Is Blockchain the Ultimate Cybersecurity Weapon?: Evidence from a Quasi-Natural Experiment in the U.S.

Abstract. Blockchain technology has sparked significant interest and investment across various industries. Practitioners, however, are divided in their views on the technology's cybersecurity impact: some see blockchain technology as an important cybersecurity advancement, while others believe it introduces considerable cybersecurity risks. To probe the validity of these competing positions on blockchain technology, we conduct a quasi-natural experiment in the U.S., where the staggered implementation of pro-blockchain laws serves as an exogenous shock on blockchain implementation among local firms. Our difference-in-differences (DiD) analyses reveal that blockchain implementation has unexpected dual-edged implications and dynamic impact on firms' cybersecurity: in the short term, adopting blockchain heightens data breach risks, especially those caused by firms' insiders; over the long term, as firms adapt, these risks decrease, notably with earlier reductions in external breach risks. Furthermore, we find that ample managerial IT industry experience and sufficient human resources mitigate the short-term adverse effects linked to blockchain implementation. This study provides groundbreaking empirical evidence on blockchain's cybersecurity impact, offering crucial insights for executives charged with managing the technology's implementation.

Keywords: blockchain, cybersecurity, data breach, organizational information processing theory

"*The debate about blockchain security is polarized. At one end of the spectrum, blockchain technology is perceived to be inherently insecure and unfit for most use cases requiring privacy protections. At the other end, it is viewed as a cryptography-native and hence "unhackable" technology. The truth lies somewhere in the middle.*" —2019 World Economic Forum paper[1]

1. Introduction

The emergence of blockchain technology has sparked significant interest and investment across various industries, establishing itself as a foundational technology in the ongoing wave of digital innovation and transformation (Jaradat et al. 2022; Yaga et al. 2019). Originally devised as the underlying technology for cryptocurrencies like Bitcoin, blockchain has transcended its initial application to become a cornerstone of the Fourth Industrial Revolution (Khalil et al. 2022). Its decentralized and largely immutable nature has enabled novel solutions to age-old challenges tied to process and information sharing, offering unprecedented levels of transparency, security, and efficiency. As blockchain technology gains wider acceptance, recent literature has explored the economic and innovative impacts of blockchain implementation (e.g., Chen et al. 2023). Despite substantial evidence outlining the opportunities presented by blockchain technology, a significant gap remains in understanding its impact on firms' cybersecurity posture. This study seeks to address this gap through an empirical examination of blockchain implementation's cybersecurity implications.

Among practitioners, the discourse on blockchain security is sharply divided. On the one side, some advocates have lauded blockchain technology as the "ultimate weapon in the fight against cybercrime."[2] They argue that blockchain is inherently secure by design. For instance, the decentralized storage architecture of blockchain ensures that each block contains only a fraction of information within a much larger dataset, minimizing the vulnerability of hackable data to nearly negligible levels (Kshetri 2017; Yadav et al. 2022). Consequently, these advocates contend that blockchain technology may revolutionize security measures and significantly bolstering cybersecurity in the realm of digital transformation.

On the flip side, skepticism regarding blockchain's security capabilities is also prevalent. Despite the touted security advantages, the blockchain market has encountered a plethora of cybersecurity challenges. According to Chainalysis, cryptocurrency-related crimes reached over $20.6 billion in illicit transactions in 2022, up from $18.1 billion in 2021.[3] Moreover, researchers have documented around 500 cybersecurity attacks linked to blockchain, resulting in financial losses of $9 billion.[4] Skeptics cite such evidence when arguing that the implementation of blockchain technology brings considerable cybersecurity threats. In light of this phenomenon, a 2019 World Economic Forum paper cautions that

[1] https://www3.weforum.org/docs/WEF_Inclusive_Deployment_of_Blockchain_for_Supply_Chains_Part_5.pdf
[2] https://www.encora.com/insights/blockchain-the-weapon-for-cybersecurity
[3] https://go.chainalysis.com/2023-crypto-crime-report.html
[4] https://www.pwc.com/gx/en/issues/technology.html

the hype surrounding blockchain has led to "exaggerated security expectations that have affected trust in the technology…. Security violations and volatility in crypto markets (e.g., hacking of crypto wallets and volatile coin prices) have adversely affected the brand of enterprise blockchains."[5]

The deeply polarized debate on blockchain cybersecurity in practice prompts the question: *How will the implementation of blockchain affect a firm's cybersecurity*? To address this question, we present groundbreaking empirical research on the impact of blockchain implementation on cybersecurity, employing a dual focus on the cybersecurity advantages and disadvantages of blockchain. Specifically, on the one hand, we acknowledge the cybersecurity advancements inherent in the technology's core design, emphasizing its potential to strengthen firms' cybersecurity posture. We term this positive outcome of leveraging blockchain for security enhancement as the *security-enhancing design effect*. On the other hand, building upon the organizational information processing theory (OIPT) (Galbraith 1973; Srinivasan and Swink 2018; Tatikonda and Montoya-Weiss 2001), we posit that blockchain implementation may introduce significant operational uncertainty for firms. This uncertainty can hinder internal security operations, leading to challenges such as a lack of understanding of threat patterns, configuration errors, and inadequate security measures, ultimately increasing data breach risks. We term this adverse impact on a firm's cybersecurity landscape as the *technology uncertainty effect*.

Subsequently, we integrate these opposing effects (i.e., *security-enhancing design effect* and *technology uncertainty effect*) of blockchain *dynamically* and predict a dual-edged impact of blockchain implementation on cybersecurity: in the short-term aftermath of adoption, the prevailing *technology uncertainty effect* accompanying the implementation of cutting-edge blockchain technology tends to dominates, potentially leading to a net increase in a firm's data breach risks. However, in the long term, as firms progressively address and diminish the technology uncertainties arising from blockchain implementation (Stock and Tatikonda 2008; Tatikonda and Montoya-Weiss 2001), the growing prominence of the *security-enhancing design effect* may offset these uncertainties, ultimately leading to a net decrease in a firm's data breach risks.

Nevertheless, empirically testing these predictions poses challenges because of the potential endogeneity between blockchain implementation and cybersecurity. Such endogeniety could result from unobservable attributes of firms or industries that might concurrently affect both variables. Moreover, there is a possibility that the acceptance of blockchain technology could be influenced by security performance in reverse, leading to concerns about reverse causality. Consequently, a correlation between blockchain implementation and cybersecurity performance doesn't necessarily imply a causal explanation.

To overcome these challenges, we conduct a quasi-natural experiment. Various states in the U.S. have implemented legislation aimed at reducing the cost of developing and utilizing blockchain technology for local businesses and commerce, which we term as pro-blockchain laws. In this

[5] https://www3.weforum.org/docs/WEF_Inclusive_Deployment_of_Blockchain_for_Supply_Chains_Part_5.pdf

experiment, we leverage the staggered implementation of these pro-blockchain laws as an external shock to encourage the adoption of blockchain technology among local firms. Subsequently, we conduct a difference-in-differences (DiD) analysis to estimate differences in cybersecurity performance before and after the enactment of the pro-blockchain laws (the first difference) between the treatment and control groups (the second difference). This approach allows us to address concerns about endogeneity and establish a causal link between the adoption of blockchain and the subsequent performance of cybersecurity.

