Mergers Effect on Data Breaches in Hospitals

Nan Clement
MIT Sloan
Email: nanc@mit.edu

September 23, 2024
Click here for the latest version.

Keywords: mergers, health IT, cyber attacks, software security
Abstract: This study quantifies the effects of mergers on hospital data breaches, disrupting care, leading to fatal consequences, violating privacy rights, and incurring significant costs to remedy. Using U.S. hospital data over ten years, I provide causal evidence that data breach rates double during hospital mergers. The results suggest high pre-signing online visibility contributes to doubled data breach rates during mergers. Increased online visibility makes mergers more noticeable to malicious actors and increases external threats. Post-signing integration technical challenges is another factor for data breach risks. Effective management can mitigate the data breach risks in certain types of hospitals. By contrast, I find no evidence that the experience or resources of large multi-hospital health systems reduce the data breach risks. The study discusses the implications of predicting and managing data breach risks for hospital managers, health IT leaders, and healthcare authorities.

1. Introduction

Ten years after the U.S. health providers finished digitizing patient records (Office of the National Coordinator for Health Information Technology 2021), large-scale privacy breaches and compromised security are commonplace. Healthcare leaders are concerned about cybersecurity, with 94% of hospitals reporting financial impacts from recent data breaches (HealthTech 2024). Ransomware attacks on electronic medical record systems have set health IT-equipped hospitals back to pen and paper for weeks (HealthExec 2024). In 2022, healthcare data breaches in the U.S. hit more than 40 million victims, violating their privacy rights. Nearly 600 hospitals spent more than ten million dollars on ransom payments, class action lawsuits, incident response, and health IT recovery. As the most vulnerable sector on data breach and privacy-related issues, healthcare faced a 50% increase in incidents in 2023 (ForgeRock 2023, IBM 2023). Despite the escalating risks, hospitals lack a common cybersecurity practice. Note that the percentage of cybersecurity investments in the total hospital revenue can span a 166% difference (DHHS 2023). As an increasing number of data breaches are hacks involving malicious actors, the argument does not settle on whether management helps to reduce data breach risks or whether hacks are beyond the hospitals' control.

Measures to reduce data breaches are of significant practical relevance for healthcare leaders and policymakers because of the substantial cost of data breaches. "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). Ransomware attacks cause business disruption. For example, the WannaCry cyber attack on the National Health Service England in 2017 disrupted outpatient treatments, inpatient treatment, and emergency visits and had large effects on low-income and minority groups (Deng, Lambrecht and Tucker 2020). Regardless of whether a data breach is hack by malicious actors, its impact on privacy is profound, compromising the confidentiality of patients' medical records. As listed in Table 1, more costs include reduced revenue, remediation costs, and legal consequences, including class action settlements, fines, and payments to malicious actors. For example, in the U.S., the cyberattack on Change Healthcare costed UnitedHealth Group more than $2.3 billion in 2024. Compared with clinics, physician offices, and healthcare providers, hospitals are more likely to have operation disruptions during ransomware attacks (Neprash, McGlave, Cross, Virnig, Puskarich, Huling, Rozenshtein and Nikpay 2022). By investigating data breach risks during hospital mergers, this study offers insights to improve health IT management practices. Given the significant challenges and high costs associated with data breaches, the managerial implications are meaningful.

The practical motivation for this study is to understand the surge in data breaches in hospitals and suggest best practices, while the theoretical motivation is to evaluate the economic and management factors contributing to data breach risks. There is limited empirical evidence on whether and how management factors enhance the function of health IT, as observing intangible assets is challenging. To this end, I study the causal effects of mergers on hospital data breach risks. Merging progress involves multiple steps over a long time, providing a rich opportunity to study economic and management factors at various stages of

Table 1 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), Deng, Lambrecht and Tucker (2020)
Stock Market Impact	Decreased stock price by loss of investor confidence as seen in Campbell, Gordon, Loeb and Zhou (2003), Cavusoglu, Mishra and Raghunathan (2004), Chatterjee and Sokol (2019)
Publicity Costs	Hire for crisis public relations management as in Bana, Brynjolfsson, Jin, Steffen and Wang (2023) and communicate with investors as in Nikkhah and Grover (2022)
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 of 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 (2015)
Loss of Life	Possible adverse effects on patient well-being as seen in Choi and Johnson (2019)
Other Market and Non-market Harms for Consumers	Labor/insurance/product market harms, social stigma, and reputation risks brought about by privacy violations, as seen in Miller (2022)

the mergers. For example, inside hospitals, mergers are disruptive periods where managers are distracted. Externally, malicious actors find merging hospitals attractive. I find the probability of a data breach doubles during mergers. By further dividing the sample based on the economic and management factors and comparing their data breach rates, I provide suggestive evidence on whether and how the factors contribute to data breach risks.

This study employs stacked difference-in-differences (Deshpande and Li 2019) to document that data breach rates double during mergers. The advantage of using stacked difference-in-differences, with future mergers as control groups, lies in its ability to avoid biases inherent in using already treated cases as controls in staggered treatments, as highlighted by Goodman-Bacon (2021), and its ability to address the selection problem of mergers. Using future merger groups means that the treatment is not the merger itself but rather the time of the merger. Specifically, this estimation strategy considers mergers to be signed two years or later as the control/pre-treated group, isolating the effect of merger time on data breaches. I test whether hospitals undergoing mergers experience more data breaches than the pre-treated group without ongoing mergers. The result is robust against alternative explanations, as extending the window symmetrically and asymmetrically does not change the conclusion from the main analysis. The study uses comprehensive U.S. hospital data, including proprietary merger records from Levin's Associates and archived healthcare breach reporting data from the Office of Civil Rights of the U.S. Department of Health and Human Services (HHS), spanning from 2010 to 2022. It is plausible that hospitals hide their data breach, but the reliability of HHS breach data is validated through several sources. Compared with the Identity Theft Resource Center data in Jiang, Khanna, Yang and Zhou (2024), the advantage of the HHS hospital breach data is that it is bound by law that

hospitals are obligated to report breaches to HHS, and the data is audited by the Office of Civil Rights. The Identity Theft Resource Center data is more advantageous for studying consequences because it includes information on whether sensitive information is revealed or not. Mergers' effect on doubled data breaches is further decomposed for mechanism analysis and event study, eliminating alternative explanations. A natural question that follows the main result of doubled data breach risks is the reason for the escalated risks during mergers. Another advantage of the HHS data is its rich details on each data breach, which help identify whether the data breach relates to malicious actors.

Why do data breach rates double during hospital mergers? One of the main challenges to studying management and economic factors for data breach risks lies in the fact that some data breaches are hacks, which are attacks executed by malicious actors and increase the number of moving factors. A framework is necessary and serves as a guide for the analysis to separate the external threats of the malicious actors' behavior from the internal vulnerability of management actions within the hospitals. I emphasize how economic and management factors can be separated into five categories:

1. Online Visibility
2. Attractiveness
3. Technical Challenges
4. Management Skills
5. Scale of Resources

Online visibility may induce a higher external threat because malicious actors are more aware of the value of the hospitals and their potential vulnerabilities. Information asymmetry of the malicious actors is a critical factor to consider in cybersecurity policy (Mitra and Ransbotham 2015). Owing to transparency requirements, the market is flushed with information about the merging hospitals. Public announcements of the intention to merge, media coverage, and various stakeholders' voices provide malicious actors with more information about merging hospitals. From the malicious actors' perspective, merging hospitals become enticing targets. Such heightened external threats may come from the surged visibility. Changes during mergers are an opportunity to study malicious actors' reactions to the first factor, online visibility.

For malicious actors, merging hospitals may be attractive attack targets since the consolidated firm has a bigger market share and, thus, more data to harvest. The increased market share suggests a higher volume of sensitive patient information, making the merging hospital a more lucrative target. Additionally, larger mergers often involve larger financial transactions, which may encourage attackers to attempt ransom demands. The theory of the economics of cybersecurity argues that a company attracts at least its market share of attacks (Arce 2018). As hospitals grow in size in mergers, their external threats of being targeted by malicious actors can increase.

Not all data breaches are caused by external threats; some stem only from internal vulnerabilities. Internally, mergers can create new vulnerabilities within hospitals. A significant challenge is the technical

difficulties that arise when integrating different information systems, such as misconfigurations during the harmonization of electronic medical record systems or frictions in adopting new digital protocols. Furthermore, the process of merging disparate systems often requires extensive reconfiguration, leading to potential oversights and weaknesses as the organization charts and controls structure change. The technical hurdles introduce security gaps.

Another factor is management skills and experience in handling the threats and challenges of mergers. Mergers require a special set of management skills beyond routine operations. Organizations with strong risk management backgrounds and previous merger experience are better positioned to manage threats and challenges from health IT. Effective management practices can mitigate potential risks and streamline the integration process.

The last factor is the health IT resources. The scale of resources can counteract the intensified internal vulnerability challenges. Hospitals operate on a thin margin, so it is essential to investigate whether hospitals possessing a larger scale of resources have substantial comparative advantages as data breach costs escalate.

Considering the malicious actors is the key to investigating why data breach rates double during mergers, but such consideration introduces challenges. Data breach risk management extends beyond the implementation of privacy-enhancing technologies. While these technologies—such as encryption, access controls, and data anonymization—are essential components, effective data breach risk management requires more. One of the main differences between the economics of cybersecurity (Mitra and Ransbotham 2015, Anderson 2020, August, Dao and Niculescu 2022) and the economics of privacy (Acquisti, Taylor and Wagman 2016, Goldfarb and Tucker 2024) is the analyses of economic factors for strategic encounters with malicious actors. Without observing the motivation and behaviors of the malicious actors, empirical analysis of the reason is challenging, and my research design tests how mergers affect malicious actors' behavior and affect the final data breach results through indirect approaches.

In detail, for the external threat factor of online visibility (factor 1), an analysis comparing highly visible mergers to mergers without such visibility shows that online visibility plays an important role in data breach increases. Similarly, an analysis compares merging large and small target hospitals when they both face high visibility to analyze attractiveness (factor 2). In other words, holding visibility equal, the comparison examines whether larger mergers are more attractive. There is no evidence that acquiring a larger target hospital results in a higher data breach rate.

Similar to external factors, without observing technical challenges, management skills, and security resources, this study provides suggestive results from indirect research designs. The results show that large multi-hospital health systems struggle with technical challenges (factor 3), even when equipped with large scale of resources for security (factor 5). Publicly traded hospitals have better security outcomes during mergers, even when facing the same level of external threat. The result suggests that publicly traded hospitals' more advanced management skills (factor 4) reduce data breach risks.

After all, more than technology management and internal vulnerability control, advancing cybersecurity management practices means incorporating strategic thinking by considering external threats. Healthcare leaders should not doubt that advancing management practices reduces data breach risks in today's challenging environment. Further discussion of the five factors are in Section 2.1, and empirical analyses are in Section 6.

Literature and Contribution

This study contributes to three streams of literature. The first stream focuses on the complementary effect of organizational capital on digitization. "Organizational capital and organizational structure" (Brynjolfsson, Hitt and Yang 2002, Goldfarb and Tucker 2019) includes business process redesign, co-invention of new products and business models, and investments in human capital. Organizational capital is regarded as the reason why American companies are more ready for IT adoption and are more advanced in their digital transformation (Brynjolfsson et al. 2002, Bloom et al. 2012, Goldfarb and Tucker 2019). There is empirical literature focuses on quantifying costs of health IT (Dranove, Forman, Goldfarb and Greenstein 2014) and policies' impacts (Miller and Tucker 2009, Angst and Agarwal 2009, Adjerid, Acquisti, Telang, Padman and Adler-Milstein 2016). The vast majority of literature focuses on the value of health IT in enhancing performance (Dobrzykowski and Tarafdar 2015, Eftekhari et al. 2023), improving decision-making (Ransbotham et al. 2021), and organizational efficiency (Janakiraman et al. 2023, Ganju et al. 2022). Instead of focusing on what having health IT means, I focus on how hospitals make health IT work (Devaraj and Kohli 2000, Menon and Kohli 2013, Bardhan, Bao and Ayabakan 2023). This study contributes to the literature by investigating the contribution of health IT organizational capital to reducing data breach risks during hospital mergers. It provides insights into whether management factors facilitate Health IT success by showing certain types of hospital mergers struggle less with data breach risks.

