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

Nan Clement

February 4, 2024

Updated frequently. Click here for the latest version.

Abstract

Data breaches in hospitals disrupt care, potentially leading to fatal consequences, violating privacy rights, and incurring significant costs to remedy. Mergers and acquisitions serve as an essential source of financing but also induce substantial management challenges. Using proprietary hospital merger records and 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 study whether and how hospital mergers increase the probability of a data breach. On average, the probability of a data breach in two years for pre-merger deals is approximately 3%, while for the hospitals undergoing the merging process, the data breach rate reaches 6%. The effect is robust to changes of the two-year window. The effect is robust in alternative control group constructions. The effect is also robust to the changes in sample size due to the data availability of the control variables and in how standard errors are clustered. Increased attention online one year before the merger deal is signed, identified with Google Trends score, causes a large increase in pre-signing hacks, especially in recent years through ransomware attacks. Such an effect of attention does not extend to the post-signing period. The increase in post-signing hacks is due to the incompatibility of merging information systems. More complicated information system integration in multi-hospital systems leads to greater elevated post-signing breaches. 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 mergers. The dynamic analysis shows that the data breach situation during mergers is getting worse because of soaring cases of hacks, even though insider misconduct has become less of a problem since 2014. Recent post-signing hacks exhibit shorter attack cycles compared to conventional malware attacks. These faster cycles catch unprepared hospitals off guard before hospitals get integration in order.

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 and reviewers in the following events: the 2022 WEIS rump session organized by Tyler Moore, Laura Brandimarte, and Sadia Afroz, AEA-CSWEP online and SEA mentoring sessions organized by Catherine Maclean, Orgül Öztürk, Melanie Guldi and Maya Rossin-Slater, the Texas Applied Microeconomics Student Workshop organized by Francisco Pardo Pajuelo, the Cybersecurity Summer Institute at Georgia Tech organized by Nadiya Kostyuk, the Emerging Scholar on Healthcare Competition organized by Ellie Prager at ASHEcon and the 2023 WEIS organized by Svetlana Abramova, Josephine Wolff, and Thomas Maillart. I am in debt to my ASHEcon discussant, Ryan McDevitt. I benefit from conversations with Rajiv Kohli, Idris Adjerid, Pinar Yildirim, Caitlin Carroll, Steve Schwab, Chuqing Jin, and many others. 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

When 30 servers at the University Hospital Düsseldorf in Germany fell victim to a ransomware attack, the hospital had no choice but to turn away ambulances. A 78-year-old critically ill woman was forced to go to Wuppertal for care, which is 20 miles away. The delay? It cost her life (Ralston, 2020). "The FBI and DOJ are now treating the patient and public safety risk that cyber-attacks are posing on hospitals as 'threat to life' crimes", DHHS (2023). These situations are not unique, as in 2022, healthcare data breaches in the US hit more than 40 million victims, violating their privacy rights, and nearly 600 hospitals spent more than ten million dollars on average for ransom, lawsuits, incident response, and recovery. This year, healthcare is still the most vulnerable sector, with a 50% increase in breaches in 2023. (ForgeRock, 2023; IBM, 2023). Now the fire alarm has gone off, the hospitals are forging their own security paths. Notably, the divergence in cybersecurity investments, measured as a proportion of total revenue, can span a 166% difference as documented by DHHS (2023). I investigate whether, and how, hospital mergers increase the probability of data breaches to provide more effective directions to act. This paper is among the first empirical attempts to test what may be a reason that some hospitals have more data breaches rather than others.

The practical motivation for this study is to understand surged data breaches in hospitals, while the theoretical motivation is to empirically evaluate factors contributing to the breaches from the perspectives of technology, information, and organizational capital. By doing so, this paper contributes to the Economics of Cybersecurity. Multi-firm information system cooperation is in a complex adaptive system environment, and Information System Integration (ISI) during mergers is a challenging process and a key to generating merger synergies (Brynjolfsson, Malone, Gurbaxani and Kambil, 1994; Zaheer and Venkatraman, 1994; Tanriverdi, Rai and Venkatraman, 2010; Tanriverdi and Uysal, 2011; Du, 2015; Tanriverdi and Du, 2020; Du and Tanriverdi, 2022). At the same time, the success during the transition period of ISI heavily relies on the acquirer's capability. For example, Tanriverdi and Bülent Uysal (2015) show that buyers with superior IT capabilities, and buying a target company with less compatible problems, reduce the capital market's negative reaction due to the concern about the ISI. I contribute to this discussion by showing the immediate cybersecurity consequences for buyers with different capabilities for data breaches that are solely their own responsibility and that involve hackers seperately. It is worth noting that incorporating the attacker's perspective nurtures a more comprehensive understanding of information security issues (Mahmood, Siponen, Straub, Rao and Raghu, 2010). I also contribute to the latest trend of research on attackers (Hughes, Chua and Hutchings, 2021; Li and Chen, 2022; Ebrahimi, Chai, Samtani and Chen, 2022; Samtani, Chai and Chen, 2022; Chua, 2023) by partially revealing malicious actors' preferences and attack duration with respect to their reactions to information and technology changes during market structure transformation.

Information, technology, and organizational capital factors all impact breaches during mergers. Specifically, as listed in Table 1, these factors include incompatibility during integration, insider misconduct, heightened attention attracting attacks, variations in organizational capital, and the evolving landscape of security threats and technology. To capture these three aspects of effect, both the pre-

signing period and post-signing period need to be considered. In the main regression, I test whether hospital data breaches happen more often in the two years surrounding the merger signing date [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 signing date in my observation. The signing 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 electronic medical record system integration, data migration, and cybersecurity protocol incorporation. The two-year window is the shaded area to include the risk both during and before the operational integration.

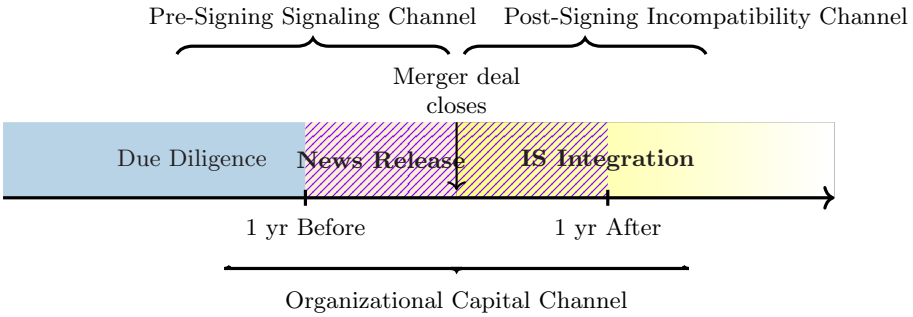


Figure 1: Merger Timeline and 2-year Window

Notes: The figure illustrates the two-year window. The Incompatibility Channel does not start until the merger deal closes. Cyber-attacks that occur before this point are accounted for in the pre-signing Signaling Channel. In the main model, the pre-signing Signaling Channel is assumed to begin one year prior to the merger deal's closure. Alternative assumptions are also explored. The Operational Capital Channel illustrates how the hospital's leadership, control process, organizational structure, and other organizational capital complement IT security throughout the process.

I use stacked difference-in-differences (Deshpande and Li, 2019) to document the cybersecurity results of mergers. The advantage of using stacked difference-in-differences and using future mergers as control groups is that I avoid using already treated cases as controls in staggered treatment that bias the mean of the control group, as pointed out in Goodman-Bacon (2021). 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, which does not have an undergoing merger, has more data breaches in the same time window. The result is robust to the changes in the time window. I extend the window symmetrically to include a four-year and six-year timeframe and present the corresponding results. An asymmetric window, focusing on one year before the deal's signing and three years after the merger is completed, yields similar findings. As in Gaynor, Sacarny, Sadun, Syverson and Venkatesh (2021), following a merger deal closing, target hospitals initiate the installation of EMR from the acquirer's vendor, with modest progress initially that later accelerates, resulting in a third of the hospitals implementing the system within three years. 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. Using future mergers/pre-treated only groups means that the treatment is not the merger itself, which involves a selection process, but the time of the merger. In Appendix Section F, I also construct an alternative data set with additional data from CMS Hospital Compares for 2016-2022 to include never-treated, hospitals that have never been merged during 2009-2022, and show that the result is robust to changes in the control group construction. Additionally, I apply multiple stratifications and dynamic event studies to analyze the causation mechanisms.

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. To ensure accuracy, I only use archived data from 2010 and up until 2022. Hajizada and Moore (2023) compare the hospital-reported data with the news reports and show that the hospital-reported attacks do not have an omission problem in 2017-2022 compared with the Hackmaggedon data report. Neprash, McGlave, Cross, Virnig, Puskarich, Huling, Rozenshtein and Nikpay (2022) raise concerns about delayed reporting of ransomware attacks. It's important to note that my analysis focuses on a quarter as the observation unit, allowing for some reporting delay. At the same time, to better verify the pre-signing Signaling Channel, I incorporate Google Trends data. Google Trends score for the merging target hospitals identifies the changes in the attention online around the merging time.

I begin by documenting that data breaches happen more during the two-year window. Aggregated comparison for this longer time window is later accompanied by event study that shows the comparison on each quarter. By examining the entire period, I demonstrate that data breaches occur twice as often during mergers. On average, the probability of a data breach for pre-merger deals is approximately 3%, while for the mergers that are going on right now, the data breach rate reaches 6%. The increase in the mean occurs in the target hospitals for mergers, as well as among the buyers and sellers. The result verifies the hypothesis that a higher data breach probability during mergers, thereby making ISI more challenging. Insider misconduct happens more during the chaotic state of management, but more hacks are the main reason for the increase. Specifically, for the pre-merger group, the probability of hacks is 0.52% for the mergers during the two-year window, and for the treated group during the merger, the probability increases 5 times to 2.6%, similar to the observed probability in insider misconduct.

To understand the reasons for the increased data breaches during mergers, I first run a simple linear regression to see how different hospital characteristics correlate with the probability of a data breach. These factors include the publicly traded status of the targets and the acquirers, whether the acquirer is a multi-hospital system (MHS), a professional investor (Private Equity or Real Estate Investment Trust), whether the buyer CEO is female or has an MBA, Ph.D. or MD title, whether the target hospital is a struggling target (have negative EBITDA the year before the merger deal is signed or have filed for bankruptcy) and the target hospitals' bed count, revenue and EBITDA. Simple linear regression is also performed separately on the pre- and post-signing periods. The result indicates that multi-hospital systems escalate data breaches in the post-signing period compared to the pre-signing period. Furthermore, publicly traded companies decrease data breaches, but with a much smaller negative effect in the pre-signing period during the intensified attention time. To sum up, different factors representing different organizational capital levels impact security, and stratification

Table 1: WHY DO SOME HOSPITALS EXPERIENCE DATA BREACHES

Inside the Organization	
Organizational Capital (OC)	Insider Misconduct
Buyers' acquisition experience Hospitals' risk management capability The proactive stance of professional investors, like Private Equity, against data breaches Larger deals come with a larger scale of resources to address security risks	Inefficiency yields both honest mistakes and more malicious insider misconduct Insider misconduct is easier to address since the hackers are not involved Reduced number in insider misconduct reflect hospitals' control effort
Hacks	
Incompatibility Channel (IC)	Pre-signing Signaling Channel (SC)
Vulnerability rises due to incompatibility during Information System Integration (ISI) Incompatibility emerges as a substantive concern for multi-hospital systems despite the economies of scale	Increased information exposure or heightened attention attracts more attacks Facing the same heightened attention, the hospitals can still have different security results Hackers find the buyers more attractive during mergers as the buyer's financial resources concentrate The increased attention has a different effect during different merger stages

Notes: The table lists the potential factors that can explain the heterogeneous increase in data breaches during mergers.

based on hospital characteristics is necessary for understanding the mechanisms. More importantly, some factors have different effects during the two periods, and such diverged results suggest that the pre-signing and post-signing periods have different challenges and need separate investigations. A separate investigation of the pre-signing period is a chance to discuss the economic risk factors without the ISI technical challenges.

For the pre-signing period, labeled as Pre-Signing Signaling Channel in Figure 1, the public becomes aware of the potential merger, attracting online attention to the merging hospitals. As listed in Table 1, this heightened visibility also draws hackers. At the same time, publicity on hospital IT is a new way for hospitals to maintain media reputation (Salge, Antons, Barrett, Kohli, Oborn and Polykarpou, 2022). The Pre-signing Signaling Channel accounts for a 1.98 percentage point increase in hacks during consolidations. In detail, before the deal is signed, the probability of hacks for a pre-merger group is 0.14%, and it increases ten times for the merging deals to 1.41%. 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). Incorporating Google Trends data shows that mergers with intensified online attention one year before the signing date exhibit a higher increase in data breaches right before they sign the deal compared to those without such heightened attention. These results indicate that the Signaling Channel is the driving mechanism for the pre-signing increase in breaches. These results have a significant theoretical contribution by suggesting how evolving social and economic motivations and environmental changes for hospitals and hackers are as important as the technical challenges. Such conclusions align with previous discussions in the literature on the human reasons for hacks (Arce, 2018; Geer, Jardine and Leverett, 2020).

However, I do not find the same effect of attention in the post-signing period. The post-signing

period is important since integrating information systems (ISI) is crucial in reducing costs and generating revenue synergies during mergers and acquisitions (Henningsson, Yetton and Wynne, 2018). However, ISI also introduces vulnerabilities that hackers can exploit (Moore, 2010), especially when a multi-hospital system purchases a target hospital that uses a different Electronic Medical Record (EMR) vendor. Even with the same vendor, various layers of configurations need to be adjusted to merge two information systems. Management and organizational charts are also rearranged. These configuration and management changes can only happen during the operational merging stage after signing the deal. As listed in Table 1, multi-hospital system buyers intend to standardize the IT (Du and Tanriverdi, 2022) and presumably face more challenges with different EMR vendors from the hospital they are purchasing, encounter more severe incompatibility issues (Gaynor, Sacarny, Sadun, Syverson and Venkatesh, 2021). To investigate the vulnerabilities during the ISI, I identify the post-signing breaches as the Incompatibility Channel in Figure 1. The result shows that hacks owing to incompatibility increased by 1.62 percentage points in the year after the deal closes. In detail, after the deal is signed, the probability of hacks for the pre-merger group is 0.38%, increasing 3 times to 1.19%. I also document that multi-hospital system buyers who control more than 40 hospitals or have more than 3 merging experiences during the observational window do not reap the benefits of their scale of resources or experience. Instead, they experience higher increases in data breaches than other multi-hospital system buyers. This result has important theoretical implications by showing evidence for a non-linear economies of scale of security resources. Over time, hacker-hospital interaction changes as well, so I conduct a dynamic event study for mergers by individual years during 2012-2019. From the graphic analysis, the impact of the Incompatibility Channel has become less persistent in recent years. This result has important management implications. As the incompatibility causes problems right after the merger signing date, there is a greater likelihood that these attacks catch the hospitals off guard in the early stages of ISI, even before they have a chance to consider business-IS alignment (Mehta and Hirschheim, 2007).

It is crucial to investigate ransomware attacks separately due to their disruptive impact on hospital operations and potentially life-threatening consequences. More importantly, my results suggest that ransomware attacks on hospitals are primarily an economic issue, where motivations and behaviors play a dominant role. During mergers, ransomware attacks increase significantly through both the pre-signing Signaling Channel and the post-signing Incompatibility Channel, with an even higher occurrence observed through the pre-signing Signaling Channel. This finding indicates that the merger process can significantly jeopardize patients' well-being because of their IT systems. In particular, ransomware increases by 1.34 percentage points during mergers, and such an increase contributes significantly to the total data breach increases during mergers. In line with these findings, the truncated regression analysis over the past 5 years indicates that ransomware attacks during mergers are notably more severe, particularly the pre-signing ransomware attacks. In particular, in the past 5 years, ransomware attacks account for more than half of the total attacks on hospitals and increase 6.25 percentage points during mergers, and 5.29 percentage points increase is from the pre-signing period.

Facing these challenges, the buyers' risk management knowledge and experience can alter the

cybersecurity results. Larger deals usually come with a larger scale of resources for cybersecurity. These are the Organizational Capital Channel (OC) that influences the whole merging process in Figure 1. By stratification, I evaluate the contribution of organizational capital. These results suggest the theoretical importance of cybersecurity motivation and efforts from the defenders' side and the possibility of measuring the contribution of organizational capital to the impact and payoff of Health IT. Practically, these results also show that publicly traded companies and professional investors are where best practices can be learned to navigate the risks. Publicly traded and professional-investor-controlled hospitals possess a comparative advantage in organizational capital, possibly leading to better cybersecurity results and business success. Future studies should evaluate how specific organizational capital contributes to a smooth organizational and digital transformation process. The commercialization process of US health providers and increased professional investors' involvement has attracted significant attention (Gao, Sevilir and Kim, 2021; Scheffler, Alexander and Godwin, 2021; Richards and Whaley, 2023). By investigating the cybersecurity consequences of publicly traded and professional-investor-controlled hospital mergers, I contribute to the evaluation of their increasing participation in healthcare.

This paper contributes to several strands of related literature, summarized in the next section. 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 more data breaches in some hospitals rather than others. The rise in data breaches during these mergers can be traced not only to technical challenges but mainly to the evolving social environment and economic incentives impacting hackers and hospitals. Second, by comparing the results for different levels of organizational capital during the particular transformation period of a merger, I verify the importance and prove the measurement possibility of the organizational capital's impact from the cybersecurity perspective. The unique economies of scale for the organizational capital is not a simple linear positive contribution to mitigating cybersecurity threats when considering the changing scale of risk. Third, by recording how hackers' actions shift during the merger process, I shed light on the preferences and attack duration of malicious actors in response to changes in the healthcare market structure. By showing the contrast between the progress of insider misconduct and the progress of hacks, I highlight that the difference between the economics of cybersecurity and the economics of privacy is mainly from the hackers' perspective. In recent years, increased costs of data breaches, as listed in Table 2, increase the willingness to pay for ransomware attacks and motivate the hackers to exploit such surplus. Lastly, I contribute to the discussion of privacy protection and competition, especially recent literature on the effect of Private Equity (PE) on healthcare. The results have important managerial implications. The results are also well-timed both for the active debate of data breach disclosure policy at the federal/state levels and worldwide and for the antitrust regulation reforms that consider new evaluations for data-driven mergers.

