, whereas the $75^{th}$ percentile suggests a peak as close as 8 months before the merger signing date. These findings from Google Trends align with the main research design. Alternative assumptions are also tested and discussed in section 8.

m*modal
systems
eclinicalworks
allscripts
cpsi
inc.
agfa
sap
self−developed
scc
computer
soft
oracle
epic
secure
harris
computing
cerner
microsoft
healthcare
versus
meditech
mckesson
kronos
technology
systems
eclinicalworks
healthcare
ultimate
meditech
oracle
cpsi
epic
allscripts
cerner
inc.
konica
m*modal
medisolv
medent
harris
microsoft
mckesson
minolta
cisco
fujifilm
ibm
avaya

(a) Buyer's Software Vendor (b) Target Hospitals' Software Vendor

Figure 11: Word Clouds of the Software Vendors in 2018-2019

*Notes:*The figures show the vendors of the target hospitals and the buyers signing a deal in 2018 and 2019. Data source: HIMSS 2017-2018.

#### 6.2.3 Incompatibility Channel

The previous section reveals a large positive pre-signing signaling effect. Is the Signaling Channel the only reason that elevates the data breach probability?

Vendors' quality and vendors' market share have impacts on cybersecurity risks (Vasek, Wadleigh and Moore, 2015). In figure 11, I show the word cloud for software vendors of the target hospitals and the buyers signing a deal in 2018 and 2019. The vendor information is from Healthcare Information and Management Systems Society (HIMSS). Leading healthcare information services vendors such as Epics, Cerner, Avaya, GE, CPSI, and Microsoft serve both the targets and buyers. However, if the target hospital uses a different vendor before it joins a new health system, the target hospital will experience a major information system migration on top of all the operational changes. Such incompatibility can lead to larger vulnerability (Moore, 2010).

Table 9 presents the Incompatibility Channel results: data breaches due to EMR differences increased by 1.62 percentage points during the M&A process. The incompatibility of the two information systems is identified with the timing. Only post-closure hacking activities that happen within one year after the deal closure is counted. After the merger is closed, the operation of merging starts. Normally, if a large health system purchases a hospital, it would let the hospital adopt its own EMR and other software. Especially when the vendors (as in the word cloud in figure 11a and 11b) are different or when it comes to a data-driven merger when their previous two systems could not share data, the first operation merging task would be merging the data. The magnitudes for the Signaling Channel and the Incompatibility Channel are similar. However, an

Table 9: EFFECT OF M&A ON HACKINGS: INCOMPATIBILITY CHANNEL

| | (1) | (2) | (3) | (4) |
|---|---|---|---|---|
| Treatment Effect | 0.0161$^{**}$ | 0.0161$^{**}$ | 0.0162$^{**}$ | 0.0162$^{**}$ |
| | (0.0067) | (0.0067) | (0.0067) | (0.0067) |
| Public Acquirer | -.0000435 | 0.0007 | -.0000389 | 0.0005 |
| | (.0000374) | (0.0007) | (.0000392) | (0.0011) |
| Public Target | 0.0003 | 0.0005$^{*}$ | .0000101 | 0.0003 |
| | (0.0002) | (0.0003) | (0.0001) | (0.0005) |
| Target Hospital's Bed Count | -0.0004 | -0.0003 | -.0000167 | -0.0001 |
| | (0.0004) | (0.0004) | (0.0003) | (0.0001) |
| Target Hospital's Revenue | | 0.0001 | | 0.0001 |
| | | (0.0001) | | (0.0001) |
| Target Hospital's EBITDA | | | -0.0010$^{*}$ | -0.0006 |
| | | | (0.0006) | (0.0011) |
| $N$ | 500832 | 500832 | 500832 | 500832 |
| $R^2$ | 0.0878 | 0.0878 | 0.0878 | 0.0878 |
| Mean on Nontreated % Effect | 0.38 | 0.38 | 0.38 | 0.38 |
| Mean on Treated % Effect | 1.19 | 1.19 | 1.19 | 1.19 |

Note: The table shows the effect of M&A on data breaches that were reported after the deal is signed as identification of the technical Incompatibility Channel. The table is on a sample that excludes the misconduct and the pre-signing breaches. The explanatory variable of main interest is a dummy $Treated_{i,m}$ that equals 1 for the hospital $i$ to be involved in deal $m$ and reported a data breach in $[t-a, t+a]$. Date $t$ is when deal $m$ is signed, and $a \in [0, 4]$ quarters. The control group includes hospitals involved in a merger to be signed at least two years after $t$. All the regressions include a full set of hospital-year fixed effects. The table also reports the baseline mean outcome for the treated and the control groups. Standard errors clustered at the deal level are displayed in parentheses.

alternative interpretation of the post-closure effect is that hospitals intentionally delay their data breach reporting. I use event study to investigate such delay.

## 6.3 Ransomware Attacks

Ransomware attacks are particularly harmful compared to other types of hacking activities due to the significant disruption they can cause to hospital operations. In September 2020, Universal Health Services (UHS), a prominent US hospital chain, experienced a severe ransomware attack by Ryuk, which persisted for several days. The attack damaged UHS's computer networks across approximately 400 facilities, disrupting critical systems and services. In addition, the attack significantly impacted patient care since access to medical records and prescription processing became impossible. It happens so often in the past 5 years that hospitals have designed reaction plans. For instance, Children's National Hospital in Washington, D.C. created a "code dark" following ransomware attacks (Rundle, 2022). Calling "code dark" means all hospital employees shut down machines nearby.

Table 10 shows that ransomware attacks occur more frequently both before and after the merger signing date. These results suggest that not only are there more privacy violations during mergers, but also a greater likelihood of hacking-related operation disruptions to hospital operations. Plus, on average, hospitals have a higher probability of a ransomware attack through the Signaling Channel.

## 6.4 Dynamic Effects

I use an event study to test the pre-trend and dynamics of data breaches. Pre-trends need to be analyzed to justify the assumptions for the difference-in-differences method. The dynamics of data breaches help to understand whether there are intentional delays in reporting data breaches. If there is a such delay, it means the signaling channel is underestimated. The event study graph in figure 12 shows no pre-trends difference, but there is no evidence to reject the null that there may be intentional delays in reporting data breaches around the merger signing date.

Figure 12 displays coefficients for the main regression with lead and lag indicators for up to 10 quarters prior to or 20 quarters following a merger for mergers that closed between Q1 2018 and Q4 2019. This time frame was chosen because mergers in or after 2020 are too late to have controls, and earlier mergers cannot produce a sufficient number of pre-merger events in the control group. The variable $t$ represents the quarter in which the treatment group signed the merger deals. The event study shows the quarterly dynamics of 10 quarters (2.5 years) before and 20 quarters (5 years) after the merger signing date, with $t-4$ assumed to be when the treatment effect starts.

Table 10: EFFECT OF M&A ON RANSOMWARE ATTACKS

| | More Sample | | | All Controls | | |
|---|---|---|---|---|---|---|
| | All | Pre | Post | All | Pre | Post |
| Treatment Effect | 0.0134$^{***}$ | 0.0067$^{*}$ | 0.0067$^{**}$ | 0.0172$^{***}$ | 0.0077 | 0.0094$^{**}$ |
| | (0.0048) | (0.0038) | (0.0029) | (0.0065) | (0.0051) | (0.0041) |
| Public Acquirer | 2.0129 | 1.0025 | 1.0104 | 5.7751 | 2.6005 | 3.1746 |
| | (14.6407) | (7.3049) | (7.3535) | (11.2741) | (5.2620) | (6.2332) |
| Public Target | -7.3601 | -3.6655 | -3.6946 | 3.1381 | 1.4131 | 1.7250 |
| | (15.1154) | (7.7013) | (7.6414) | (5.1766) | (2.4493) | (2.8686) |
| Target Hospital's Bed Count | -0.4785 | -0.2383 | -0.2402 | -0.1422 | -0.0640 | -0.0781 |
| | (63.6771) | (31.7126) | (31.9648) | (0.1304) | (0.0679) | (0.0735) |
| Target Hospital's Revenue | | | | 0.0739 | 0.0333 | 0.0406 |
| | | | | (0.1381) | (0.0647) | (0.0764) |
| Target Hospital's EBITDA | | | | -0.5839 | -0.2629 | -0.3209 |
| | | | | (1.1873) | (0.5526) | (0.6561) |
| $N$ | 673847 | 673847 | 673847 | 500832 | 500832 | 500832 |
| $R^2$ | 0.0351 | 0.0355 | 0.0079 | 0.0367 | 0.0370 | 0.0106 |
| Mean of Data Breach on Pre-treated % Effect | 0.16 | 0.16 | 0.00 | 0.19 | 0.19 | 0.00 |
| Mean of Data Breach on Treated % Effect | 0.98 | 0.56 | 0.42 | 1.41 | 0.76 | 0.65 |
| Mean of Data Breach on Pre-treated Targets % Effect | 0.05 | 0.05 | 0.00 | 0.07 | 0.08 | 0.00 |
| Mean of Data Breach on Treated Targets % Effect | 1.00 | 0.62 | 0.23 | 1.20 | 0.72 | 0.48 |
| Mean of Data Breach on Pre-treated Seller % Effect | 0.05 | 0.04 | 0.00 | 0.09 | 0.06 | 0.00 |
| Mean of Data Breach on Treated % Effect Seller | 1.09 | 0.55 | 1.08 | 3.50 | 1.40 | 1.39 |
| Mean of Data Breach on Pre-treated Acquirer % Effect | 0.06 | 0.07 | 0.00 | 0.07 | 0.08 | 0.00 |
| Mean of Data Breach on Treated Acquirer % Effect | 1.04 | 0.63 | 0.31 | 1.58 | 0.94 | 0.47 |

Note: The table shows the effect of M&A on ransomware attacks. The explanatory variable of main interest is a dummy $Treated_{i,m}$ that equals 1 for the deal $m$ if the buyer, target, or seller reported a ransomware attack in $[t-a, t+a]$. Date $t$ is when deal $m$ is signed, and $a \in [0,4]$ quarters. The treated groups are the hospitals that participate in the deal $m$. The control group includes hospitals involved in a merger to be signed at least two years after $t$. All the regressions include a full set of hospital-year fixed effects. The table also reports the baseline mean outcome for the treated and the control groups. Standard errors are clustered at the deal level and are displayed in parentheses.