The second stream of literature focuses on the economics of cybersecurity, which examines equilibrium security behavior by considering the motivations and strategies of the malicious actors (Gordon and Loeb 2002, Mitra and Ransbotham 2015, Arce 2018, Clement and Arce 2024). Incorporating an attacker's perspective nurtures a more comprehensive understanding of information security issues (Mahmood, Siponen, Straub, Rao and Raghu 2010). Much of the empirical work focuses on consequences by quantifying the economic effects of a breach on negative stock price reactions (Campbell et al. 2003, Acquisti et al. 2006, Islam et al. 2022), credit financial resources reactions (Huang and Wang 2021, Blascak and Toh 2022b), publicity cost (Bana, Brynjolfsson, Jin, Steffen and Wang 2023), and long-term effect on competition (Acquisti and Varian 2005, Kwon and Johnson 2015, Bonatti and Cisternas 2020, Chen et al. 2022). A limited number of prior works focuses on consequences of health data breaches such as business disruption (Neprash et al. 2022), emotional reaction (Shandler and Gomez 2022), and loss of life (Choi and Johnson 2019), as listed in Table 1. Instead of focusing on the consequences, this study focuses on the economic causes by

Table 2 Conceptual Framework of Five Hospital Data Breach Risk Factors

No.	Factors	Explanation	Big Merger deals	Publicly Traded Hospitals	Large Health Systems
1	Online Visibility	The extent to which a hospital's information is accessible online affects its exposure to external threats. An increased online presence can make a hospital more noticeable to malicious actors.	✓	✓	
2	Attractiveness	Larger hospitals are more attractive targets for cyber attacks due to malicious actors' potential higher financial gains from harvesting more data.	✓		
3	Technical Challenges	Misconfigurations in health IT infrastructure and weaknesses in risk control management arise.			✓
4	Management Skills	The ability of hospital management to organize resources and implement data breach risk management practices. Hospitals with more risk management experience can mitigate data breach risks.		✓	
5	Scale of Resources	The hospital's capacity to manage data breach risks is bounded by the scale of its resources dedicated to health IT.	✓		✓

providing new empirical evidence for the association between economic motivation and data breach risks (Anderson 1993, Arce 2022) to support the hypothesis that economic factors matter in data breach risks. Emerging literature focuses on the economic motivation and behavior of the malicious actors through analyzing hacker community (Li and Chen 2022, Ebrahimi, Chai, Samtani and Chen 2022, Samtani, Chai and Chen 2022, Chua 2023). Instead of observing the behaviors, this study takes advantage of changing management and economic factors during mergers and records the effect of malicious actors' reactions. In detail, Mitra and Ransbotham (2015) shows that full disclosure of information on technical vulnerability details accelerates the diffusion of attacks, while this study shows that an abundance of online visibility about hospitals increases attacks.

The third stream is a nascent literature on healthcare information system integration (Zaheer and Venkatraman 1994, Tanriverdi, Rai and Venkatraman 2010, Tanriverdi and Uysal 2011) and multi-firm information system coordination (Brynjolfsson, Malone, Gurbaxani and Kambil 1994, Du 2015, Tanriverdi and Bülent Uysal 2015), with recent emphasis on long term effect on healthcare improvement (Tanriverdi and Du 2020) and the role of emerging technology (Du and Tanriverdi 2022). This research stream focuses on hospital production and the capital market's negative reactions to technical challenges during information system integration. To understand the challenges in health IT management, considering the growing large multi-hospital health system is necessary. This study contributes to the discussion by demonstrating the immediate data breach risk consequences for buyers with different capabilities.

2. Conceptual Framework and Background

To analyze why mergers increase data breaches, including the increases caused by malicious actors, I first present a framework outlining the management and economic factors that influence data breach risks. Afterward, I discuss why hospital mergers provide a unique opportunity to study the management and economic factors and how the factors change during the merger process.

2.1. Mergers and Data Breach Risks: Conceptual Framework of Five Factors

A framework organizes unobservable factors complicating the interpretation of indirect evidence. The thought experiment in this section summarizes economic and management factors of data breach risks into 5 categories, as listed in Table 2, from the perspectives of both the defenders and the attackers (i.e., malicious actors). It is based on a heuristic model of Gordon and Loeb (2002), a seminal treatment of cybersecurity expenditure. At its foundation, the Gordon-Loeb model differentiates between vulnerability and security. A hospital becomes more vulnerable if management neglects IT management, such as failing to update software (Murciano-Goroff, Zhuo and Greenstein 2024). The data breach risks also arise from malicious actors' intensified attacks. Accordingly, the probability of a data breach is a function of internal vulnerability and external threats. Not all data breaches involve external threats. External threats are zero for insider misconduct that does not relate to malicious actors at all. For example, a lost hard drive is insider misconduct solely because of internal control mismanagement and not initiated by external threat factors. Internal vulnerabilities and external threats fluctuate over time. At times, hospitals become more attractive to malicious actors, while at other times, they face greater issues with mismanaged risk controls.

During a merger, the landscape of external threats evolves, with different stages presenting unique challenges. First, mergers often heighten a hospital's online visibility since news about the merger is announced publicly before the deal is finalized, making online visibility the first factor. Note that when considering information, the external threats are not beyond the control of the defenders, who can decide how much the malicious actors know of them from more online visibility. Managing data breach risk does not only mean advancing technology management and reducing internal vulnerability.

The attractiveness of a hospital as a target fluctuates over time, and mergers can increase this attractiveness because they often lead to a larger market share and more valuable data to exploit. For example, a larger merger deal can be more attractive than a smaller merger deal. Note that the larger merger deal also may induce a higher online visibility. Thus, to analyze the effect of attractiveness, controlling for the first factor, heightened online visibility, is necessary. This increased attractiveness is the second external threat factor to consider, and the research design needs to control for the first factor when analyzing the effect of this second factor.

Not all data breaches involve external threats from attractiveness or online visibility. The third factor to consider is internal vulnerability due to technology challenges. During a merger, technical difficulties often arise not only from existing technology debts and integration but also from organization chart changes and control restructuring around digital transformation, leading to misconfiguration, oversights, and mistakes. For example, post-merger technical challenges arise from several sources, such as harmonizing two different electronic medical record systems, integrating various software platforms, initiating new digital transformations within the acquired hospital, adapting to new protocols, and re-architecting network infrastructure. The technical difficulties contribute to increased internal vulnerabilities once the merger deal is

finalized, highlighting the complexity of maintaining robust data breach risk control right after signing the merger deal. In other words, technical challenges intensify in a specific stage of mergers.

Effective management skills can help reduce data breach risks. The fourth factor to consider is the quality of management skills. The managerial skills extend beyond routine business tasks and involve specific decisions and strategies. The unique set of management skills, such as past merger experience, general risk management abilities, and a proactive stance by hospital leaders, may contribute to a large comparative advantage due to the escalated data breach costs by reducing data breach risks. Without observing the specific management skills, this study focuses on whether some hospitals can mitigate the data breach risks when facing intensified external threats.

The fifth factor is the scale of resources. Besides health IT, finance planning, price negotiation, due diligence auditing, and legal compliance need management attention and financial resources. Thus, during a merger, resources are often spread thinly, as management must balance the demands of the merger process while maintaining robust cybersecurity measures. The scale of resources bounds health IT management; it plays an even more vital role during mergers because many other aspects of a merger require management's attention and determine whether the merger is successful.

Different stages of mergers affect various parties' motivations and behaviors, which affects data breach risks. Next, I introduce more background on hospital mergers, including specific kinds of mergers related to the fourth and fifth factors. This framework classifies them into five factors for systematic tracking. Verifying that mergers cause data breaches to increase, in turn, means that the economic and management factors matter.

2.2. Hospital Merger Processes in the U.S.

The merger process is a unique opportunity to study how management conquers internal vulnerability with limited resources and how external threats change with attractiveness and online visibility. First, the empirical analysis of data breach risks is challenging because data breaches are rare events. Hospital mergers in the U.S. have been active because of financial distress and the pursuit of strategic partnerships. In 2010-2022, there has been more than 1,200 hospital mergers. Hospital mergers are a rich opportunity because of the large volume of merging activities and the increasing cybersecurity threats to the healthcare industry. Second, hospital mergers take time, from the announcement of the intention to merge to the completion of the information system integration. The extended time allows for comparing changes in data breach probability over time. Various stages of mergers also offer opportunities to focus on temporal factors. Third, hospital mergers can also take various forms. Different mergers are heterogeneous with regard to the many factors that shape the data breach risks. For example, an increasing number of mergers are being performed by large or experienced multi-hospital health systems with large-scale resources and rich risk management experience. Large volumes of various forms of mergers are opportunities for analyses on subsamples to

isolate different economic and management factors with meaningful statistical inferences. Mergers are a rich setting for studying the effects of economic and management factors on data breach risks.

Specifically, multi-hospital health systems play a crucial role in the U.S. healthcare landscape. Multi-hospital health systems control more than half of the U.S. hospitals: according to Becker's Hospital Review, at the end of 2023, more than 20 large multi-hospital health systems contain more than 40 hospitals, and even larger health systems such as HCA Healthcare, Ascension, and Trinity Health each control over 100 hospitals. With centralized management, the health systems aim to reduce costs. To facilitate centralized management and easier health information exchange, they require harmonized electronic medical record systems for the newly acquired member hospital (Gaynor et al. 2021). Harmonizing the electronic medical record systems takes substantial work, from rearchitecting the network infrastructure to data migration and integration. New privacy and cybersecurity protocols also require extra work if the merger is across states. Multi-hospital health system merger deals are an opportunity to understand the technical challenges. Large multi-hospital health systems also possess greater bargaining power with insurance companies and enhanced operational efficiency. They may have more resources for health IT management. Multi-hospital health system merger deals are also an opportunity to study the effect of the scale of resources.

Another type of merger involves publicly traded hospitals. Like the rest of the industrialized countries, some U.S. hospitals are government-owned or non-profit organizations. However, some for-profit hospitals seek access to capital and liquidity trade on the stock markets, such as the New York Stock Exchange and the National Association of Securities Dealers Automated Quotations. Given that disclosure of data breaches causes negative stock price fluctuations (Campbell et al. 2003, Chatterjee and Sokol 2019), publicly traded hospitals may have higher incentives to mitigate data breach risks. Owned by shareholders, publicly traded hospitals fall under shareholders' and boards of directors' oversights and may have more robust risk control skills. At the same time, the Securities and Exchange Commission also imposes more disclosure rules on publicly traded hospitals, leading to higher online visibility. Publicly traded hospital merger deals are an opportunity to understand the effect of management skills on data breach risks, and controlling for online visibility is necessary.

Despite the rich opportunities in analyzing hospital mergers, several challenges exist.

First, using mergers as a shock in causal design is challenging. A merger is a selection process. A comparison of the data breach risks of merging hospitals with the data breach risks of never-merged hospitals introduces selection bias. Merging hospitals have unique financial and organizational characteristics compared to never-merged hospitals, and the comparison is problematic if the control group is the never-merged hospitals. Instead of comparing merged to never-merged hospitals, the main research design focuses on comparing ongoing mergers with future mergers to analyze the treatment effect of merger times.

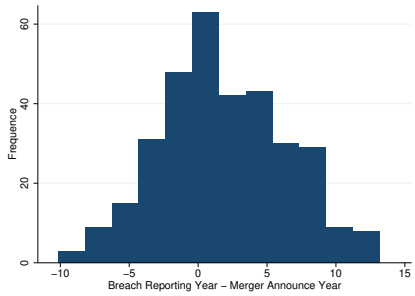
Second, even though the merger process takes a long time, the data breach probability in a short time of observation is still a rare event with large variation. For the main result, I do not focus on the average

effect of each quarter. Instead, I add the quarterly effects together to gauge whether the merging time as a whole has more breaches than the future mergers in the control group. Using a two-year aggregation period around the merger, instead of focusing on individual quarters, provides a statistically meaningful comparison, particularly for the mechanism analysis where my sample is further divided. For different stages of the merger, I include an event study as a supplement to validate the results, though I anticipate and do observe greater heterogeneity when comparing quarterly data separately in the event study. At the same time, individual-level fixed effects may not be informative for the rare dependent variable. In the robustness checks, results without individual fixed effects do not change the main conclusion.

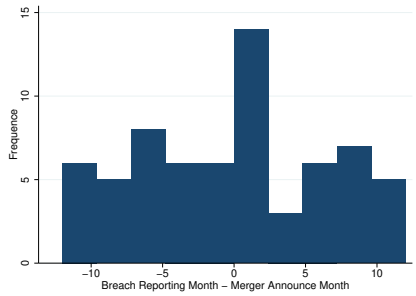
Third, another challenge is the heterogeneous merger processes. Due to negotiation and compliance requirements, a hospital merger deal can take more than five years from disclosing the intention to closing the deal. For example, in Massachusetts, Beth Israel Deaconess and Lahey Health first expressed the intention to merge in 2013. The negotiations experienced delays, and it took considerable time before the merger deal was signed in 2019. If a merger was first initiated seven years before the merger deal closed, attributing all data breaches during that period to the merger is challenging, given the presence of other confounding factors. Thus, in the main analysis, I focus on the immediate year before and the year after signing the merger deal. Another advantage of using the year before signing the merger deal, rather than a longer period, is the elimination of the inverse causation concern because hospital mergers cannot be completed within one year owing to the time-consuming due diligence process, extensive negotiations, and the need to comply with complex federal and local government regulations (including state attorney general reviews, Certificate of Need applications, state pre-merger notification periods, and filings with the Federal Trade Commission or Department of Justice for review). For robustness against alternative explanations, various changes in the time windows do not influence the results, and an event study is presented to show the trend of the effect for each quarter separately. The next section discusses the data resources and shows the plot of the distribution of data breaches reported around the merger signing date for ten years before to fifteen years after the merger signing date.