Managerial and Policy Suggestions

Given the high cost of data breaches, hospital managers, cybersecurity experts, and health, defense, and finance authorities must work together to enhance hospital cybersecurity measures during mergers. These findings give clear directions for different market participants to act. For best practice, publicly traded hospitals and professional investors have a comparative advantage in managing cybersecurity during mergers. Hospital managers should consider adopting the risk management processes commonly employed by professional investors and publicly traded hospitals. This integration of risk management practices can improve overall organizational capital for protecting the hospitals. Early and tailored ISI plans are also essential to merging healthcare institutions successfully. Prioritizing cybersecurity investments during mergers is a cost-effective way to reduce overall cybersecurity risks. Preparing for a potential data breach during mergers can be crucial to achieving merger synergies. Hospitals should develop and practice an incident response plan to mitigate the damage and minimize downtime in case of an attack. For policymakers, requiring a written plan of digital integration strategy for proposed hospital mergers is one way to guide hospitals in incorporating the risks during mergers. The results also suggest directions for better cybersecurity risk prediction models. This paper shows that the social and economic environment and other institutional characteristics, beyond the security attitude and current security measures, can influence cybersecurity results. Adding public attention and evaluation of the organizational capital to the existing risk assessment model is a direction for cybersecurity insurance and vendors to predict cybersecurity risk better and help their clients facing increasing threats from hackers. Authorities must focus on addressing specific technical challenges, particularly the increasing prevalence of ransomware attacks on our critical infrastructures and the unique technical difficulties large multi-hospital systems face. This paper shows why Health Industry Cybersecurity Practices (HICP) guidance and the new HIPPA cybersecurity guidance must differ based on organization size, IT capability, and system complexity. I also offer empirical evidence for more angles to tailor best practice guidelines for specific types of hospitals and their vendors. As cybersecurity technologies are still developing, allowing some hospitals to gain market advantage through their cybersecurity investment encourages innovation. More importantly, incorporating the Economics of Cybersecurity and considering the unintended effect on hackers' behavior is vital for future policy makings.

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 the "data-based technological process" exists (Acquisti, Taylor and Wagman, 2016). Information technology adoption improves revenue management (Qi and Han, 2020) and 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,

Table 2: CONSEQUENCES OF DATA BREACH IN HOSPITALS

Consequence	Example
Direct Costs	Payment to ransomware attackers, loss of patient records
Cyber-Insurance Impact	Increased cyber-insurance premium rates
Business Disruption	Decreased revenue, patient loss due to reputation damage, as seen in Neprash, McGlave, Cross, Virnig, Puskarich, Huling, Rozenshtein and Nikpay (2022)
Stock Market Impact	Decreased stock price due to loss of investor confidence as seen in Campbell, Gordon, Loeb and Zhou (2003); Cavusoglu, Mishra and Raghunathan (2004); Chatterjee and Sokol (2019)
Financial Market Impact	Effects on bond market, as seen in Blascak and Toh (2022a)
Privacy Breach	Compromised patient data and confidentiality, as seen in Miller and Tucker (2014)
Cybersecurity Remediation	Costs for recovering and strengthening security measures
Medicare and Commercial Health Insurance	Downgraded rating metrics by insurers
Litigation	Class action settlements and fines
Emotional Reaction	Anxiety, Anger, and Sadness as in Bachura, Valecha, Chen and Rao (2022); Shandler and Gomez (2022)
Market Share	Changes in demand and consumer confidence as seen in Kwon and Johnson (2015a)
Loss of Life	Possible adverse impact on patients' well-being, as seen in Choi and Johnson (2019)

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, 2011a, 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 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). Karahanna et al. (2019) quantify the organizational capital in hospitals and they include institutional-arrangement-based social capital that results in knowledge sharing through parent organization membership and cultural capital that reflects HIT knowledge stock and show that the institutional-arrangement-based social capital that results in knowledge sharing and cultural capital can complement the hospital IT expertise. Dobrzykowski and Tarafdar (2015) shows how social ties among physicians can enhance the benefit of using health IT. Dranove, Forman, Goldfarb and Greenstein (2014) shows IT-intensive locations can reduce the Electronic Medical Record (EMR) adoption cost. To further understand how these organizational capitals play a role during the ISI process, 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 M&A and sheds light on how different levels of organizational capital can impact cybersecurity outcomes in merger deals.

2.3 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 (Nikkhah and Grover, 2022; Gordon, Loeb and Sohail, 2010; 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, 2022b), 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. The impact of security investments on healthcare data breaches yields conflicting outcomes, as demonstrated in prior research (Angst, Block, Arcy and Kelley, 2017; Kwon and Johnson, 2014). However, the objective of this study is to examine the influence of a hospital's security efforts, considering both the temporal dynamics and a narrower time frame that centers on different stages of the merger process.

2.4 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. 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 multi-hospital 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.

2.5 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, 2023; 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. This analysis presents a unique opportunity to examine the cybersecurity experiences of target hospitals internally.

3 Setting, Data and Descriptive Evidence

This section briefly describes the data and introduces the statistics of the control variables. This section also discusses the quality of data. Appendix Section A and B provide more details. Before proceeding to the data source and descriptive evidence, I introduce the consequences of hospital data breaches.

3.1 Data Breach Consequences

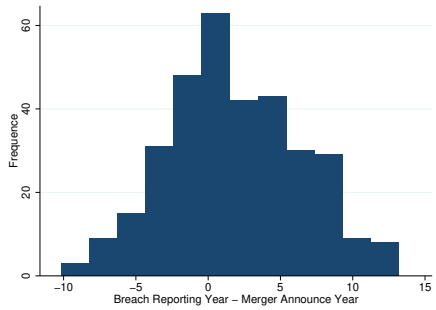
Data breaches carry significant implications. As shown in Table 2, direct costs incurred from paying ransomware attackers exemplify the financial burden. The costs also extend to cyber-insurance, causing escalated premium rates, and business disruption leads to reduced revenue and patient attrition due to reputational harm. Moreover, the stock market responds negatively with a drop in stock prices driven by eroded investor confidence. The breach's impact on privacy is profound, jeopardizing the confidentiality of the patient's medical records. Substantial costs are further incurred for cybersecurity remediation efforts to recover and strengthen defenses. The repercussions extend to the healthcare sector, adversely influencing Medicare and commercial health insurance rating metrics. Legal consequences manifest as class action settlements and fines, underscoring the significance of litigation. Tragically, these breaches could potentially result in loss of life due to their adverse impact on a patient's well-being. Compared with clinics and other healthcare delivery organizations, hospitals are most likely to have operation disruptions during ransomware attacks (Neprash, McGlave, Cross, Virnig, Puskarich, Huling, Rozenshtein and Nikpay, 2022). Choi and Johnson (2019) show that a

data breach at a non-federal acute-care inpatient hospital resulted in an estimated additional 34 to 45 deaths per 1000 acute myocardial infarction (AMI) discharges per year. 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. The disruption goes beyond the hacked hospital. In a cohort study conducted on nearby Emergency Departments (ED) (Dameff, Tully, Chan, Castillo, Savage, Maysent, Hemmen, Clay and Longhurst, 2023), a ransomware attack lasting a month at a hospital leads to a rise in ED visits and a decrease in ED service quality. Note that in Table 20, I also show that data breaches are correlated with mortality rate using Centers for Medicare & Medicaid Services Hospital Compares for 2016-2022.

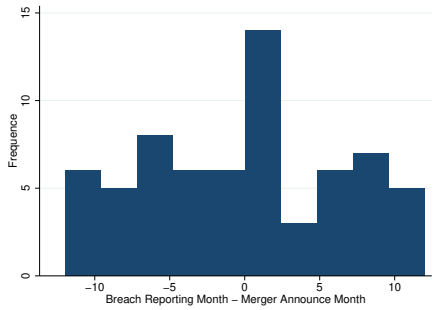
3.2 Data Source

To answer the question of whether mergers cause more data breaches or not, I combine two data sets at the quarterly level for the main analysis, and I incorporate two additional data for robustness check and mechanism analysis. The first data set is the merger deals closed in 2009-2022 from the proprietary merger data platform. 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 2010-2022 (DHHS)). 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. Hajizada and Moore (2023) on underreported data breaches analyze the 2017-2022 Hackmaggedon and the SEC 10-K filings and showed a substantial gap between the two, but in comparison, there is no gap where the Hackmaggedon data report more than the HHS data reported by hospitals. They also show that there is no gap when it comes to ransomware attacks. Neprash, McGlave, Cross, Virnig, Puskarich, Huling, Rozenshtein and Nikpay (2022) shows that for the 82 hospital ransomware attacks and 461 ransomware attacks on other types of health service providers, there is an increase in delay in reporting ransomware attacks during the pandemic. Such delay does not impact my main result since my observational unit is a quarter. I look at a two-year time window that leaves space for the delay in reporting, and the recent two years are too late to be treated to have any control group in my research. 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. More discussion with descriptive evidence on data breaches and mergers are in Section A and B in Appendix.

To find out which hospitals or multi-hospital 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



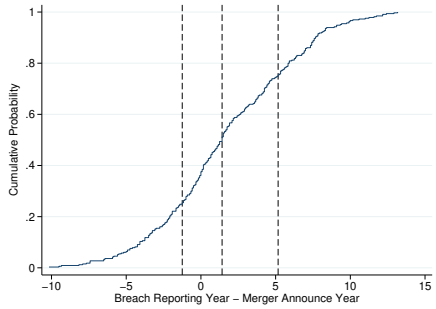
(a) Breach Reporting Year - Merger Closing Year (matched)



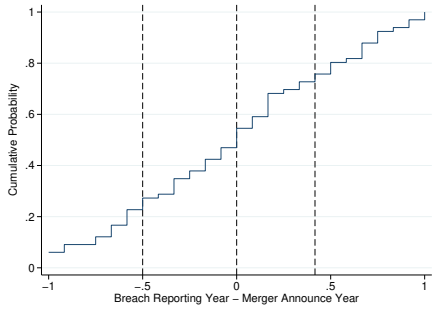
(b) Whithin 1 year: Breach Reporting Month - Merger Closing Month (matched)

Figure 2: 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.



(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 3: 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.

entity in the data breach database. 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 3a. 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 3b. Note that both graphs are stewed distribution towards the post-merger period.

Two additional data sources are used for mechanism analysis and robustness check.

The first data is Google Trends data. I incorporated the daily Google Trends scores for the year before the merger deal is signed and the year after the merger deal is signed for the target hospitals to evaluate the information and online attention change. I identify the dynamic attention changes on the merger with the highest monthly mean Google Trends score for stratification. For the mergers with the highest monthly mean Google Trends score at different stages of mergers, I analyze the security outcome in Section 10.

The second data is the Centers for Medicare & Medicaid Services (CMS) Hospital Compares data for 2016-2022. The advantage of incorporating the CMS data is that it provides quarterly-level hospital information that allows additional control for never-treated patients. An important advantage of this Robustness Check is that it allows the inclusion of a different group of binary control variables that represent the comparative level of image availability, patient experience, timeliness, safetiness, effectiveness, mortality, and readmission rate relative to the national average. Another advantage is that including never-treated allows the analysis to extend beyond the year 2020 when the mergers are too recent to find any pre-treated group. Including the never-treated, which are the hospitals that never merge during the observational period, checks the robustness with different control group construction.

4 Empirical Strategy

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 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.

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 advantage of using pre-treated groups, which are the hospitals eventually will engage in a merger, partially addressing the endogeneity problem. For comparison, I also construct an alternative data set that includes never-treated and show that the result is robust to changes in the control group construction in Appendix Section F using CMS Hospital Compares. This alternative method with never-treated also shows the effect of mergers that happened in 2021 and 2022, as these are the years that are too recent to have a non-contaminated control/pre-merger group and are not included in the main analysis.

The period is a two-year window for each deal, including the year before and the year after the treated group's merger signing date, and it 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 8 underpin the sufficiency of the two-year window. The effects of the timing of the mergers are estimated in the following equation:

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

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 τ 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 listing status of the acquirers and targets infers the impact of the deal. Additionally, I include the hospital and time fixed effects. The coefficients of interest are the β_{τ}s. β_{τ} is the difference between cyber attacks on treated and pre-treated hospitals in merger deals τ quarters after the deal. The standard errors are clustered at the deal level. Further discussion on difference-in-difference assumption and robustness check is in Section D and E. Robustness check on the regression without the individual-level fixed effect is in section J.

Table 3: 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

Notes: 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 one 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 and time 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.

5 Impacts of Mergers

Table 3 shows my initial results when I examine whether mergers cause more data breaches in the two-year window [one year before, one year after merger closure] from 2010 to 2022, with various control combinations. I examine the total effect in my main model, which includes all types of breaches in both the pre and post-merger periods. In each column, the specification includes various combinations of control variables, controlling for/not controlling for the sample size. All specifications include hospital and quarter fixed effects.

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 process, and it is statistically significant at the 5% level.

With different combinations of control variables, the effects across the columns are reasonably consistent, ranging from 3.61 to 4.24 percentage points. 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). The effects across columns with constant sample sizes (columns 2, 4, 6, and 7) are constant. On average, hospitals encounter twice as many data breaches during the merger closure period.

Despite their substantial effects, the control variables' point estimate uncertainty is also noteworthy. The target hospitals' size and profitability have unclear effects. For columns 2, 4, 6, and 7 with the same sample sizes, the target hospital's pre-merger EBITDA is negatively correlated with data breach probability, while the target hospital's pre-merger revenue is positively correlated with data breach probability. At the same time, the target hospital's bed count has unclear effects. This unclear effect is interesting because it relates to multiple factors that determine data breach probability, such as financial profitability for an attack, available information online that determines whether the merger deals are noticeable to the hackers, and the scale of resources for security investment from the defenders – hospitals.

The public trading status also has diverged effects. For columns 2, 4, 6, and 7 with the same sample sizes, public acquirers have more data breaches, while public target hospitals face an uncertain effect. This lack of precise estimates for the public trading status may reflect the fact that it is possible that publicly traded companies may have more information disclosure online, making them more visible, while their more intense regulatory environment benefits their organizational capitals.

The results in Table 3 fulfill the purpose of showing whether mergers cause more data breaches using the main model. Event study plots in later sections and robustness checks using different time windows or different ways to construct the control groups in the Appendixes also support the results. The question is why mergers cause more data breaches, whether the effect changed over my very long observational window, and how different hospitals cop with this risk. In the next section, I first run a correlation analysis for all the factors and show how they correlate with total data breaches, as well as pre and post-merger breaches separately.

6 Organizational Capital and Pre- vs. Post-merger Contrast

Simple linear regression is conducted on all breaches, pre-signing breaches, and post-signing breaches to perform the initial analysis of the underlying reasons for increased data breaches during mergers presented in Table 1. Such analysis guides the identification of the mechanisms for how mergers cause more data breaches differently in different kinds of mergers.

In Table 4, first, publicly traded companies involve complexities due to variations in the pre-signing Signaling Channel (SC) and the Organizational Capital Channel (OC). These companies attract more attention and have greater financial information available publicly online, indicating a positive SC effect. Conversely, their ability to manage short-term shocks might be enhanced due to the pressure exerted by short-sighted analysts, leading to a negative OC effect. The predominance of the negative effect in the first two columns in Table 4 suggests that the second assumption holds more weight. Notably, there is a substantial disparity between the results in the pre-signing (columns 3-4) and post-signing breaches (columns 5-6) in Table 4. During the pre-signing period, the magnitude of the reduction effect from the public acquirers' OC is significantly smaller compared to the post-signing period. Second, when considering system buyers and investor buyers, the multi-hospital system buyer scenario introduces additional complexities related to the Organizational Capital Channel (OC) and the Incompatibility Channel (IC). The notable divergence between the pre and post-signing breaches provides support for the IC channel. Third, investor buyers typically do not encounter IC issues. Last, the size and profitability of target hospitals are relevant factors to consider. These aspects are associated with their attractiveness to hackers (SC) and their organizational capital levels (OC). These factors, especially those involving multiple mechanisms, are analyzed separately in the next section, Section 7.

Table 4: WHAT CAUSE DATA BREACHES: CORRELATION RESULTS

Channels		Overall Data Breaches		Pre-signing Data Breaches		Post-signing Data Breaches	
SC/OC	Public Target	-0.0782**	-0.0655**	-0.0574**	-0.0432*	-0.0209	-0.0222
		(0.0394)	(0.0328)	(0.0288)	(0.0229)	(0.0323)	(0.0272)
	Public Acquirer	-0.2303***	-0.2359***	0.0908***	-0.0927***	-0.1395***	-0.1432***
		(0.0483)	(0.0365)	(0.0352)	(0.0255)	(0.0395)	(0.0303)
IC/OC	System Buyer	0.0727**	0.0664***	-0.0045	-0.0010	0.0773***	0.0674***
		(0.0296)	(0.0246)	(0.0216)	(0.0172)	(0.0242)	(0.0204)
OC	Investor Buyer	-0.1397*	-0.1194**	-0.0579	-0.0597	-0.0818	-0.0597
		(0.0728)	(0.0547)	(0.0531)	(0.0382)	(0.0596)	(0.0454)
	Female CEO	-0.0329	-0.0092	-0.0165	0.0053	-0.0165	-0.0145
		(0.0490)	(0.0431)	(0.0357)	(0.0302)	(0.0401)	(0.0358)
	CEO with Title	0.0008	-0.0054	-0.0048	0.0006	0.0057	-0.0060
		(0.0472)	(0.0416)	(0.0344)	(0.0291)	(0.0386)	(0.0346)
OC/SC	Target Hospital's Bed Count	-0.7299**	0.4401***	-0.5755**	0.3800***	-0.1544	0.0600
		(0.3109)	(0.1552)	(0.2266)	(0.1085)	(0.2544)	(0.1288)
	Target Hospital's EBITDA	0.5348*		0.9588***		-0.4241*	
		(0.3120)		(0.2274)		(0.2552)	
	Target Hospital's Revenue	1.0135***		0.3149		0.6986**	
		(0.3802)		(0.2771)		(0.3110)	
	Struggling Target Hospitals	-0.0539	-0.0614**	-0.0077	-0.0249	-0.0462	-0.0365
		(0.0343)	(0.0293)	(0.0250)	(0.0205)	(0.0281)	(0.0243)
N		903	1228	903	1228	903	1228
R^2		0.0822	0.0646	0.0573	0.0263	0.0454	0.0390

Notes: The table displays the correlation between several factors and all data breaches, pre-signing breaches, and post-signing breaches based on the results of simple linear regression. The binary dependent variable indicates whether a data breach has been reported by the engaging buyer, seller, or target hospital at any time. Standard errors are presented in parentheses. The factors are categorized into groups. The publicly traded status influences the information accessible to hackers and represents the level of organizational capital. Other factors that represent different levels of organizational capital include whether the buyer is a multi-hospital system, a professional investor (PE, REITs), and the gender and title of the CEO. Furthermore, there are factors that signal information and impact the attractiveness of the target hospitals, such as the target hospital's bed count, EBITDA, and revenue. This table shows the divergence impact of several factors on the pre and post-signing breaches. Data source: Proprietary merger data and DHHS 2010-2022.

7 Evidence on Channels of the Mergers' Effect on Data Breaches

I conduct separate analyses in four stages to understand the channels that augment data breaches. First, I isolate the impact on hacks from insider misconduct as outlined in Section A.2. Concerning hacks, I examine the pre-signing Signaling Channel and the post-signing Incompatibility Channel separately. All the non-hacking insider misconduct breachs are analyzed in Section G in the Appendix. Sections 8 and 9 provide further empirical analysis and theoretical explanation for the dynamic changes of hacks and non-hacking insider misconduct in recent years. Second, I analyze a specific type of hacks, the ransomware attack, and show that, on average, ransomware attacks happen even more often through the pre-signing Signaling Channel. Third, I compare the regression outcomes on varying levels of organizational capital to show that different types of mergers with various levels of organizational capital have different cybersecurity consequences. Fourth, in examining multi-hospital health system acquisitions, I specifically analyze larger and more experienced systems, demonstrating that substantial organizational capital doesn't solve compatibility issues and asserts the risks faced by these health systems. The findings suggest that various elements in the categories of information, technology, and organizational capital, influencing both the hackers and the hospitals, play a significant role in the cybersecurity results during mergers. Specifically for information element and its interaction with organizational capital, Section 10 provides more evidence with alternative identification incorporating Google Trends data.