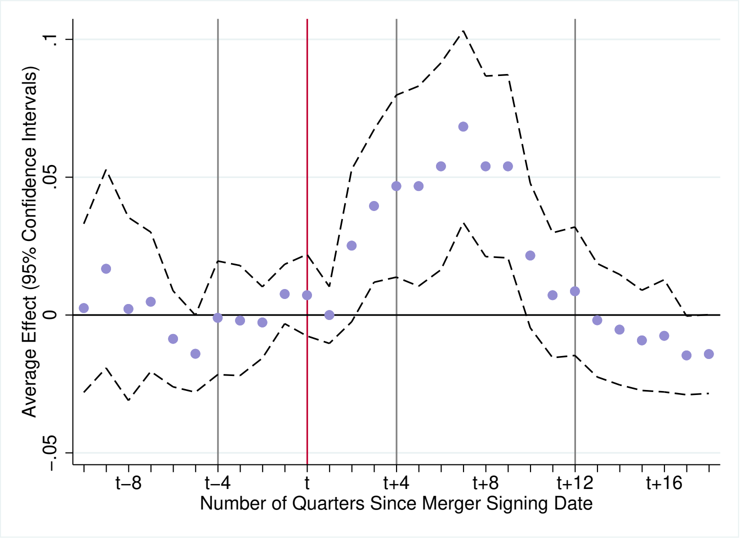


Figure 12: Event Study: Mergers in Q1 2018-Q4 2019

*Notes:*The figure plots coefficients for the main regression with lead and lag indicators up to two and half years prior to or 5 years following a merger happened in 2018 or 2019. Standard errors are clustered at the deal level. Vertical distances represent 95% confidence intervals. $t$ represents the quarter in which the treatment group signed the deals, and is assumed to be when the incompatibility channel starts. $t-4$ is assumed to be when the treatment starts for the signaling channel in my analysis. $t-4$ to $t+4$ is the two-year time window I compare the main analysis. $t-4$ to $t+12$ is the alternative analysis in table 16.

Table 11: EFFECT OF M&A ON STRUGGLING/NON-STRUGGLING TARGET DEALS

| | Insider Misconduct | | Insider Misconduct and Hacking | |
|---|---|---|---|---|
| | STR Target | Non-STR | STR Target | Non-STR |
| Treatment Effect | 0.0045 | 0.0053 | $0.0352^{*}$ | $0.0462^{**}$ |
| | (0.0147) | (0.0089) | (0.0206) | (0.0207) |
| $N$ | 18197 | 290316 | 18197 | 290316 |
| $R^2$ | 0.2353 | 0.2529 | 0.2348 | 0.2411 |
| Mean on Nontreated % Effect | 2.02 | 1.97 | 2.12 | 3.02 |
| Mean on Treated % Effect | 3.09 | 2.28 | 5.64 | 6.38 |

Note: The table presents a comparison of the impact of M&A on data breaches for deals with struggling targets and those that do not involve struggling targets. The first two columns refer specifically to breaches related to misconduct, while the last two columns regress on all types of data breaches. The explanatory variable of main interest is a dummy $Treated_{i,m}$ that equals 1 for the hospital $i$ to be involved in deal $m$ and reported a data breach in $[t-a, t+a]$. Date $t$ is when deal $m$ is signed, and $a \in [0,4]$ quarters. The control group includes hospitals involved in a merger to be signed at least two years after $t$. All the regressions include a full set of hospital-year fixed effects. The table also reports the baseline mean outcome for the treated and the control groups. Standard errors clustered at the deal level are displayed in parentheses.

## 6.5 Organizational Capital Channel

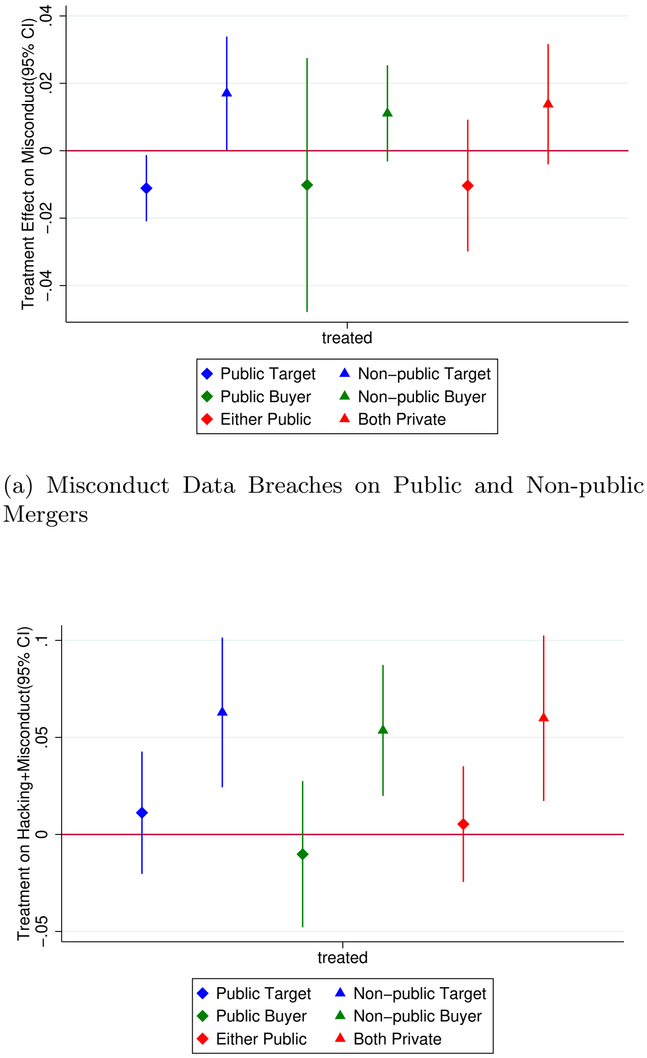
### 6.5.1 Organizational Capital: Publicly Traded Hospitals

Public companies fall under more supervision and regulation from the government, shareholders, and media and are sensitive to cybersecurity incident shocks in regard to stock prices. For example, SEC has started to propose a cybersecurity reporting policy before many other federal agencies since 2022.

Figure 13 shows the impact of publicly traded and non-publicly traded mergers on data breaches. Specifically, the first blue line in Figure 13a shows that when the target hospital is publicly traded, there are significantly fewer incidents of misconduct breaches during mergers as compared to the pre-treated group. In contrast, deals involving publicly traded buyers (first green line in Figure 13a) do not necessarily manage the risk of misconduct breaches better. The comparison becomes more obvious when hacking breaches are also taken into account. Interestingly, such deals exhibit greater efficiency in dealing with hacking incidents, as demonstrated in Figure 13b.

### 6.5.2 Organizational Capital: Bankrupt Acquisitions

Many hospital mergers in America are driven by financially distressed hospitals seeking to avoid bankruptcy or closure by being acquired by larger, more



(a) Misconduct Data Breaches on Public and Non-public Mergers

(b) Hacking and Misconduct Breaches on Public and Non-public Mergers

Figure 13: Impact of Publicly-traded and Private Deals: 2010-2022

*Notes:*The figures show the stratified regression coefficients specified in the main model by deals that involve some publicly traded hospitals and health systems. Control variables include target hospitals' bed count, revenue, and EBITDA before the merger signing year, the public trading status of the target and the buyers, and the individual and time-fixed effects. The bars are 95% intervals. Standard errors are clustered at the deal level. The top panel pertains to misconduct breaches, while the bottom panel includes all types of breaches. The blue lines represent a comparison of merger deals with a public target versus those without, while the green lines compare deals with a public buyer to those without. The red lines compare merger deals with either a public target or buyer to those without. Data source: Proprietary merger data and DHHS 2010-2022.

stable healthcare systems. In some cases, larger healthcare systems purchase closed hospitals with the intention of reopening them under their own management, thereby expanding their reach into new communities. The hypothesis is that target hospitals that are financially distressed should have lower-quality of organizational capital, so they are less able to mitigate data breach risks. I identify this group with the target hospitals that mentioned "bankrupt" in their description or have a negative EBITDA in the pre-merger year.