3. Data and Sample

To answer the question of whether mergers cause more data breaches, I combine two quarterly datasets for the main analysis and incorporate two additional datasets for robustness checks and mechanism analysis. The first dataset consists of merger deals closed in 2009-2022 obtained from a proprietary merger data platform, Levin's Associates. The advantage of the data is merger records include information such as the hospital's size, market visibility, and profitability. Another advantage is that the data includes the date when the merger deal was signed, allowing for a more granular analysis of the hospital's experience surrounding the signing date. The second dataset is the U.S. Department of Health and Human Services, Office of Civil Rights' archived healthcare breach reporting data for 2010-2022. The two data sets are merged under



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



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

Figure 1 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 from Levin's Associate and DHHS 2010-2022.

hospital names. Mergers acquiring multiple target hospitals in Levin's data are each manually separated into individual observations to merge the data by names, with a unique merger number for each target hospital. Specifically, to determine which hospitals or multi-hospital health systems report a data breach during mergers, the names of the target, buyer, and seller are matched to the reporting entity for data breaches. Such matching includes data breaches that occur before or after a merger closes. I manually confirm the matching with further details for the matches where both merger and data breach data detail the state or the state and the city of the hospital. For each match, the dependent variable data breach equals one for the matched merger, and I calculate the days between the merger signing date and the data breach reporting date. The difference between the merger signing date and the matched data breach reporting date is plotted in Figure 1a. As discussed in Section 2.2, I limit my analysis of the merger impact to data breaches that occurred within one year before or after the merger closure date, as shown in Figure 1b. Note that both graphs show slightly skewed distributions towards the post-merger period, meaning that more data breaches are reported after signing the merger deal. Overall, from Figure 1a, there is a clear pattern that data breaches are more frequent near the merger signing date compared to periods further from the merger signing date.

Figure 1a also informs the elimination of alternative explanations. An alternative explanation for surged data breaches during mergers is that mergers do not cause more data breaches, but more data breaches are discovered through due diligence checks, although due diligence checks on IT systems have only recently emerged following an increase in hacks over the past five years and my findings cover a more extended period. The distribution of data breaches around merger time further supports the notion that this alternative explanation can be eliminated. Specifically, Figure 1a shows no abrupt decrease in breaches reported after the merger deal was signed, but more data breaches were reported far beyond the time of due diligence checks. Similarly, another alternative explanation is that hospitals are more motivated to intentionally report

data breaches around merger time for compliance reasons. Figure 1a shows a gradual increase in data breach rates since ten years before the merger deal was signed. The smooth distribution suggests a smaller possibility for this alternative explanation. The merger process is not predictable five years before the merger deal is signed, and it is impossible that more data breaches reported five years ago are intentionally timed. The same with the increase in data breaches during the post-merger years, year 1 to year 5, intentional reporting can not be an explanation. On the contrary, instead of the possibility that hospitals intentionally report more data breaches for compliance reasons before signing the deal, the skewed distribution suggests there may be reporting delays. The possible biases from the delays are indeed considered in Section 6.5. More discussions considering the alternative explanations are in mechanism analyses in Section 6 and event studies in Section 5.2. Note that the volume of data breaches reported around merger time is large, and the result is also not driven by several data breach events. To further validate the results against the alternative explanations, Appendix Section A.11 symmetrically and asymmetrically change the definition of "during merger" time and shows that the conclusion in the main analysis is robust.

An additional data is the Centers for Medicare & Medicaid Services Hospital Care Compare dataset on hospital information for robustness check. The advantage of incorporating the data is that they provide quarterly hospital information that allows for additional control for never-treated hospitals. An advantage of the robustness check is that it allows the inclusion of a different group of binary control variables representing comparative levels of image availability, patient experience, timeliness, safety, effectiveness, mortality, and readmission rates relative to the national average. Another advantage is including never-treated firms allows the analysis to extend beyond 2020 when the mergers are too recent to find any pre-treated group. Including the never-treated hospitals that never merged during the observational period helps with checking the robustness of different control group constructions. Details are in Appendix Section A.2.

The quality of the HHS data breach reports is considered. The official reporting period for data breaches in healthcare began in 2009 for the HHS data; however, only a limited number of reports were produced during the ramp-up period with possible delays. Therefore, they were removed to ensure accuracy. Compared with other data breach information used in the literature, such as the Privacy Rights Clearinghouse or the Identity Theft Resource Center (Jiang, Khanna, Yang and Zhou 2024), the advantage of the HHS data is that hospitals are bound by law to report breaches, and the data are audited by the Office of Civil Rights. Moreover, the HHS offers a paragraph detailing what helped in determining whether the breach relates to malicious actors, while the Identity Theft Resource Center data contain information on whether sensitive records are exposed or non-sensitive records are exposed and it is more suitable for investigating the consequences and harm. For robustness, I manually compared the Identity Theft Resource Center data for 2020-2021 with the HHS data and found no missed hospital data breach in the HHS report. Hajizada and Moore (2023) show evidence of other industries' under-reporting problems using the 2017-2022 Hackmaggedon data and found

no under-reports in HHS where the Hackmaggedon data report more than the HHS data. They also demonstrated there is no gap in ransomware attacks. It is reasonable that ransomware attacks are difficult to hide compared with internal misconduct. Neprash, McGlave, Cross, Virnig, Puskarich, Huling, Rozenshtein and Nikpay (2022) showed that for 82 hospital ransomware attacks and 461 ransomware attacks on other types of health service providers, there was an increase in delay in reporting during the pandemic. In pre- and post-merger studies, the delay affects the size of the effects. For example, some of the breaches in Figure 1b can occur before the merger signing date and can be reported after the merger signing date. Reporting delays can cause underestimated pre-merger effects and overestimated post-merger effects, but a short delay does not affect my main result since my observational unit is quarterly, and I do not include the pandemic period in the main analysis. I examine a two-year time window that leaves space for delays in reporting.

An advantage of the HHS data is its rich details on each data breach. I use the HHS detailed reports to separate hacks from other data breaches, which are insider misconduct. Insider misconduct is employee-related issues, including loss, theft, improper disposal, and impermissible insider access and disclosure that are not initiated by a malicious actor bringing in external threats. In contrast, hacks involve data breaches caused by malicious actors through techniques such as email phishing, malware, zero-day attacks, and ransomware attacks. Insider misconduct could occur because of 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 are indicative of management issues, and a well-established risk control procedure can reduce the likelihood of such incidents. I first rely on machine learning text analysis to separate hacks from insider misconduct, and then I hand-pick each one that is miscategorized.

4. Design and Empirical Method

To investigate the effect of merger timing in the baseline causal design overcoming challenges described in Section 2.2, this study implements stacked difference-in-differences (Deshpande and Li 2019). The stacked difference-in-differences method prevents the use of already treated units in comparison with newly treated units. The stacked difference-in-differences also addresses selection bias by using future mergers to represent what would happen if merging hospitals were not undergoing the merger process. With a control group for each staggered treatment that does not include the hospitals already treated, the stacked difference-in-differences method is one of the solutions developed in the past five years for combating biases from negative weighting in two-way fixed effect estimators for staggered treatments (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)).

In detail, all the merger deals are each treated group in a sub-sample, with a set of future mergers as control groups. The control groups include all the pre-treated hospitals that will encounter a merger deal at

least two years after the treatment group's merger signing date. For example, for a treated deal that occurred on July 31st, 2010, all the merging observations signed on or after July 31st, 2012, will form the pre-treated groups/control groups. In other words, for each treated deal that closed on t, the control/pre-treated group is all the merger deals that will close in time [t+2years, T]. The comparison is over the period of a two-year window for each deal, including the years before and after the treated group's merger signing date. The controls are deals signed in at least two years; thus, the gap in time guarantees that no hospital in the control group is treated in the two-year window. In other words, the 2-year gap ensures that the control group is not contaminated – the earliest control group is not treated (undergoing a merger). Thus, for each merger, the created dataset includes one treated group and a group of future mergers as controls. The created datasets are then stacked into one dataset for regression. As all the treated and pre-treated groups are stacked together, I 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 during the same period. The advantage of using pre-treated groups, which are hospitals that eventually engage in mergers, addresses the endogeneity problem. For comparison, the study also constructs an alternative dataset that includes the never-treated group and shows that the result is robust to changes in the control group construction (Appendix Section A.2, using the CMS Hospital Care Compare). The alternative method with never-treated also shows the effect of mergers persist to mergers in 2021 and 2022, which are too recent to have a non-contaminated pre-merger group and are not in the main analysis. For robustness, the study also shows the results for alternative time windows. The results on alternative windows are similar to the main result with two years. In addition, even with large variations, event study is shown for quarterly data breach risks during mergers.

The effects of the timing of the mergers are estimated using the following equation,

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

where $Breached_{i,m,t}$ is a binary result indicating whether any hospital i in deal m has reported a data breach in quarter t. $Treated_{i,m}$ is the indicator variable for the 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 merger closure date of the treated groups are recorded as one in the binary dependent variable. The coefficients of interest are the β_{τ}s. β_{τ} is the difference between data breach probabilities on treated and data breach probabilities on pre-treated hospitals τ quarters before or after the treated deal is signed. As discussed in Section 2.2, β_{τ} is shown in the event study, and the main result table displays $\sum_{\tau} \beta_{\tau}$. X_m includes the control variables. The target hospitals' bed counts, revenue, and EBITDA indicate the deal size and profitability. The listing status of the

acquirers and targets indicates the effect of risk management skills. Additionally, I include hospital and time fixed effects. Standard errors are clustered at the deal level. A robustness check on the regression without the individual-level fixed effect is in Section A.3.

The difference-in-difference analysis relies on several assumptions. The first assumption is that merger signing time is not confounded by factors related to data breaches. Mergers involve a selection process. However, the likelihood that the signing dates of all mergers over the past 10 years coincided with factors affecting data breaches is minimal. For example, profitability is a candidate factor affecting data breach risks, but profitability is less likely to relate to whether a merger deal is signed in July or November. On the contrary, if the treatment is not merger time but whether the hospital is merged or not, the treatment is not random regarding profitability, as many mergers are from the bankruptcy courts. In the current research design, both treatment and control groups are mergers to be signed, and the difference is the merger time. Furthermore, the control variables eliminate alternative explanations by considering what may determine the merger signing time. In the previous example, in case profitability also affects the merger signing dates, I include revenue and EBITDA control variables. Similarly, if the size of the merger target is associated with both the signing date and the attractiveness affecting the dependent variable, including the target hospitals' bed counts is necessary. The listing status may also link to the length of procedures before signing the deal, so I include the listing status of the acquirers and targets. For other unobservables, hospital and time fixed effects are included. Thus, the exogenous treatment assumption is fulfilled in the current research design. Similarly, future mergers better represent what would happen if the merger date is not approaching, and using future mergers as the control group is an effort to fulfill the parallel trend assumption. In addition, there is no evidence of violation of the parallel trend assumption in event study graphs. The stable unit treatment value assumption requires the outcome of a unit only depend on its own treatment. The assumption for this study is that a sufficient number of malicious actors exist, and whether one hospital has data breaches does not decrease the data breach risks for other hospitals. Using all future mergers instead of only a subset-matched group as control means it is more reasonable to assume that the average cyber risk of a large number of future mergers does not depend on the treatment of one merger. Violation of the assumption introduces a positive bias to the estimators, but there is no evidence of an entry barrier to being a malicious actor. Further discussion on difference-in-difference assumption and robustness check can be found in Section A.7 and A.11.

5. Data Breaches During Mergers

This section presents the main results accompanied by event studies for mergers from separate years. For mergers in 2010-2020, data breach rates doubled during mergers, and the main effect is from increases in hacks relating to malicious actors. Suggestive evidence supports that economic and management factors determine data breach rates and is presented in Section 6.

Table 3 Effect of Mergers on Data Breaches

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Does mergers 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 on Pre-treated % Effect	2.68	3.22	3.20	3.22	3.24	3.22	3.22
Mean on Treated % Effect	4.97	6.06	5.85	6.06	6.11	6.06	6.06
Mean on Pre-treated Targets % Effect	1.96	2.32	2.31	2.34	2.32	2.33	2.33
Mean on Treated Targets % Effect	4.48	5.65	6.02	5.38	5.53	5.25	5.50
Mean on Pre-treated Seller % Effect	1.35	1.78	1.66	1.81	1.80	1.68	1.66
Mean on Treated % Effect Seller	7.10	9.03	7.79	9.35	9.09	9.86	10.14
Mean on Pre-treated Acquirer % Effect	1.94	2.39	2.38	2.36	2.40	2.36	2.40
Mean 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 mergers 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 signing deal m, and $a \in [0, 4]$ quarters. The treated groups comprise the hospitals that participated 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 standard errors clustered at the deal level are shown in parentheses.