The results of our analyses support all our predictions. Specifically, we find that in the short term, the pro-blockchain legislations increases a firm's data breach risks, while in the long term, such legislations reduce these risks. This implies a dynamic and dual-edged influence of blockchain implementation on the cybersecurity of firms. To ensure the robustness of our main findings, we conduct a series of validation checks and sensitivity tests. These include examining parallel pre-trends, employing propensity score matching (PSM), employing alternative model specifications, and conducting a placebo test to mitigate biases resulting from randomness or other potential time series factors. Across all these tests, our primary findings remain consistent, indicating the robustness of our results.

Following our primary analyses, we delve deeper into the nuanced effects of blockchain on data breach risks and identify underlying mechanisms. A variation that we examine revolves around distinct types of data breaches: internal data breaches, caused by internal actors such as employees, and external data breaches, caused by external actors like hackers (Cheng et al. 2017). In our theory, as described previously, we propose that the short-term impacts of blockchain in increasing data breach risks are predominantly driven by the *technology uncertainty effect*. However, this effect tends to disproportionately impact internal and external data breach risks. Specifically, it primarily affects a firm's susceptibility to internal data breaches by introducing complexity and obstacles to internal operations within the organization (Stock and Tatikonda 2008; Tatikonda and Montoya-Weiss 2001). Therefore, we predict that in the short term, blockchain implementation will more notably increase internal data breach risks. Conversely, as described above, the long-term impacts of blockchain implementation are predominantly driven by the *security-enhancing design effect*. This effect operates by enhancing a firm's resilience to external hacker attacks, thereby primarily shaping the firm's susceptibility to external data breaches (Kshetri 2017; Yadav et al. 2022). Therefore, we predict that, in the long term, the *security-enhancing design effect* will assume dominance earlier in impacting external breach risks, leading to an earlier net reduction in such risks associated with blockchain implementation. We conduct empirical investigations into these concepts to broaden our research scope and uncover evidence that bolsters our predictions.

As a further extension, we examine how organizational capabilities influence the short-term effects of blockchain implementation. According to OIPT, a firm's existing capabilities can effectively mitigate the operational uncertainties brought by new technology adoption ((Mackelprang et al. 2015; Stock and

Tatikonda 2008; Tatikonda and Montoya-Weiss 2001; Tatikonda and Rosenthal 2000). We, therefore, predict that organizational capabilities, such as managerial expertise and adequate resources, will reduce the short-term increase in data breach risks associated with blockchain implementation. Our empirical findings support these predictions.

Taken together, our findings shed light on the dual-edged impact of blockchain implementation on cybersecurity and the complex dynamics involved. By introducing the concepts of the *security-enhancing design effect* and *the technology uncertainty effect* into a unified framework, we highlight how blockchain can both improve and challenge cybersecurity. Furthermore, we identify underlying mechanisms and explore contextual factors that influence these effects, deepening and expanding our understanding of blockchain's cybersecurity implications. Our findings have significant research and practical implications, as discussed in the later sections of our paper.

2. Literature Review

A data breach refers to the unauthorized acquisition, access, disclosure, theft, or exposure of sensitive information or personal data to unauthorized third parties (Cheng et al. 2017; Sen and Borle 2015). Data breaches arise from many causes, including cyber-attacks, internal security vulnerabilities, and malicious data theft. The ongoing cybersecurity vulnerabilities pose continuous risks to businesses. A considerable body of academic research has investigated the detrimental impacts of data breaches, such as declines in stock prices (Cavusoglu et al. 2004; Foerderer and Schuetz 2022; Kamiya et al. 2021; Modi and Mishra 2011), erosion of market share (Huang and Wang 2021), heightened concerns regarding litigation (Romanosky 2016; Romanosky et al. 2014), disruption of productivity (Hilary et al. 2016), and damage to reputation (Gwebu et al. 2018; Janakiraman et al. 2018)

In light of the significant repercussions of data breaches, security scholars have devoted considerable efforts to developing effective data breach prevention strategies. Conventional practices for combatting cybersecurity threats have predominantly centered on technological solutions, such as sensitive data scanning (Shu et al. 2015), machine learning (Hart et al. 2011), collection intersection (Liu et al. 2015), and watermarking (Papadimitriou and Garcia-Molina 2011). Moreover, many scholars and managers increasingly recognize that mitigating data breach risks requires going beyond technological solutions to also consider a firm's management practices, operational procedures, and strategic approaches (Bulgurcu et al. 2010; Cram et al. 2019). Consequently, recent research has increasingly examined data breach solutions from organizational and managerial perspectives, investigating how firms' data breach risks are determined by organizational factors such as IT frameworks (Angst et al. 2017; Kwon and Johnson 2014; Li et al. 2021; McLeod and Dolezel 2018; Wang et al. 2015), governance protocols (Higgs et al. 2016; Liu et al. 2020), strategic initiatives (D'Arcy et al. 2020; Kwon and Johnson 2018), and managerial attributes (Haislip et al. 2021). We review the literature on how organizational factors affect firms' data breach risks in Table 1.

In particular, as outlined in Table 1, some literature suggests that the implementation of IT can exert a dual-edged influence on cybersecurity. Studies such as those by Kwon and Johnson (2014) and Angst et al. (2017) highlight the context-dependent nature of IT security investment, suggesting that achieving optimal results in mitigating data breach risks may necessitate proactive approaches and take time to materialize. Conversely, findings from Sen and Borle (2015) and Wang et al. (2023) underscore the unintended consequences of IT investments, particularly innovative ones, on weakening firms' cybersecurity posture, rendering them more susceptible to data breaches. Thus, while IT holds promise in fortifying cybersecurity defenses and mitigating breach risks, it simultaneously introduces complexities (e.g., expanded attack surfaces and operational uncertainties), ultimately exacerbating cybersecurity challenges. Our research applies this dual-edged perspective and unpacks the intricate interplay between blockchain technology and cybersecurity.

Despite the valuable insights from the research above, most IS literature connects *aggregated* IT measures to cybersecurity risk, while the effects of *individual* IT components on cybersecurity outcomes are still largely unexplored. This oversimplification hinders a comprehensive understanding of the complex IT–cybersecurity relationship. Our study offers a more nuanced, comprehansive understanding the cybersecurity effects of a specific IT technology: blockchain.

Table 1. A Literature Review on Data Breach Risk Research

Literature	**Organizational Determinants**	**Main Findings**
Higgs et al. (2016)	IT governance	Firms that implement technology committees tend to experience fewer reported breaches compared to those that do not.
Liu et al. (2020)	IT governance	The implementation of centralized IT governance within universities correlates with a lower number of data breaches. The influence of this effect is contingent upon the diversity of universities, including factors such as university type and research intensity.
Sen and Borle (2015)	IT security investment	The likelihood of data breaches within state and industry sectors is positively associated with levels of investment in IT security.
Angst et al. (2017)	IT security investment	The cybersecurity effectiveness of investments in IT security is contingent upon institutional factors. The effect of IT investment on cybersecurity requires time for its benefits to materialize and become evident.
Kwon and Johnson (2014)	IT security investment	The implementation of proactive security strategies is associated with a decrease in security risks.
Kwon and Johnson (2018)	Meaningful-use attestation	Hospitals that have achieved Stage 1 meaningful-use standards tend to have a lower likelihood of experiencing external breaches in the short term. In addition, hospitals that attest to having reached Stage 1 meaningful-use standards tend to have a higher likelihood of experiencing accidental internal breaches in the short run, which tends to decrease in the long term.
Wang et al. (2015)	Features of IT applications	IT applications are more likely to be targeted if they possess high value, lack comprehensive controls, are highly visible and accessible, and have minimal protective measures in place.