Table 11 illustrates that merging a struggling target can potentially result in a greater increase in misconduct breaches. Additionally, merging both struggling and non-struggling targets can lead to more hacking, although the increase is relatively smaller when merging a struggling target. This could be attributed to the fact that a struggling target is less appealing to attackers, or it may be because the bankrupt target hospital seized operation.

### 6.5.3 Organizational Capital: Female CEO

In this section, I investigate whether a deal with a female CEO is impacted differently from a deal with a male CEO. There are less than 10% deals with a female CEO, as shown in figure 14. The female CEOs are identified by applying the "gender" and "genderdata" package with 2012 SSA data on the CEO's first name. Since there is a very small number of such deals, the regression result for such deals in table 12 is with a very large variation. At the same time, because of the limited sample size, the regression does not include any control variable. The Wild Bootstrap result in figure 15 shows that the effect is a very large variation. The current study does not have a clear conclusion about whether buyers with a female CEO are impacted differently by a merger.

## 7 Coasian Solution

In this section, I investigate the effectiveness of the market in mitigating the rise in data breaches during mergers. Initially, I present the theoretical framework and its relevance to the phenomenon under study. I then focus on the period between 2018 and 2022 to assess whether the market has taken sufficient measures to manage the risks associated with mergers and acquisitions. Given the increasing awareness among practitioners of the potential hazards associated with such transactions, it is critical to evaluate the success of the Coasian Solution. Additionally, I scrutinize the role of professional investors, namely Private Equities and Real Estate Investment Trusts, by analyzing their merger deals separately. The study findings suggest that the market's efforts to address misconduct issues were effective, but the emergence of hacking activities undermined these endeavors. Furthermore, the result reveals that professional investors contribute to mitigating pre-merger data breach risks.

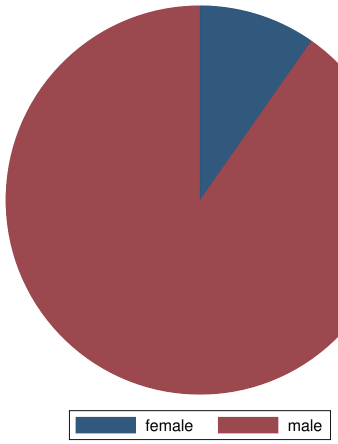


Figure 14: Deals with a Female CEO: 2010-2022

*Notes:* The figures show the number of deals with a female leading the buyer between 2010 and 2022. Notably, female CEOs have less than 10 percent representation in the sample.

Table 12: What if the Buyer has a Female CEO

| | Female | Male | All |
|---|---|---|---|
| Treatment Effect | 0.1397 | 0.0249*** | 0.0360*** |
| | (0.0865) | (0.0075) | (0.0116) |
| $N$ | 5033 | 527719 | 675255 |
| $R^2$ | 0.2773 | 0.2384 | 0.2434 |
| Mean of Data Breach on Nontreated % Effect | 1.70 | 1.89 | 2.29 |
| Mean of Data Breach on Treated % Effect | 13.55 | 3.94 | 5.15 |

Note: The table presents the impact of M&A deals involving female CEOs buying hospitals. The main variable of interest is a binary dummy, $Treated_{i,m}$, which equals 1 if a data breach was reported by the buyer, target, or seller for deal $m$ within the time period $[t-a, t+a]$. Date $t$ is when deal $m$ is signed, and $a \in [0, 4]$ quarters. The treated groups are the hospitals that participate in the deal $m$. The control group includes hospitals involved in a merger to be signed at least two years after $t$. Given the small sample size of deals with a female CEO, no control variables were included. All the regressions include a full set of hospital-year fixed effects. The table also reports the baseline mean outcome for the treated and the control groups. Standard errors are clustered at the deal level and are displayed in parentheses.

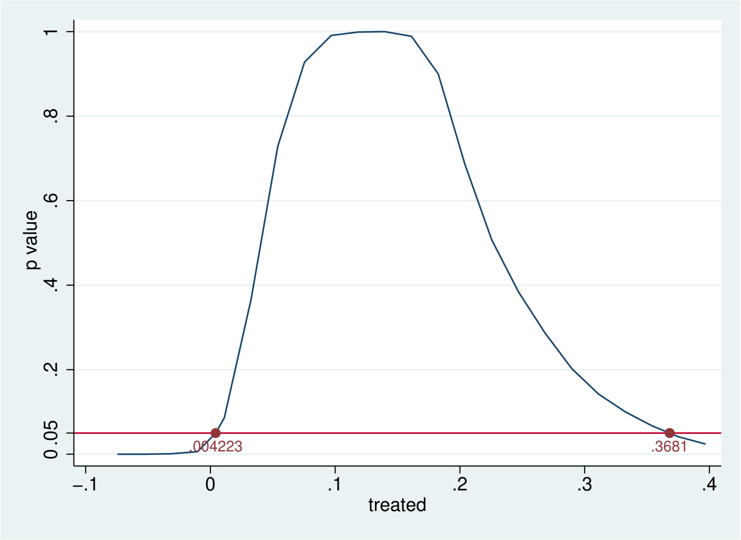


Figure 15: Wild Bootstrap on Deals with a Female CEO

*Notes:* The figure displays the wild bootstrap results for the coefficients specified in the main model, specifically examining the impact of mergers on data breaches when the buyer has a female CEO. The female CEOs are identified by applying the “gender” and “genderdata” package with 2012 SSA data. The coefficient is positive with a large variation, so the impact of a female CEO is not clear.

## 7.1 Theory of the Coasian Solution for Privacy Protection

The term externality refers to the unintended impact of economic activity. These spillover effects can be either positive or negative and are not reflected in the prices of goods or services, so externality is a sign of market failures, as the price does not reflect these true social costs or benefits generated by the spillovers. In Ronald Coase's 1960 paper "The Problem of Social Cost," he describes the situation where the cattle-raiser's straying cattle on neighboring land causes damage to the farmer's crops as a negative externality (Coase, 2013). Coase Theorem suggests that without transaction costs, parties involved in an externality can negotiate and reach an efficient outcome regardless of who is initially assigned property rights. In the cattle-raiser and farmer example, it does not matter who is initially responsible for the damage if they can negotiate without transaction costs. Another example of a negative externality where the Coase Theorem can be applied is environmental pollution. Although governmental intervention can be one solution to address negative externalities, another approach is the European Union Emissions Trading System (EU ETS). The EU ETS assigns property rights to the allowances to emit greenhouse gases, creating a market for private bargaining and trading of allowances. This second solution reduces emissions in an efficient manner. In this paper, I refer to such a solution of building a new market to facilitate such negotiation with reduced transaction costs rather than using governmental intervention as the Coasian Solution. In a Coasian Solution, the market achieves an efficient outcome by allowing the parties involved in an externality to negotiate and reach an agreement. The key to achieving such an outcome is assigning clear property rights. When property rights are well-defined, parties can negotiate to internalize the external costs or benefits and reach an efficient allocation of resources. This is because the party that values the property rights more highly will be willing to pay the other party to acquire them, which results in an exchange that benefits both parties.

The Coase theorem application to the economics of privacy argues that privacy will be protected as long as the data owner is aware of the risk and absorbs the costs (Acquisti, Taylor and Wagman, 2016; Tucker, 2022). As digitization progresses, the search, replication, tracking, and verification costs drop (Goldfarb and Tucker, 2019). These decreasing costs result in various adverse effects on privacy protection. When hospitals adopt electronic medical record systems and a data breach occurs, the patients get spillover effects in terms of privacy, financial, or even health loss. This is a typical example of a social cost problem described above where the conduct of the hospital imposes negative externalities on the patients. In recent years, patients are gaining more legal resources and bargaining power to address data breaches that violate their rights. Instead of using governmental intervention, the Coasian Solution for the healthcare privacy problem is raising awareness of privacy risks and bargaining power among patients.

Patients' awareness of privacy protection and bargaining power are essential in motivating hospitals to prioritize data security and protection. As more patients become aware of the potential consequences of data breaches, they are increasingly demanding better privacy protections from healthcare providers. For example, the rise of data breaches has led to an increase in class action lawsuits filed against companies that have failed to protect their customers' personal information. Class actions have become a key tool for consumers seeking compensation and accountability for the damages caused by such breaches. The high cost of settlements, such as the $350 million T-Mobile settlement, and the potential for significant reputation damage provide a strong incentive for companies to take proactive measures to prevent data breaches. Data breach class actions and other lawsuits can be seen as an indication of people's bargaining power for their privacy right over their data. Class actions are a cost-effective solution for individuals facing prohibitively high litigation costs, as they enable the pooling of resources and sharing of legal expenses, resulting in reduced transaction costs for negotiation. When companies face the possibility of significant financial liability for data breaches, they have a greater incentive to invest in stronger data security measures and to take responsibility for any breaches that do occur.

Therefore, by participating in data breach class actions and lawsuits, individuals are effectively asserting their privacy rights and using their collective bargaining power to hold companies accountable for any harm caused by data breaches. This can help to promote greater data security and protect individuals' privacy rights in the long term.

Moreover, as individual patients' awareness of privacy protection raise, hospitals that prioritize privacy protection can enjoy a competitive advantage, attracting patients who prioritize data security and privacy when choosing healthcare providers. Ultimately, prioritizing privacy protection can help hospitals build trust with patients and safeguard their reputations. Even more, when the harm from data breaches is recognized as too high, individual patients will be willing to pay higher prices for health services with more privacy protection.