5.1. Main Effect

Table 3 shows the initial results examining whether mergers cause more data breaches during mergers, with various control combinations. 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. The result is robust without the hospital fixed effect, as shown in Appendix Section A.3.

Hospitals undergoing mergers are twice as likely to experience a data breach than those in the pre-treated group. Specifically, Column 7 corresponds to the regression with all control variables. I observe a large positive effect on data breach probability from the merger process. Mergers result in a 4.20 percentage points increase in data breaches, from 3.22% to 6.06%, statistically significant at the 5% level.

With different combinations of control variables, the effects across the columns are consistent, ranging from 3.61 to 4.24 percentage points, increasing from 3% to 6%. Columns 1 to 6 pertain to individual control variables. The alternative outcomes are shown for a larger sample size (columns 1, 3, and 5) because of the

availability of data on the control variables and for a constant sample size (columns 2, 4, and 6). 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 the substantial increase in data breaches, the effects of the control variables are inconsistent. For Columns 2, 4, 6, and 7 with the same sample sizes, the target hospital's pre-merger EBITDA is negatively correlated with the data breach probability, while the target hospital's pre-merger revenue is positively correlated with the data breach probability. At the same time, the effects of the target hospital's bed count are inconsistent. The inconsistent effect needs further analysis because it relates to multiple factors that determine data breach probability, such as factor 1, online visibility determining whether the merger deals are noticeable to the malicious actors, and factor 5, the scale of resources for security investment from the defenders – hospitals. The five factors are analyzed separately in the next section. Notice that the public trading status also has inconsistent effects. For Columns 2, 4, 6, and 7 with the same sample sizes, public acquirers have more data breaches, whereas public target hospitals face an inconsistent effect. The lack of precise estimates of public trading status reflects the fact that publicly traded companies may have more online visibility, increasing their external threats, while their more intense regulatory environment benefits their risk management skills. Further details are in Section 6.3.

The results presented in Table 3 use the main model to demonstrate whether mergers cause additional data breaches and show that data breach rates double during mergers. The results raise questions as to why mergers cause more data breaches, whether the effect changes over the 2010-2020 observational window, and how different hospitals cope with the risk. Before analyzing the reason for the increase in data breaches, I first show the importance of considering both external threat factors and internal vulnerability throughout the entire merger process.

5.2. Decomposing the Effect: Insider Misconduct v. s. Hacks

To study the rare event of data breaches, the main analysis compares merging hospitals with future mergers and shows that the chance of a data breach in the two-year merging period as a whole is twice as large. This section decomposes the aggregated effect of doubled data breach rates in the main analysis, first with different types of data breaches separated and then with an event study.

Figure 2 separates insider misconduct from hacks, which are data breach activities by malicious actors, using the method described in Section 3. Figure 2 shows the necessity for taking the perspective of malicious actors when analyzing the external threats, as most of the increase in data breaches during mergers are increases in hacks. For further detail, Table 6 in the Appendix shows the increase in hacks for mergers in the last five years, including ransomware attacks and phishing attacks, which happened more prior to the merging signing date than afterward, and Appendix Section A.1 discusses how ransomware attacks on hospitals intensified. The escalated ransomware attacks during mergers are not possible from the alternative

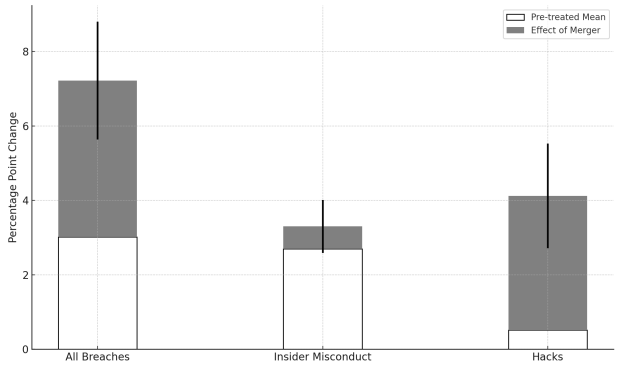


Figure 2 Percentage Point Change: Effect of Mergers on Different Types of Breaches

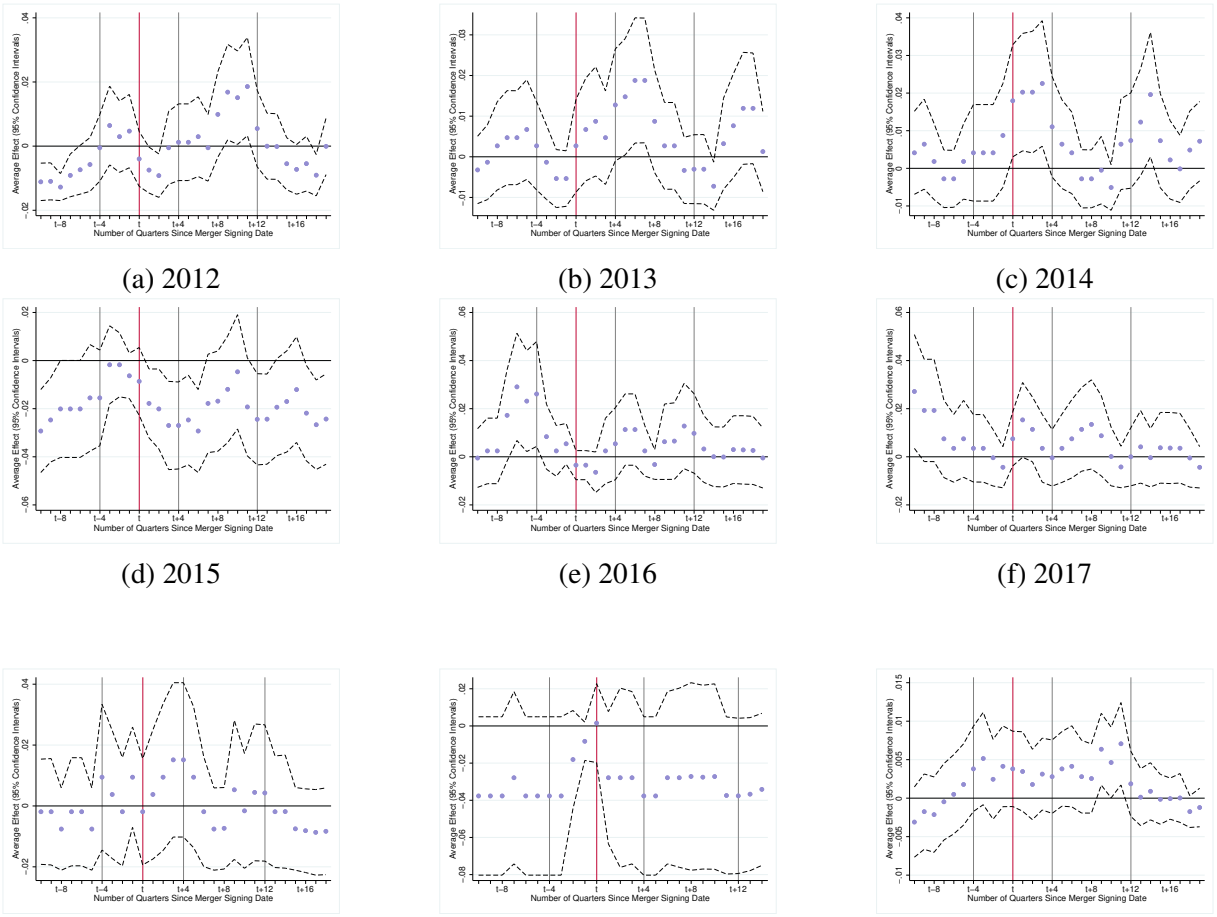
Notes: The figure shows the baseline means and the percentage point effects in Table 3, and further divide data breaches to insider misconduct and hacks. Data source: Levin's Associates and DHHS 2010-2022.

explanation that due diligence during mergers discovers more data breaches. The reason is that malicious actors behind ransomware attacks aim to be noticed quickly rather than remain hidden until discovered. After all, considering external threats from malicious actors is the key to mechanism analysis.

Figure 2 shows that insider misconduct - data breaches unrelated to malicious actors - does not increase much during mergers even though the merger time is chaotic and managers' attention is distracted. Were hacks the predominant reason for data breaches during the 10-year-long observational window? To answer this question, I use event study. An event study is not ideal for analyzing rare events like data breaches. However, even with the expectation that the variance may be high, event study plots provide a unique perspective for understanding the different stages of mergers and provide directions for the next step of the analysis. The event study also offers further evidence against alternative explanations by demonstrating no clear patterns of intentional timing in reporting data breaches. Specifically, I conduct separate event studies on insider misconduct and hacks between 2012 and 2019.

The following two conclusions stem from the graphic analysis. First, insider misconduct, which does not relate to malicious actors and solely depends on hospitals' management, was once a reason for the increase in data breaches during mergers but has become less of a problem over time. Specifically, Figure 3 shows 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 thereafter. One interpretation is that over the years, hospitals have become more capable of reducing mismanagement and reducing the number of insider misconduct.

Second, examining the data breaches over time, I find the magnitude of hacks has increased. As hacks are rare events, Figure 4 shows the results for different combinations of years. The result indicates that the risk of hacks during mergers intensified over time. Specifically, in Figure 4, the highest interval of the probability of hacks remains at 2 percentage points for 2012-2019 and 2014-2019, then rises to 4 percentage points in 2016-2019, and increases to 10 percentage points in 2018-2019. This result aligns with anecdotes



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

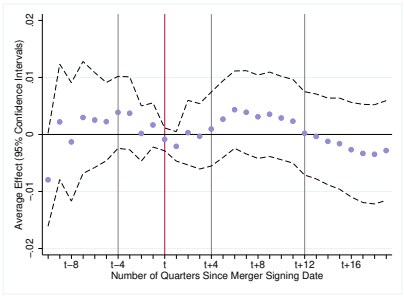
(d) 2015 (e) 2016 (f) 2017

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

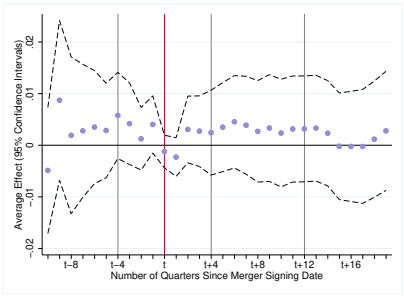
Figure 3 Dynamic Event Study: Insider Misconduct

Notes: The figures depict the coefficients for the primary regression on insider misconduct with lead and lag indicators up to two and a half years before or five years after a merger that occurred in different time frames. This event uses all future mergers over 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. Panels A to H represent the time frames 2012-2019 mergers, separately. The final panel includes the entire study period. The 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 operational integration starts. $t-4$ is assumed to be when the treatment starts in the main analysis. I compare the main analysis in the two-year time window, $t-4$ to $t+4$. $t-4$ to $t+12$ is the alternative analysis in Table 12. The figures show how insider misconduct has decayed as a problem in recent years. Data source: Levin's Associates and DHHS 2010-2022.

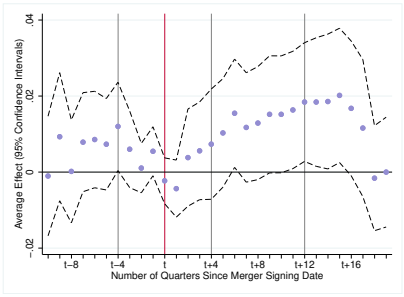
and industry reports that hacks are an increasing threat and confirms the importance of adopting the lens from the economics of cybersecurity and considering external threats. Merging hospitals should be vigilant, as early preparation with increased security investment and advanced management practices is increasingly essential for achieving successful merger synergies, especially given the potential for hacks before full operational integration is achieved.



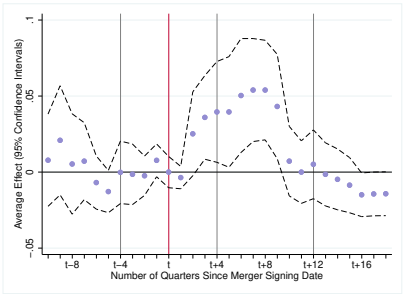
(a) Event Study Over 2012-2019



(b) Event Study Over 2014-2019



(c) Event Study Over 2016-2019



(d) Event Study Over 2018-2019

Figure 4 Dynamic Event Study: Insider Misconduct and Hacks

Notes: The figures depict the 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 after 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, whereas Panel B displays data from 2014 to 2019. Panels C and D represent the time frames 2016 to 2019 and 2018 to 2019, respectively. Specifically, it includes mergers that are at least two years but less than five years in the future. On the contrary, Figure 4d includes all future mergers in at least two years as control. The 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 operational integration starts. $t-4$ is assumed to be when the treatment starts for the pre-signing period in my analysis. $t-4$ to $t+4$ is the two-year time window in which I compare the main analysis. $t-4$ to $t+12$ is the alternative analysis presented in Table 12 in the Appendix.

In addition, The event study graphs align with the distribution plot in Section 3 and provide additional evidence to remove alternative explanations by showing no apparent patterns of intentional timing on reporting data breaches.