Mcleod and Dolezel (2018)	Technical facilitates, and organizational factors	Technical facilities like EMR systems, neonatal intensive care units, lab barcoding systems, and health information exchange initiatives are particularly susceptible to data breaches. In addition, organizational characteristics such as the number of births, staff beds, and surgical operations are linked to a higher incidence of data breaches.
D'arcy et al. (2020)	Social performance	The probability of data breaches is elevated for firms involved in extensive social-facing activities, particularly those with a deficient record in social performance.
Haislip et al. (2021)	IT expertise of executives	Executives' IT expertise is linked to a lower likelihood of data breaches.
Wang et al. (2023)	IT innovativeness	There is a positive association between firm IT innovativeness and the risk of data breaches. In addition, the positive relationship between IT innovativeness and data breach risk is mitigated when managers possess IT expertise or when firms have boards that are well-connected with external cybersecurity managers.

3. Theoretical Background and Hypotheses

The 2019 World Economic Forum paper highlights that: "blockchain technology, including solutions based on it, is not infallible. Like any other technology, it has pros and cons related to security."[6] In line with this view, this section presents our theoretical exploration of blockchain technology and cybersecurity, as we describe next, balancing the cybersecurity implications of blockchain implementation, both favorable and unfavorable.

3.1. Exploring the Security Landscape of Blockchain

3.1.1. Cybersecurity Advantages of Blockchain: The "Security-Enhancing Design Effect"

Blockchain technology operates as a distributed database, organizing data into interconnected blocks, each encompassing a distinct set of transactions (Jaradat et al. 2022; Yaga et al. 2019). Blockchain is celebrated for its inherent cybersecurity advantages (Bansal et al. 2020; Kshetri 2017; Yadav et al. 2022). Given that the analysis of cybersecurity advantages of blockchain is primarily grounded in computer science, the present study refrains from delving into detailed explanations and instead offers a concise overview of these advantages identified in the computer science literatures in Table 2.

Table 2. Cybersecurity Advantages in the Design of Blockchain Technology

Design Elements	**Cybersecurity Advantages**	**Example References**
Decentralized Structure	The decentralized nature of blockchain ensures data storage and validation are distributed across multiple nodes or computers. This eliminates vulnerabilities associated with single points of failure, as data isn't centralized. Even if one node is compromised, the rest of the network can seamlessly continue to operate, maintaining system stability and security.	Zhuang et al. (2020); Kshetri (2017); He et al. (2022); Sriram et al. (2023);
Built-in Security Features	Blockchain integrates various security features, including encryption, public and private keys, consensus mechanisms, smart contracts, and identity control. These features are meticulously designed to ensure	

[6] https://www3.weforum.org/docs/WEF_Inclusive_Deployment_of_Blockchain_for_Supply_Chains_Part_5.pdf

	comprehensive data protection and integrity. They facilitate verification of access, authentication of transaction records, traceability, and privacy protection within the blockchain network.	Gimenez-Aguilar et al. (2021)
Immutability	Once data is added to the blockchain, cryptographic hash algorithms ensure it remains unchanged, unmodifiable, or deletable. This fundamental characteristic of blockchain design guarantees data integrity and traceability by making historical records nearly impossible to alter, effectively preventing fraudulent or tampering attempts.	
Resilience to DDoS Attacks	The distributed architecture of blockchain effectively disperses network load across multiple nodes, making it highly challenging for attackers to overwhelm any single node and disrupt the entire system. Furthermore, the implementation of blockchain-based Domain Name Systems (DNS) further mitigates DDoS attacks by fairly distributing network loads, ensuring continuous network availability and stability. This resilience stems from the decentralized and redundant core design principles of blockchain.	
Smart Contracts	An innovative feature of blockchain technology is smart contracts, which automate and enforce contract agreements. These self-executing contracts operate based on predefined rules and conditions, enhancing transaction security and reliability. Leveraging encryption techniques and distributed control, smart contracts effectively mitigate risks associated with fraud or unauthorized access within the blockchain network.	

In summary, blockchain technology is theoretically positioned to provide exceptional security benefits due to its key design features, including decentralization, robust security integration, immutability, resilience to DDoS attacks, and the transformative potential of smart contracts. Advocates argue that these characteristics should provide superior security over existing technologies. Therefore, the implementation of blockchain technology is likely enhance a firm's cybersecurity performance, a phenomenon we term as the *security-enhancing design effect* of blockchain.

3.1.2. Cybersecurity Disadvantages of Blockchain: The "Technology Uncertainty Effect"

Although blockchain technology boasts strong security features, it operates within the framework of complex sociotechnical systems. As a result, real-world operational challenges may restrict the full realization of blockchain's cybersecurity promises, leaving it exposed to common issues like human error, biases, and contextual weaknesses.

We apply the organizational information processing theory (OIPT) to explain how blockchain technology can result in security challenges (Galbraith 1973; Srinivasan and Swink 2018; Tatikonda and Montoya-Weiss 2001). According to OIPT, firms encountering new tasks face task uncertainty when available information fails to meet task requirements adequately. Task uncertainty implies potential suboptimal outcomes, such as "performance standards will not be met, the task will not be completed on time, and/or the task will be completed at a higher than desired cost" (Stock and Tatikonda 2008, p. 67). In the context of IT adoption, task uncertainty aligns with technology uncertainty. Past studies define technology uncertainty as "the lack of knowledge regarding how to move and implement the technology of interest" (Stock and Tatikonda 2000, p. 724), and have extensively explored the operational challenges posed by technology uncertainty under the umbrella of OIPT (Mackelprang et

al. 2015; Stock and Tatikonda 2008; Tatikonda and Montoya-Weiss 2001; Tatikonda and Rosenthal 2000).