An important question to consider is whether the consumers' increased awareness and improved bargaining power have motivated hospitals to effectively mitigate the increase in data breaches during mergers. In other words, has Coasian Solution worked? I investigate this question by analyzing the truncated result of the baseline model for the latest five years.

As consumers gain bargaining power, financial markets that provide the financial resources for healthcare providers react quickly, especially the private market funding investors who pursue short-term turnover. At the same time, as the vertical structure of hospitals becomes more complex, there is an increased risk of moral hazard and agency problems. In such control structures, hospital operators may be incentivized to prioritize their own interests over the hospital as a whole. This can lead to suboptimal decision-making. As consumers utilizing legal resources gain more bargaining power in the Coasian Solution for data breaches, investors who pursue short-term profit are more incentivized to check a hospital's due diligence on cybersecurity to prevent potential losses. It, in fact, is what investors are doing nowadays (Rundle and Nash, 2023). During mergers and acquisitions, more security due diligence audits are involved. The buyers hire financial and legal agencies for information technology and information security due diligence investigation on the target. More recently, cybersecurity agencies have performed cybersecurity audits on the target hospitals as well. It could include network scanning, control method audit, or even penetration test, where specialists will actively perform attacks to stress-test the target hospitals' information systems. Increased popularity and the increased fee of cybersecurity insurance should also induce more protection measures. To sum up, investors can play a critical role in motivating hospitals to prioritize data security and protection, facing the increasing bargaining power of consumers regarding their privacy rights. I test whether investors play such a role in mitigating the risks by analyzing merger deals with private market funding investor buyers separately. Another benefit of this analysis is that if private market funding investors can effectively mitigate the risks during mergers, their measures should be applied more widely.

## 7.2 Results on the Past 5 Years

This section first presents the main regression analysis on the truncated period of 2018-2022 to investigate the hypothesis that the Coasian Solution has been effective in mitigating the harm caused by data breaches, considering the significant rise in cybersecurity efforts during this period. However, the findings indicate that while the incidence of misconduct-related data breaches has decreased in recent years compared to before, the upsurge in hacking activities means that the two-year period surrounding the signing date of the merger remains a risky time window.

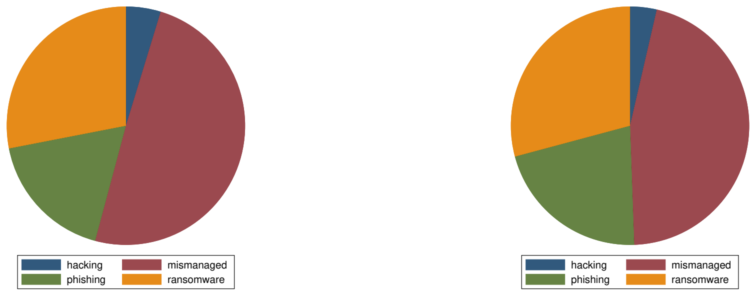
Table 13 presents the impact of mergers on data breaches for deals that were completed between 2018 and 2022. The same model used in the main results is utilized; however, given the shorter time frame, all treatments occurring in 2021 and 2022 are removed and used exclusively as control groups since they are too recent to have future mergers as control. The initial three columns pertain to all types of data breaches, while the middle three columns examine misconduct-related data breaches, and the final three columns analyze hacking-related data breaches. First, the effort to mitigate misconduct data breaches during the pre-merger period is effective, especially when public companies are involved. Second, unfortunately, the increase in hacking activities during the same time window overturns the results. Third, the increase in hacking data breaches during M&A is attributed mainly to post-signing-date hacking activities.

Furthermore, figure 16 shows the proportion of cases and individuals impacted by different types of data breaches that happened to merging hospitals in recent 5 years. Table 14 shows in the last 5 years, hacking activities, including ransomware attacks and phishing attacks, happen more before the merging signing date than afterward. These findings suggest that the signaling channel is the primary driver of the increase in organized and targeted attacks by hackers. In contrast, general hacking such as zero-day exploits less targeted. For instance, the Accellion file transfer application (FTA) zero-day exploit data breach affected over one hundred universities and hospitals in 2020 and 2021, and such hacking activities are less targeted and have less direct relevance to

Table 13: 2018-2022 EFFECT OF M&A ON DATA BREACHES

| | (T)all | (T)post | (T)pre | (M)all | (M)post | (M)pre | (H)all | (H)post | (H)pre |
|---|---|---|---|---|---|---|---|---|---|
| Treatment Effect | 0.0984** | 0.1028** | -0.0044 | -0.0147 | -0.0038 | -0.0109* | 0.1131** | 0.1066** | 0.0066 |
| | (0.0463) | (0.0502) | (0.0113) | (0.0134) | (0.0121) | (0.0063) | (0.0484) | (0.0499) | (0.0087) |
| Public Buyer | 0.0646** | 0.0675** | -0.0029 | -0.0097 | -0.0025 | -0.0072* | 0.0743** | 0.0699** | 0.0043 |
| | (0.0304) | (0.0330) | (0.0074) | (0.0088) | (0.0079) | (0.0041) | (0.0317) | (0.0328) | (0.0057) |
| Public Target | 0.0323** | 0.0337** | -0.0014 | -0.0048 | -0.0012 | -0.0036* | 0.0371** | 0.0350** | 0.0022 |
| | (0.0152) | (0.0165) | (0.0037) | (0.0044) | (0.0040) | (0.0021) | (0.0159) | (0.0164) | (0.0028) |
| REIT Buyers | -0.0323** | -0.0337** | 0.0014 | 0.0048 | 0.0012 | 0.0036* | -0.0371** | -0.0350** | -0.0022 |
| | (0.0152) | (0.0165) | (0.0037) | (0.0044) | (0.0040) | (0.0021) | (0.0159) | (0.0164) | (0.0028) |
| $N$ | 24549 | 24549 | 24549 | 24549 | 24549 | 24549 | 24549 | 24549 | 24549 |
| $R^2$ | 0.3973 | 0.3403 | 0.4823 | 0.5444 | 0.5647 | 0.5388 | 0.2563 | 0.1314 | 0.4248 |

Note: The table shows the effect of M&A on data breaches as estimated from the difference-in-differences equation during 2018-2022. The main variable of interest is a binary dummy, $Treated_{i,m}$, which equals 1 if a data breach was reported by the buyer, target, or seller for deal $m$ within the time period $[t-a, t+a]$. Date $t$ is when deal $m$ is signed, and $a \in [0, 4]$ quarters. The treated groups are the hospitals that participate in the deal $m$. The control group includes hospitals involved in a merger to be signed at least two years after $t$. All the regressions include a full set of hospital-year fixed effects. The 2021-2022 mergers are pure control groups for the truncated regression. Standard errors clustered at the deal level are displayed in parentheses. The first three columns are with total results (T), misconduct (M), and hacking (H) data breaches, where the first column is for all the time period $[t-a, t+a]$, the second column is for only post signing date $[0, t+a]$ and the third column is for the pre-signing date period$[t-a, 0]$. The following two sets, columns 4-6 and 7-9, are for misconduct (M) and hacking (H) data breaches separately on different treatment periods.



(a) 2018-2022: Data Breach Cases

(b) 2018-2022: Individual impacted

Figure 16: Data Breach Types on Merging Hospitals: 2018-2022
*Notes:* The figures show the number of reported data breaches (left) and the corresponding number of affected individuals (right) resulting from hospital mergers between 2018 and 2022. Notably, ransomware attacks accounted for more than half of the total hacking incidents.

hospital mergers.

### 7.3 Investors' Impact on Data Breaches

I then run the baseline model on deals with a professional investor buyer, PE or REIT. Interestingly, all the 7 data breaches within the two-year treatment period in the 76 professional investor deals are all misconduct data breaches. This is probably because of the absence of incompatibility between two merging EMRs in such deals. Table 15 shows the results of all data breaches, post-signing data breaches, and pre-signing data breaches separately. Given the considerable reduction in treatment size resulting from the stratification, the results are further subjected to wild-bootstrap analysis (Cameron, Gelbach and Miller, 2011; Roodman, Nielsen, MacKinnon and Webb, 2019), as shown in Figure 17. The analysis reveals a positive effect of the merger on post-period data breaches and a negative effect on pre-period data breaches.