Overall, the event study indicates a decrease in certain risks of insider misconduct while pointing to the emerging challenges of immediate and more severe hacks that deserve attention. Insider misconduct was once a reason for increased data breaches during mergers.

6. Mechanisms

The analyses above show data breaches double during mergers. The discussion includes consideration of alternative explanations. Separating hacks from insider misconduct shows the necessity to consider malicious

actors. Additional analysis in this section investigates why mergers cause more data breaches, focusing on the economic and management factors.

The complexity of the merger process, with a range of varying management and economic factors—particularly external threat factors—makes it challenging to pinpoint the underlying reasons. To track the management and economic factors, the conceptual framework in Section 2.1 organizes the reasons surrounding five categories. The discussion includes three internal vulnerability factors and two external threat factors. External threats emphasize how mergers increase a hospital's attractiveness and online visibility. The intensified internal vulnerabilities are from post-merger technical challenges, mitigated by management skills and bounded by the scale of resources.

The entangled external and internal factors are difficult to separate. For example, buying a big hospital may mean that the merger has a larger attractiveness, which increases data breach risks, but it also may mean that there are more resources for security management and a bigger scale of resources, which reduces the data breach risks. Similar to a bigger deal, multi-hospital health systems possess a larger scale of resources. However, multi-hospital health systems can encounter more technical challenges during the post-merger time. The analyses address the complexities by controlling for other interactive factors. Specifically, the analyses start with the effect of online visibility in Section 6.1, which is controlled when analyzing attractiveness in Section 6.2 and management skills in Section 6.3. Technical Challenges are controlled in analyzing the scale of resources in Section 6.4.

6.1. Pre-merger Online Visibility

First, I investigate the effect of intensified online visibility on merger deals. Specifically, I focus on the subset of the sample with mergers receiving significant online visibility one year before signing the deal to show that pre-signing visibility changes the pre-signing data breach risks.

An additional data source measures the online visibility for this mechanism analysis. I incorporate daily Google Trends scores of the target hospitals' names for the year before signing the merger deal and the year after signing the merger deal for the target hospitals to measure changes in online visibility. Target hospitals' name is used because Google Trends scores depend on a larger size of the search beyond a threshold, and target hospitals' names plus the term "merger" (or other alternatives such as "acquisition", "acquirer", and "bought") most times do not return Google Trends scores. The sample is divided into two groups. The sample with high pre-merger online visibility includes mergers with the highest monthly mean Google Trends score during the third or fourth quarter before signing the merger deal, compared to other quarters in the merger process. In this way, the analysis tests whether online visibility at the beginning of the merger process is a factor for increased data breaches later during mergers.

To examine the effect of increased online visibility in the third or fourth quarter before a merger deal is signed, I focus on the following two quarters. In this way, the increased online visibility happens before the

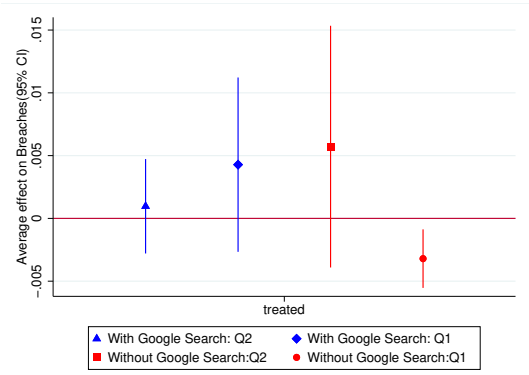


Figure 5 Active Pre-signing Search: Pre-signing Breach

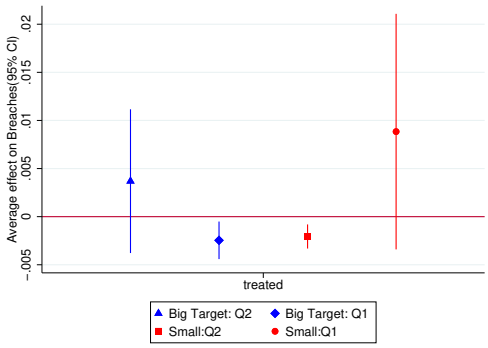
Notes: The figure displays the coefficients for the main regression on all data breaches (insider misconduct and hacks) reported in the two pre-signing periods separately. The first period, Q2, is the second quarter before signing the deal. The second period, Q1, is the quarter immediately after, which is the first quarter before, the deal was signed. The triangular knob on the far left represents the mean treatment effect on pre-signing breaches in the sample with an active pre-signing search. The diamond knob in the middle left represents the mean treatment effect on pre-signing breaches in the next quarter for the sample with active pre-signing search. Squares and circles represent breaches in these two quarters within hospitals without an active pre-signing search. The bars indicate 95 percent confidence intervals. The control variables include the target hospital's bed count, the public trading status of the target and buyers, and hospital and time fixed effects. The standard errors are clustered at the deal level. Active pre-signing search means having the highest monthly mean one year before signing the deal during the period $[t4, t3]$, which corresponds to 7-12 months before signing the merger deal. The graph shows that the first quarter after signing the merger deal, $t1$, is when the visibility on merging hospitals has a different effect. Date t indicates when siging deal m. Data sources: Levin's Associates, Google Trends, and DHHS 2010-2022.

period I study. The same applies to the next two sections, where I control for the surged online visibility to isolate the effect of other factors. The analyses focus on the two quarters after the surged online visibility.

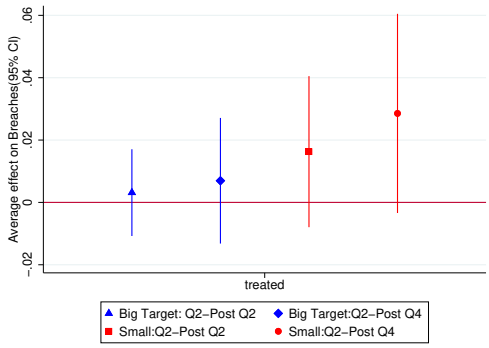
Figure 5 illustrates the immediate effects of online visibility. The first group includes merger deals with the highest monthly mean Google Trends score for their target hospitals' names during the third or fourth quarter before signing the merger deal. The treatment effect during the subsequent two quarters is displayed for each group. For merger deals that receive intensified online visibility, the pre-signing data breach risks in the quarter immediately before signing the merger deal are higher than those without such visibility. Note that there is a significant decrease in data breaches without such visibility.

By contrast, pre-signing online visibility does not affect post-signing data breach risks. Figure 16 in the Appendix shows the difference does not persist beyond the merger signing date.

The management implication from the result is that managing data breach risks is not only about managing internal vulnerability in health IT systems. In addition to marketing purpose (Salge, Antons, Barrett, Kohli, Oborn and Polykarpou 2022), managing online presence means adopting a strategic view and controlling external threats.



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



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

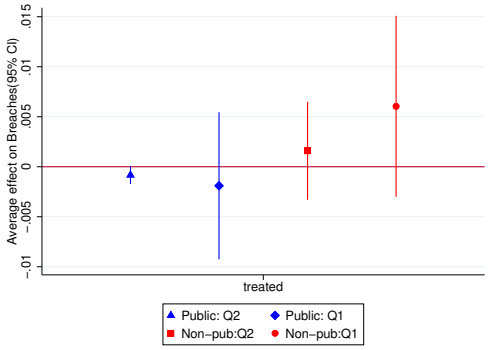
Figure 6 Active Search: Big/Small Deal Data Breach

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

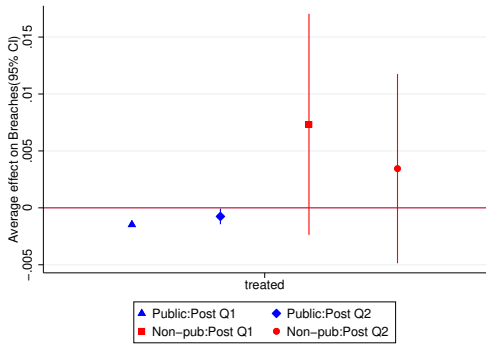
6.2. Attractiveness of the Larger Mergers

This section focuses on the second external threat, attractiveness, by analyzing large hospital mergers. For larger mergers, it is difficult to distinguish the effect of online visibility from attractiveness. To control for online visibility and analyze attractiveness, I compare data breach risks facing high online visibility of large merger deals with those of small deals facing the same high online visibility.

Figure 6a and Figure 6b demonstrate that there is no significant effect of being large. The sub-sample of larger mergers is compared with other mergers, and only mergers with high online visibility are included for both groups. A merger deal is in the larger sub-sample when the target hospital's bed count is greater than the mean bed count in the whole sample. Specifically, Figures 6a and 6b display the data breach event study for the two pre-merger quarters and two post-merger quarters when they receive high online visibility and



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



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

Figure 7 Active Search: Public/Non-public Data Breach

*Notes:*The figure on the left displays the coefficients for the main regression for all data breaches (insider misconduct and hacks) reported in two pre-signing periods separately for the deals that received more visibility in the third and fourth quarters $[t-4, t-3]$, before signing the deal. The first period, Q2, is the second quarter before signing the deal. The second period, Q1, is the quarter immediately after, which is the first quarter before, signing the deal. The triangular knob on the far left represents the mean treatment effect on pre-signing breaches with deals involving a publicly traded hospital. The diamond knob in the middle left represents the mean treatment effect on pre-signing breaches in the next quarter with deals involving a publicly traded hospital, either the buyer or the target. The squares and circles represent breaches in these two quarters within hospitals without publicly traded hospitals. The right figure displays the coefficients for the main regression on all data breaches (insider misconduct and hacks) reported in the post-signing Q1 and post-signing Q2. The triangle and diamonds represent mergers with publicly traded hospitals. The squares and circles represent breaches in these two quarters within hospitals without 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 signing the deal during the period $[t4, t3]$, which corresponds to 7-12 months before signing the merger deal. Date t indicates when signing deal m. The only difference between the two groups is whether they worked in a publicly traded hospital. The graph shows that even with more visibility, deals involving a publicly traded hospital are better off in both the pre-and post-signing periods. Data sources: Levin's Associates, Google Trends, and DHHS 2010-2022.

show similar patterns. Figure 6a shows that, facing high online visibility, larger merger deals have higher pre-merger data breach risks quicker than smaller merger deals, but on average, no evidence shows that pre-merger risks are different for bigger mergers. Similarly, facing high online visibility, the post-merger risks are not different, as shown in Figure 6b. One possible explanation is that larger merger deals may be more attractive targets for malicious actors, but they also possess richer health IT management resources. Whether attractiveness is a factor for increased breaches during mergers remains unsettled. No evidence shows larger targets are more attractive and experience more data breaches after controlling for online visibility.

6.3. Publicly Traded Hospitals' Management Skills

This section focuses on publicly traded hospitals to study the effect of management skills. Appendix Section A.13 shows that mergers involving publicly traded hospitals experience less data breach increase during

mergers. Specifically, buying a publicly traded target hospital means a significant decrease in the probability of insider discount. Similar to bigger mergers, publicly traded companies may face more online visibility. To control for the difference from online visibility and focus on management skills, I compare the data breach risks of publicly traded deals with those that do not involve publicly traded hospitals when they both face high online visibility.

Figures 7a and 7b reveal that when merger deals receive intensified online visibility, those involving publicly traded hospitals experience significantly smaller increases in pre-signing and post-signing data breaches. Note that during the post-signing period, there is a significant decrease in the probability of data breaches for publicly treated hospital mergers. One possible explanation is that publicly traded firms have more robust risk control management skills because of the shareholders' and board's oversights. The results imply that external threats from online visibility do not mean disaster for hospitals, and proper management matters in the face of such threats, in line with Murciano-Goroff, Zhuo and Greenstein (2024).

6.4. Post-merger Technical Challenges Versus the Scale of Resources

This section focuses on multi-hospital health systems to study the effect of the scale of resources on tackling technical challenges. Multi-hospital health systems are growing in the U.S. as a result of mergers, in which hospitals combine to create more integrated systems. Regarding data breach risks, the question is whether large multi-hospital health systems have comparative advantages in health IT management because of their scale of resources. Compared with regular multi-hospital health systems, large multi-hospital health systems have significant advantages, including greater bargaining power with insurance companies and improved operational efficiency. The comparative advantages in revenue and costs with a larger volume of transactions spare more resources for health IT management.

The results on multi-hospital health systems have entangled effects from technical challenges and resources. Appendix Section A.4 shows multi-hospital health systems' post-merger breaches increase from 1.33% to 3.33%, statistically significant at the 5% level. However, Comparing multi-hospital health system deals with all other mergers does not isolate the effect of the scale of the resources. Additional analysis is required to understand the effect of resources. Multi-hospital health system buyers have one other potential unique quality: technical challenges. Multi-hospital health system buyers harmonize new member hospitals' electronic medical record system vendors (Gaynor et al. 2021), creating extra technical challenges. Comparing large multi-hospital health systems with regular multi-hospital health systems is necessary to control for technical challenges.