We contend that the adoption of blockchain technology introduces significant technology uncertainty, which in turns increases the cybersecurity risks for firms, due to the following reasons. First, blockchain disrupts firm operations by requiring an overhaul of existing information flows and technology architectures, introducing technology uncertainty and security challenges. Specifically, firms must redesign their business processes and operations to adapt to the new technological landscape. As a private sector expert noted in interviews by Toufaily et al. (2021, p. 5): "Since it [blockchain] is a new system for us, there are implementation costs. Starting with the new interface we are getting to use blockchain, the new hardware, and most importantly the new employees that we will be hiring for our IT department." These adjustments often necessitate discarding accumulated information and extensively integrating new data, which is a time-consuming process fraught with risk (Lind and Zmud 1991; Swanson and Ramiller 2004; Tatikonda and Montoya-Weiss 2001). Gupta (2018, p. 23) highlights the challenges of blockchain implementation: "Change, whether positive or negative, disturbs people as people want stability." Therefore, in the short term of blockchain implementation, insufficient integration of new information likely makes insider actions uncertain and error-prone, often leading to data breaches associated with employee errors and negligence.[7]

Second, the groundbreaking nature of blockchain technology implies restricted availability of cybersecurity information channels connected with the technology, exacerbating technology uncertainty and security vulnerabilities. Given that blockchain technology is a new and relatively undeveloped field for most firms and world at large, there is a lack of established cybersecurity measures and accumulated knowledge to steer its implementation (Hasanova et al. 2019; Wylde et al. 2022). As a result, its adoption frequently occurs without adequate security support. Moreover, the potential vulnerabilities of the technology are often insufficiently identified. Therefore, firms are prone to encountering increased uncertainty in ensuring secure blockchain operations or implementing effective security defenses, leading to an increase in security challenges and a rise in cybersecurity risks.

Third, the complex nature of blockchain technology requires extensive information reservoirs, thereby leading to heightened technology uncertainty and security challenges in practical scenarios. Blockchain technology, being a cutting-edge innovation, is inherently complex and intricate (Hasanova et al. 2019). Such complexity and intricacy is widely recognized as "the worst enemy of security" (Schneier 2015, p. 354) and impedes secure operations and demands a robust reserve of expertise to securely and effectively operate blockchain systems. However, in the early phases of adoption, firms often encounter difficulty in amassing adequate relevant experience, thus resulting in significant technology uncertainty and significant cybersecurity challenges.

[7] Verizon's 2022 Data Breaches Investigations Report suggests that approximately 80% of data breaches involve some human element (source: https://www.verizon.com/business/en-gb/resources/reports/dbir/).

In summary, blockchain technology, as a disruptive and complex innovation, introduces significant technology uncertainty upon adoption, amplifying firms' cybersecurity challenges and risks. We term such a detrimental impact on cybersecurity as the *technology uncertainty effect* of blockchain.

3.2. Hypotheses: The Dynamic Dual-Edged Effect of Blockchain Implementation on Data Breach Risks

The discussion in Section 3.1 delineates the following two competing effects of blockchain implementation on cybersecurity:

(1) *Security-enhancing design effect* of blockchain, in which cybersecurity features inherent in blockchain systems can bolster a firm's defense against cyberattacks, and

(2) *technology uncertainty effect* of blockchain, in which the new integration of blockchain technology may introduce task uncertainty and weaken the firm's security landscape.

However, as the relative strengths of these two effects evolve over time, their combined impact is not static. In the early stages of implementing blockchain, technology uncertainty is especially pronounced as firms frequently have not had enough opportunities to fill information gaps linked to blockchain implementation. Therefore, in the short term, the *technology uncertainty effect*, which is detrimental to cybersecurity, tends to dominate. Yet, over time, the influence of the *technology uncertainty effect* usually diminishes as firms gather information and accumulate knowledge to counteract technological uncertainties. Thus, in the long term, the *security-enhancing design effect* likely outweighs the *technology uncertainty effect*, ultimately resulting in improved cybersecurity for firms. Therefore, we propose the following hypotheses:

HYPOTHESIS 1 (H1): *In the short term, blockchain implementation increases data breach risks*.

HYPOTHESIS 2 (H2): *In the long term, blockchain implementation reduces data breaches risks*.

4. Research Design

4.1. Data and Sample Development

Our research focuses on publicly listed firms in the U.S. To construct our main sample, we compile data from several databases.

We collect data breach data from the Audit Analytics cybersecurity database.[8] If any publicly listed firm in the U.S. is recorded as experiencing a data breach in this source between 2006 and 2022,[9] we include this breach in our data breach sample. Through this process, we accumulate a total of 1,137 data breaches involving 758 publicly listed firms in the U.S. from 2006 to 2022. Table OA-1 (Online Appendix) provides a classification of the 1,137 data breaches recorded in the U.S. during our sample

[8] Audit Analytics cybersecurity database (Source: https://wrds-www.wharton.upenn.edu/pages/get-data/audit-analytics/accounting-oversight/cybersecurity/)

[9] This timeframe (2006 to 2022) represents our sample period (2005 to 2021) lagged by one year.

period. Figure OA-1 (Online Appendix) presents the frequency distribution of these breaches by state, indicating their occurrences across multiple states. Notably, publicly listed firms in California, New York, and Texas experienced significantly more breaches compared to firms in other states.

We utilize state pro-blockchain legislation information provided by Chen et al. (2023). This study sources information on state-level legislation concerning blockchain or distributed ledger technology from the "Blockchain State Legislation" publication by the National Conference of State Legislatures (NCSL). Legislation pertaining to blockchain, distributed ledger, smart contracts, or cryptocurrency is identified by reviewing all summaries of blockchain-related laws on the NCSL website. This thorough process results in the discovery of 41 blockchain legislation bills enacted by 20 states. Subsequently, through the examination of these bill summaries, laws that did not explicitly support the use of blockchain in private sector business and commerce are excluded, resulting in 16 state-level pro-blockchain legislation bills passed by 13 different states. Approximately 12.7% of firm-years in the sample have implemented pro-blockchain laws during our sample period. Table OA-2 (Online Appendix) lists these laws and provides details such as the adopting state, bill number, date of first introduction to a legislative session, date of enactment, and core provisions of each law.

Additionally, we source all accounting data from Compustat, involving 202,401 firm-year observations, to quantify our control variables. We merge the collected data with stock codes and years, then exclude observations with missing control variables, with missing state information, or those from firms located outside the U.S. This results in a final sample of 113,071 firm-year observations from 2005 to 2021, encompassing 870 data breaches that occurred from 2006 to 2022.[10]

Table 3 exhibits the industry distribution within the final sample. As illustrated, the computers/IT sector represents the highest proportion of data breaches in the overall sample, making up 19.18% of all breaches, with the finance sector ranking second at 19.03%. These sectors are particularly vulnerable to data breaches due to the necessity of storing extensive volumes of sensitive customer information.

[10] We only consider the first data breach for each firm within a given year.

Table 3. Sample Distribution by Industry

Industry	SIC Codes	# Observations	% Observations	# Firms	%Firms	#Breaches	%Breaches
Agriculture	1–999	310	0.27	44	0.31	4	0.46
Mining and Construction	1000–1999, excluding 1300–1399	10,874	9.62	1,318	9.2	10	1.15
Food	2000–2111	1,970	1.74	231	1.61	16	1.84
Textiles and Printing	2200–2790	2,853	2.52	333	2.32	29	3.33
Chemicals	2800–2824, 2840–2899	2,185	1.93	254	1.77	11	1.26
Pharmaceuticals	2830–2836	9,774	8.64	1,524	10.64	30	3.45
Extractive Industries	2900–2999, 1300–1399	6,625	5.86	939	6.56	4	0.46
Durable Manufacturers	3000–3999, excluding 3570–3579 and 3670–3679	15,748	13.93	1,926	13.45	100	11.49
Computers/IT	7370–7379, 3570–3579, 3670–3679	12,501	11.06	1,815	12.67	162	18.62
Transportation	4000–4899	4,461	3.95	544	3.8	107	12.3
Energy	4900, 4911–4991	5,062	4.48	485	3.39	10	1.15
Retail	5000–5999	7,474	6.61	874	6.1	120	13.79
Finance	6020–6799	24,513	21.68	2,743	19.15	171	19.66
Services	7000–8999, excluding 7370–7379	7,373	6.52	985	6.88	91	10.46
Others	9000 and above	1,348	1.19	309	2.16	5	0.57
Total		113,071	100	14,324	100	870	100

Note. "# Observations" and "% Observations" represent the number and percentage of firm-year observations; "# Firms" and "% Firms" represent the number and percentage of unique firms; "# Breaches" and "% Breach" represent the number and percentage of data breaches. We adopt the industry classification method proposed by Easton and Pae (2004), which is based on the firms' primary Standard Industrial Classification (SIC) codes.