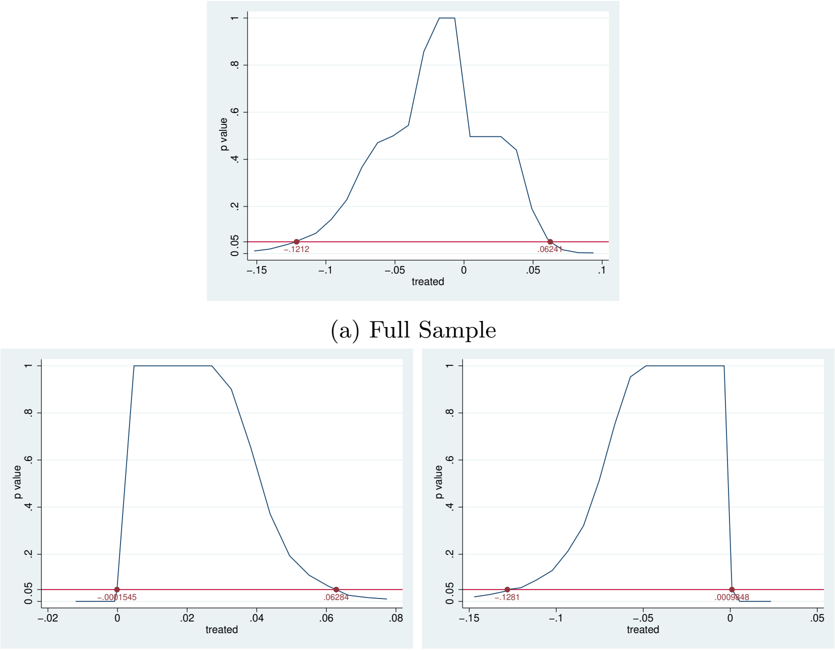
## 8 Alternative Time Windows

To assess the sensitivity of the merger's impact to different time frames, I conduct a two-stage robustness analysis. First, I test the regression results assuming that the treatment effect lasts longer than one year before the signing date and persisted for more than one year. I examine the robustness of the results by changing the time window to be longer. Second, given that it takes target hospitals more than a year to gradually adopt the buyer's EMR, I present an alternative assumption with a more persistent treatment effect. This tests whether data breaches occur more frequently during the time frame of one year before the merger signing date and three years after the merger signing date.

Table 14: EFFECT OF M&A ON DIFFERENT TYPES OF DATA BREACHES: 2018-2022

| | All Hacking | | | Ransomware Attacks | | | Phishing Attacks | | | General Hacking | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | All | Pre | Post | All | Pre | Post | All | Pre | Post | All | Pre | Post |
| Treatment | 0.1131$^{**}$ | 0.1066$^{**}$ | 0.0066 | 0.0625$^{***}$ | 0.0529$^{**}$ | 0.0096 | 0.0356$^{*}$ | 0.0360$^{*}$ | -0.0003 | 0.0150 | 0.0177 | -0.0027 |
| | (0.0484) | (0.0499) | (0.0087) | (0.0226) | (0.0217) | (0.0068) | (0.0187) | (0.0199) | (0.0045) | (0.0170) | (0.0166) | (0.0028) |
| Public Buyer | 0.0743$^{**}$ | 0.0699$^{**}$ | 0.0043 | 0.0410$^{***}$ | 0.0347$^{**}$ | 0.0063 | 0.0234$^{*}$ | 0.0236$^{*}$ | -0.0002 | 0.0098 | 0.0116 | -0.0018 |
| | (0.0317) | (0.0328) | (0.0057) | (0.0148) | (0.0142) | (0.0044) | (0.0123) | (0.0131) | (0.0030) | (0.0111) | (0.0109) | (0.0018) |
| Public Target | 0.0371$^{**}$ | 0.0350$^{**}$ | 0.0022 | 0.0205$^{***}$ | 0.0174$^{**}$ | 0.0032 | 0.0117$^{*}$ | 0.0118$^{*}$ | -0.0001 | 0.0049 | 0.0058 | -0.0009 |
| | (0.0159) | (0.0164) | (0.0028) | (0.0074) | (0.0071) | (0.0022) | (0.0061) | (0.0065) | (0.0015) | (0.0056) | (0.0054) | (0.0009) |
| REIT Buyers | -0.0371$^{**}$ | -0.0350$^{**}$ | -0.0022 | -0.0205$^{***}$ | -0.0174$^{**}$ | -0.0032 | -0.0117$^{*}$ | -0.0118$^{*}$ | 0.0001 | -0.0049 | -0.0058 | 0.0009 |
| | (0.0159) | (0.0164) | (0.0028) | (0.0074) | (0.0071) | (0.0022) | (0.0061) | (0.0065) | (0.0015) | (0.0056) | (0.0054) | (0.0009) |
| $N$ | 24549 | 24549 | 24549 | 24549 | 24549 | 24549 | 24549 | 24549 | 24549 | 24549 | 24549 | 24549 |
| $R^2$ | 0.2563 | 0.1314 | 0.4248 | 0.1680 | 0.1237 | 0.3651 | 0.2349 | 0.2021 | 0.2370 | 0.6995 | 0.0253 | 0.7375 |
| Pre-treated | 2.47 | 1.31 | 1.16 | 1.63 | 1.31 | 0.32 | 0.47 | 0.00 | 0.47 | 0.37 | 0.00 | 0.37 |
| Treated | 8.87 | 7.06 | 1.81 | 4.64 | 3.63 | 1.01 | 3.02 | 2.42 | 0.60 | 1.21 | 1.01 | 0.20 |

Note: The table shows the effect of M&A on different types of hacking activities as estimated from the difference-in-differences equation during 2018-2022. The main variable of interest is a binary dummy, $Treated_{i,m}$, which equals 1 if a data breach was reported by the buyer, target, or seller for deal $m$ within the time period $[t-a, t+a]$. Date $t$ is when deal $m$ is signed, and $a \in [0, 4]$ quarters. The treated groups are the hospitals that participate in the deal $m$ in 2018-2020. The control group includes hospitals involved in a merger to be signed at least two years after $t$. All the regressions include a full set of hospital-year fixed effects. I also control whether the merger deal involves a publicly traded buyer or target or whether the buyer is a REIT. The change of the control variables may be a reason why $R^2$ increases. The 2021-2022 mergers are pure control groups for the truncated regression. Standard errors clustered at the deal level are displayed in parentheses. Four types of hacking activities are presented, all hacking, ransomware attacks, phishing attacks, and general hacking, where the first column for each group is for all the time period $[t-a, t+a]$, the second column is for only the pre-signing date period$[t-a, 0]$ and the third column is for post signing date $[0, t+a]$.



(a) Full Sample

(b) Post-merger Breaches

(c) Pre-merger Breaches

Figure 17: Wild Clustered Bootstrap Estimation for 2010-2022 Mergers with Investor Buyers

*Notes:* The figure displays the wild bootstrap results for the coefficients specified in the main model, specifically examining the impact of mergers on data breaches when the buyers are PE or REIT. The results suggest that there is a large chance that investor buyers can have fewer data breaches before the merger signing date.

Table 15: 2010-2022 EFFECT OF INVESTOR BUYER ON DATA BREACHES

| | All Breaches | Post | Pre |
|---|---|---|---|
| Treatment Effect | -0.0179 | 0.0215 | -0.0394 |
| | (0.0446) | (0.0223) | (0.0358) |
| $N$ | 993 | 993 | 993 |
| $R^2$ | 0.5155 | 0.0380 | 0.6095 |

Note: The table shows the effect of M&A involving a PE or REIT investor on breaches 2010-2022. The main variable of interest is a binary dummy, $Treated_{i,m}$, which equals 1 if a data breach was reported by the buyer, target, or seller for deal $m$ within the time period $[t-a, t+a]$. Date $t$ is when deal $m$ is signed, and $a \in [0,4]$ quarters. The treated groups are the hospitals that participate in the deal $m$. The control group includes hospitals involved in a merger to be signed at least two years after $t$. All the regressions include a full set of hospital-year fixed effects. Standard errors clustered at the deal level are displayed in parentheses.

## 8.1 Other Windows: Symmetric Stretch

The critical issue is not how I assume the persistence of the treatment effect, but rather how far back before the merger signing date I assume the treatment is - in other words, when did the hackers become aware of the mergers? If my assumption is too distant, my sample size will be inadequate, and the treatment effect will be inaccurate. Conversely, if my assumption is too close, some of the early controls in the Pre-treated group will be contaminated. I demonstrate that the effect is robust when I adjust the assumption to two or three years.

Figure 18 illustrates the changes in the coefficient (with its 95% confidence interval) when I symmetrically adjust the two-year window to include two years before and after the mergers (a four-year window represented by a triangle) and then to three years before and after the mergers (a six-year window represented by a square). However, a longer time window can result in more mergers without a control group, so I also included the shorter time window assumption with the same treatment samples that ends early for comparison. If the time window is a four-year window, mergers that occur after 2018 will be too late to find any Pre-treated group without contamination. The green lines show the coefficients for different time windows for mergers before 2018. If the time window is six years, the latest treatment that can be tested is in 2016, and the black data points represent the coefficients that end in 2016. The blue data points represent the original design that can test the treatment effect up to 2020. The six-year window has a smaller sample size, resulting in a larger standard error.