7.1 Hacks: Pre-signing and Post-signing Channels

In this section, I remove all the insider misconduct and investigate hacks in the two years surrounding the merger deal closure date separately. A hospital merger is an event that can change the behavior of hackers. On one hand, mergers can signal potential increases in financial benefits of a successful hack 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 hacks after the signing date to remove incompatibility-triggered hacks with no false negative problem to identify the Pre-signing Signaling Channel in Section 7.1.2. Results for the Incompatibility Channel are in Section 7.1.3.

7.1.1 Hacks versus Non-Hacking Insider Misconduct

Inefficient IT management can also lead to increased insider misconduct, where employees either unintentionally make errors or deliberately exploit data (Miller and Tucker, 2011b). Such negligence is an important sign of cybersecurity attitude and behavior inside the organization. However, it should

Table 5: EFFECT OF M&A ON HACKS

	(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

Notes: The table shows the effect of M&A on hacks 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 and time 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.

be easier to address than hacking situations since external factors like hackers' efforts and targeting are not involved. In Section G, I show that the probability of insider misconduct for a pre-merger group is 2.7%. During the merger, it increases by around 30% but with significant variation. Thus, the increase in data breaches during mergers is primarily driven by a rise in hacks rather than insider misconduct.

Data breaches during mergers mainly rise due to more hacks. Table 5 isolates the mergers' impact on hacks from other non-hacking insider misconduct and reveals that hacks are reported more frequently during the two-year treatment window, and the result is statistically significant. The average probability of hacks in the treated group is 2.6%, which is comparable to the probability of insider misconduct in the pre-treated group as shown in Table 21. This represents a fivefold increase from the pre-treated group mean of 0.52% to the same level of insider misconduct.

I interpret these findings as evidence that insider misconduct is still common among hospitals, but outside cyber-attacks significantly challenge hospitals' operations during merger periods. KLAS/CENSINET/AHA (2023) shows how hospitals are increasingly devoting more resources to cybersecurity. To evaluate the result of the cybersecurity effort, I estimate stratified event studies on insider misconduct for each year in 2012-2019 in Section 8. The graphic analysis shows how insider misconduct increases significantly during mergers in the early years but has become less of a problem since 2014. These changes through time make an important theoretical contribution. It shows how hospitals have tried to mitigate the risks of data breaches in recent years. It has been challenging to observe the individual companies' security efforts. The reduction in insider misconduct can be one way to measure the effort.

7.1.2 Pre-signing Signaling Channel

This section provides an explanation for the increased pre-signing breaches, the pre-signing Signaling Channel. It is challenging to separately account for all the changes in the hackers' and the hospitals' motivation and behavior listed below with reduced form studies; 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 hacks include competitors hiring hackers or hacktivists opposing the merger deal. Hackers utilize news and information for their attacks, as shown by Moore and Clayton (2009), who demonstrated hackers' use of Google to identify potential targets.

Table 6: EFFECT OF M&A ON HACKS: PRE-SIGNING 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

Notes: The table shows the effect of M&A on pre-signing hacks 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 and time 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 provides the first pass of results of the pre-signing Signaling Channel and verifies the assumption that incompatibility during ISI is not the only way a merger causes more breaches. The pre-signing 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 19 where public visibility does not have a clear outcome. I analyze publicly traded hospitals in Section 7.3.1.

Investigating increased breaches in the pre-signing period is challenging, so further analysis utilizing expanded datasets has been conducted in Section 10. This analysis reveals that heightened online attention significantly impacts cybersecurity with stratification. Section 10 also shows that the increased attention has a different effect during different merger stages.

One alternative explanation for the pre-signing increased breaches is that the increase is not a result of more hacks, 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 hacks 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 to insider misconduct or small-scale misconfigurations (as discussed in Section 7.2). The second result is based on the findings from the past five years, which demonstrate a significant decrease in insider misconduct during the pre-signing window in Section 8. 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 8, reveals neither a sudden surge in data breach reports approaching the merger signing date nor a sudden decrease afterward.

Another alternative explanation for the pre-signing increased breaches is that not the breaches happen more before the merger but the breaches accelerated the merger process. This is an important question for the financial market, and future studies with more information on the multiple third parties' behavior are also needed for this inverse effect. Section 10 addresses this concern with alternative identification of the pre-signing Signaling Channel with Google Trends scores. Section 10 also shows that such information effect is not the main reason for the post-signing increase in breaches.

7.1.3 Post-signing Incompatibility Channel

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

This section shows that post-signing Incompatibility Channel is also an important reason for the increase in data breaches during mergers. When the buyer is a multi-hospital health system, the increase in data breaches during the post-signing period is even higher. It aligns with the information system integration discussed in Gaynor, Sacarny, Sadun, Syverson and Venkatesh (2021) and the ISI literature (Brynjolfsson, Malone, Gurbaxani and Kambil, 1994; Zaheer and Venkatraman, 1994; Tanriverdi, Rai and Venkatraman, 2010; Tanriverdi and Uysal, 2011; Du, 2015; Tanriverdi and Du,

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

Figure 4: 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.

2020; Du and Tanriverdi, 2022).

Table 7: POST-SIGNING CHANGES

Post-Signing Changes	**Examples**
Electronic Medical Record System Harmonization	Gradually migrate data and operation to the same vendor as the buyer.
Harmonization of various other kinds of Healthcare Software	Supply Chain Management, Customer Relationship Management, and Enterprise Resource Planning changes, and many of them talk directly to EMR system.
Communication Systems Network Infrastructure	Email, phone, pager, telemedicine service systems Establish secure VPN access for remote connections. Bandwidth or even hardware adjustments.
Data Management Integration	Moving to Cloud. Moving to different Cloud Services Providers (CSPs). Rearrange or even update hardware for the server infrastructure.

New Protocols and State Laws	Authentication and access methods change. Cybersecurity and privacy control methods change (Encryption rule, patching schedule, stress test, etc.). Compliance requirement changes for interstate M&A.
Digital Transformation	Electronic Medical Devices (smart beds, infusion pumps, and monitoring devices) as an example of Internet of Things (IoT) in healthcare. AI adoption for medical judgement.
Management, Team and Leadership Restructuring and Transformation	Responsibility and evaluation metrics change. Reporting flow and project management change. Culture changes.

Notes: This table summarizes changes in the post-signing stage of hospital mergers that may have an effect on cybersecurity results based on my conversations with practitioners.

What causes the increase in data breaches in the post-signing stage? The first reason is the technical challenges during ISI. Vendors' quality and vendors' market share have impacts on cybersecurity risks (Vasek, Wadleigh and Moore, 2015). In Figure 4, 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 the Healthcare Information and Management Systems Society (HIMSS). Leading EMR 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 multi-hospital 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). In Table 7, such EMR harmonization is listed as the first post-signing change for digitization.

EMR harmonization is not the only incompatibility problem. Table 7 also lists other changes. Other healthcare software also talk to EMR. For example, ERP bookkeeping and revenue management sections talk to EMR for the treatment-claim-payment cycle. Network Infrastructure, such as bandwidth, changes to facilitate more users and VPN access. Different cloud service choices also bring challenges for data management. Cybersecurity protocols and compliance changes can also be challenging. An unbalanced digitization process between the buyers and the target hospitals brings opportunities for digital transformations and revenue boosts but also can introduce vulnerability. Lastly, the organizational structure and management changes impact the employees' actions.

Table 8 presents the Incompatibility Channel results: data breaches due to incompatibility 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 hacks 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 multi-hospital system purchases a hospital, it would let the hospital adopt its own EMR and other software.

Table 8: EFFECT OF M&A ON HACKS: 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

Notes: 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 $[t, t+a]$. 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 and time 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 9: MULTI-HOSPITAL SYSTEM BUYERS: PRE AND POST SIGNING BREACHES

	All	Pre-signing	Post-signing
Treatment Effect	0.0456***	0.0176*	0.0280***
	(0.0164)	(0.0107)	(0.0104)
Target Hospital's Bed Count	0.0915***	0.0911***	0.0004***
	(0.0002)	(0.0002)	(0.0002)
Target Hospital's Revenue	0.0173	-0.0052	0.0225***
	(0.0132)	(0.0086)	(0.0084)
Target Hospital's EBITDA	-0.0035***	-0.0018***	-0.0017***
	(0.0010)	(0.0007)	(0.0006)
N	140763	140763	140763
R^2	0.2529	0.1438	0.1268
Mean on Nontreated % Effect	3.18	1.85	1.33
Mean on Treated % Effect	6.49	3.16	3.33

Notes: The table shows the effect of M&A on data breaches that were reported before and after the deal is signed. The table is on a sample where the buyer is a multi-hospital system. 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 and time 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.

Especially when the vendors (as in the word cloud in Figure 4a and 4b) 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. Even without the EMR difference, incompatibility can still be a problem for other configuration processes that involve various operations and business analytics software and database vendors, as listed in Table 7. Analysis for each technical difficulty is beyond this paper's scope. I leave it for future studies. The magnitudes for the pre-signing Signaling Channel and the post-signing Incompatibility Channel are similar. However, an alternative interpretation of the post-closure effect is that hospitals intentionally delay their data breach reporting when the merger is pending. I use event study to rule out such delay in the next section.

Multi-hospital system buyers, due to their more complicated control structure and harmonization process listed in Table 7, can experience more cybersecurity challenges during mergers. Table 9 displays stratified results focusing on acquisitions where the buyer is a multi-hospital system, revealing that multi-hospital systems encounter a higher increase and observe a greater probability of data breaches during the post-signing period. The underlying theory suggests that system buyers are the ones facing incompatibility issues since they require newly acquired target hospitals to adopt their information system vendors. The results demonstrate that, during the post-signing period, merger deals involving a multi-hospital system as the buyer experience a 2.8 percentage point increase to 3.33%, which is larger than the pre-signing period average. Additionally, both the bed count and the EBITDA significantly

affect data breaches during both the pre-signing and post-signing periods. This indicates that when a multi-hospital system undertakes an acquisition, the cybersecurity strategy needs to be tailored to the size and profitability of the target hospital.

The issue at hand is whether the substantial organizational capital of larger and more experienced multi-hospital health systems makes them more resilient against cyber threats or, conversely, more appealing targets for hackers. As outlined in Section 7.4, evidence indicates that these large health systems, despite their experience and resources, are encountering more severe cybersecurity challenges.

In conclusion, post-signing Incompatibility Channel is an important mechanism for the increase in breaches during mergers. This is supported by the fact that hacks occur more frequently during the post-signing period, and multi-hospital systems, which may encounter challenges in this regard, experience a greater increase in breaches. The competition between the post-signing Incomatibility Channel and Organizational Capital Channel is analyzed in Section 7.4.

7.2 Ransomware Attacks

Ransomware attacks are particularly harmful compared to other types of hacks 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.

Table 10 shows that ransomware attacks occur more frequently both before and after the merger signing date. The categorization of hacks is done with Keyword Searching in text analysis and hand cleaning. 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 pre-signing Signaling Channel.

Ransomware attacks have happened so often in the past 5 years that some 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. Section 8 provides a dynamic analysis of hacks and compares ransomware attacks with other types of hacks.

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

Notes: 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 and time 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.

7.3 Organizational Capital Channel

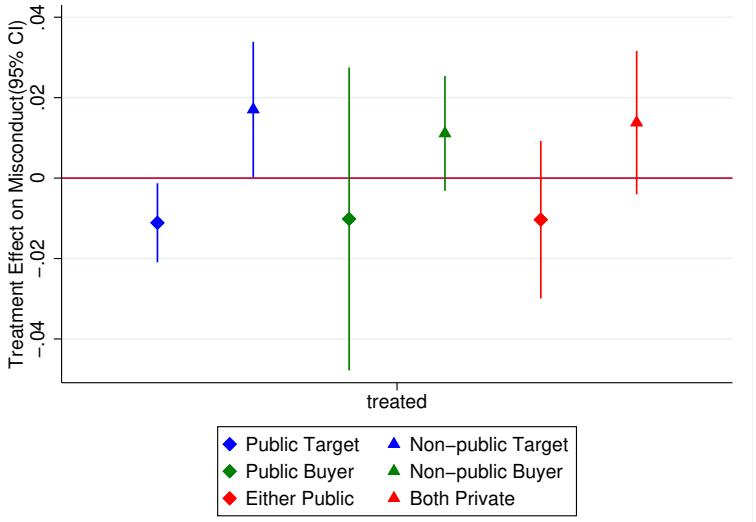
Digital technology involves representing information using bits instead of atoms, resulting in reduced costs for data storage, computation, and transmission (Goldfarb and Tucker, 2019). The cost of computing has continued to decrease in recent years, leading to the emergence of more powerful and swift hackers. While implementing the latest information technology in hospitals offers significant benefits, it's important to recognize that cyberattacks often exploit human errors. As a result, the complementary effect of organizational capital becomes a substantial comparative advantage.

This segment delves into the Organizational Capital Channel, considering the merging hospitals' size, public trading status, and financial and managerial teams. Initial characterization (as detailed in Section 6) indicates that factors like publicly traded status, system buyers, professional investor buyers, and struggling target hospitals can potentially influence data breaches. However, characteristics such as the CEO's gender (see Appendix section H.1.1), educational background (e.g., Ph.D./MD/MBA), and deal size do not exhibit a clear pattern. To further analyze these factors, within this section, the deals are stratified into distinct groups to compare the cybersecurity outcomes between those with the advantage of organizational capital and those without. As emphasized in Section 6, studying the individual channels in isolation only scratches the surface of understanding. Subsequent sections explore intersections from various angles. Publicly traded hospitals appear to experience fewer impacts. Acquiring a publicly traded target hospital significantly reduces insider misconduct during mergers. Similarly, acquiring a struggling target hospital correlates with reduced insider misconduct. However, conclusions are less evident when considering a female CEO or a CEO with specialized educational titles like Ph.D./MD/MBA. Larger or more experienced multi-hospital system buyers show a significant and substantial increase in pre-signing data breaches, possibly due to their increased attractiveness as targets. These results suggest that organizational capital undoubtedly confers a competitive advantage, and different types of deals call for tailored ISI plan to address their unique risk. Factors that touch both Organizational Capital Channel and other channels are further analyzed in the following sections.

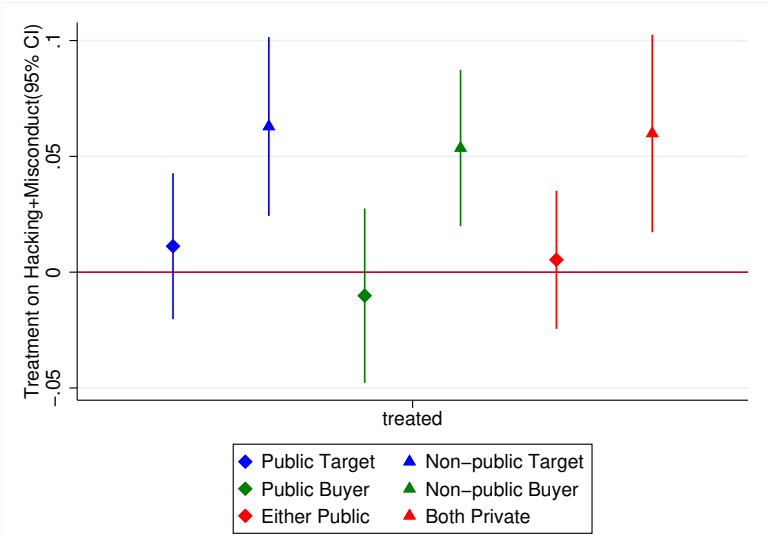
7.3.1 Organizational Capital: Publicly Traded Hospitals

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 5 shows the impact of publicly traded and non-publicly traded mergers on data breaches. Specifically, the first blue line in Figure 5a shows that when the target hospital is publicly traded, there are significantly fewer incidents of insider misconduct during mergers as compared to the pre-treated group. In contrast, deals involving publicly traded buyers (first green line in Figure 5a) do not necessarily manage the risk of insider misconduct better. The comparison becomes more obvious when hacks are also taken into account. Interestingly, such deals exhibit greater efficiency in dealing with hacks, as demonstrated in Figure 5b.



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



(b) Hacks and Insider Misconduct on Public and Non-public Mergers

Figure 5: 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 multi-hospital 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 hospital and time fixed effects. The bars are 95% intervals. Standard errors are clustered at the deal level. The top panel pertains to insider misconduct, 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.

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

	Insider Misconduct		Insider Misconduct and Hacks	
	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

Notes: 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 and time 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.

7.3.2 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 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 insider misconduct. Additionally, merging both struggling and non-struggling targets can lead to more hacks, 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 the operation.

Table 12: LARGE OR EXPERIENCED MULTI-HOSPITAL SYSTEMS

	Large or Experienced			Regular multi-hospital systems		
	All	Pre	Post	All	Pre	Post
Treatment Effect	0.0466**	0.0259*	0.0206	0.0161	0.0108	0.0053
	(0.0227)	(0.0142)	(0.0157)	(0.0121)	(0.0078)	(0.0088)
N	24379	24379	24379	66648	66648	66648
R^2	0.2660	0.1360	0.1703	0.3282	0.1698	0.1901
Mean on Nontreated	4.39	1.62	2.77	2.39	0.99	1.40
Mean on Treated	7.44	3.31	4.13	3.19	1.47	1.72

Notes: The table presents the impact of M&A deals involving large or experienced multi-hospital systems. Experienced multi-hospital systems are the multi-hospital systems that have more than 3 deals in 2009-2022. Large multi-hospital systems are the multi-hospital systems that manage more than 40 hospitals. The number of hospitals each large multi-hospital system manages is according to Becker's 100 of the largest hospitals and multi-hospital systems in America list (updated on Feb. 28th, 2023). The main variable of interest is a binary dummy, $Treated_{i,m}$, which equals one 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, no control variables were included. All the regressions include a full set of hospital and time 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.

7.4 Organizational Capital Channel and Incompatibility Channel: Large or Experienced multi-hospital system Buyers

Table 12 shows how large or experienced multi-hospital systems are the ones with a larger risk of data breaches. Large multi-hospital systems are growing in America as a result of mergers and acquisitions, where hospitals and medical facilities combine to create larger, more integrated systems. These large multi-hospital systems have significant advantages, including greater bargaining power with insurance companies, improved efficiencies in operations, and the ability to offer a wider range of services to patients. However, some critics argue that the growth of large multi-hospital systems could lead to reduced competition, higher prices, and a loss of community-based healthcare services. Figure 6 plots the coefficients for all breaches and shows that on average, the large or experienced multi-hospital systems experience a larger increase in data breaches. It is a surprising result because my original assumption is that they should have both better resources and experiences to manage these risks. The result implies that even though large or experienced multi-hospital systems have more rich resources and experience in managing merger risk, they can not do it better. One possible reason may be because they are more attractive since they are large and they have more information available to the hackers, as there is an increase in the post-signing period, but most increases are in the pre-signing period through the pre-signing Signaling Channel.