4.2. Identification Strategy

To evaluate the impact of blockchain implementation on data breach risks, we employ a DiD design. The staggered introduction of pro-blockchain legislation across different states serves as the external shock, enabling us to control for unobserved confounding effects through differencing. To apply the DiD method, we first define the treatment group as firms located in states that have implemented pro-blockchain laws, while the control group comprises firms in states that have not implemented such laws during the same period. Our baseline DiD model, which is a standard staggered DiD model with two-way fixed effects (Dai et al. 2020; De Chaisemartin and d'Haultfoeuille 2020; Huang et al. 2021), is presented as follows:

$$Breach\ Risk_{i,j} = \beta_0 + \beta_1 Post\ Enactment_{i,j} + \alpha_r Control_{i,j} + Firm\ FE + Year\ FE + \epsilon_{i,j+1}. \quad (1)$$

In this equation, i represents firm, and j represents year. Our main outcome variable is *Breach Risk*. Consistent with previous literature (Liu et al. 2015; Wang et al. 2023), we operationalize *Breach Risk* as a binary variable, which equals 1 if a firm experiences at least one breach in the subsequent year, and equals 0 otherwise. Moreover, our main explanatory variable is *Post Enactment*, which is a time indicator variable that equals 1 if at least one pro-blockchain legislation has been passed in the past in states where a firm operates, and equals 0 otherwise.

In our model, we account for various firm-specific and time-varying characteristics that may impact a firm's cybersecurity performance. First, we incorporate controls for firm size (*Size*) as larger firms are more prone to experiencing data breaches. Second, considering the influence of firms' economic performance and available capital on their investment in cybersecurity, we include controls for firm leverage (*Leverage*) and return on assets (*ROA*). Third, we control whether a firm is in a loss position (*Loss Position*) because severe economic problems encountered by such firms will decrease their attention to cybersecurity issues (Higgs et al. 2016). Fourth, we address the vulnerability of firms with significant innovations to external hackers by including research and development expenses (*R&D*). Fifth, we control for IT governance (*IT Governance*), which can dictate the governance model of a firm's cybersecurity (Higgs et al. 2016). For detailed definitions of all variables, please refer to Table OA-3 (Online Appendix).

We also control for fixed differences between the treatment and control groups through firm and year fixed effects. Firm fixed effects control for all time-invariant variables that may affect cybersecurity performance, while year fixed effects control for time variation in the performance across all firms in the sample.

Table 4. Summary Statistics

	All Observations					Treatment Group				Control Group	
						Before Enactment		*Post Enactment*			
	(a)					(b)		(c)		(d)	
	N	Mean	*S.D.*	Min	Max	Mean	*S.D.*	Mean	*S.D.*	Mean	*S.D.*
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
Breach Risk	113,071	0.008	0.087	0.000	1.000	0.008	0.089	0.046	0.209	0.007	0.084
Post Enactment	113,071	0.012	0.111	0.000	1.000	0.000	0.000	1.000	0.000	0.000	0.000
Size	113,071	5.469	2.983	−3.442	11.643	5.953	3.011	6.370	3.196	5.393	2.968
Leverage	113,071	1.203	3.729	0.010	33.619	1.311	3.905	1.637	4.816	1.183	3.687
ROA	113,071	−0.503	2.367	−20.277	0.417	−0.507	2.504	−0.653	2.976	−0.501	2.338
Loss Position	113,071	0.069	0.211	0.000	1.495	0.051	0.183	0.050	0.187	0.072	0.214
R&D	113,071	0.445	0.497	0.000	1.000	0.356	0.479	0.392	0.488	0.458	0.498
IT Governance	113,071	0.038	0.191	0.000	1.000	0.049	0.217	0.056	0.229	0.036	0.187

Notes. This table presents the summary statistics of the main variables. All variables are defined in Table OA-3 (Online Appendix). Column (a) presents descriptive statistics for the overall sample. Columns (b) reports the mean and standard deviation of observations in the treatment group in or before the year of the treatment. Column (c) reports the mean and standard deviation of observations in the treatment group after the enactment of the treatment. Column (d) reports the mean and standard deviation of observations in the control group.

5. Results

5.1. Summary Statistics and Model-Free Estimates

Table 4 presents descriptive statistics for the variables used in the subsequent DiD analysis, divided into three different groups: (1) treatment firms in the pre-treatment period, consisting of 12,929 firm-years, (2) treatment firms in the post-treatment period, comprising 1,404 firm-years, and (3) control firms, totaling 98,738 firm-years.

Table 4 also provides model-free estimates of the impact of exposure to pro-blockchain laws on data breach risks. Prior to the exposure to these laws, treatment firms have an average data breach risk of 0.008, which significantly increases to 0.046 after the exposure. In contrast, control group firms have an average data breach risk of 0.007. These results collectively indicate that exposure to pro-blockchain laws tend to heighten firms' data breach risks.

When assessing treated and control firms, differences in firm characteristics are observed. For example, treatment firms frequently display larger sizes and a tendency towards experiencing fewer losses. This observation is to be expected. The reason is that states that adopt pro-blockchain measures are unlikely to do so randomly; instead, those with stronger economic performance are more likely to embrace blockchain-supportive legislation. Consequently, firms situated in these states are prone to exhibit variations in firm characteristics compared to firms in states that have not adopted such legislation. To mitigate the impact of these unobserved variables, as a robustness check, we further perform a PSM approach. To mitigate the effect of outliers in our subsequent tests, we winsorize all firm-year continuous variables at the 1% and 99% levels, respectively.

5.2. Baseline Results

5.2.1. Testing for Hypothesis 1

We first test H1, which pertains to the short-term impact of blockchain implementation on firm cybersecurity. Table 5 displays the baseline DiD regression results regarding this effect. We employ fixed effects linear probability model (LPM) regression, consistent with prior research on data breach risks (D'Arcy et al. 2020; Haislip et al. 2021; Wang et al. 2023). In each case, we control for firm and year fixed effects.

Column (1) includes only *Post Enactment* as the independent variable. The estimated coefficient for *Post Enactment* is 0.015, significant at the 1% level, indicating that firms experience more data breach risks after exposure to pro-blockchain laws compared to those not exposed to such laws. Thus, this evidence supports H1. Column (2) additionally introduce all the control variables. Despite these controls, the coefficient for *Post Enactment* remains significantly positive (at the 1% level). The coefficient is also economically significant. According to column (2), firms experience a 1.5% increase in data breach risks after exposure to supportive blockchain laws compared to those not exposed to such laws; this increase accounts for 187.5% of the sample mean breach probability of 0.8%.