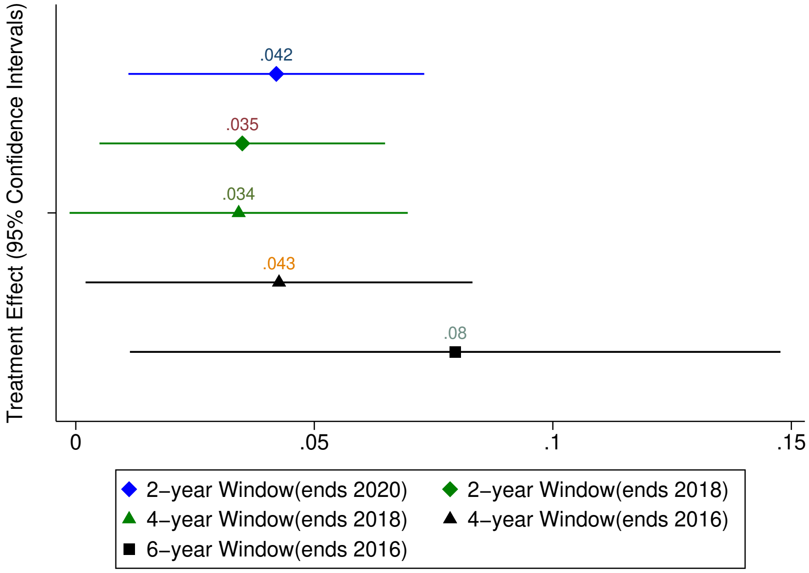


Figure 18: Robustness to Changes in Time Window

*Notes:* The figure plots coefficients specified in the main model but compares the data breach probability of the treated mergers with the pre-treated mergers in different time windows. Corresponding control/pre-merger groups are set further away enough to avoid contamination. Control variables include target hospitals' bed count, revenue, and EBITDA before the merger signing year, the public trading status of the target and the buyers, and the individual and time-fixed effects. The bars are the 95 percent confidence intervals. Standard errors are clustered at deal level. The blue line with a diamond nob is the original two-year window. The green line with a triangle nob is on the four-year window, [two years before the merger deal is signed, two years after]. The black line with a square nob is on the three-year window. The rest are robustness checks with the same sample but different time windows. Data source: Proprietary merger data and DHHS 2010-2022.

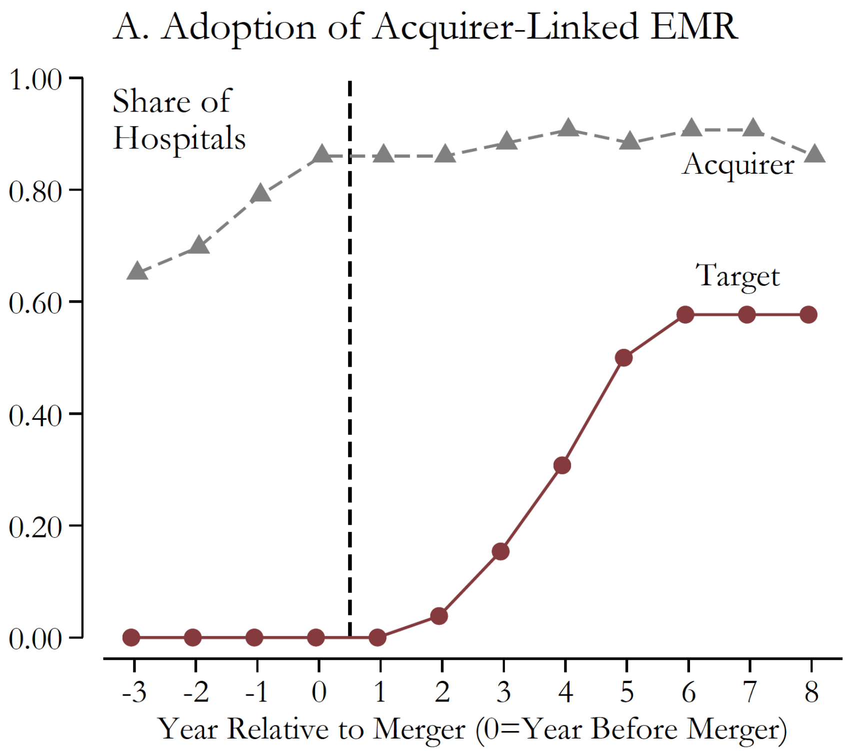


Figure 19: Gaynor et al. (2021) Graph

*Notes:*Gaynor, Sacarny, Sadun, Syverson and Venkatesh (2021), “As expected, no target hospital had installed EMRs from this niche’s vendor before the merger, but the rollout began soon after. Progress was modest at first, then accelerated. Three years after the merger, a third of the target hospitals had the EMR system. By the fifth year, adoption had risen to just under 58%, where it plateaued. In target hospitals, we also noted a pattern of dropping chain-specific EMRs during the post-merger period: 59% of targets dropped a vendor they uniquely used while 34% dropped a self-developed EMR system. These patterns strongly suggest that the target hospitals harmonized their EMR system with the acquirers.” This graph is in the appendix of Gaynor, Sacarny, Sadun, Syverson and Venkatesh (2021).

### 8.2 One Year Before and Three Year After Results

EMR integration cannot begin until a merger closes. Gaynor, Sacarny, Sadun, Syverson and Venkatesh (2021) suggests the installation of EMRs from a niche vendor begins soon after the merger, and adoption progresses modestly at first, but accelerated over time (as shown in figure 19). Notably, three years after the merger, a third of the target hospitals had adopted the EMR system. This suggests that the three-year mark was a critical turning point in the adoption of the new system. Prior to the three-year mark, malicious actors have a window to exploit system incompatibilities.

The main model analyzes the time window $[t-4, t+4]$, while table 16 analyzes the time window $[t-4, t+12]$. The results indicate no significant differences in pre-trends in the probability of data breaches between the treatment and pre-treated groups. However, during the two-year time window surrounding the merger signing date, there is no evidence to reject the null that there may be an intentional delay in reporting data breaches.

Table 16 displays the baseline outcomes for the effect of mergers on data breaches reported in the asymmetric four-year window: one year before, three years after merger closure from 2010 to 2022, with various control combinations. Hospitals that go through mergers are more than twice as likely to experience a data breach relative to the pre-treated group. It is consistent with the alternative symmetric two-year window [one year before, one year after merger closure]. Specifically, Column 7 corresponds to the main regression equation, which includes all control variables. I observe a large positive effect, 3.49 percentage points, on data breach probability from the merger signing date, and it is statistically significant at the 5% level. Columns 1, 3, and 5 show regression results with gradually added control variables. Due to the availability of the control variables, the sample size varies, so columns 2, 4, and 6 control for the sample sizes by dropping all the observations without all the controls. The effect is comparable to table 2 with the original research design. On average over the course of four years, the probability of a data breach in the pre-treated group is approximately 1% instead of 3%. Similarly, the treated group experiences a data breach probability of around 2.5% compared to 6% in the original design.

Another alternative is to adopt other assumptions from the Google Trends analysis in figure 10. Instead of one year before the merger deal is signed, 17 months and 27 months are tested and shown in figure 20.

# 9 Conclusion

This paper examines cybersecurity risks during the two-year window around the merger closure date, presenting how the event of a hospital merger doubles the data breach probability from 2010 to 2022 and how the organizational capital, strategic interaction with hackers, and delay reporting issues impact the result. Hacking activities rather than misconduct breaches are the main reason for the increase. When I truncate the data to show the more recent period effect and

Table 16: M&A EFFECT ON DATA BREACHES: [ONE YEAR BEFORE, THREE YEAR AFTER]

| | (1) | (2) | (3) | (4) | (5) | (6) | (7) |
|---|---|---|---|---|---|---|---|
| Does M&A cause data breaches? | 0.0377*** | 0.0349*** | 0.0340*** | 0.0349*** | 0.0346*** | 0.0349*** | 0.0349*** |
| | (0.0086) | (0.0103) | (0.0100) | (0.0103) | (0.0102) | (0.0103) | (0.0103) |
| Public Acquirer | -0.0883 | 1.5869** | -0.1141 | 5.5891 | 2.9696** | 1.0973 | 14.9614 |
| | (0.0827) | (0.6561) | (0.0754) | (6.0061) | (1.4186) | (0.6831) | (15.8289) |
| Public Target | -0.1051 | -2.3627 | -0.2678* | -1.1877 | 0.0005 | 2.1259 | 7.5266 |
| | (0.0861) | (1.6674) | (0.1407) | (1.4814) | (1.3717) | (2.4016) | (6.8258) |
| Target Hospital's Bed Count | 0.2922 | 0.6515 | 0.4055* | 0.6674 | 0.3172 | 0.1469 | 0.0576 |
| | (0.3353) | (0.5454) | (0.2337) | (0.5639) | (0.3324) | (0.1621) | (0.0622) |
| Target Hospital's Revenue | | | -0.0280 | 0.0473 | | | 0.1655 |
| | | | (0.0221) | (0.0729) | | | (0.1909) |
| Target Hospital's EBITDA | | | | | 1.0082 | 2.1828 | 2.8096* |
| | | | | | (0.6514) | (1.5230) | (1.6572) |
| $N$ | 447507 | 336984 | 352299 | 336984 | 339152 | 336984 | 336984 |
| $R^2$ | 0.3370 | 0.3377 | 0.3434 | 0.3377 | 0.3342 | 0.3376 | 0.3376 |
| Mean of Data Breach on Pre-treated % Effect | 0.94 | 0.95 | 1.09 | 0.95 | 1.01 | 0.95 | 0.95 |
| Mean of Data Breach on Treated % Effect | 2.34 | 2.53 | 2.13 | 2.53 | 2.50 | 2.53 | 2.53 |
| Mean of Data Breach on Pre-treated Targets % Effect | 0.63 | 0.58 | 0.74 | 0.70 | 0.60 | 0.58 | 0.60 |
| Mean of Data Breach on Treated Targets % Effect | 2.21 | 2.39 | 2.34 | 2.38 | 2.56 | 2.23 | 2.23 |
| Mean of Data Breach on Pre-treated Seller % Effect | 0.90 | 1.06 | 0.99 | 1.01 | 1.09 | 1.05 | 1.11 |
| Mean of Data Breach on Treated % Effect Seller | 1.32 | 1.75 | 3.17 | 1.59 | 3.33 | 1.69 | 1.79 |
| Mean of Data Breach on Pre-treated Acquirer % Effect | 0.80 | 0.67 | 0.86 | 0.81 | 0.68 | 0.67 | 0.69 |
| Mean of Data Breach on Treated Acquirer % Effect | 2.44 | 2.40 | 2.03 | 2.56 | 2.20 | 2.57 | 2.57 |

Note: The table shows the effect of M&A on hacking activities with different sets of controls. The explanatory variable of main interest is a dummy $Treated_{i,m}$ that equals 1 for any of the hospitals $i$ in merger $m$ to be involved in deal $m$ and reported a data breach in $[t-a, t+b]$. Date $t$ is when deal $m$ is signed. $a \in [0,4]$ quarters. $b \in [0,12]$ quarters. The control group includes hospitals involved in a merger to be signed at least four years after $t$. All the regressions include a full set of hospital-year fixed effects. Columns 1, 3, 5, and 7 show results with different control variable combinations. Columns 2, 4, and 6 represent robustness checks conducted with the smallest sample size. The table also reports the baseline mean outcome for the treated and the control groups. Standard errors are clustered at the deal level and are displayed in parentheses.