The analysis compares large or experienced multi-hospital health system mergers with other regular multi-hospital health system mergers. Large or experienced health systems are multi-hospital health systems with more than 40 hospitals or have more than 3 merger deals between 2010-2022. The comparison between the larger and fast-growing health systems and regular health systems forms the basis for investigating the scale of resources by controlling for the technical challenges.

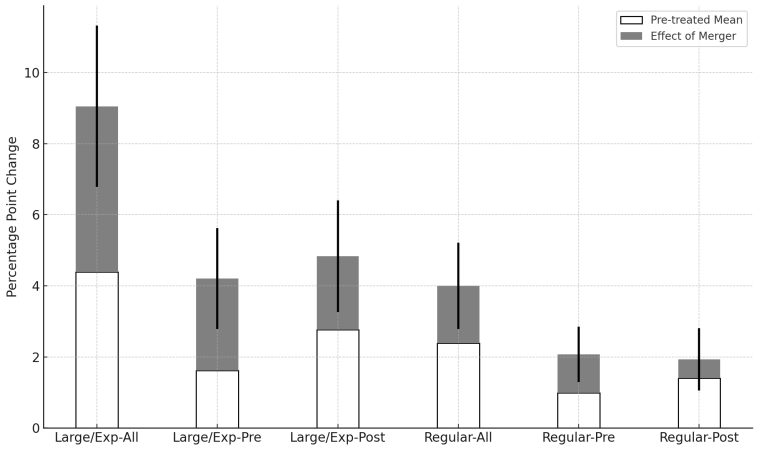


Figure 8 Percentage Point Changes: Large or Experienced Multi-hospital Health Systems

Notes: The figures show baseline and percentage point changes. Experienced multi-hospital health systems are multi-hospital systems with more than three deals between 2009-2022. Large multi-hospital health systems are those that manage more than 40 hospitals. The number of hospitals managed by each large multi-hospital system was based on Becker's 100 list of the largest hospitals and multi-hospital health systems in the United States (updated on Feb. 28th, 2023). Bars represent one standard error. Coefficients are also presented in Table 11. Data source: Levin's Associates, Becker's, and DHHS 2010-2022.

Large or experienced multi-hospital health systems do not benefit from their scale of resources. Instead, they struggle more with post-merger technical challenges. Specifically, Figure 8 compares large or experienced health system buyers with regular health system buyers, showing that the contrast is large for the post-signing period. The regular multi-hospital health systems do not have the post-merger data breach risks. The average data breach rate for the control group is 1.4%, and that of the treated group is 1.72%, with no certainty of an increase. When the health system operates more than 40 hospitals or grows fast, post-merger data breach risks are a main challenge. The large and experienced health systems' mean post-merger data breach rates rise from 2.77% to 4.13% with a certain increase. Health authorities should help large and fast-growing multi-hospital health systems understand and manage the technical challenges of information system integration. The results are in agreement with previous literature on information system integration and complicated systems (Tanriverdi et al. 2020, Gaynor et al. 2021, Du and Tanriverdi 2022).

6.5. Limitations and Future Studies

While various resources validate the reported hacks, underreporting may be true for insider misconduct, where verification of underreporting can be challenging without audit and enforcement measures from authorities. Specifically, hospitals may have a higher incentive to under-report insider misconduct during mergers, which introduces a negative measurement bias to my results. Similarly, the delayed reporting bias can cause overestimated post-merger effects and underestimated pre-merger effects. Although potential under-reports and delays cause bias in the estimation, the HHS data is the only data with enforcement and auditing and has been validated by existing literature.

In addition, the rich details on each data breach in the HHS data are the key to analyzing which economic or management factor matters. Various subsets of the merger sample are used to control for other conflicting factors and isolate each mechanism. The rare dependent variable means that sample size is a constraint. For example, isolating mergers in which the buyer's CEO has an MBA degree or is female does not yield statistically meaningful results, even with bootstrapping. An open question from this study is that the results show no evidence of the effect of the attractiveness factor, even controlling for the high online visibility. Future studies should discover whether attractiveness matters. I also acknowledge that this study does not focus on uncovering the exact set of technical challenges that multi-hospital health systems struggle with during the post-merger information system integration process. Future research using more detailed data on multi-hospital health systems should look into solutions for their post-merger difficulties.

This study focuses on why data breaches increase by analyzing the five economic and management factors and does not address the consequences. Data breaches carry significant implications, and understanding the consequences can, in turn, inform the hospitals' health IT management. Future studies should focus on the consequences without any empirical measurements in Table 1. Despite these limitations, this study offers useful insights into the effects of hospital mergers on data breaches.

7. Discussion and Conclusion

Although prior works adopt the view that economic and management factors matter for data breach risks, which I confirm, little empirical evidence has verified this assumption. The healthcare industry faces the greatest risk of data breaches. Understanding the reasons for large-scale data breaches in hospitals is relevant today. This study uses the stacked difference-in-differences causal inference method on 2010-2022 U.S. hospital data and shows that data breaches double during hospital mergers. Average data breach probability rises to 6.06% from 3.22% during mergers. I find no evidence of data breach increases from the attractiveness of larger merger targets. In contrast, evidence suggests that increased data breach risks during mergers are driven by pre-merger online visibility and post-merger technical challenges. Without increased pre-merger online visibility, hospitals can have decreased data breach risks in the quarter before the merger deal is signed. Publicly traded hospitals do not experience an increase in data breaches even when facing high online visibility. Merger deals involving publicly traded hospitals have decreased data breach risks, especially insider misconduct risks. One explanation is that even when faced with high external threats, publicly traded hospitals have a comparative advantage from their mature risk management skills. On the contrary, Large multi-hospital health systems, compared with regular multi-hospital health systems, do not benefit from their scale of resources and struggle more with technical challenges. Their post-merger data breach rates rise from 2.77% to 4.13% with a certain increase, while regular health systems do not experience escalated post-merger data breach risks.

Managerial and Policy Implications

The high cost of data breaches necessitates a collaborative approach among stakeholders. Stakeholders include health, financial, and cybersecurity authorities; hospital and multi-hospital system management teams; health IT vendors; cybersecurity insurance providers; and consultants. They must recognize the significant data breach risks posed by mergers and bolster health IT and risk management measures. A crucial element in bolstering management measures is considering management and economic factors. For example, when they model and monitor data breach risks, realizing data breach risks change over time and viewing merger time as extra challenging is necessary. In addition, one way to address the intensified hacks is taking malicious actors' behavior into account and manage online visibility. Indeed, one difficulty during mergers is the technical challenges of information system integration. Such heightened data breach risks from technical challenges are severe for large multi-hospital health systems, making early and tailored IT integration plans essential for successful mergers. To help hospitals overcome these challenges, cybersecurity authorities should focus on the intensified ransomware attack attempts and the technical challenges multi-hospital health systems face, issuing best practice suggestions and recommending licensed security services. To guide hospitals to early preparation, the authorities should consider mandating a written digital integration strategy for the proposed mergers. Health insurance administrators have a role to play, too, by awarding robust IT security practices through value-based payments or other advanced payment models. Healthcare leaders should gain confidence from the result that advancing cybersecurity management practices mitigates data breach risks.

During mergers, hospitals face a significant risk as the likelihood of data breaches doubles. Given the elevated and escalating costs of data breaches, hospitals that can manage such risks gain a substantial comparative advantage. The key to staying ahead of data breach risks is strategic thinking toward external threats, early preparations for IT integration, and confidence in advancing management practices.

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.

Anderson, Ross, "Why cryptosystems fail," in "Proceedings of the 1st ACM Conference on Computer and Communications Security" 1993, pp. 215–227.

___ , *Security engineering: a guide to building dependable distributed systems*, John Wiley & Sons, 2020.

Angst, Corey M and Ritu Agarwal, "Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion," *MIS quarterly*, 2009, pp. 339–370.

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.

August, Terrence, Duy Dao, and Marius Florin Niculescu, "Economics of ransomware: Risk interdependence and large-scale attacks," *Management Science*, 2022, *68* (12), 8979–9002.

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.

Bana, Sarah, Erik Brynjolfsson, Wang Jin, Sebastian Steffen, and Xiupeng Wang, "Human capital acquisition in response to data breaches," *Available at SSRN 3806060*, 2023.

Bardhan, Indranil R, Chenzhang Bao, and Sezgin Ayabakan, "Value implications of sourcing electronic health records: the role of physician practice integration," *Information Systems Research*, 2023, *34* (3), 1169–1190.

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.

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, 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.

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, 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.

Clement, Nan and Daniel Arce, "Dynamics of Shared Security in the Cloud," *Information Systems Research*, 2024.

Deng, Yiting, Anja Lambrecht, and Catherine E Tucker, "Asymmetric Consequences of Cyber-Vulnerability on Health Services," *Available at SSRN 3642485*, 2020.

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

Devaraj, Sarv and Rajiv Kohli, "Information technology payoff in the health-care industry: a longitudinal study," *Journal of management information systems*, 2000, *16* (4), 41–67.

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.

Eftekhari, Saeede, Niam Yaraghi, Ram D Gopal, and Ram Ramesh, "Impact of health information exchange adoption on referral patterns," *Management science*, 2023, *69* (3), 1615–1638.

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

Ganju, Kartik K, Hilal Atasoy, and Paul A Pavlou, "Do electronic health record systems increase medicare reimbursements? The moderating effect of the recovery audit program," *Management Science*, 2022, *68* (4), 2889–2913.

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

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.

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

___ and ___ , *The Economics of Privacy*, University of Chicago Press, 2024.

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 and Martin P Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security (TISSEC)*, 2002, *5* (4), 438–457.
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.
HealthExec, "Ascension reverts to pen and paper operations after ransomware attack," 2024. Accessed: 2024-07-13.
HealthTech, "How Healthcare Organizations Are Making the Case to Strengthen Cybersecurity," 2024.
Huang, Henry He and Chong Wang, "Do Banks Price Firms' Data Breaches?," *The Accounting Review*, 2021, *96* (3), 261–286.
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*, 2023, *69* (2), 791–811.
Jiang, Hao, Naveen Khanna, Qian Yang, and Jiayu Zhou, "The cyber risk premium," *Management Science*, 2024.
Kwon, Juhee and M Eric Johnson, "The market effect of healthcare security: Do patients care about data breaches?," in "WEIS" 2015.
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.
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.
Menon, Nirup M and Rajiv Kohli, "Blunting Damocles' sword: A longitudinal model of healthcare IT impact on malpractice insurance premium and quality of patient care," *Information Systems Research*, 2013, *24* (4), 918–932.
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 ___ , "Health information exchange, system size and information silos," *Journal of health economics*, 2014, *33*, 28–42.
Mitra, Sabyasachi and Sam Ransbotham, "The effects of vulnerability disclosure policy on the diffusion of security attacks," *Information Systems Research*, 2015, *26* (3), 565–584.
Moore, Tyler, "The economics of cybersecurity: Principles and policy options," *International Journal of Critical Infrastructure Protection*, 2010, *3* (3-4), 103–117.
Murciano-Goroff, Raviv, Ran Zhuo, and Shane Greenstein, "Navigating Software Vulnerabilities: Eighteen Years of Evidence from Medium and Large US Organizations," Technical Report, National Bureau of Economic Research 2024.
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.
of the National Coordinator for Health Information Technology, ONC Office, "'Office-based Physician Electronic Health Record Adoption,' Health IT Quick-Stat 50," 2021.
Ransbotham, Sam, Eric M Overby, and Michael C Jernigan, "Electronic trace data and legal outcomes: The effect of electronic medical records on malpractice claim resolution time," *Management Science*, 2021, *67* (7), 4341–4361.
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.
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.
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.
Tanriverdi, Huseyin, Juhee Kwon, and Ghiyoung Im, "Data Breaches in Multihospital Systems: Antecedents and Mitigation mechanisms," *2020 ICIS Proceeding*, 2020.
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.

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.

A. Appendices

A.1. Ransomware Attacks

Ransomware attacks are particularly harmful compared to other types of hacks because of the significant disruption they can cause to hospital operations. In September 2020, Universal Health Services (UHS), a prominent U.S. 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 affected patient care since access to medical records and prescription processing became impossible.

Table 4 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. The 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 during the pre-signing time.

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.

A.2. Most Recent Years

Mergers in 2021 and 2022 are too recent to have any pre-treated group without contamination. For mergers that are too recent to have future mergers as a control group, I create an alternative dataset by incorporating CMS Hospital Care Compare, which includes the never-treated group: hospitals that never merged throughout the observational period. In this data set, the control group consists of both pre and never-treated groups. Table 5 shows that there is an increase in data breaches during mergers and an especially significant increase for mergers in 2021-2022 compared with the never-treated group. The new data set also validate the main results with an alternative set of control variables. The results suggest that for mergers in 2021 to 2022, less digitized hospitals experience fewer breaches since less image availability correlates with fewer breaches. Note that a worsening mortality rate correlates significantly with more data breaches.

A.3. Without the Individual Fixed Effect

Individual-level fixed effects might not be 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, one hospital reports multiple breaches in different periods of time is rare, but some hospitals do report data breaches in more than one period. It is reasonable to include individual-level fixed effects. In Table 7, 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.