However, ensuring the validity of the DiD estimates necessitates fulfilling the parallel trends assumption. This assumption underscores the necessity for the trends in data breach risks to follow parallel trajectories between the treatment and control groups during the pre-treatment phase. Significant differences in pre-treatment trends would violate the assumption of parallel pre-trends, indicating potential confounding factors that could affect causal interpretation. To ensure meeting the parallel trends assumption, in column (3) of Table 5, we conduct a parallel trend test using the following model equation:

$$Breach\ Risk_{i,j} = \beta_0 + \sum_{-3\le t\le 3} \beta_t Year_{i,j}^{t} + \alpha_r Control_{i,j} + Firm\ FE + Year\ FE + \epsilon_{i,j+1}. \quad (2)$$

In this equation, t represents the number of years relative to the enactment of pro-blockchain laws in the state where the firm is located (e.g., if a state passes a pro-blockchain law in 2010, then for firms operating within this state, $t = -1$ for the year 2009 and $t = 1$ for the year 2011). $Year^t$ is defined as an indicator that equals 1 if the year corresponds to the relative t-th year following the enactment of pro-blockchain laws. To avoid multicollinearity, we follow the standard practice of dynamic DiD and exclude the period closest to the data breach before the treatment (i.e., $Year^{-1}$) (e.g., Baker et al., 2022; Zhang et al., 2023).

In column (3), Table 5, the coefficients for the pre-treatment period ($Year^{-3}$, $Year^{-2}$) are insignificant, suggesting fulfillment of the parallel trends assumption. Conversely, the coefficient for $Year^{2}$ is significant and positive, indicating an increase in firms' data breach risks following exposure to pro-blockchain laws. Additionally, the significant differences between lagged and lead indicators suggest that the results are not influenced by reverse causality. Section (a) of Figure OA-4 (Online Appendix) offers supplementary visualization of the parallel trend test results (with the 90% confidence intervals). This figure shows that for $t < 0$ (i.e., the pre-treatment years), the point estimates of β_t are centered around the zero level, reinforcing the conclusion that the assumption of parallel pre-trends in the DiD analysis holds.

Table 5. Blockchain and Data Breach Risks: Short-Term Analysis

	Dependent variable: *Breach Risk*		
	(1)	(2)	(3)
Post Enactment	0.015***	0.015***	
	(2.606)	(2.607)	
Year 3-			0.002
			(0.373)
Year -2			0.007
			(1.087)
Current			0.001
			(0.117)
Year +1			0.010
			(1.332)
Year +2			0.033***
			(2.761)
Year 3+			0.013
			(0.773)
Firm Size		0.002***	0.002***

		(4.824)	(4.828)
Leverage		0.000	0.000
		(0.146)	(0.161)
ROA		0.002***	0.002***
		(4.824)	(4.828)
Firm Loss		0.000	0.000
		(0.146)	(0.161)
R&D		−0.000***	−0.000***
		(−3.053)	(−2.995)
IT Governance		0.003***	0.003***
		(3.332)	(3.277)
Intercept	Yes	Yes	Yes
Firm FE	Yes	Yes	Yes
Year FE	Yes	Yes	Yes
N	111,405	111,405	111,405
Adjusted R^2	0.067	0.067	0.067

Notes. Results of the baseline analysis (short-term analysis). The table provides the baseline analysis that examine the short-term impact of blockchain implementation on data breach risks. The sample includes 113,071 observations. 1,666 singleton observations are removed from each regression, leaving 111,405 observations remain for each regression. The dependent variable is *Breach Risk*. Column (1) presents results without any control variables, while column (2) presents results with further introducing all control variables. Column (3) presents results of the parallel trend test. Definitions for all other variables can be found in Table OA-3 (Online Appendix). Standard errors are adjusted to account for heteroskedasticity. *t* statistics in parentheses, * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

5.2.2. Testing for Hypothesis 2

Then, we test H2, which pertains to the long-term impact of blockchain implementation on firm cybersecurity. We examine the dynamic impacts of exposure to pro-blockchain laws on data breach risks, which vary across different time frames surrounding the exposure, as in Dai et al. (2020).

Table 6 reports the relevant baseline results. Columns (1)-(7) and columns (8)-(14) are similar to columns (1) and (2) of Table 5, respectively, except for the replacement of the *Breach Risk* with constructing this variable seven periods prior to and following the focal year. The findings in this table indicate that across different specifications, the effect of exposure to pro-blockchain laws on increasing data breach risks becomes significant from the Year *t* (i.e., the current year) onwards, and this increase in data breach risks is of a relatively short duration, fading away after Year *t*+1. Over time, the security benefits of pro-blockchain law adoption gradually become predominant, with a significant reduction in data breach risks observed starting from Year *t*+4. Thus, the results above support H2, which predicts that in the long term, blockchain implementation helps reduce a firm's data breach risks.

Table 6. Blockchain and Data Breach Risks: Long-Term Analysis

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Breach Risk in	Year *t*−2	Year *t*−1	Year *t*	Year *t*+1	Year *t*+2	Year *t*+3	Year *t*+4
Post Enactment	−0.000	0.002	0.015***	0.024**	0.004	−0.038	−0.181***
	(−0.089)	(0.554)	(2.606)	(2.327)	(0.225)	(−0.520)	(−11.499)
Intercept	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Controls	No	No	No	No	No	No	No
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	(8)	(9)	(10)	(11)	(12)	(13)	(14)
Breach Risk in	Year *t*−2	Year *t*−1	Year *t*	Year *t*+1	Year *t*+2	Year *t*+3	Year *t*+4
Post Enactment	−0.000	0.002	0.015***	0.024**	0.004	−0.038	−0.180***
	(−0.108)	(0.551)	(2.607)	(2.322)	(0.218)	(−0.520)	(−11.426)
Intercept	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Notes. Results of the baseline analysis (long-term analysis). The table provides coefficients estimated from DiD regressions examining the long-term impact of blockchain implementation on data breach risks. The sample includes 113,071 observations. The dependent variable is *Breach Risk* measured for each focal year, spanning from two years before to three years after the treatment year. Columns (1)-(7) presents results without any control variables, while columns (8)-(14) presents results with further introducing all control variables. Definitions for all other variables can be found in Table OA-3 (Online Appendix). Standard errors are adjusted to account for heteroskedasticity. *t* statistics in parentheses, * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

5.3. Robustness Checks

To further establish the evidence of the dynamic dual-edged effects of blockchain implementation on firm data breach risks as causal, in this section, we first employ PSM to reduce heterogeneity between groups, and then, we address a range of potential issues that may introduce bias.