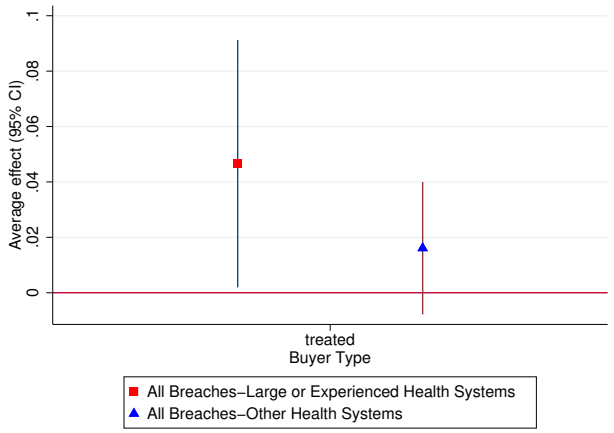
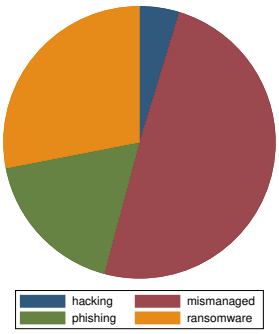


Figure 6: Large or Experienced multi-hospital systems

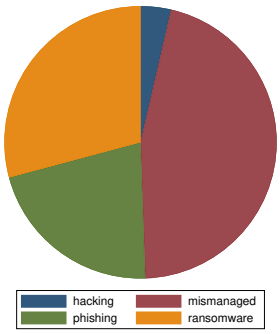
Notes: The figures show the stratified regression coefficients specified in the main model by deals that involve large or experienced multi-hospital systems. Experienced multi-hospital systems are the multi-hospital systems that have more than 3 deals in 2009-2022. Large multi-hospital systems are the multi-hospital systems that manage more than 40 hospitals. The number of hospitals each large multi-hospital systems manage are according to Becker's 100 of the largest hospitals and multi-hospital systems in America list (updated on Feb. 28th, 2023). The bars are 95% intervals. Standard errors are clustered at the deal level. The red square symbol is the mean increase in data breaches among large or experienced multi-hospital systems while the blue triangle represents the one for other regular multi-hospital systems. Data source: Proprietary merger data, Becker's, and DHHS 2010-2022.

8 Dynamic Effects

This section presents stratified analysis from a dynamic perspective. Considering the rather long observational window in the previous analysis, it aims to explore recent trends. Notably, there has been a decrease in insider misconduct instead of an increase during mergers in recent years. By analyzing the truncated data for the past five years, I show that the data breach situation has been even worse since hacks have happened more, especially the increase in ransomware during mergers. The next section examines one potential reason for these changes: professional investors, and shows that the increased involvement of private equities and other professional investors in the health industry does not worsen the cybersecurity results. Documenting the early years becomes crucial as it helps to comprehend the evolution of the hospital's behavior over time. I show the leads and lags with the event study for 2012-2019 separately for insider misconduct and hacks. The results show that the early years (2012-2014, mid to late stage of health digitization in the US) and more recent years (2015-2019, 96% hospitals have certified EHRs in 2015 according to healthit.gov while organized cyberattacks surge) have different cybersecurity risks during mergers. In recent years, misconduct has become less of a problem, and post-signing increases in hacks are more immediate.



(a) 2018-2022: Data Breach Cases



(b) 2018-2022: Individual impacted

Figure 7: 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 hacks. The data breach types are from Keyword Search combined with hand cleaning. Data Source: HHS 2018-2022.

8.1 Recent Development

8.1.1 Growing Challenges in the Last Five Years

This section presents the main regression analysis on the truncated period of 2018-2022 to investigate whether the cybersecurity result is changed considering the significant rise in cybersecurity awareness and efforts during this period. The findings indicate that while the incidence of misconduct-related data breaches has decreased in recent years compared to before, the upsurge in hacks 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. 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 hacks. 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 hacks during the same time window overturns the results.

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

Notes: 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 and time 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), insider misconduct (M), and hacks (H), 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 insider misconduct (M) and hacks (H) separately on different treatment periods.

As shown in Figure 7, the proportion of cases and individuals impacted by different types of data breaches in recent 5 years. Table 14 shows in the last 5 years, hacks, including ransomware attacks and phishing attacks, happen more before the merging signing date than afterward. These findings suggest that the pre-signing Signaling Channel is the primary driver of the increase in organized and targeted attacks by hackers. In contrast, general hacks, 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 hacks are less targeted and have less direct relevance to hospital mergers.

8.1.2 Merger Deal with Professional Investors are Better

The surge in professional investors' role in health and hospital M&A in recent years deserves further analysis to understand the dynamic changes. Tax treaties on hospitals since the Tax Reform Act of 1986 and the financial deregulation, especially the Commodity Futures Modernization Act in 2000 that allows shadow banking are the reasons for the increasing professional investors' participation in hospital business (Grogan, 2023, Chapter 8). and the latest literature debate on the welfare effect of PE but focuses on the relatively longer terms (Bruch, Gondi and Song, 2020; Liu, 2021; Richards and Whaley, 2023; Gao, Sevilir and Kim, 2021). PE leveraged buyouts (LBO) are with high leverage and expect high returns. Healthcare has the highest cost of a data breach (IBM, 2023) that hurts the returns. Previous analysis in this paper also calls for a deeper examination of professional investors' impact. In Table 17, none of the breached hospitals are bought by private equity investors, while the instances of breached mergers involving REITs are markedly fewer. In Table 4, investor buyers (PE or REIT) are correlated with significantly fewer breaches. In Table 13, the probability of post hacks for REIT buyers is lower, while in Table 14, REIT buyers have significantly fewer hacks.

To fulfill this goal, I run the baseline model on deals with a professional investor buyer, PE or REIT. Notably, in this scenario, private equity funding is not a healthcare provider and does not report data breaches, and the acquisition process involves zero EMR merging issues. Additionally, the signaling effects are minimal due to its positioning outside of the regulatory radar. Thus, analyzing the investor-buyer deals is necessary. 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. The analysis reveals a positive effect of the merger on post-signing data breaches and a negative effect on pre-signing data breaches. Appendix Section H.1 verifies the result with bootstrapping.

As discussed in Rundle and Nash (2023), private equity firms are taking action on the cybersecurity risk and IT due diligence of the acquisition targets. My result suggests that their efforts during the pre-signing period are effective. Theoretically, I contribute to the welfare effect of professional investors by analyzing the short-term cybersecurity results for professional M&A. "Short-sighted" investors take effective actions and have better cybersecurity outcomes during mergers.

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

	All Hacks			Ransomware Attacks			Phishing Attacks			General Hacks		
	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

Notes: The table shows the effect of M&A on different types of hacks 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 and time 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 hacks are presented: all hacks, ransomware attacks, phishing attacks, and general hacks, 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 $[0, t+a]$.

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

Notes: 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 one 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 and time fixed effects. Standard errors clustered at the deal level are displayed in parentheses.

8.2 Hospital vs. Hacker Effort: Evolving Effect for 2012-2019

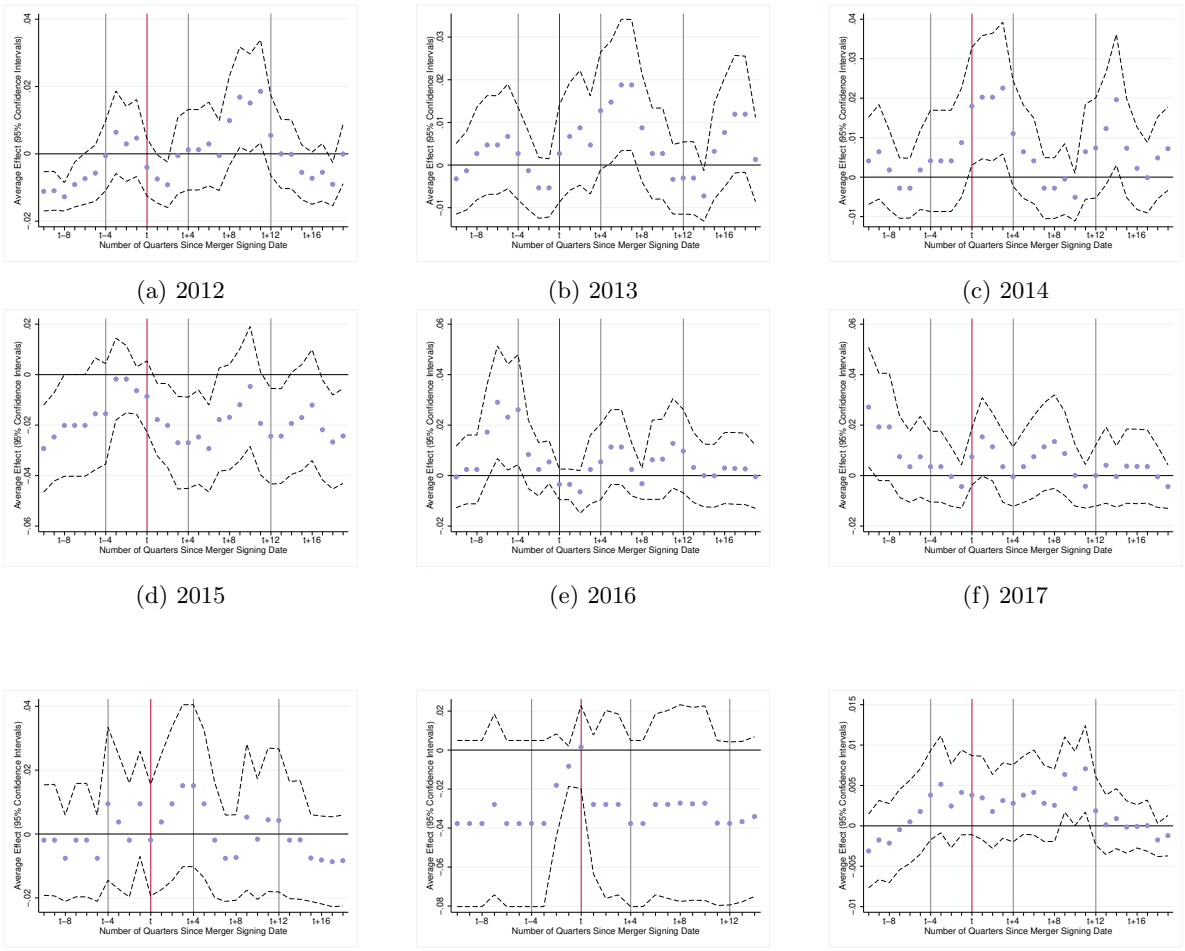
By conducting separate event studies on insider misconduct and hacks between 2012 and 2019, I observe the trajectory of hospitals' security efforts and the evolving nature of their cybersecurity challenges and come to the following three conclusions from the graphic analysis.

First, insider misconduct has become less of a problem over time. In Figure 8, we observe that insider misconduct was an issue during mergers in the early years (2012-2014 in panels a-c), but its effect varied in later years and decreased. This finding aligns with the results discussed in Section 8.1, where insider misconduct decreases instead of increasing before the merger deal was signed.

Second, as I analyze the data breaches over time, I find that the magnitude increases both when considering only hacks. In Figure 9, the highest interval remains at 0.02 for 2012-2019 and 2014-2019, then rises to 0.04 in 2016-2019, and further increases to 0.1 in 2018-2019. Figure 10 shows even more dramatic results for hacks. The highest interval goes from 0.01 to 0.015, then jumps to 0.03, and eventually reaches 0.1. This indicates that security breaches worsen during mergers over time.

Third, hacks during the post-signing period become less persistent. This trend might be due to the decreasing use of malware attacks and the faster integration of information systems. Additionally, Figure 10 highlights an interesting observation approximately two and a half years before the merger deal is signed.

Overall, the event study provides valuable insights into the dynamics of insider misconduct and data security during mergers, indicating a decrease in certain risks in insider misconduct while pointing to emerging challenges of immediate and more severe hacks that deserve attention.



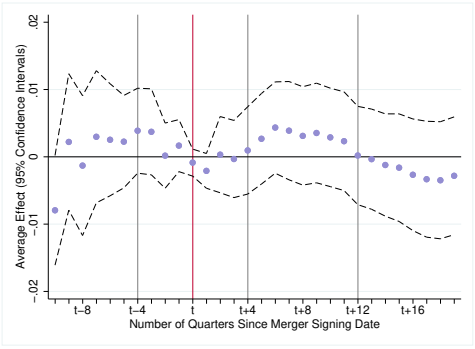
(a) 2012 (b) 2013 (c) 2014

(d) 2015 (e) 2016 (f) 2017

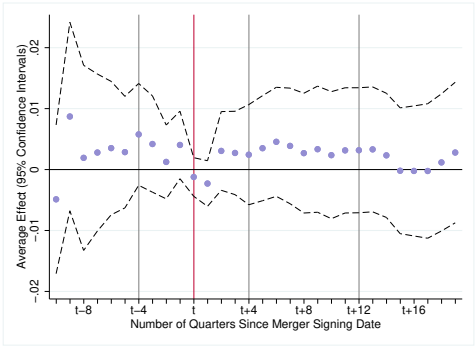
(g) 2018 (h) 2019 (i) 2012-2019

Figure 8: Dynamic Event Study: Insider Misconduct

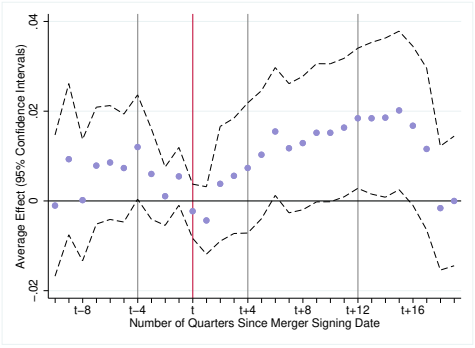
Notes: The figures depict coefficients for the primary regression on insider misconduct with lead and lag indicators up to two and a half years before or five years following a merger that occurred in different time frames. This event uses all future mergers in at least 2.5 years as control. Each regression compares whether the treated group or the pre-treated group reports more data breaches in each current period. Panel A to H represents the time frames 2012-2019 mergers, separately. The last panel includes the whole period. 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 in the main 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 18. The figures show how insider misconduct has decayed as a problem in recent years. Data source: Proprietary merger data and DHHS 2010-2022.



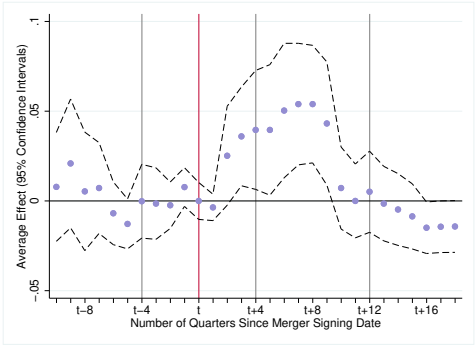
(a) Event Study Over 2012-2019



(b) Event Study Over 2014-2019



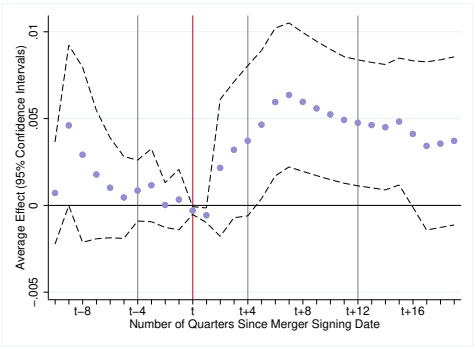
(c) Event Study Over 2016-2019



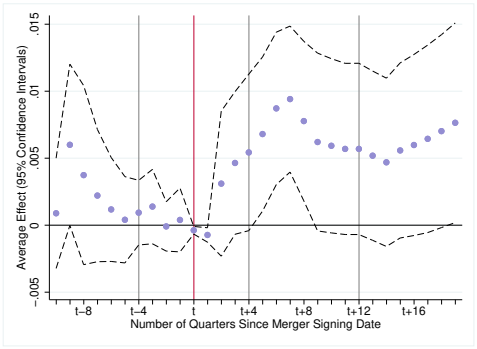
(d) Event Study Over 2018-2019

Figure 9: Dynamic Event Study: Insider Misconduct and Hacks

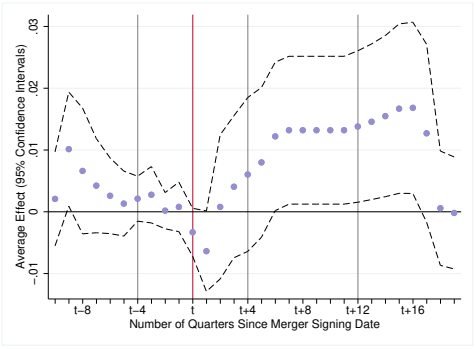
Notes: The figures depict coefficients for the primary regression on all data breaches (insider misconduct and hacks) with lead and lag indicators up to two and a half years before or five years following a merger that occurred in different time frames. This event study uses all future mergers (data breaches reported in each current period) as control. Panel A shows the longest period from 2012 to 2019, while Panel B displays data from 2014 to 2019. Panels C and D represent the time frames 2016 to 2019 and 2018 to 2019, respectively. The reason why the results in Figure 9d and Figure 21 appear slightly different is that Figure 21 employs a more recent set of mergers as controls. Specifically, it includes mergers that are at least two years but less than five years in the future. On the other hand, Figure 9d includes all future mergers in at least two years as control. 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 pre-signing 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 18.



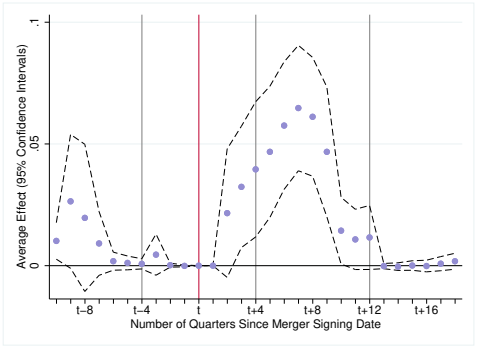
(a) Event Study Over 2012-2019



(b) Event Study Over 2014-2019



(c) Event Study Over 2016-2019



(d) Event Study Over 2018-2019

Figure 10: Dynamic Event Study: Hacks

Notes: The figures depict coefficients for the primary regression on hacks with lead and lag indicators up to two and a half years before or five years following a merger that occurred in different time frames. This event study all future mergers (data breaches reported in each current period) as control. Panel A shows the longest period from 2012 to 2019, while Panel B displays data from 2014 to 2019. Panels C and D represent the time frames 2016 to 2019 and 2018 to 2019, respectively. 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 pre-signing 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 18.