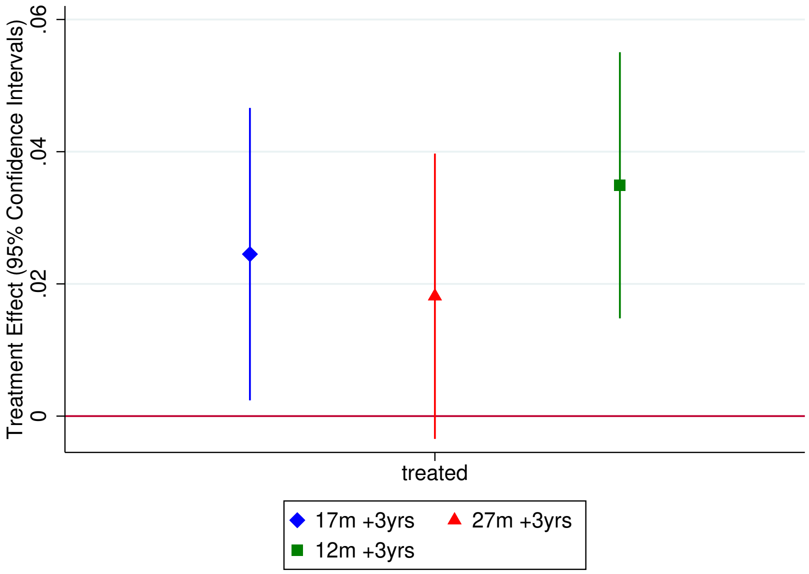


Figure 20: Robustness to Changes in Time Window: Google Trends

*Notes:* The figure illustrates the coefficients specified in the main model, presenting alternative assumptions regarding the duration of time before the merger signing date when the treatment begins. The three scenarios considered are one year, 17 months, and 27 months prior to the merger signing date. The controls in the analysis include the target hospitals' bed count, revenue, and EBITDA prior to the year of merger signing, as well as the public trading status of the target and the buyers. Additionally, individual and time fixed effects are accounted for. The bars represent the 95% confidence intervals, while standard errors are clustered at the deal level. The green (square) coefficient corresponds to Table 16. The blue (diamond) coefficient utilizes the median Google search peak, as shown in figure 10, occurring 17 months before the merger signing date. The red (triangle) coefficient uses the 25th percentile in figure 10, which corresponds to 27 months before the merger signing date. Data source: Proprietary merger data and DHHS 2010-2022.

stratify the deals with private market funding investors, I argue that the hacking activities in recent years made things worse despite the increasing security efforts during the merger process. For hacking activities, the pre-signing data breach accounts for a 1.98 percentage points increase, and the post-closure data breach accounts for a 1.62 percentage points increase compared with the pre-treated group. The post-closure hackings represent the incompatibility problems of the two merging information systems, and the pre-signing data breaches are from the hackers' information asymmetry reduction on the merging hospitals.

While information transparency aids in mitigating agency costs during merger events, my findings indicate a possible rise in cyber threats when the financial and operational information of merging hospitals is made public. Furthermore, my results highlight that ransomware attacks, which disrupt healthcare services, occur more frequently during this period of time as well. Understanding the development of the reasons for large-scale data breaches in the healthcare industry is particularly relevant today to avoid public health emergencies and maintain financial market stability. Hospital mergers have patients, health insurance, cybersecurity insurance, financial agents, public market investors, and PE and REIT investors all tied into it. As more ransomware attacks invade hospitals with significant disruption of operations, when reporting the problem is not under the control of the hospitals, a massive shock to the financial market volatility can also be an issue in the future. Finance, security, and health authorities should be prepared for market shocks, and issue pre-merger warnings and best practice guidance.

# References

**Acquisti, Alessandro, Allan Friedman, and Rahul Telang**, "Is there a cost to privacy breaches? An event study," *ICIS 2006 proceedings*, 2006, p. 94.

_ **and Hal R Varian**, "Conditioning prices on purchase history," *Marketing Science*, 2005, *24* (3), 367–381.

_ **, Curtis Taylor, and Liad Wagman**, "The economics of privacy," *Journal of economic Literature*, 2016, *54* (2), 442–92.

**Adjerid, Idris, Alessandro Acquisti, Rahul Telang, Rema Padman, and Julia Adler-Milstein**, "The impact of privacy regulation and technology incentives: The case of health information exchanges," *Management Science*, 2016, *62* (4), 1042–1063.

**Arce, Daniel**, "Cybersecurity For Defense Economists," *Defence and Peace Economics*, 2022, pp. 1–21.

**Arce, Daniel G.**, "Malware and market share," *Journal of Cybersecurity*, 2018, *4* (1).

**Athey, Susan and Guido W Imbens**, "Design-based analysis in difference-in-differences settings with staggered adoption," *Journal of Econometrics*, 2022, *226* (1), 62–79.

**Baker, Andrew C, David F Larcker, and Charles CY Wang**, "How much should we trust staggered difference-in-differences estimates?," *Journal of Financial Economics*, 2022, *144* (2), 370–395.

**Bittner, Dave and Johannes Ullrich**, "Cyberwire podcast Ep 1781: CISA warns of Telerik vulnerability exploitation," *Cyberwire*, 2023.

**Blascak, Nathan and Ying Lei Toh**, "Prior Fraud Exposure and Precautionary Credit Market Behavior," *Working paper*, 2022.

**Bloom, Nicholas, Raffaella Sadun, and John Van Reenen**, "The organization of firms across countries," *The quarterly journal of economics*, 2012, *127* (4), 1663–1705.

**Bonatti, Alessandro and Gonzalo Cisternas**, "Consumer scores and price discrimination," *The Review of Economic Studies*, 2020, *87* (2), 750–791.

**Borusyak, Kirill, Xavier Jaravel, and Jann Spiess**, "Revisiting event study designs: Robust and efficient estimation," *arXiv preprint arXiv:2108.12419*, 2021.

**Bresnahan, Timothy F, Erik Brynjolfsson, and Lorin M Hitt**, "Information technology, workplace organization, and the demand for skilled labor: Firm-level evidence," *The quarterly journal of economics*, 2002, *117* (1), 339–376.

**Bruch, Joseph D, Suhas Gondi, and Zirui Song**, "Changes in hospital income, use, and quality associated with private equity acquisition," *JAMA Internal Medicine*, 2020, *180* (11), 1428–1435.

**Brynjolfsson, Erik, Daniel Rock, and Chad Syverson**, "The productivity J-curve: How intangibles complement general purpose technologies," *American Economic Journal: Macroeconomics*, 2021, *13* (1), 333–72.

**_ , Lorin M Hitt, and Shinkyu Yang**, "Intangible assets: Computers and organizational capital," *Brookings papers on economic activity*, 2002, *2002* (1), 137–181.

**Butts, Kyle and John Gardner**, "{did2s}: Two-Stage Difference-in-Differences," *arXiv preprint arXiv:2109.05913*, 2021.

**Cameron, A Colin, Jonah B Gelbach, and Douglas L Miller**, "Robust inference with multiway clustering," *Journal of Business & Economic Statistics*, 2011, *29* (2), 238–249.

**Campbell, Katherine, Lawrence A Gordon, Martin P Loeb, and Lei Zhou**, "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," *Journal of Computer security*, 2003, *11* (3), 431–448.

**Cavusoglu, Huseyin, Srinivasan Raghunathan, and Wei T Yue**, "Decision-theoretic and game-theoretic approaches to IT security investment," *Journal of Management Information Systems*, 2008, *25* (2), 281–304.

**Cecere, Grazia, Fabrice Le Guel, Vincent Lefrere, Catherine E Tucker, and Pai-Ling Yin**, "Privacy, Data and Competition: The Case of Apps for Young Children," *Available at SSRN 4073931*, 2022.

**Chaisemartin, Clément De and Xavier d'Haultfoeuille**, "Difference-in-differences estimators of intertemporal treatment effects," Technical Report, National Bureau of Economic Research 2022.