5.3.1. Difference-in-Difference Estimations with Matched Samples

Although our parallel trend test provides evidence indicating parallel pre-trends between the treatment and control groups, we further employ PSM to enhance comparability between groups and further mitigate potential issues of self-selection (Rosenbaum and Rubin 1983). For treatment firms, we identify their respective matches using the generated propensity score, with all control variables and industry dummy variables serving as the matching criteria. We perform 1:2 nearest neighbor matching, ensuring that the absolute difference in propensity scores between matched firms is limited to within 0.01. Once a matching control firm is selected from the control sample, it is removed from the matching pool. We retain only successfully matched firms. Through this process, we obtain a matched sample containing 37,877 observations (14,251 in the treatment group and 23,626 in the control group).

For brevity, additional details of the PSM method are reported in Table OA-5 (Online Appendix). Panel A of Table OA-5 (Online Appendix) compares the characteristics of treated and control firms before exposure to pro-blockchain law. The results indicate that before this exposure, treatment and control firms exhibit similar characteristics across all control variables, suggesting that these characteristics are unlikely to lead to differences in firms' data breach risks post-treatment. We also examine the differences in propensity scores between treatment firms and matched control firms. Panel

B shows that these differences are very small. Overall, diagnostic tests reported in Table OA-5 (Online Appendix) suggest that the PSM process aids in eliminating evident sample selection bias and in creating balanced comparison groups.

In Table 7, we present the results of the DiD regression analysis on the short-term effects of blockchain implementation, utilizing the PSM sample. Columns (1) and (2) employ the same specifications as columns (1) and (2) in Table 5, respectively. Both columns show significant positive coefficients for *Post Enactment*, consistent with the findings in the baseline analyses of Table 5.

Furthermore, in Table 7, column (3) performs a parallel trend test to evaluate whether the PSM sample satisfies the parallel trend assumption, employing the same specification as column (3) in Table 5. Similarly, the insignificant coefficients for the pre-treatment periods (*Year* $^{3-}$, *Year* $^{-2}$) suggest no deviation from this assumption. Conversely, significant positive coefficient for *Year* $^{+2}$ once again suggest an increase in data breach risks following exposure to pro-blockchain laws. Figure OA-4 (Section (b)) of the Online Appendix provides additional visual evidence supporting the fulfillment of the parallel pre-trends assumption in the DiD analysis with the PSM sample.

Then, we provide the DiD regression results on the long-term impact of blockchain implementation, utilizing the PSM sample. We employ the same models as in Table 6 and obtain estimates (please see Table 8) that are largely consistent to those previously obtained. These results further underscore that exposure to pro-blockchain laws is associated with a reduction in firms' data breach risks in the long run.

Table 7. Blockchain and Data Breach Risks: Short Term Analysis (PSM Sample)

	Dependent variable: *Breach Risk*		
	(1)	(2)	(3)
Post Enactment	0.015**	0.015**	
	(2.238)	(2.241)	
Year $^{3-}$			0.004
			(0.778)
Year $^{-2}$			0.006
			(0.835)
Current			0.000
			(0.021)
Year $^{+1}$			0.012
			(1.424)
Year $^{+2}$			0.033**
			(2.572)
Year $^{3+}$			0.012
			(0.672)
Intercept	Yes	Yes	Yes
Controls	No	Yes	Yes
Firm FE	Yes	Yes	Yes
Year FE	Yes	Yes	Yes
N	34,445	34,445	34,445
Adjusted R^2	0.064	0.064	0.064

Notes. PSM results (short-term analysis). The table provides coefficients estimated from DiD regressions examining the short-term impact of blockchain implementation on data breach risks. The sample is a PSM sample, which includes 37,877 observations;

however, 3,432 singleton observations are removed from each regression, leaving 34,445 observations remain for each regression. The dependent variable is *Breach Risk*. Column (1) presents results without any control variables, while column (2) presents results with further introducing all control variables. Column (3) presents results of the parallel trend test. Definitions for all other variables can be found in Table OA-3 (Online Appendix). Standard errors are adjusted to account for heteroskedasticity. *t* statistics in parentheses, * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

Table 8. Blockchain and Data Breach Risks: Long Term Analysis (PSM Sample)

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Breach Risk in	Year *t*−2	Year *t*−1	Year *t*	Year *t*+1	Year *t*+2	Year *t*+3	Year *t*+4
Post Enactment	−0.004	−0.000	0.015**	0.017*	−0.017	−0.136	−0.269***
	(−1.069)	(−0.069)	(2.238)	(1.647)	(−0.797)	(−1.639)	(−5.646)
Intercept	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Controls	No	No	No	No	No	No	No
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	(8)	(9)	(10)	(11)	(12)	(13)	(14)
Breach Risk in	Year *t*−2	Year *t*−1	Year *t*	Year *t*+1	Year *t*+2	Year *t*+3	Year *t*+4
Post Enactment	−0.005	−0.000	0.015**	0.017	−0.017	−0.136	−0.267***
	(−1.085)	(−0.084)	(2.241)	(1.630)	(−0.793)	(−1.638)	(−5.579)
Intercept	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Notes. PSM results (long-term analysis). The table provides coefficients estimated from DiD regressions examining the long-term impact of blockchain implementation on data breach risks. The sample is a PSM sample, which includes 37,877 observations. The dependent variable is *Breach Risk* measured for each focal year, spanning from two years before to three years after the treatment year. Columns (1)-(7) presents results without any control variables, while columns (8)-(14) presents results with further introducing all control variables. Definitions for all other variables can be found in Table OA-3 (Online Appendix). Standard errors are adjusted to account for heteroskedasticity. *t* statistics in parentheses, * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

5.3.2. Additional Robustness Checks

To further enhance the robustness of our research findings, we perform a series of supplementary robustness tests, as shown in Tables 9 and 10. We describe our testing procedures below.

First, PSM entails a considerable loss of sample data during the matching process, which may undermine the persuasiveness of the results. Moreover, employing a single matching approach may introduce bias into our analysis. In order to address these concerns, we adopt an alternative matching approach of entropy balancing, which is an alternative and novel multivariate matching method. Entropy balancing, as introduced by Hainmueller (2012), has gained widespread adoption in recent research endeavors (e.g., Hendricks et al. 2019; Zhang et al. 2023). By employing sample weight adjustments, this approach enables the construction of a control group sample with covariate distributions that closely resemble those of the treatment group, without compromising sample size (Hainmueller 2012). We utilize entropy balancing matching as a replacement for PSM in our sample to achieve covariate balance in our matched samples. All control variables are included in the entropy balancing process as covariates for balancing. The results of the entropy balancing process are presented in Online Appendix OA-6, which support the effectiveness of this method. We replicate our baseline analyses from Tables 5 and 6 using the entropy balancing-matched sample. Columns (1) and (2), Table 9, presents the results of the relevant short-term analysis, while Panel A of Table 10 displays the results

of the relevant long-term analysis. All findings remain consistent with the baseline results, further reinforcing the robustness of our findings.

Second, we cluster robust standard errors at different levels. In our primary analysis, to address potential issues related to heteroscedasticity in regression analysis, we employ heteroscedasticity-robust standard errors. Additionally, considering the enactment of pro-blockchain laws at the state level, we alternatively cluster standard errors at the state and year levels, and then we replicate the baseline long-term and short-term analyses. Columns (3) and (4) in Table 9 present the results of the corresponding short-term analysis, while Panel B of Table 10 shows the outcomes of the relevant long-term analysis. All results are consistent with the baseline findings, further substantiating the robustness of our findings.