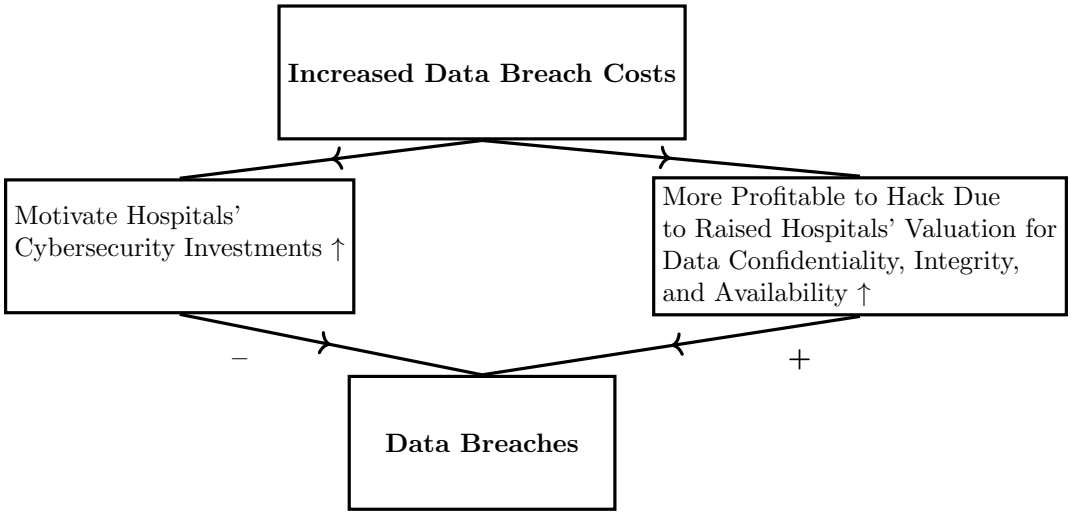


Figure 11: Theoretical Framework for Recent Development

9 Harmful Cost: Theoretical Framework for Recent Trends

This section provides a more in-depth theoretical explanation of the dynamic effects over the years and underscores the significance of including the attacker's perspective in information security analysis. By doing this, the section highlights the theoretical contribution and distinguishes the Economics of Cybersecurity from the Economics of Privacy.

Numerous factors have contributed to the rising costs of data breaches in recent years, as highlighted in IBM (2023). One crucial factor is the increasing bargaining power of patients, particularly through class-action lawsuits, which incentivizes hospitals to prioritize the prevention of data breaches. Additionally, government-imposed fines and penalties for data breaches and heightened privacy protection and risk management metrics enforced by health insurance payers share a similar objective.

To examine what may be the cybersecurity consequence during mergers for the increased cybersecurity cost, Section 8 shows how, gradually, insider misconduct has become less of a reason for increased data breaches while despite such increased efforts, hacks have been worse. The contrast between improved insider misconduct and the severe deterioration of hacks is obvious and curious.

The contrast between the progress of insider misconduct and the progress of hacks highlights the difference between the Economics of Cybersecurity and the Economics of Privacy. When discussing privacy matters, the impact is relatively direct. The expenses associated with increased privacy protection are absorbed by both hospitals and patients, while the increased patients' bargaining power stemming from the judicial and legislative system encourages hospitals to take more proactive measures. This is the Coasian Solution for privacy issues framed in Acquisti, Taylor and Wagman (2016); Goldfarb and Tucker (2019). The Coase theorem - first introduced into economic of privacy literature

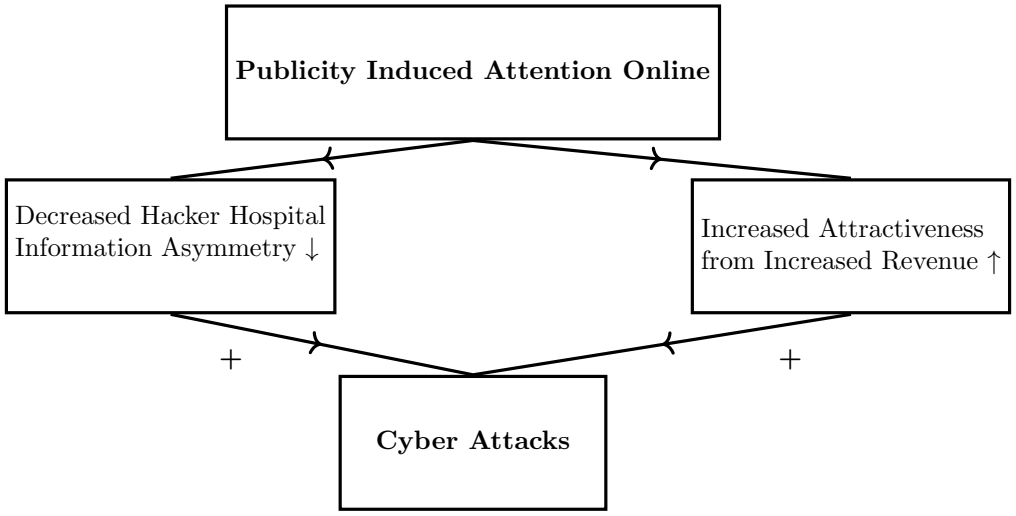


Figure 12: Theoretical Framework for Attention Generated Hacks

in the early 1990s - argues that we can depend upon data owners, in this case the patients, to internalize the costs of privacy protection so as to reach an efficient state where their data will be protected without government intervention (Tucker, 2022).

Nonetheless, the influence of cybersecurity issues follows a less straightforward path. The fundamental disparity between the Economics of Privacy and the Economics of Cybersecurity centers on the involvement of an extra player: hackers. In the case of hackers, the heightened costs associated with data breaches augment hospitals' "willingness to pay" for ransomware attacks. As shown in figure 12, the increased data breach costs stemming from the increase bargaining power of the patients and the increased punishment from the government can lead to an increase in effort from both the defender and the offender. A larger surplus to exploit translates to a greater incentive for hackers to take action, offering a rationale for the varied effects, decreased insider misconduct and increased hacks, discussed in Section 8.

The following section, Section 10 provides further evidence to support this explanation. Specifically, I present the evidence for the Signalling Channel by comparing the merger deals that receive substantial attention and the ones that do not. As shown in Figure 12, increased attention online aids hackers by reducing the information asymmetry about the hacking targets and increase attractiveness. These results provide further insights into the hackers' behavior and align with the latest literature (Li and Chen, 2022; Ebrahimi, Chai, Samtani and Chen, 2022; Samtani, Chai and Chen, 2022).

10 Attentions: Analysis with Google Trends

This section incorporates Google Trends data to answer two questions to provide further information about the pre-signing Signaling Channel: does pre-signing attention online matter, and does the post-signing signaling effect exist? Section 10.1 shows that the target hospitals that receive significant attention one year before the deal is signed experience a higher number of data breaches just before finalizing the deal. Section 10.2 shows that the target hospitals that receive significant attention right after the merger deal is signed do not experience more data breaches in the later post-signing period; such attention is from the data breaches reported in the previous quarter.

10.1 Pre-signing Attention Cause More Breaches

This section investigates the effect of intensified online attention on merger deals, particularly focusing on the merging target hospitals that receive significant attention one year before the deal is signed. The analysis considers the effect of such pre-signing attention both before and after the merger signing date. Additionally, the interaction between the signaling effect and the organization channel, as displayed in Table 4, is examined in Appendix Section I. Notably, merger deals involving publicly traded hospitals or larger deals exhibit different cybersecurity outcomes when they receive substantial online attention, compared to deals without such characteristics.

Pre-signing attention changes pre-signing cybersecurity results. Figure 13 illustrates the immediate effect of online attention. The sample is divided into two groups: the first group includes merger deals with the highest monthly mean Google Trends score for their target hospitals during the third or fourth quarter before the merger deal is signed. The treatment effect during the following two quarters is then displayed for each group. The results indicate that for merger deals that receive intensified pre-signing online attention, the pre-signing cybersecurity outcome in the quarter immediately before the merger deal is signed differs from those without such attention.

Pre-signing attention does not impact the post-signing cybersecurity results. Figure 14 examines whether this difference persists beyond the merger signing date. It demonstrates that merger deals receiving substantial attention one year before the merger deal is signed do not show different post-signing cybersecurity outcomes compared to deals without such attention. This result supports the theory of the Signaling Channel in the pre-signing period and suggests a potential time span between the point when attention intensifies and when an actual cybersecurity incident occurs.

10.2 Post-signing Attention Comes from Pre-signing Breaches

There is no evidence for the post-signing Signaling Channel. It is a question of whether the attention is still on the hospitals after they sign the deal and causes more breaches and whether it means that the Signaling Channel extends beyond the post-signing period. This section analyzes the attention on hospitals right after they sign the deal. Figure 15a looks at the year after the merger deal is signed. The left bar represents those merger deals that attract attention right after they sign the deal. The

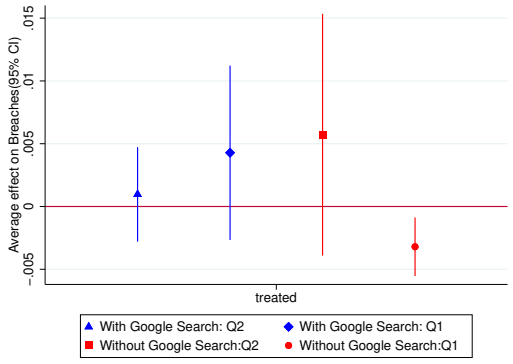


Figure 13: Active Pre-signing Search: Pre-signing Breach

Notes: The figure displays coefficients for the main regression on all data breaches (insider misconduct and hacks) reported in two pre-signing periods of time separately. The first period, Q2, is on the second quarter before the deal is signed. The second period, Q1, is the quarter immediately after, which is on the first quarter before the deal is signed. The blue triangle knob on the far left represents the mean treatment effect on pre-signing breaches with the sample with active pre-signing search. The blue diamond knob on the middle left represents the mean treatment effect on pre-signing breaches in the next quarter with the sample with active pre-signing search. The red square and red circle represent breaches in these two quarters within hospitals without the active pre-signing search. The bars indicate the 95 percent confidence intervals. Control variables include the target hospitals' bed count, the public trading status of the target and the buyers, as well as hospital and time fixed effects. Standard errors are clustered at the deal level. Active pre-signing search is defined as having the highest monthly mean one year before the deal is signed during the period $[t-4, t-3]$, which corresponds to 7-12 months before the merger deal is signed. The graph shows that the first quarter after the merger deal is signed, $t-1$, is when the attention on merging hospitals has a different effect. Date t is when deal m is signed. Data sources: Proprietary merger data, Google Trends, and DHHS 2010-2022.

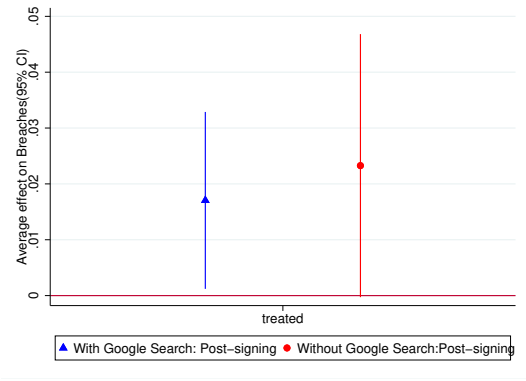
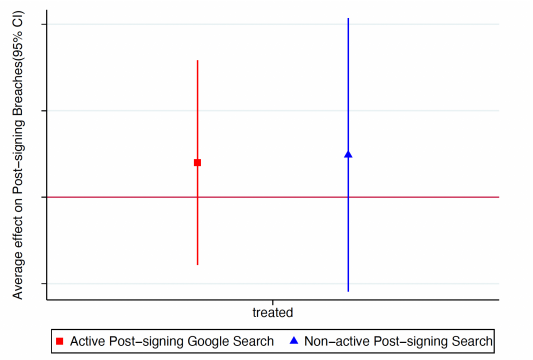


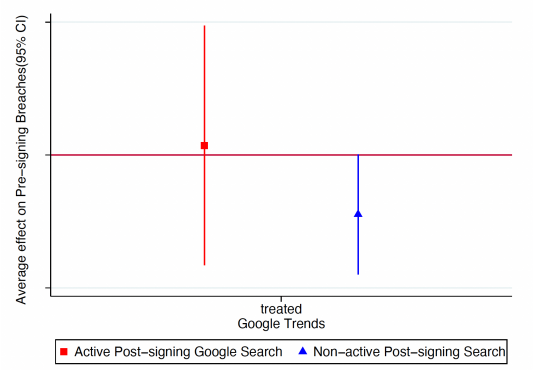
Figure 14: Active Pre-signing Search: Post-signing Breach

Notes: The figure displays coefficients for the main regression on all data breaches (insider misconduct and hacks) reported in the year after the deal is signed. The blue triangle knob represents the mean treatment effect on post-signing breaches with the sample with active pre-signing search. The red circle represents the treatment effect on all breaches during the year after the deal is signed within hospitals without an active post-signing search. The bars indicate the 95 percent confidence intervals. Control variables include the target hospitals' bed count, the public trading status of the target and the buyers, as well as hospital and time fixed effects. Standard errors are clustered at the deal level. Active pre-signing search is defined as having the highest monthly mean one year before the deal is signed during the period $[t-4, t-3]$, which corresponds to 7-12 months before the merger deal is signed. Date t is when deal m is signed. The graph shows that the attention before the deal is signed does not have a significant effect on post-signing breaches. Data sources: Proprietary merger data, Google Trends, and DHHS 2010-2022.

hospitals in this group receive at least two 100 of 100 Google Trends score days in the first quarter after the merger deal is signed, while all the rest are in the other group. The regression is on whether they report a data breach in the rest of the year. The figure shows that the hospitals that receive post-signing attention and the ones that do not receive attention do not have much different increases in data breaches in the second to fourth quarter of the year. It implies that the signaling channel does not dominate the post-signing data breach increases. Then the question is, where did this attention come from? Figure 15b shows whether they report any data breaches right before the merger deal is signed is different. It turns out that the merger deals that have no post-signing attention actually have significantly decreased data breaches reported during the quarter right before the signing date.



(a) Active Post-signing Search: Post-signing Breach



(b) Active Post-signing Search: Pre-signing Breach

Notes: The left figure displays coefficients for the main regression on all data breaches (insider misconduct and hacks) reported from the second quarter to the fourth quarter of the year following the merger deal signing. The red square knob on the left represents the mean treatment effect on such post-signing breaches with the sample of active Google Search. The blue triangle represents hospitals without the active post-signing search. The right figure displays coefficients for the main regression on all data breaches (insider misconduct and hacks) reported in the first quarter immediately before the merger signing date. The red square knob on the left represents the mean treatment effect on hospitals with active post-signing search. The blue triangle represents the mean effect on hospitals without the active post-signing search. The bars indicate the 95 percent confidence intervals. Control variables include the target hospitals' bed count, the public trading status of the target and the buyers, as well as hospital and time fixed effects. Standard errors are clustered at the deal level. Active post-signing search is defined as having a Google Trends score higher than 100 for more than two days within the first 90 days (one quarter) after the merger deal is signed. The graph shows that the attention after the deal is signed does not significantly affect breaches, and the attention comes from pre-signing breaches. Data sources: Proprietary merger data, Google Trends, and DHHS 2010-2022.

11 Conclusion

In this paper, I evaluate the impact of hospital mergers and acquisition activity on the occurrence of insider misconduct and hacks around merger signing time. To address this question, I employ stacked difference-in-differences to identify the causal effect of mergers and use these causal estimates to identify how different changes in the hacker's and the hospital's behavior are the reasons for increased data breaches in hospitals. The pre-signing breaches and post-signing breaches are analyzed separately. I identify the information and attention changes during this process using Google Trends data to test whether and how increased attention leads to higher data breaches. The event study demonstrates the dynamic effect during stages of mergers and throughout the time of 2012-2019. Using stratification, I analyze the characteristics of the buyers and the target hospitals, which are also reasons for different security experiences during mergers. Hospitals experience a dramatic increase in data breaches during the mergers and acquisition period. Data breaches during mergers double compared with the pre-merger groups. The complete set of findings is summarized in Table 16.

Table 16: CONCLUSION TABLE

Theory	**Empirical Evidence**
Incompatibility Channel	
Incompatibility during Information System Integration (ISI) generates vulnerability	Post-signing data breaches increase from 0.38% to 1.19%. The system buyer experiences greater elevated post-signing breaches
Incompatibility emerges as a substantive concern for multi-hospital systems despite the economy of scale for their resources	Larger and more experienced multi-hospital systems are actually reporting more data breaches
Insider Misconduct	
Inefficiency allows for more malicious insider misconduct and honest mistakes, but it has become less significant in recent years	Insider misconduct doesn't solely account for the increase in data breaches during mergers, and its impact has reduced over time
Pre-signing Signaling Channel	
Increased information exposure or heightened attention attracts more attacks	Pre-signing data breaches increase from 0.14% to 1.41%. The target hospitals that receive significant attention one year before the deal is signed experience a higher probability of data breaches just before finalizing the deal
Hackers find the buyers more attractive as the buyer's financial resources concentrate	The buyers do experience more data breaches during mergers

The signaling effect varies across different situations and is not an external shock completely beyond control	Public traded hospitals are attacked less even if they get a lot of attention. In the short term, larger merger deals are subject to attacks later than the smaller ones
The signaling effect has minimal impact once the merger deal is signed when the incompatibility channel is dominant	The target hospitals that receive significant attention right after the deal is signed do not experience more data breaches in the latter post-signing period
Organizational Capital Channel	
The acquisition experience and the risk management capability vary	Publicly traded hospitals experience less impact, whereas large or experienced multi-hospital systems are more affected
Larger deals are more attractive targets, but they come with a larger scale of resources to address them	Bigger deals are subject to fewer attacks in the longer term given the same level of attention
Professional investors are proactive in preventing data breaches	Professional investors manage pre-signing breaches better
Lack of security resources in struggling target hospitals	Struggling target hospitals experience a greater increase in insider misconduct, but they are less attractive to hackers
Dynamic Changes	
Hospitals have shown increased motivation to enhance their security investments in recent years	In the Recent 5 years, insider misconduct during mergers is under control
Hacking and defense technology have evolved over the years, and hackers have shown increased motivation to attack as well	Ransomware surged in the last five years, and hacks during mergers intensified, while post-signing effects reduced gradually

Notes: This table summarizes all the empirical results on the mechanisms in the second column with the corresponding hypothesis on the left.

These results highlight two pressing and severe cybersecurity challenges faced by the health industry. The first challenge is ransomware attacks. In recent years, hacks have surged, and ransomware has become one of the main reasons for data breaches during mergers. On average, ransomware happens even more during the pre-signing period. This implies that ransomware attacks are not solely driven by technical reasons during IT integration, but information and motivation also play crucial roles in their occurrence, thus understanding the economics of cybersecurity becomes essential to address the ransomware attack problem. Moreover, it highlights that ransomware has the potential to disrupt financial market activities, including mergers and acquisitions. The second challenge is the

increasing difficulty of managing large multi-hospital system expansion. Large and more experienced multi-hospital systems are more heavily impacted by the increase in data breaches during mergers. Larger and more experienced multi-hospital systems may have greater resources, but this does not necessarily translate to better security outcomes.