Table 4 Effect of Mergers 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

Notes: The table shows the effect of mergers 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 signing deal m, 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 are clustered at the deal level and are displayed in parentheses.

A.4. Post-signing Incompatibility Struggles during Operational Mergers: Multi-hospital System Buyers

Multi-hospital system buyers, with their more complicated control structure and harmonization process listed in Table 10, can experience more data breach risks during mergers. Table 8 displays stratified results focusing on mergers where the buyer is a multi-hospital system, revealing that multi-hospital health 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 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 increase to 3.33% from 1.33%.

A.5. Correlation Analysis

I 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. 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. Such analysis guides the identification of the mechanisms for how mergers cause more data breaches differently in different kinds of mergers.

Table 5 Effect of mergers on Breaches: CMS Hospital Care Compare 2021-2022

	21-22
Does mergers cause data breaches?	0.0119**
	(0.0052)
Image	-0.0046
	(0.0039)
Experience	0.0011
	(0.0027)
Timeliness	0.0078***
	(0.0027)
Safety	-0.0016
	(0.0028)
Effectiveness	-0.0048
	(0.0031)
Mortality	0.0066*
	(0.0037)
Readmission	0.0020
	(0.0024)
N	299889
R^2	0.2253
Mean on Pre-treated % Effect	1.01
Mean on Treated % Effect	2.09

Notes: The table shows the effect of mergers on breaches as estimated from the main equation since 2021. 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 signing deal m, 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 Care Compare metrics. The never-treated groups include hospitals that did not merge during the observational period, 2021-2022. All the regressions include a full set of hospital and time fixed effects. I also control for the Hospital Care Compare scores. All controls are equal to 1 when they are unavailable or their performance is below the national average. The standard errors clustered at the state level are shown in parentheses.

In Table 9, first, publicly traded companies attract more visibility and have greater financial information available publicly online, indicating a positive SC effect. Conversely, their ability to manage short-term shocks might be enhanced by 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 9 suggests that the second assumption holds more weight. Notably, the pre-signing (columns 3-4) and post-signing breaches (columns 5-6) in Table 9 show different effects from the control variables.

A.6. Alternative Window: Google Trends

To determine when the merger deal gains public visibility, an analysis of search score growth rates using Google Trends is conducted, focusing on the period leading up to the merger signing date.

Another reason for analyzing Google Trends data is that the treatment period does not necessarily begin one year before the signing date, as assumed in the main analysis. Through data examination, it is determined that the mean of the highest growth rate in Google searches indicates a peak in search activity approximately 18 months prior to the merger signing date, while the median suggests a peak around 17

Table 6 Effect of Mergers on Different Types of Data Breaches: 2018-2020

	Ransomware Attacks			Phishing Attacks			General Hacks		
	All	Pre	Post	All	Pre	Post	All	Pre	Post
Treatment	0.0625***	0.0529**	0.0096	0.0356*	0.0360*	-0.0003	0.0150	0.0177	-0.0027
	(0.0226)	(0.0217)	(0.0068)	(0.0187)	(0.0199)	(0.0045)	(0.0170)	(0.0166)	(0.0028)
Public Buyer	0.0410***	0.0347**	0.0063	0.0234*	0.0236*	-0.0002	0.0098	0.0116	-0.0018
	(0.0148)	(0.0142)	(0.0044)	(0.0123)	(0.0131)	(0.0030)	(0.0111)	(0.0109)	(0.0018)
Public Target	0.0205***	0.0174**	0.0032	0.0117*	0.0118*	-0.0001	0.0049	0.0058	-0.0009
	(0.0074)	(0.0071)	(0.0022)	(0.0061)	(0.0065)	(0.0015)	(0.0056)	(0.0054)	(0.0009)
REIT Buyers	-0.0205***	-0.0174**	-0.0032	-0.0117*	-0.0118*	0.0001	-0.0049	-0.0058	0.0009
	(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
R^2	0.1680	0.1237	0.3651	0.2349	0.2021	0.2370	0.6995	0.0253	0.7375
Pre-treated	1.63	1.31	0.32	0.47	0.00	0.47	0.37	0.00	0.37
Treated	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 mergers on different types of hacks as estimated from the difference-in-differences equation for mergers in 2018-2020. 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 signing deal m, 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 Real Estate Investment Trust (REIT). Analysis of professional investors' effect is in Appendix Section A.12. The change of the control variables may be a reason why R^2 increases. The 2021-2022 mergers are 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 $[0, t+a]$.

months. Figure 9 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. The findings from Google Trends align with the main research design. Alternative assumptions are also tested and discussed in Section A.11.

A.7. 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.

Table 7 Without the Individual Fixed Effect

	Insider Misconduct and Hacks	
Does mergers 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

Notes: The table presents the impact of mergers 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 signing deal m, 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.

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 treatment of other hospitals. Without this assumption, the results on hacks may contain a positive bias. It is because if malicious actors only have limited resources to target hospitals, the possibility of data breaches in 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. We know that cyber attacks on hospitals have regional effects Neprash et al. (2022), but there is no existing evidence on the network effect of cyber attacks – whether cyber attacks on one hospital in the region drive down the probability of attacks from other regions. From the malicious actors' perspective, there is no evidence that an entry barrier to being a hacker exists and that malicious actors have a capacity limit on how many U.S. hospitals can be under attack.

Table 8 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 mergers on data breaches that were reported before and after signing the deal. 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 signing deal m, 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.

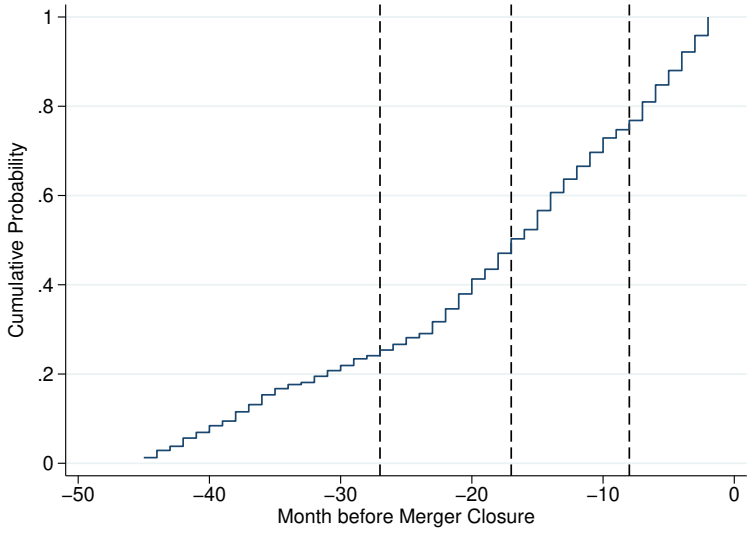


Figure 9 Google Trends: CDF of the Peak Growth Rate

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.

Table 9 What Cause Data Breaches: Correlation Results

	Overall Data Breaches		Pre-signing Data Breaches		Post-signing Data Breaches	
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)
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)
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)
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. Data source: Levin's Associates and DHHS 2010-2022.

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. With mergers happening over 10 years, the chance that all the mergers coincide with other factors that affect data breaches is slim.

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. 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.

The event study graph in Figure 10 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

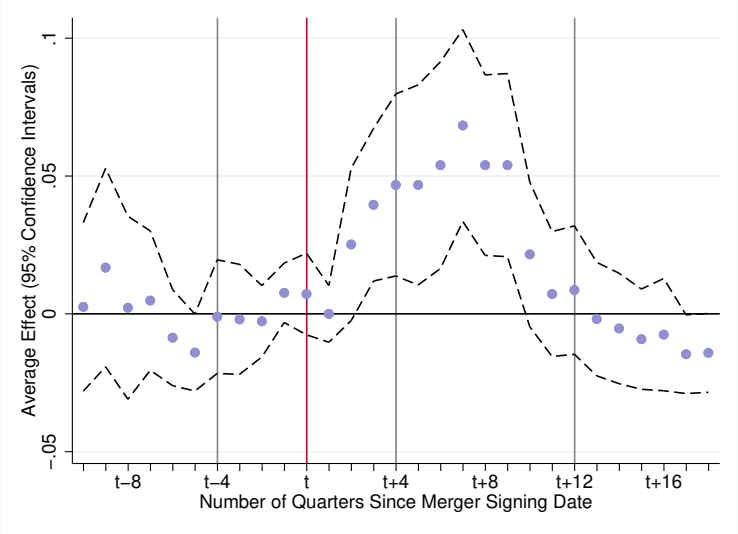


Figure 10 Event Study: Mergers in Q1 2018-Q4 2019

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 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 12.

reason for the slight difference between Figures 10 and 4 is from the change in the observational period in the control group, thus the mean I am comparing. In the previous analysis, Figure 10 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 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 4 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 because of 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 data breach risks during mergers compared with pre-merger groups and such challenges over time.

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

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

Notes: The figures show the vendors of the target hospitals and the buyers signing a deal in 2018 and 2019. Data source: Healthcare Information and Management Systems Society 2017-2018.

The control variables 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 because of the governance requirements of risk controls, the difference in available public information, and the difference in financial structure. Especially in the pre-signing analysis, online visibility matters. I then control the target hospital revenue and EBITDA. It 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 affect the time trend of data breaches.

A.8. Post-signing Operational Integration: Incompatibility

Table 10: 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 interact with the EMR system.
Communication Systems	Email, phone, pager, telemedicine service systems
Network Infrastructure	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 across-state mergers.
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 data breach risks 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 information system integration. Vendors' quality and vendors' market share affect data breach risks (Vasek, Wadleigh and Moore 2015). In Figure 11, I show the word cloud for software vendors of the target hospitals and the buyers signing a deal in 2018 and 2019. The vendor information is from the Healthcare Information and Management Systems Society. 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 10, such EMR harmonization is listed as the first post-signing change for digitization.

EMR harmonization is not the only incompatibility problem. Table 10 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 affect the employees' actions.

A.9. Large or experienced Health System Buyer

A.10. Alternative Window: One Year Before and Three Year After Results

EMR integration cannot begin until a merger closes. Gaynor, Sacarny, Sadun, Syverson and Venkatesh (2021) suggest 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 12). Notably, three years after

Table 11 Large or Experienced Multi-hospital Health 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 mergers deals involving large or experienced multi-hospital health systems. Experienced multi-hospital health systems are the multi-hospital health systems that have more than 3 deals in 2009-2022. Large multi-hospital health systems are the multi-hospital health 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 health 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 signing deal m, 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.

the merger, a third of the target hospitals had adopted the EMR system. It 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 12 examines the time window $[t-4, t+12]$. The results indicate no significant differences in pre-trends in the probability of data breaches between the treatment and pre-treated groups. However, during the two-year time window surrounding the merger signing date, there is no evidence to reject the null that there may be an intentional delay in reporting data breaches.

Table 12 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,

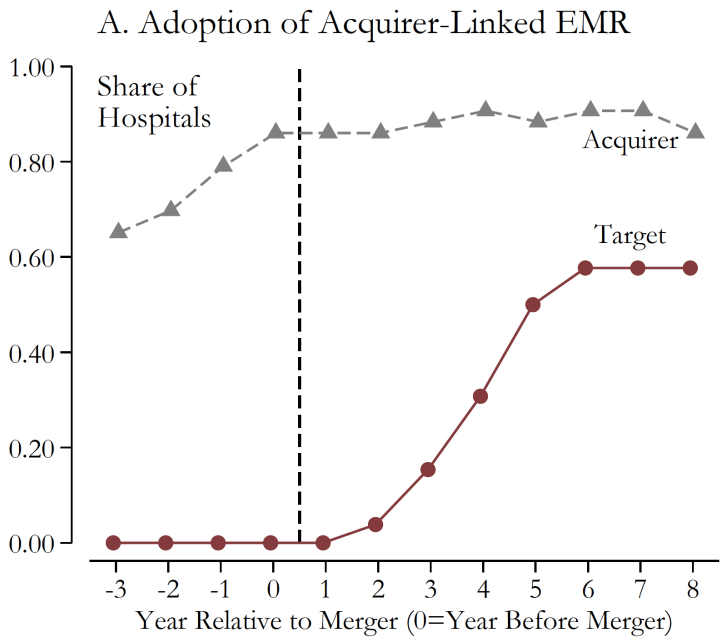


Figure 12 Graph from Gaynor et al. (2021)

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. The patterns 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).

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. Owing 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 9. Instead of one year before signing the merger deal, 17 months and 27 months are tested and shown in Figure 13.