**Chen, Zhijun, Chongwoo Choe, and Noriaki Matsushima**, "Competitive personalized pricing," *Management Science*, 2020, *66* (9), 4003–4023.

**_ , _ , Jiajia Cong, and Noriaki Matsushima**, "Data-driven mergers and personalization," *The RAND Journal of Economics*, 2022, *53* (1), 3–31.

**Choi, Sung J and M Eric Johnson**, "Do Hospital Data Breaches Reduce Patient Care Quality?," *arXiv preprint arXiv:1904.02058*, 2019.

**Coase, Ronald H**, "The problem of social cost," *The journal of Law and Economics*, 2013, *56* (4), 837–877.

**Corniere, Alexandre De and Greg Taylor**, "Data and competition: a general framework with applications to mergers, market structure, and privacy policy," 2020.

**Deshpande, Manasi and Yue Li**, "Who is screened out? Application costs and the targeting of disability programs," *American Economic Journal: Economic Policy*, 2019, *11* (4), 213–48.

**Gao, Janet, Merih Sevilir, and Yong Seok Kim**, "Private equity in the hospital industry," *European Corporate Governance Institute–Finance Working Paper*, 2021, (787).

**Garcia, Alfredo, Yue Sun, and Joseph Shen**, "Dynamic platform competition with malicious users," *Dynamic Games and Applications*, 2014, *4* (3), 290–308.

**Garicano, Luis**, "Policemen, managers, lawyers: New results on complementarities between organization and information and communication technology," *International Journal of Industrial Organization*, 2010, *28* (4), 355–358.

**Gaynor, Martin, Adam Sacarny, Raffaella Sadun, Chad Syverson, and Shruthi Venkatesh**, "The anatomy of a hospital system merger: the patient did not respond well to treatment," Technical Report, National Bureau of Economic Research 2021.

**Gaynor, Martin S, Muhammad Zia Hydari, and Rahul Telang**, "Is patient data better protected in competitive healthcare markets?," in "WEIS" 2012.

**Geer, Dan, Eric Jardine, and Eireann Leverett**, "On market concentration and cybersecurity risk," *Journal of Cyber Policy*, 2020, *5* (1), 9–29.

**Georgiadou, Anna, Spiros Mouzakitis, and Dimitris Askounis**, "Detecting insider threat via a cyber-security culture framework," *Journal of Computer Information Systems*, 2022, *62* (4), 706–716.

**Goldfarb, Avi and Catherine Tucker**, "Digital economics," *Journal of Economic Literature*, 2019, *57* (1), 3–43.

**Gondi, Suhas and Zirui Song**, "Potential implications of private equity investments in health care delivery," *Jama*, 2019, *321* (11), 1047–1048.

**Goodman-Bacon, Andrew**, "Difference-in-differences with variation in treatment timing," *Journal of Econometrics*, 2021, *225* (2), 254–277.

**Greitzer, Frank L, Andrew P Moore, Dawn M Cappelli, Dee H Andrews, Lynn A Carroll, and Thomas D Hull**, "Combating the insider cyber threat," *IEEE Security & Privacy*, 2008, *6* (1), 61–64.

**Huang, C Derrick, Ravi S Behara, and Jahyun Goo**, "Optimal information security investment in a Healthcare Information Exchange: An economic analysis," *Decision Support Systems*, 2014, *61*, 1–11.

**Huang, Henry He and Chong Wang**, "Do Banks Price Firms' Data Breaches?," *The Accounting Review*, 2021, *96* (3), 261–286.

**Islam, Md Shariful, Tawei Wang, Nusrat Farah, and Tom Stafford**, "The spillover effect of focal firms' cybersecurity breaches on rivals and the role of the CIO: Evidence from stock trading volume," *Journal of Accounting and Public Policy*, 2022, *41* (2), 106916.

**Janakiraman, Ramkumar, Eunho Park, Emre M. Demirezen, and Subodha Kumar**, "The effects of health information exchange access on healthcare quality and efficiency: An empirical investigation," *Management Science*, 2022.

**Kannan, Karthik, Jackie Rees, and Sanjay Sridhar**, "Market reactions to information security breach announcements: An empirical analysis," *International Journal of Electronic Commerce*, 2007, *12* (1), 69–91.

**Kwon, Juhee and M Eric Johnson**, "The market effect of healthcare security: Do patients care about data breaches?," in "WEIS" 2015.

**_ and _** , "Protecting patient data-the economic perspective of healthcare security," *IEEE Security & Privacy*, 2015, *13* (5), 90–95.

**Lin, Yu-Kai, Mingfeng Lin, and Hsinchun Chen**, "Do electronic health records affect quality of care? Evidence from the HITECH Act," *Information Systems Research*, 2019, *30* (1), 306–318.

**Liu, Tong**, "Bargaining with private equity: implications for hospital prices and patient welfare," *Available at SSRN 3896410*, 2021.

**Marthews, Alex and Catherine Tucker**, "Privacy policy and competition," 2019.

**Milgrom, Paul and John Roberts**, "The economics of modern manufacturing: Technology, strategy, and organization," *The American Economic Review*, 1990, pp. 511–528.

**Miller, Amalia R**, "Privacy of digital health information," *Economics of Privacy*, 2022.

**_ and Catherine Tucker**, "Privacy protection and technology diffusion: The case of electronic medical records," *Management science*, 2009, *55* (7), 1077–1093.

**_ and _** , "Can health care information technology save babies?," *Journal of Political Economy*, 2011, *119* (2), 289–324.

**_ and _** , "Privacy protection, personalized medicine, and genetic testing," *Management Science*, 2018, *64* (10), 4648–4668.

**Moore, Tyler**, "The economics of cybersecurity: Principles and policy options," *International Journal of Critical Infrastructure Protection*, 2010, *3* (3-4), 103–117.

_ **and Richard Clayton**, "Evil searching: Compromise and recompromise of internet hosts for phishing," in "Financial Cryptography and Data Security: 13th International Conference, FC 2009, Accra Beach, Barbados, February 23-26, 2009. Revised Selected Papers 13" Springer 2009, pp. 256–272.

**Nykodym, Nick, Robert Taylor, and Julia Vilela**, "Criminal profiling and insider cyber crime," *Computer Law & Security Review*, 2005, *21* (5), 408–414.

**O'Donnell, Adam J**, "When malware attacks (anything but windows)," *IEEE Security & Privacy*, 2008, *6* (3), 68–70.

**Payne, Thomas H, David W Bates, Eta S Berner, Elmer V Bernstam, H Dominic Covvey, Mark E Frisse, Thomas Graf, Robert A Greenes, Edward P Hoffer, Gil Kuperman et al.**, "Healthcare information technology and economics," *Journal of the American Medical Informatics Association*, 2013, *20* (2), 212–217.

**Ralston, William**, "The untold story of a cyberattack, a hospital and a dying woman," *WIRED*, 2020.

**Rambachan, Ashesh and Jonathan Roth**, "A more credible approach to parallel trends," *Review of Economic Studies*, 2023, p. rdad018.

**Richards, Michael R. and Christopher M. Whaley**, "Hospital Behavior Over the Private Equity Life Cycle," *NBER Health Care Program Meeting, Spring 2023.*

**Roodman, David, Morten Ørregaard Nielsen, James G MacKinnon, and Matthew D Webb**, "Fast and wild: Bootstrap inference in Stata using boottest," *The Stata Journal*, 2019, *19* (1), 4–60.

**Rundle, James**, "Code Dark: Children's Hospital Strives to Minimize Impact of Hacks," *The Wall Street Journal*, 2022.

_ **and Kim S. Nash**, "Private-Equity Firms Tighten Focus on Cyber Defenses at Portfolio Companies," *The Wall Street Journal*, 2023.

**Savage, Lucia, Martin Gaynor, and Julia Adler-Milstein**, "Digital health data and information sharing: A new frontier for health care competition," *Antitrust LJ*, 2018, *82*, 593.

**Scheffler, Richard M, Laura M Alexander, and James R Godwin**, "Soaring private equity investment in the healthcare sector: Consolidation accelerated, competition undermined, and patients at risk," *University of California, Berkeley*, 2021.

**Shaw, Eric D**, "The role of behavioral research and profiling in malicious cyber insider investigations," *Digital investigation*, 2006, *3* (1), 20–31.

**Tucker, Catherine**, "The Economics of Privacy: An Agenda," *NBER Chapters*, 2022.

**Vasek, Marie, John Wadleigh, and Tyler Moore**, "Hacking is not random: a case-control study of webserver-compromise risk," *IEEE Transactions on Dependable and Secure Computing*, 2015, *13* (2), 206–219.

**Wilde, Anna and Brent Kendall**, "Judge Rejects Antitrust Challenge to UnitedHealth Acquisition," 2022.

**Yuan, Bocong, Jiannan Li, and Peiguan Wu**, "The effectiveness of electronic health record promotion for healthcare providers in the United States since the Health Information Technology for Economic and Clinical Health Act: An empirical investigation," *The International Journal of Health Planning and Management*, 2021, *36* (2), 334–352.

**Zhu, Jane M, Lynn M Hua, and Daniel Polsky**, "Private equity acquisitions of physician medical groups across specialties, 2013-2016," *JAMA*, 2020, *323* (7), 663–665.