These results are relevant for understanding the hospitals' security behavior when facing these challenges. The formative major challenges do not mean hospitals are entirely passive in facing the threats. Publicly traded hospitals experience less of an increase in data breaches during mergers, even facing increased attention online. Decreasing insider misconduct also indicates that hospitals are putting in the effort. Deals with professional buyers can manage pre-signing breaches better (Rundle and Nash, 2023). The bigger deals (the mergers with a bigger target hospital), with richer cybersecurity resources, are less hacked in the long term.

These results improve our understanding of the hackers' behavior. The results partially reveal the changes in the hackers' behavior facing merging hospitals. The merger deals receive more attention online one year before the deal is signed and have more data breaches right before the deal is signed. However, such attention does not have a spill-over effect on the post-signing period. These results suggest that hackers' behavior changes as information changes. Another reason mergers attract hacks is that hackers find the buyers more attractive as the buyers' financial resources concentrate. My result shows that buyers do experience more data breaches during mergers. For example, classic economics of cybersecurity theory (Cavusoglu, Raghunathan and Yue, 2008) emphasize how hackers do a cost-benefit analysis for hacking decisions.

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. These findings also offer valuable insights for more stakeholders to address the cybersecurity challenges. These stakeholders include health, financial, cybersecurity authorities, hospital and multi-hospital system management teams, health IT vendors, cybersecurity insurance providers, and consultants. Given the elevated and escalating cost of data breaches (IBM, 2023), hospitals, such as publicly traded hospitals and professional investors, that can manage cybersecurity risks effectively gain a substantial comparative advantage. Investing in cybersecurity during mergers is a cost-effective way to reduce cyber risk. The results emphasize especially the need for early and tailored IT integration plans to address different hospitals' diverse challenges. These challenges start way before the merger deal is signed. For the hospitals, their IT and cybersecurity vendors, and cybersecurity insurance providers, it is beneficial to consider information and attention online when predicting potential risk increases. To offer technical support, cybersecurity authorities need to focus on ransomware attacks and challenges faced by multi-hospital systems. Issuing best practice suggestions and suggesting licensed security services can also be beneficial. Suggesting the risk management process adopted by professional investors and publicly traded hospitals to all merging entities is one way to improve organizational capital.

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.

Angst, Corey M, Emily S Block, John D Arcy, and Ken Kelley, "When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches," *MIS Quarterly*, 2017, *41* (3), 893–916.

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.

Bachura, Eric, Rohit Valecha, Rui Chen, and H Raghav Rao, "The OPM Data Breach: An Investigation of Shared Emotional Reactions on Twitter," *MIS Quarterly*, 2022, *46* (2), 881.

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," *Federal Reserve Bank of Kansas City Working Paper*, 2022, (22-14).

_ **and** _ , "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.

_ , Thomas W Malone, Vijay Gurbaxani, and Ajit Kambil, "Does information technology lead to smaller firms?," *Management science*, 1994, *40* (12), 1628–1644.

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, Birendra Mishra, and Srinivasan Raghunathan, "The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers," *International Journal of Electronic Commerce*, 2004, *9* (1), 70–104.

_ , 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.

Chatterjee, Chirantan and D Daniel Sokol, "Data security, data breaches, and compliance," *Cambridge Handbook on Compliance (D. Daniel Sokol & Benjamin van Rooij editors, Cambridge University Press, forthcoming)*, 2019.

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.

Chua, Yi Ting, "Sale of private, confidential, and personal data," in "Handbook on Crime and Technology," Edward Elgar Publishing, 2023, pp. 138–155.

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

Dameff, Christian, Jeffrey Tully, Theodore C Chan, Edward M Castillo, Stefan Savage, Patricia Maysent, Thomas M Hemmen, Brian J Clay, and Christopher A Longhurst, "Ransomware attack associated with disruptions at adjacent emergency departments in the US," *JAMA network open*, 2023, *6* (5), e2312270–e2312270.

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.

DHHS, "Hospital Cyber Resiliency Initiative Landscape Analysis," 2023.

Dobrzykowski, David D and Monideepa Tarafdar, "Understanding information exchange in healthcare operations: Evidence from hospitals and patients," *Journal of Operations Management*, 2015, *36*, 201–214.

Dranove, David, Chris Forman, Avi Goldfarb, and Shane Greenstein, "The trillion dollar conundrum: Complementarities and health information technology," *American Economic Journal: Economic Policy*, 2014, *6* (4), 239–270.

Du, Kui, "Research note—parenting new acquisitions: acquirers' digital resource redeployment and targets' performance improvement in the US hospital industry," *Information Systems Research*, 2015, *26* (4), 829–844.

_ and Hüseyin Tanriverdi, "Does IT Enable Collusion or Competition: Examining the Effects of IT on Service Pricing in Multi-market Multihospital Systems," *MIS Quarterly (Forthcoming)*, 2022.

Ebrahimi, Mohammadreza, Yidong Chai, Sagar Samtani, and Hsinchun Chen, "Cross-Lingual Cybersecurity Analytics in the International Dark Web with Adversarial Deep Representation Learning," *MIS Quarterly*, 2022, *46* (2), 1209.

ForgeRock, "2023 ForgeRock Identity Breach Report," 2023.

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.

Gordon, Lawrence A, Martin P Loeb, and Tashfeen Sohail, "Market Value of Voluntary Disclosures Concerning Information Security," *MIS Quarterly*, 2010, *34* (3), 567–594.

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.

Grogan, Colleen M, *Grow and Hide: The History of America's Health Care State*, Oxford University Press, 2023.

Hajizada, Abulfaz and Tyler Moore, "On Gaps in Enterprise Cyber Attack Reporting," in "2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)" IEEE 2023, pp. 227–231.

Henningsson, Stefan, Philip W Yetton, and Peter J Wynne, "A review of information system integration in mergers and acquisitions," *Journal of information Technology*, 2018, *33* (4), 255–303.

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.

Hughes, Jack, Yi Ting Chua, and Alice Hutchings, "Too much data? Opportunities and challenges of large datasets and cybercrime," *Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches*, 2021, pp. 191–212.

IBM, "IBM Security: Cost of a Data Breach Report," 2023.

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.

Karahanna, Elena, Adela Chen, Qianqian Ben Liu, and Christina Serrano, "Capitalizing on health information technology to enable digital advantage in US hospitals," *MIS quarterly*, 2019, *43* (1), 113–140.

KLAS/CENSINET/AHA, "Healthcare Cybersecurity Benchmarking Study: How Aligned Is the Industry to NIST and HICP Best Practices? White Paper," 2023.

Kwon, Juhee and M Eric Johnson, "Proactive Versus Reactive Security Investments in the Healthcare Sector," *MIS Quarterly*, 2014, *38* (2), 451–471.

_ **and** _ , "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.

Li, Weifeng and Hsinchun Chen, "Discovering Emerging Threats in the Hacker Community: A Nonparametric Emerging Topic Detection Framework," *MIS Quarterly*, 2022, *44* (4), 2337–2350.

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.

Mahmood, M Adam, Mikko Siponen, Detmar Straub, H Raghav Rao, and TS Raghu, "Moving toward black hat research in information systems security: An editorial introduction to the special issue," *MIS quarterly*, 2010, *34* (3), 431–433.

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

Mehta, Manjari and Rudy Hirschheim, "Strategic alignment in mergers and acquisitions: Theorizing IS integration decision making.," *Journal of the Association for Information Systems*, 2007, *8* (3), 8.

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** _ , "Encryption and the loss of patient data," *Journal of Policy Analysis and Management*, 2011, *30* (3), 534–556.

_ **and** _ , "Health information exchange, system size and information silos," *Journal of health economics*, 2014, *33*, 28–42.

_ **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.

Neprash, Hannah T, Claire C McGlave, Dori A Cross, Beth A Virnig, Michael A Puskarich, Jared D Huling, Alan Z Rozenshtein, and Sayeh S Nikpay, "Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021," in "JAMA Health Forum," Vol. 3 American Medical Association 2022, pp. e224873–e224873.

Nikkhah, Hamid Reza and Varun Grover, "An Empirical Investigation of Company Response to Data Breaches," *MIS Quarterly*, 2022, *46* (4), 2163–2196.

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.

Qi, Kangkang and Sumin Han, "Does IT Improve Revenue Management in Hospitals?," *Journal of the Association for Information Systems*, 2020, *21* (6), 7.

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

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

Salge, Torsten Oliver, David Antons, Michael Barrett, Rajiv Kohli, Eivor Oborn, and Stavros Polykarpou, "How IT investments help hospitals gain and sustain reputation in the media: The role of signaling and framing," *Information Systems Research*, 2022, *33* (1), 110–130.

Samtani, Sagar, Yidong Chai, and Hsinchun Chen, "Linking Exploits from the Dark Web to Known Vulnerabilities for Proactive Cyber Threat Intelligence: An Attention-Based Deep Structured Semantic Model," *MIS Quarterly*, 2022, *46* (2), 911.

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.

Shandler, Ryan and Miguel Alberto Gomez, "The hidden threat of cyber-attacks–undermining public confidence in government," *Journal of Information Technology & Politics*, 2022, pp. 1–16.

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

Tanriverdi, Hüseyin and Kui Du, "Corporate Strategy Changes and Information Technology Control Effectiveness in Multibusiness Firms.," *MIS Quarterly*, 2020, *44* (4).

_ and Vahap Bülent Uysal, "Cross-business information technology integration and acquirer value creation in corporate mergers and acquisitions," *Information Systems Research*, 2011, *22* (4), 703–720.

_ and Vahap Bülent Uysal, "When IT capabilities are not scale-free in merger and acquisition integrations: how do capital markets react to IT capability asymmetries between acquirer and target?," *European Journal of Information Systems*, 2015, *24* (2), 145–158.

_ , Arun Rai, and N Venkatraman, "Research commentary—reframing the dominant quests of information systems strategy research for complex adaptive business systems," *Information systems research*, 2010, *21* (4), 822–834.

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.

Zaheer, Akbar and Natarjan Venkatraman, "Determinants of electronic integration in the insurance industry: An empirical test," *Management science*, 1994, *40* (5), 549–566.

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.

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

Nan Clement

February 4, 2024

Updated frequently. Click here for the latest version.

A 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 hacks. Insider misconduct 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, hacks involve 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.

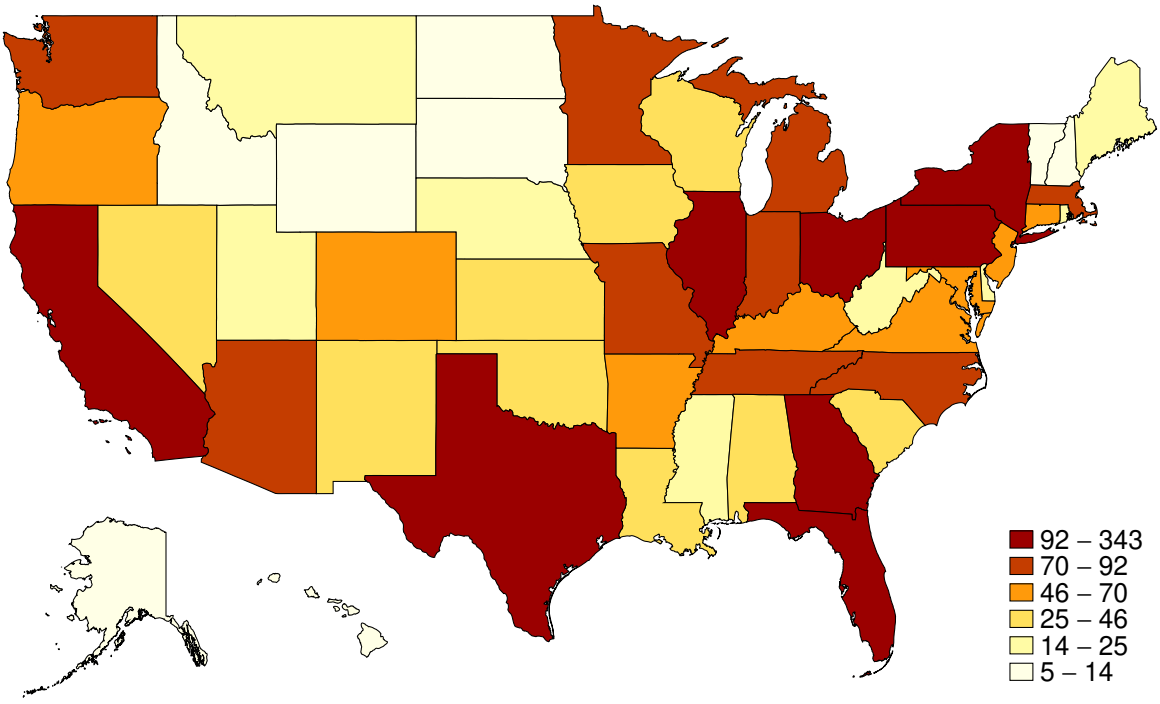
A.1 Overview

Figure 16a displays the number of data breach reports in each state over the past 13 years, while Figure 16b 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.

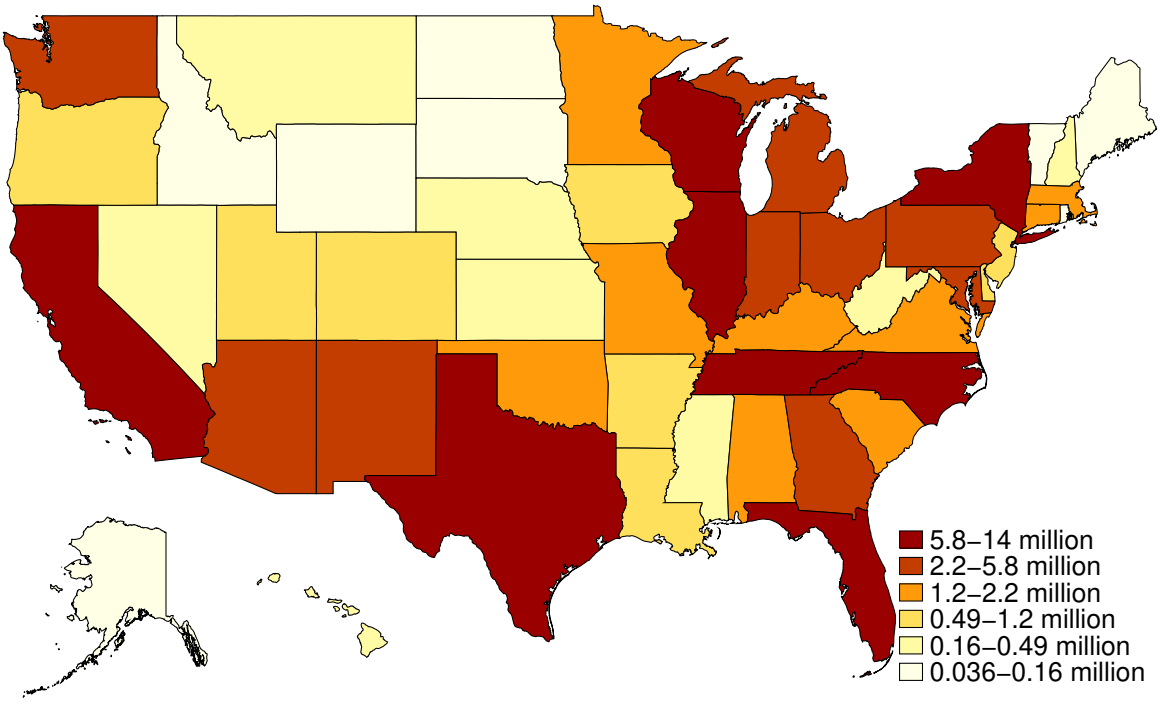
Consequently, it remains ambiguous from the map whether data breaches occur randomly across hospitals or whether specific risk factors dominate the probability of such incidents. Hence, it is worth exploring whether certain risk factors are associated with a higher probability of data breaches.

A.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 hacks, as shown in Figure 17. The category of misconduct comprises instances of loss,



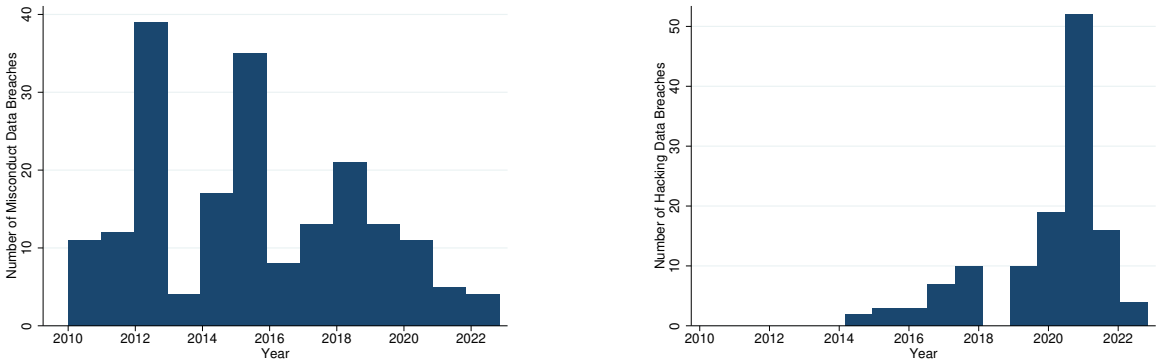
(a) Map of Data Breaches 2010.1 - 2022.12



(b) Map of Individuals Impacted by Data Breaches 2010.1-2022.12

Figure 16: 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) Hacks Over 2010-2022

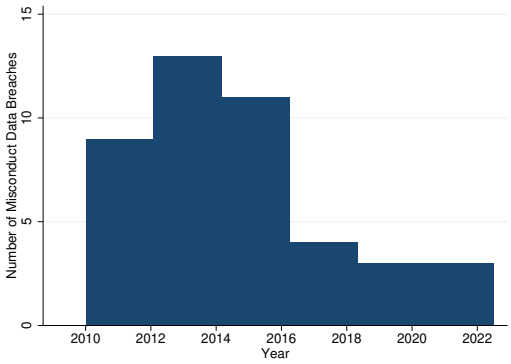
Figure 17: Two Categories of Data Breaches Over 2010-2022

Notes: The figures show the number of insider misconduct and hacks 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. Hacks targeting hospitals are more frequently reported during mergers, with a higher incidence reported by buyers. Hacks are categorized into three types: general hacks, phishing, and ransomware. General hacks cover zero-day exploits, malware, and other non-phishing-triggered accidents. Data source: DHHS 2010-2022.

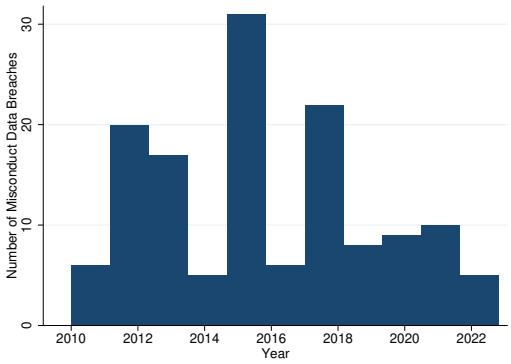
theft, improper disposal, and impermissible employee access and disclosure, which could occur due to both fraudulent motives or accidents. For instance, some cases may entail the sale of medical records by employees, while others may involve paper records mistakenly sent to the recycling center without proper shredding. Both motivated and non-motivated misconduct is indicative of management issues, and a well-established risk control procedure can effectively reduce the likelihood of such incidents. As further shown in Figures 18a and 18b, misconduct data breaches both in merging targets and in buyers are less reported in the last five years.