A.11. Alternative Time Windows

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 malicious actors become aware of the mergers? If my assumption is too distant, my sample size will be inadequate, and the treatment

Table 12 mergers Effect on Data Breaches: [One Year Before, Three Year After]

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Does mergers 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 on Pre-treated % Effect	0.94	0.95	1.09	0.95	1.01	0.95	0.95
Mean on Treated % Effect	2.34	2.53	2.13	2.53	2.50	2.53	2.53
Mean on Pre-treated Targets % Effect	0.63	0.58	0.74	0.70	0.60	0.58	0.60
Mean on Treated Targets % Effect	2.21	2.39	2.34	2.38	2.56	2.23	2.23
Mean on Pre-treated Seller % Effect	0.90	1.06	0.99	1.01	1.09	1.05	1.11
Mean on Treated % Effect Seller	1.32	1.75	3.17	1.59	3.33	1.69	1.79
Mean on Pre-treated Acquirer % Effect	0.80	0.67	0.86	0.81	0.68	0.67	0.69
Mean 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 mergers on hacks with different sets of controls. 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. Standard errors are clustered at the deal level and are displayed in parentheses.

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 15 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 include the shorter time window assumption with the same treatment samples that ends early for comparison. If the time window is a four-year window, mergers that occur after 2018 will be too late to find any Pre-treated group without contamination. The middle two 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 last two lines represent the coefficients that end in 2016. The first data points represent the original design that can test the treatment effect up to 2020. The six-year window has a smaller sample size, resulting in a larger standard error.

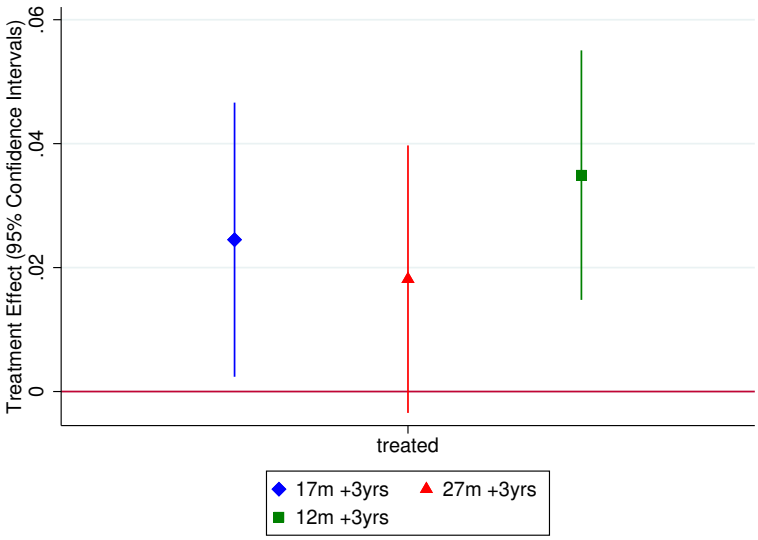


Figure 13 Robustness to Changes in Time Window: Google Trends

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 square coefficient corresponds to Table 12. The diamond coefficient utilizes the median Google search peak, as shown in Figure 9, occurring 17 months before the merger signing date. The triangle coefficient uses the 25th percentile in Figure 9, which corresponds to 27 months before the merger signing date. Data source: Levin's Associates and DHHS 2010-2022.

Table 13 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 mergers 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 signing deal m, 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.

A.12. Neither Pre Nor Post-Signing Significant Breach Increases: Merger Deal with Professional Investors

The healthcare industry has seen a significant increase in Private Equity (PE) investment in the past decade, with an estimated $800 million dollars flooding into the sector (Scheffler, Alexander and Godwin 2021).

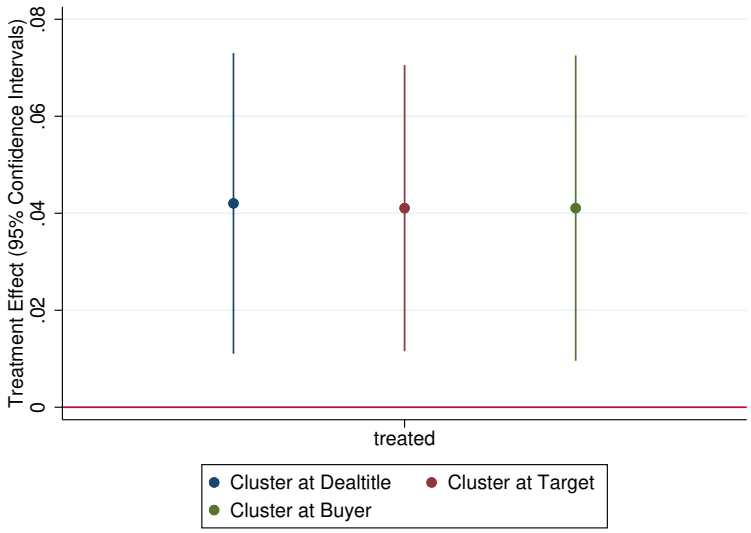


Figure 14 Standard Errors are Clustered at Different Levels

Notes: The graph shows the effect of mergers 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 signing deal m, 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.

PE and Real Estate Investment Trust (REIT) investors inherently sidestep the complexities associated with integrating information systems. 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 the objectives may not be aligned with the priorities of hospitals and patients. The 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 section focus on the immediate implications of PE investment in healthcare, specifically highlighting the potential for private equity funding to improve cybersecurity outcomes as compared to other investors. Since professional investors do not have the challenges of merging information systems and the resultant compatibility issues, verifying whether they have increased data breaches in the post-signing period is important to determine the reasons for the post-signing increase in data breaches.

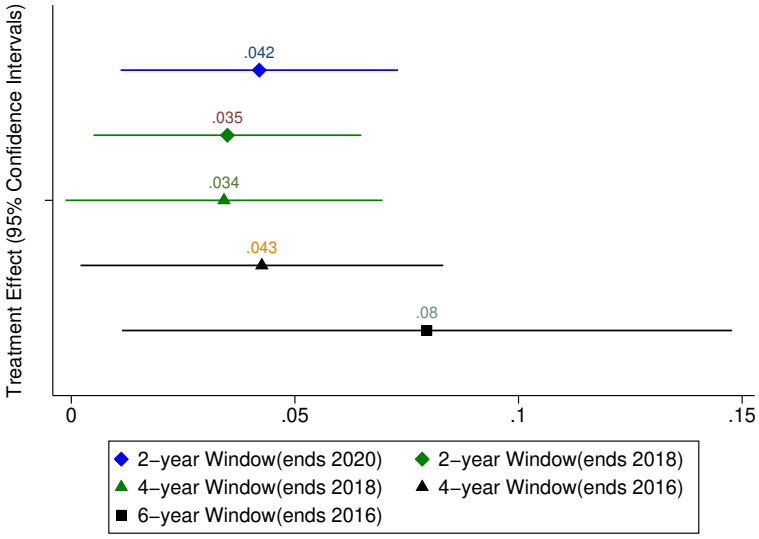


Figure 15 Robustness to Changes in Time Window

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 first line with a diamond nob is the original two-year window. The second line with a triangle nob is on the four-year window, [two years before signing the merger deal, two years after]. The last 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: Levin's Associates and DHHS 2010-2022.

To fulfill this purpose, I run the baseline model on deals with a professional investor buyer, PE or REIT. All 7 data breaches within the two-year treatment period in the 76 professional investor deals are all misconduct data breaches. It is because of the absence of incompatibility between two merging EMRs in such deals. Table 13 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, and neither effect is statistically significant. I verify the result with bootstrapping.

Tax treaties on hospitals since the Tax Reform Act of 1986 and 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). The latest literature debate on the welfare effect of PE 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. As discussed in Rundle and Nash (2023), private equity firms are taking action on the cybersecurity

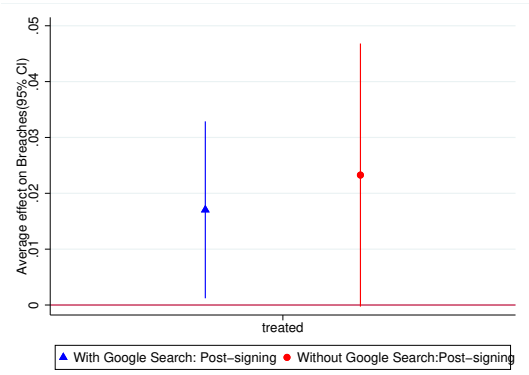


Figure 16 Active Pre-signing Search: Post-signing Breach

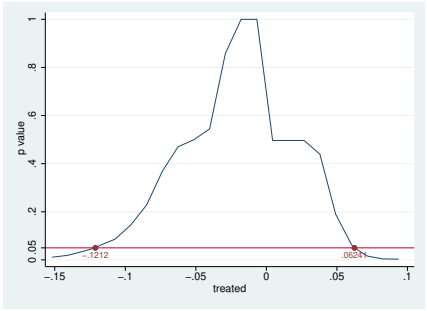
Notes: The figure displays coefficients for the main regression on all data breaches (insider misconduct and hacks) reported in the year after signing the deal. The triangle knob represents the mean treatment effect on post-signing breaches with the sample with active pre-signing search. The circle represents the treatment effect on all breaches during the year after signing the deal 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 means having the highest monthly mean one year before signing the deal during the period $[t-4, t-3]$, which corresponds to 7-12 months before signing the merger deal. Date t is when signing deal m. The graph shows that the visibility before signing the deal does not have a significant effect on post-signing breaches. Data sources: Levin's Associates, Google Trends, and DHHS 2010-2022.

risk and IT due diligence of the merger targets. My result suggests that their efforts during the pre-signing period are effective.

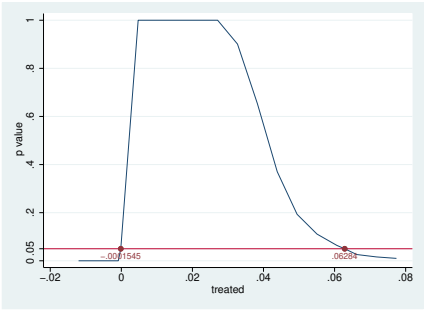
Analysis in Section A.12 yields inconsistent effect on professional investors. Given the considerable reduction in treatment size resulting from the stratification, the results are further subjected to wild-bootstrap analysis (Cameron, Gelbach and Miller 2011, Roodman, Nielsen, MacKinnon and Webb 2019), as shown in Figure 17.

A.13. Publicly Traded Hospitals

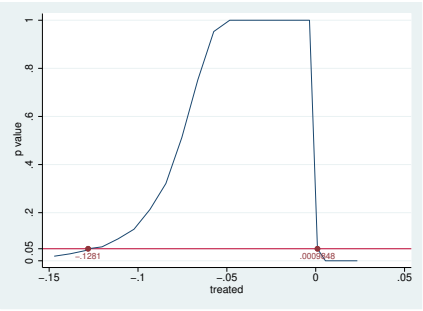
Figure 18 shows the impact of publicly traded and non-publicly traded mergers on data breaches. Specifically, the first line in Figure 18a shows that when the target hospital is publicly traded, there are significantly fewer incidents of insider misconduct during mergers as compared to the pre-treated group. Mergers involving publicly traded hospitals exhibit greater efficiency in dealing with hacks, as demonstrated in Figure 18b.



(a) Full Sample



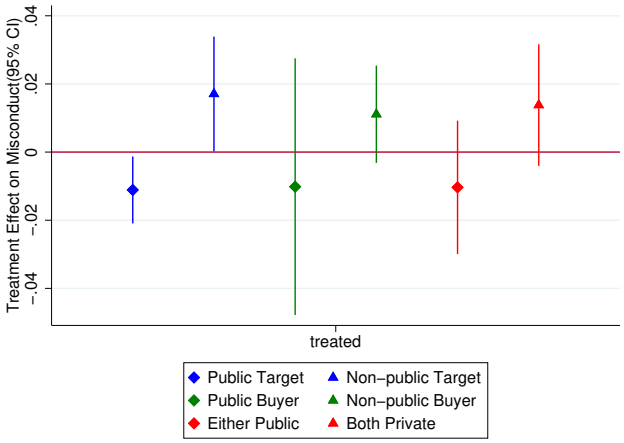
(b) Post-merger Breaches



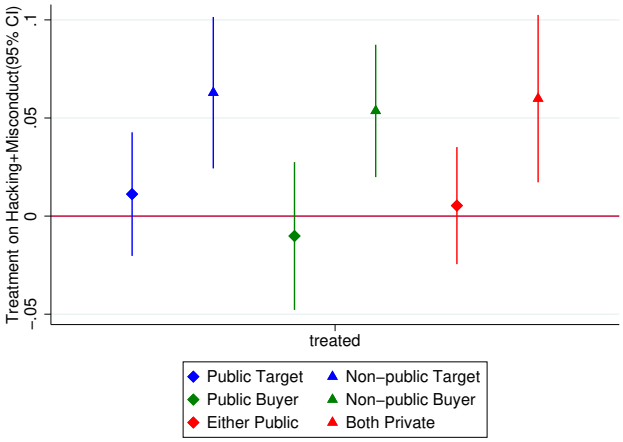
(c) Pre-merger Breaches

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

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



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



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

Figure 18 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 left two lines represent a comparison of merger deals with a public target versus those without, while the middle lines compare deals with a public buyer to those without. The right two lines compare merger deals with either a public target or buyer to those without. Data source: Proprietary merger data and DHHS 2010-2022.