Conversely, hacks targeting hospitals are more frequently reported during mergers, with a higher incidence reported by buyers. Figures 19a, 19b, and 19c show that hacks are categorized into three types: general hacks, phishing, and ransomware. General hacks cover zero-day exploits, malware, and other non-phishing-triggered accidents. Note that there has been an increasing trend of ransomware incidents in recent years.

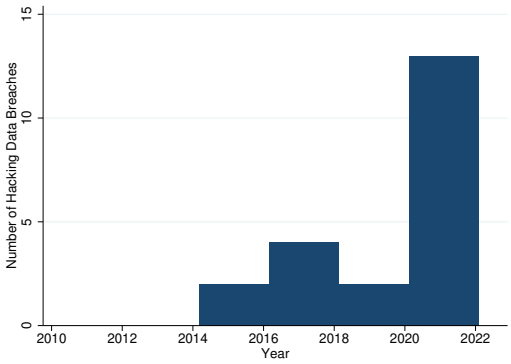
Regarding the dynamic changes, Figure 17 shows a large contrast of occurrence between the misconduct and the hacks during the pandemic. Note that in the main model, mergers that happened after December 31^{st} 2020 are not included as the treated group as they are too recent to have any control group. I investigate the mergers in 2021-2022 in Section F by comparing to never-treated using CMS Hospital Compare.



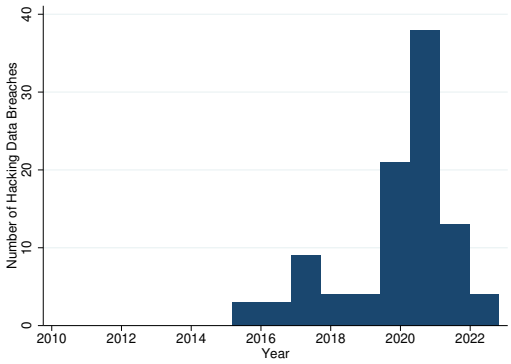
(a) Misconduct Data Breaches by Merging Target



(b) Misconduct Data Breaches by Buyers



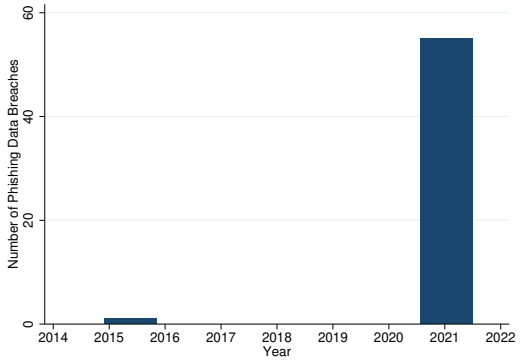
(c) Hacks by Merging Target



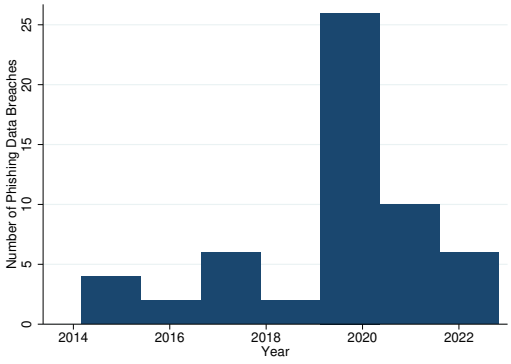
(d) Hacks by Buyers

Figure 18: Two Types of Data Breaches by Different Entities Over 2010-2022

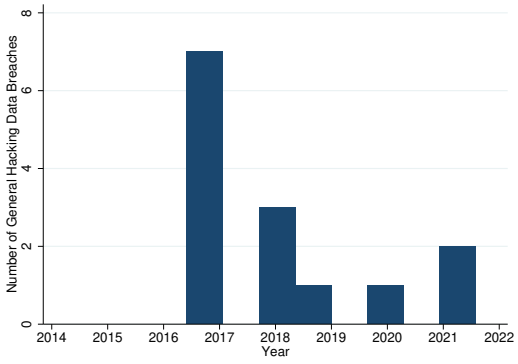
Notes: The figure shows the number of insider misconduct and hacks reported by different entities. Hacks targeting hospitals are more frequently reported during mergers, with a higher incidence reported by buyers. Data source: DHHS 2010-2022.



(a) Ransomware



(b) Phishing



(c) General Hacks

Figure 19: Three Types of Hacks Over 2014-2022

Notes: Hacks are categorized into three types: general hacks, phishing, and ransomware. General hacks 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.

A.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 8).

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.

B 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 multi-hospital system bought a new hospital either from another multi-hospital system. It can also be a multi-hospital system bought by another multi-hospital system that controls several hospitals.

The combination of the two events over time is shown in Figure 20c. 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. In the last graph, Figure 20d, the dark histogram is the number of such matched data breaches each month. It shows how many hospitals and multi-hospital systems recorded in the merger data also report a data breach. Note that as data breaches are rare events with uncertainty, the relationship between mergers and data breaches is not clear. To investigate this unique dependent variable, I start by looking into the aggregated longer window of "during mergers" in the main model. Dynamic event study on each year's mergers separately in Section 8 also shows

that data breaches increase during mergers is a problem since earlier years. The question is which merger stage should be included in the analysis.

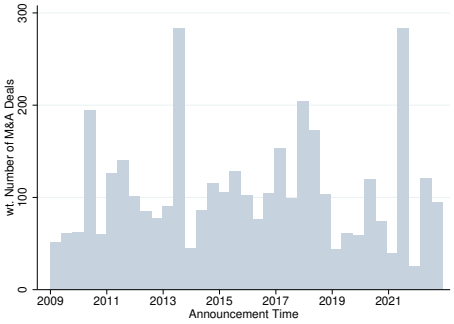
After I show the data breaches and mergers' data, one possible question about the matchings I have in Figure 3b is, why would breaches report before a merger is done count as merger-causing data breaches? The first reason is that although I observe a merger deal signing date, the merger is a long process 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 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.

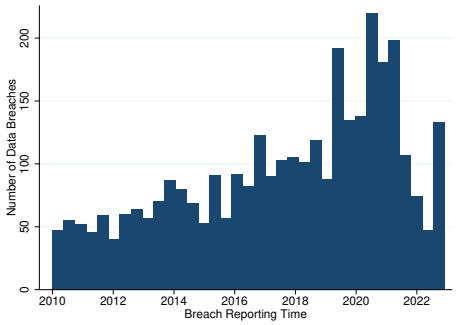
In short, the impact of the merger on operations begins well before the signing date, and a vast amount of information about the potential merger becomes available to the general public before the merger deal closure date. The general public includes hackers.

C Control Variables

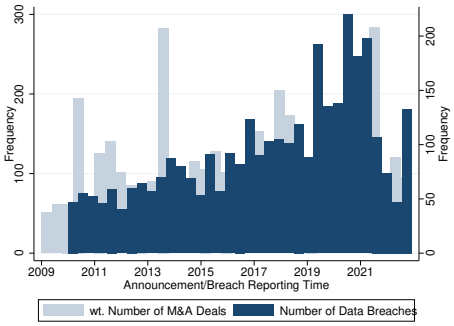
Table 17 presents summary statistics for numerical variables. The first column shows the mean and standard errors for various variables for the full sample. The second column is only for the matched samples. The sample size is reduced in both cases because of the availability of the numerical variables 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 hospitals' bed count revenue, and EBITDA are included in the baseline model introduced in the following section. The last part of Section D explains the contribution of the control variables.



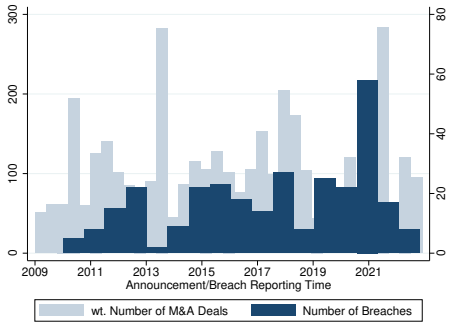
(a) M&A Deals Over 2009-2022



(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 20: M&A Deals and Data Breaches Over 2009-2022

Notes: The figure shows the number of mergers (weighted by the number of the target hospital's bed counts) and reported data breaches in each quarter from 2009-2022. Data source: Proprietary merger information and DHHS 2009-2022.

Table 17: SUMMARY STATISTICS

	(1) Full Sample	(2) 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)
Multi-hospital 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	903	218

D 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 hacks 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. 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 event study graph in Figure 21 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. The reason for the slight difference between Figure 21 and 9 is from the change in the observational period in the control group, thus the mean I am comparing. In the previous analysis, Figure 21 displayed coefficients for the main regression with lead and lag indicators up to 10 quarters prior to or 20 quarters following a merger for mergers that closed between Q1 2018 and Q4 2019. For

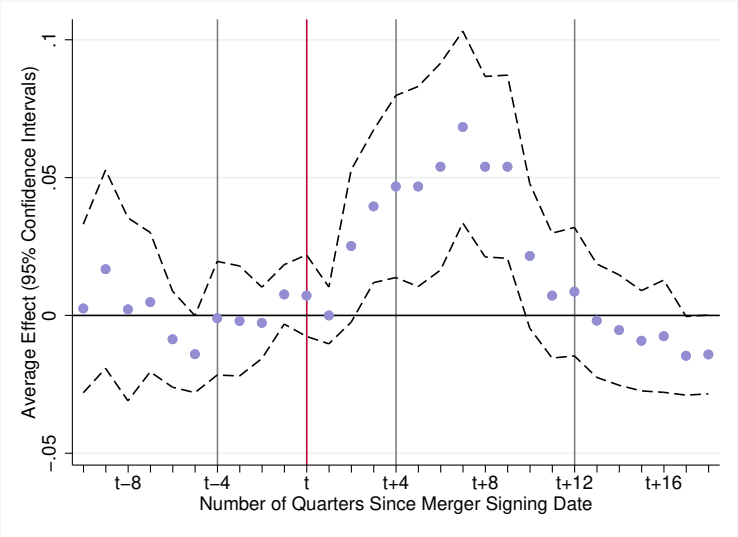


Figure 21: Event Study: Mergers in Q1 2018-Q4 2019

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 that 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 18.

each control or pre-merger deal, the observation spans 5 years before and 5 years after the merger, enabling a comparison of pre-trends with mergers that occurred 2-5 years ago. In the current study, for each control or pre-merger deal, the observation spans all the years before and 5 years after the merger, enabling a comparison of pre-trends with mergers that occurred any time before. To illustrate, in Figure 9 panel a, for a merger deal signed in 2012, all future mergers that occurred between 2015 and 2022 and reported a data breach in 2010 are used as controls, while in the previous event study, the observation period for control groups was limited to only 5 years. The result does not appear to be much different due to the large number of merger deals each year. Thus the result is robust to changing the pre-merger group from all future mergers in at least two years to more recent mergers. To sum up, from all the separate event studies, for separate periods of time, the merging hospitals do experience an increase in cybersecurity risk during mergers compared with pre-merger groups and such challenges over time.

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 pre-siging 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 con-founders that may impact the time trend of data breaches.

E 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 persists 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.

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 22 demonstrates that employing such alternative clustering methods does not significantly change the estimation results.

E.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 23 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

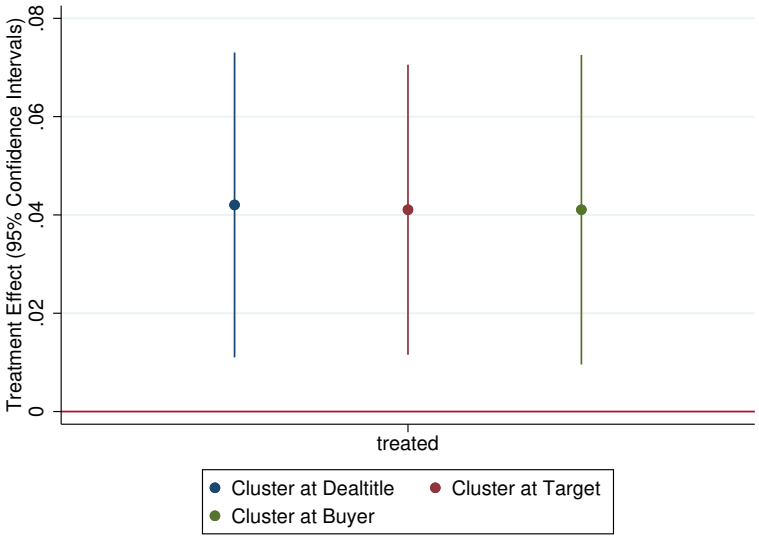


Figure 22: Standard Errors are Clustered at Different Levels

Notes: The graph shows the effect of M&A on data breaches with different standard error clustering methods. 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 and time fixed effects. The first one on the left is with standard error clustered on the deal title, and it is used in the main regression. The second one in the middle is clustered on the target hospital name. The third is clustered on the buyer's hospital name.

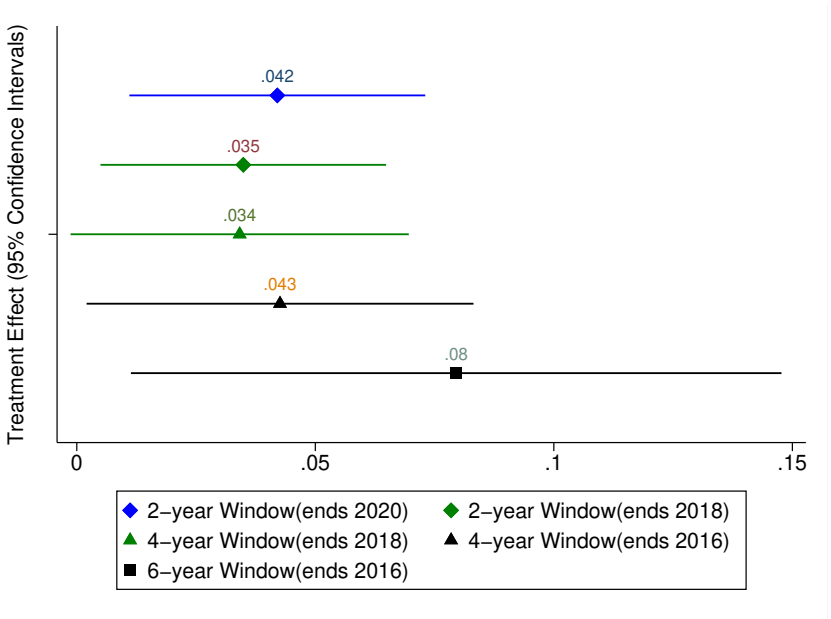


Figure 23: Robustness to Changes in Time Window

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 hospital 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.

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.

E.2 Google Trends

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

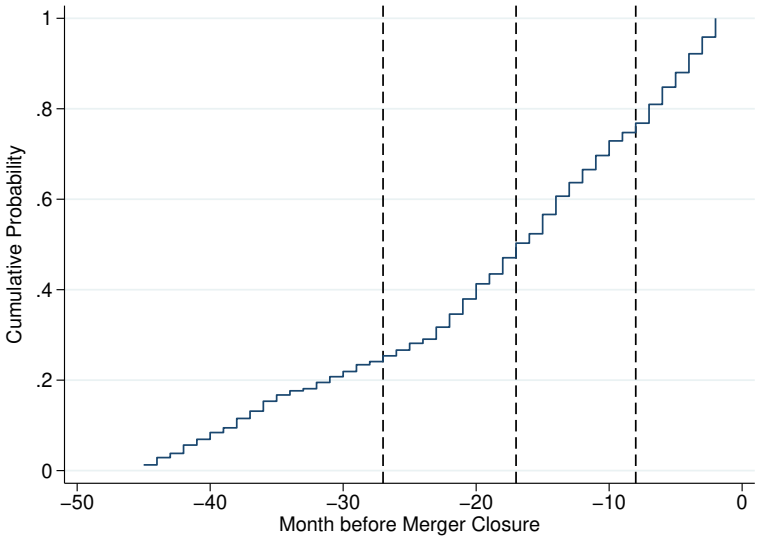


Figure 24: Google Trends: CDF of the Peak Growth Rate

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.

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 24 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 E.

E.3 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 25). 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 18 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

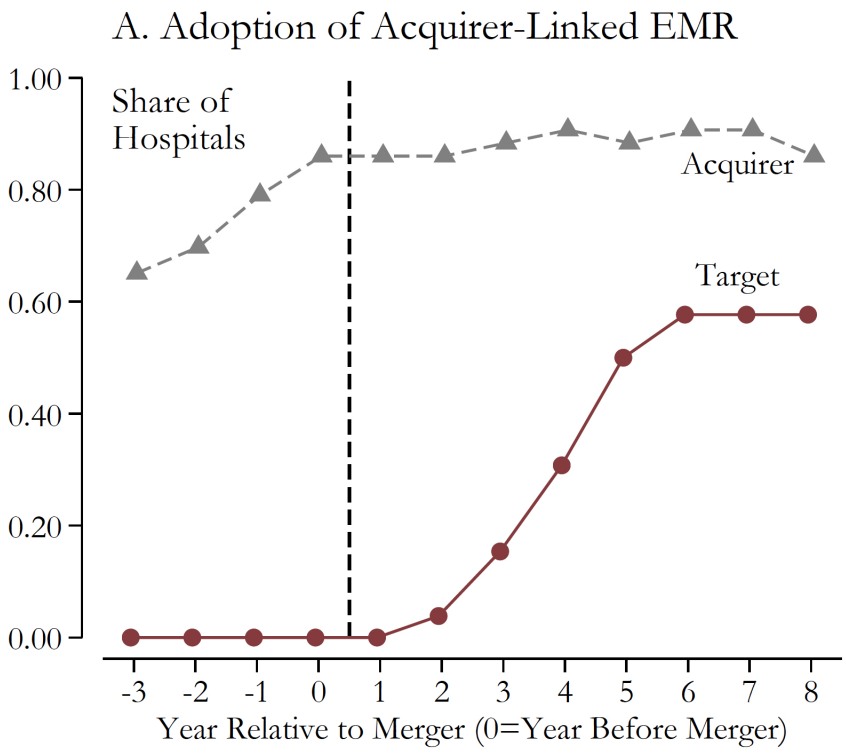


Figure 25: Gaynor et al. (2021) Graph

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).

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 18 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 3 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 24. Instead of one year before the merger deal is signed, 17 months and 27 months are tested and shown in Figure 26.

Table 19 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 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.

Table 18: 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

Notes: The table shows the effect of M&A on hacks 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 and time 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.

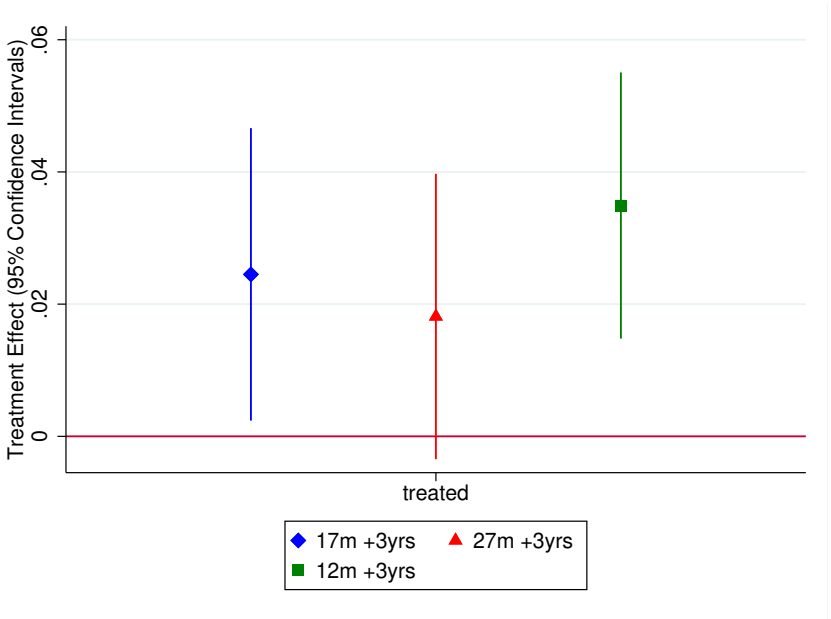


Figure 26: Robustness to Changes in Time Window: Google Trends

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, hospital 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 18. The blue (diamond) coefficient utilizes the median Google search peak, as shown in Figure 24, occurring 17 months before the merger signing date. The red (triangle) coefficient uses the 25th percentile in Figure 24, which corresponds to 27 months before the merger signing date. Data source: Proprietary merger data and DHHS 2010-2022.

Table 19: 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

Notes: 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 and time 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 20: EFFECT OF M&A ON BREACHES: CMS HOSPITAL COMPARES 2016-2022

	21-22	20-22	19-22	16-22
Does M&A cause data breaches?	0.0119**	0.0125	0.0099	0.0053
	(0.0052)	(0.0085)	(0.0080)	(0.0050)
Image	-0.0046	-0.0045	-0.0034	-0.0007
	(0.0039)	(0.0041)	(0.0041)	(0.0030)
Experience	0.0011	0.0014	0.0007	0.0005
	(0.0027)	(0.0029)	(0.0029)	(0.0021)
Timeliness	0.0078***	0.0018	-0.0005	-0.0002
	(0.0027)	(0.0023)	(0.0025)	(0.0018)
Safetiness	-0.0016	0.0012	0.0029	0.0050**
	(0.0028)	(0.0031)	(0.0033)	(0.0022)
Effectiveness	-0.0048	-0.0025	-0.0015	-0.0017
	(0.0031)	(0.0033)	(0.0033)	(0.0023)
Mortality	0.0066*	0.0123***	0.0152***	0.0117***
	(0.0037)	(0.0037)	(0.0037)	(0.0026)
Readmission	0.0020	0.0012	0.0011	-0.0004
	(0.0024)	(0.0027)	(0.0026)	(0.0018)
N	299889	457931	615751	1003659
R^2	0.2253	0.2108	0.2386	0.2497
Mean of Data Breach on Pre-treated % Effect	1.01	1.97	3.04	4.06
Mean of Data Breach on Treated % Effect	2.09	3.87	5.24	5.77

Notes: The table shows the effect of M&A on breaches as estimated from the main equation since 2016. The main variable of interest $Treated_{i,m}$ equals 1 if a data breach was reported by the buyer or the target 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 control group includes hospitals involved in a merger to be signed at least two years after t and the never-treated ones in the CMS Hospital Compares metrics. The never-treated groups include hospitals that did not merge during the observational period, 2016-2022. All the regressions include a full set of hospital and time fixed effects. I also control for the Hospital Compares scores. All controls are equal to 1 when it is unavailable or the performance is below the national average. Standard errors clustered at the state level are displayed in parentheses.

F What About the Never-Treated?

In this Appendix section, I create an alternative dataset by incorporating CMS Hospital Compares, which includes the never-treated group, the hospitals that have not been merged throughout the observational period. In this data set, the control group consists of both pre and never-treated groups. Table 20 shows that there is an increase in data breaches during mergers and an especially significant increase for the year 2021-2022 compared with the never-treated group. As for mergers in 2021 and 2022, it is too recent to have any pre-treated group without contamination. In Table 20, a second difference is the inclusion of an alternative set of control variables. The results suggest that less digitized hospitals are less breached since less image availability correlates with fewer breaches. It is worth noting that a worsening mortality rate correlates significantly with more data breaches.

Table 21: 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

Notes: 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 and time 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.

G Insider Misconduct

I present the main regression on misconduct data breaches, including loss, theft, improper disposal, and impermissible employee access and disclosure here. Tables 21, 22, and 23 suggest an increase in insider misconduct during the two-year period, but no statistically significant treatment effect is observed. These findings indicate that, counter-intuitively, the impact on insider misconduct is not significant. The large increase in data breaches is mainly due to the increase in hacks.

H Bootstrapping

H.1 Investors

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 27.

Table 22: EFFECT OF M&A ON MISCONDUCT BREACHES ON TARGETS

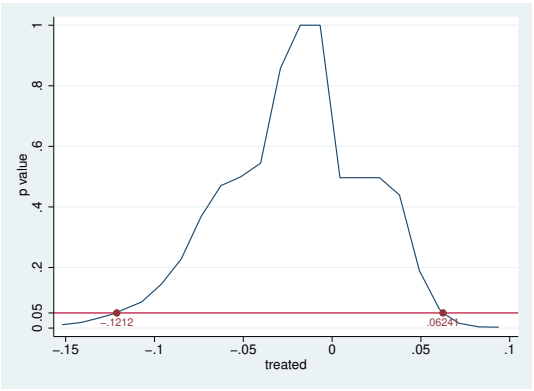
	(1)	(2)	(3)	(4)
Treatment Effect	0.0002	0.0003	0.0003	0.0003
	(0.0048)	(0.0048)	(0.0048)	(0.0048)
Public Acquirer	0.0367*	0.8722***	0.0428***	0.6009***
	(0.0218)	(0.2829)	(0.0096)	(0.1661)
Public Target	0.2088**	0.4632***	-0.0977*	0.1757**
	(0.0941)	(0.0839)	(0.0564)	(0.0756)
Target Hospital's Bed Count	-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

Notes: 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 and time 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.

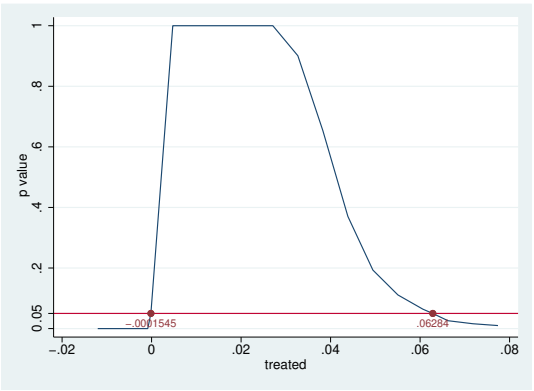
Table 23: EFFECT OF M&A ON MISCONDUCT BREACHES ON BUYERS

	(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

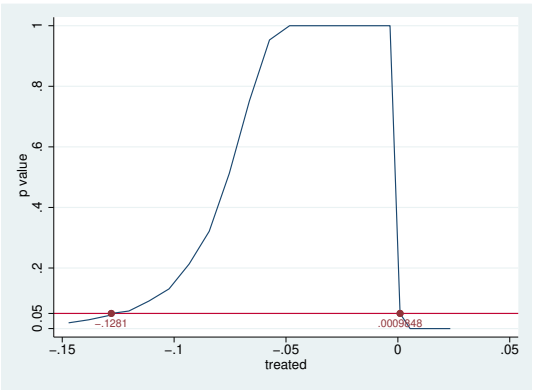
Notes: The table shows the effect of M&A on misconduct data breaches reported by buyers with different sets of controls. The explanatory variable of main interest is a dummy $Treated_{i,m}$ that equals 1 for the hospital i to be involved in deal m and reported a data breach in $[t-a, t+a]$. Date t is 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 and time 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.



(a) Full Sample



(b) Post-merger Breaches



(c) Pre-merger Breaches

Figure 27: 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 have fewer data breaches before the merger signing date.

Table 24: 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

Notes: 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 one 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 and time 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.

H.1.1 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. 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 24 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 28 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. Further study is needed to determine the female CEO's effect. Similarly, with current data, the effect of a CEO with an MBA/PhD/MD title is another future direction.

I Reaction to Attention

Figure 29a and 29b reveal that when merger deals receive intensified online attention, those involving publicly traded hospitals experience significantly less increase in pre-signing and post-signing data breaches. This finding underscores how publicly traded hospitals possess superior risk management assets, providing them with a comparative advantage in achieving better cybersecurity outcomes. Similarly, Figure 30a and Figure 30b demonstrate that, in the short term, larger deals face delayed attacks compared to smaller ones when subjected to intensified online attention. In the long term, the bigger deals display superior cybersecurity outcomes compared to smaller deals. Theoretically, larger merger

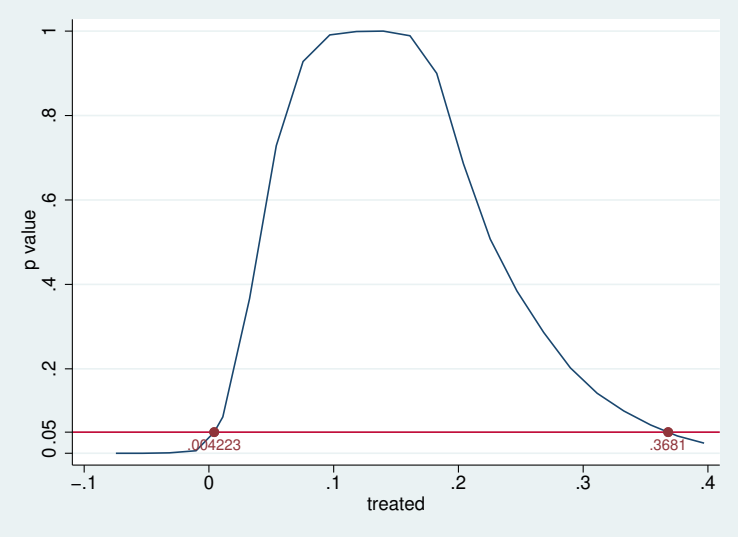


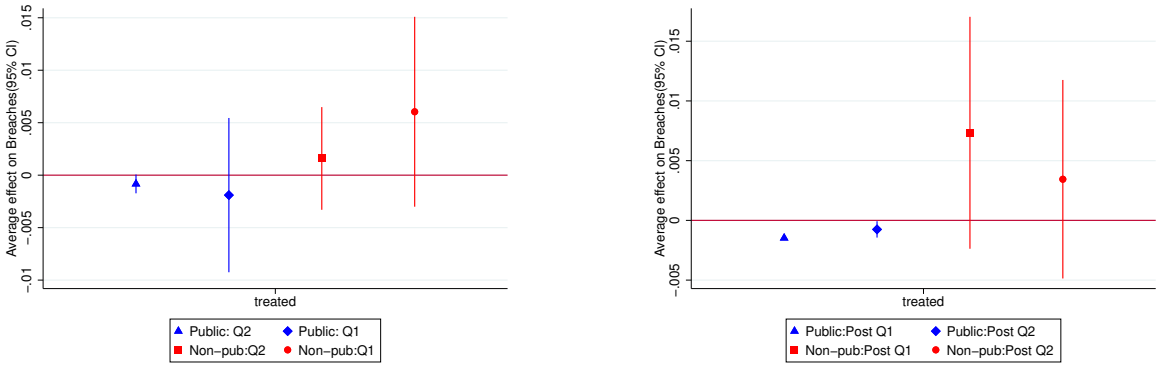
Figure 28: Wild Bootstrap on Deals with a Female CEO

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.

deals may be more attractive targets for hackers due to signaling effects, but they also possess richer security resources stemming from the Organizational Capital Channel. The results suggest that for bigger merger deals, the Organizational Capital Channel outweighs the Pre-signing Signaling Channel. These findings imply that external information and attention shocks do not necessarily spell doom for hospitals' cybersecurity outcomes. With adequate ability and experience, it is possible to effectively manage security risks during mergers. These results also verify the importance of management capability.

J Robustness Check: Without the Individual Fixed Effect

Individual-level fixed effects might not be very informative for this dependent variable. If the dependent variable never changes for a hospital (0 the whole time), that hospital cannot contribute to the estimation of the individual-level fixed effect. As the dependent variable, whether any hospitals in one merger deal report data breaches or not, is a rare event, many of the dependent variables are 0. For the hospitals that are hacked, it is rare that one hospital reports multiple breaches in different periods of time, but some hospitals do report data breaches in more than one period. It is reasonable to include individual-level fixed effects. In Table 25, I present the results for comparing the regression with or without the individual-level fixed effect. The result is robust without the individual-level fixed effect.

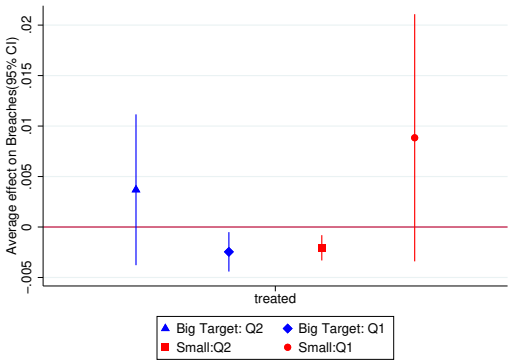


(a) Active Pre-signing Search: Public/Non-public Pre-signing Breach

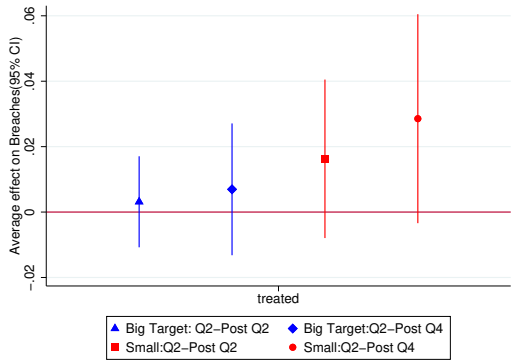
(b) Active Post-signing Search: Public/Non-public Post-signing Breach

Figure 29: Active Search: Public/Non-public Pre-signing Breach

Notes: The left figure displays coefficients for the main regression on all data breaches (insider misconduct and hacks) reported in two pre-signing periods of time separately for the deals that received a lot of attention in the third quarter and the fourth quarter, [t-4,t-3], before the deal is signed. The first period, Q2, is on the second quarter before the deal is signed. The second period, Q1, is the quarter immediately after, which is on the first quarter before the deal is signed. The blue triangle knob on the far left represents the mean treatment effect on pre-signing breaches with the deals with a publicly traded hospital involved. The blue diamond knob on the middle left represents the mean treatment effect on pre-signing breaches in the next quarter with the deals that have a publicly traded hospital, either the buyer or the target. The red square and red circle represent breaches in these two quarters within hospitals without any publicly traded hospitals. The right figure displays coefficients for the main regression on all data breaches (insider misconduct and hacks) reported in the post-signing Q1 and post-signing Q2. The blue triangle and the blue diamond are on mergers with a publicly traded hospital. The red square and red circle represent breaches in these two quarters within hospitals without any publicly traded hospitals. The bars indicate the 95 percent confidence intervals. I control for the hospital and time fixed effects. I also control for the target's bed count. All the samples have the highest monthly mean one year before the deal is signed during the period $[t-4, t-3]$, which corresponds to 7-12 months before the merger deal is signed. Date t is when deal m is signed. The only difference between the two groups is whether they involve a publicly traded hospital. The graph shows that even with a lot of attention, the deals with a publicly traded hospital involved are better off in both pre and post-signing periods. Data sources: Proprietary merger data, Google Trends, and DHHS 2010-2022.



(a) Active Pre-signing Search: Big/Small Deal Pre-signing Breach



(b) Active Post-signing Search: Big/Small Deal Post-signing Breach

Figure 30: Active Search: Big/Small Deal Post-signing Breach

Notes: The left figure displays coefficients for the main regression on all data breaches (insider misconduct and hacks) reported in two post-signing periods of time separately for the deals that receive a lot of attention in [t-4,t-3], the third quarter and the fourth quarter before the deal is signed. The first period, Q2, is in the second quarter before the deal is signed. The second period, Q1, is the quarter immediately after, which is on the first quarter before the deal is signed. The blue triangle knob on the far left represents the mean treatment effect on Q2 pre-signing breaches with the deals with a big target involved. A big target is defined as the target hospital's bed count is greater than the mean bed count. The blue diamond knob on the middle left represents the mean treatment effect on pre-signing breaches in the next quarter, Q1, with deals with a big target. The red square and red circle represent breaches in these two quarters within hospitals without a big target hospital. The right figure displays coefficients for the main regression on all data breaches (insider misconduct and hacks) reported in the long periods, [t-2,t+2] and [t-2,t+4], to include post-signing breaches. The blue triangle and blue diamond represent the mean effect on breaches within deals with a big target hospital. The red square and red circle represent breaches within deals without a big target hospital. The bars indicate the 95 percent confidence intervals. I control for the hospital and time fixed effects. I also control for the bed count and public trading status for the buyers and the targets. All the samples have the highest monthly mean one year before the deal is signed during the period $[t-4, t-3]$, which corresponds to 7-12 months before the merger deal is signed. Date t is when deal m is signed. The only difference between the two groups is whether they involve a big target. The graph shows that in the short term, the pre-signing attention has a heterogeneous effect on merging hospitals, but the pre-signing attention does not have heterogeneous longer-term effects on deals with different sizes when post-signing breaches are considered. Data sources: Proprietary merger data, Google Trends, and DHHS 2010-2022.

	Insider Misconduct and Hacks	
Does M&A cause data breaches?	0.0420***	0.0445***
	(0.0158)	(0.0155)
Public Acquirer	0.6044***	-0.0268***
	(0.1634)	(0.0072)
publictarget	0.1764**	-0.0147
	(0.0744)	(0.0110)
Target Hospital's Revenue	0.0007***	-0.0011**
	(0.0002)	(0.0004)
Target Hospital's Bed Count	0.0021	0.0050*
	(0.0017)	(0.0026)
Target Hospital's EBITDA	-0.0084***	0.0002***
	(0.0017)	(0.0001)
R^2	0.2372	0.0491
Individual Fixed Effect	✓	
Time Fixed Effect	✓	✓
Mean of Data Breach on Pre-treated % Effect	3.22	3.22
Mean of Data Breach on Treated % Effect	6.06	6.06

Table 25: Without the Individual Fixed Effect

Notes: The table presents the impact of M&A deals on data breaches in two representation forms, one with the individual-level fixed effect and one without the individual-level fixed effect. The main variable of interest is a binary dummy, $Treated_{i,m}$, which equals one 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. The first regression includes a full set of hospital and time fixed effects, and the second regression only includes time 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.