Third, for our earlier analyses, we use a staggered DiD approach because of the staggered introduction of pro-blockchain legislation across different states. However, recent research has raised a concern with this method: in staggered adoption settings, previously treated entities may later become comparison units. These entities, having already incorporated dynamic treatment effects, may act as "bad" comparisons, causing biased estimates (Callaway and Sant'Anna 2021; Goodman-Bacon 2021). To address this concern, we use a stacked DiD method, which excludes previously treated entities at each time point, thus avoiding their inclusion as "bad" comparisons (Cengiz et al. 2019; Deshpande and Li 2019; Wing et al. 2024). Similar to Cengiz et al. (2019), at each treatment time point t, we form a cohort by selecting firms in states that have not implemented such laws between $t-4$ years and $t+3$ years as the control group. We then combine all the generated cohorts into a new sample and re-run the baseline DiD analyses in Tables 5 and 6 using this stacked sample, controlling for cohort-firm FEs and cohort-year FEs (Cengiz et al., 2019). Columns (5) and (6) of Table 9 present the results of the relevant short-term analysis, while Panel C of Table 10 exhibits the outcomes of the relevant long-term analysis. All results are in line with the baseline findings, further substantiating the robustness of our findings.

Lastly, we address potential influences from random factors or other underlying time-series factors by conducting a placebo test. This test, similar to approaches by Ferrara et al. (2012) and Burtch et al. (2018), involves randomly assigning pro-blockchain enactment years to control firms to create a random experiment. To enhance the effectiveness of the placebo test, we repeat the process 500 times and generate a distribution plot of estimated coefficients. Details of the placebo test can be found in Online Appendix OA-7. Figure OA-7 (Online Appendix) displays the distribution plot of estimated coefficients from the placebo test, showing that the coefficients cluster around zero. Additionally, the dashed line represents the coefficient of the true treatment virtual variable. In nearly 500 random experiments, the estimated values for the outcome variable do not exceed this true value, indicating that occurrences of actual baseline coefficients under random sampling are rare. The integration of these findings supports our conclusion that the main effects results are not influenced by randomness or other potential time-series factors.

Table 9. Additional Robustness Tests: Short-Term Analysis

	Dependent variable: *Breach Risk*					
	Entropy balancing matching		State-year clustered		Stacked DiD	
	(1)	(2)	(3)	(4)	(5)	(6)
Post Enactment	0.015**	0.015**	0.015**	0.015**	0.016***	0.016***
	(2.238)	(2.241)	(2.209)	(2.214)	(2.820)	(2.821)
Intercept	Yes	Yes	Yes	Yes	Yes	Yes
Controls	No	Yes	No	Yes	No	Yes
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes
Industry-year FE	No	No	No	No	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes
N	111,405	111,405	111,405	111,405	178,619	178,619
Adjusted R^2	0.438	0.438	0.067	0.067	0.087	0.087

Notes. Results of the robustness tests (short-term analysis). The table provides coefficients estimated from DiD regressions examining the short-term impact of blockchain implementation on data breach risks. In columns (1) and (2), we replicate columns (1) and (2) in Table 5 by alternatively employing the entropy balancing-matched sample. In columns (3) to (4), we replicate columns (1) and (2) in Table 5 by alternatively clustering standard errors at the state and year levels. In columns (5) to (6), we replicate columns (1) and (2) in Table 5 by employing the stacked sample and controlling for cohort-firm FEs and cohort-year FEs. Definitions for all other variables can be found in Table OA-3 (Online Appendix). *t* statistics in parentheses, * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

Table 10. Additional Robustness Tests: Long-Term Analysis

Panel A. Entropy Balancing Matching

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Internal Breach Risk in	Year *t*−2	Year *t*−1	Year *t*	Year *t*+1	Year *t*+2	Year *t*+3	Year *t*+4
Post Enactment	−0.007	−0.004	0.018***	0.033***	0.005	0.006	−0.228***
	(−1.391)	(−0.856)	(3.031)	(4.122)	(0.431)	(0.142)	(−11.615)
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Panel B. State-year Clustered

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
External Breach Risk in	Year *t*−2	Year *t*−1	Year *t*	Year *t*+1	Year *t*+2	Year *t*+3	Year *t*+4
Post Enactment	−0.000	0.002	0.015**	0.024*	0.004	−0.038	−0.180***
	(−0.115)	(0.607)	(2.214)	(1.817)	(0.309)	(−1.479)	(−7.703)
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Panel C. Stacked DiD

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
External Breach Risk in	Year *t*−2	Year *t*−1	Year *t*	Year *t*+1	Year *t*+2	Year *t*+3	Year *t*+4
Post Enactment	−0.001	0.000	0.016***	0.026***	0.007	−0.029	−0.165***
	(−0.192)	(0.127)	(2.821)	(2.612)	(0.416)	(−0.412)	(−10.072)
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry-year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Notes. Results of the robustness tests (long-term analysis). The table provides coefficients estimated from DiD regressions examining the long-term impact of blockchain implementation on data breach risks. Panel A of this table replicates columns (8)-(14) of Table 6 by alternatively employing the entropy balancing-matched sample. Panel B of this table replicates columns (8)-(14) of Table 6 by alternatively clustering standard errors at the state and year levels. Panel C of this table replicates columns (8)-(14) of Table 6 by employing the stacked sample and controlling for cohort-firm FEs and cohort-year FEs. Definitions for all other variables can be found in Table OA-3 (Online Appendix). *t* statistics in parentheses, * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

6. Empirical Extensions

6.1. Mechanism Identification: Based on the Effect Heterogeneity across Different Types of Data Breach Risks

In the preceding section, using DiD specifications, we observe a dynamic dual-edged effect of pro-blockchain law adoption on firms' data breach risks. Theoretically, we attribute this effect to the dynamic counteracting effects between the *security-enhancing design effect* and the *technology uncertainty effect*. To establish effective causal inference between blockchain implementation and cybersecurity risks, identifying the above mechanisms (i.e., *security-enhancing design effect* and *technology uncertainty effect*) is crucial. However, identifying these two mechanisms in our setting is challenging as they are difficult to directly observe and measure based on available data. Therefore, we employ methods to observe treatment effect heterogeneity to offer some suggestive evidence for identifying and understanding these mechanisms (Chu et al. 2019; Goldfarb and Tucker 2014; Sun et al. 2021).

Considering the effectiveness of our mechanisms, i.e., the *security-enhancing design effect* and *technology uncertainty effect*, varies significantly depending on the types of data breach risks, we specifically examine the variability in treatment effects across these types. Typically, data breaches are classified into the following two types based on the parties directly responsible for the breach (Cheng et al. 2017; Kwon and Johnson 2014):

(i) External data breaches, which occur when external actors (e.g., hackers) directly cause the breach. External hackers may employ various tactics, including randomized attacks or targeted exploitation of employees' inadequate utilization of information technology resources, to breach corporate computer networks. Additionally, they may exploit vulnerabilities in outdated software or misconfigured network settings to gain unauthorized access. Therefore, the likelihood of a firm experiencing external breaches is influenced by the inherent security resilience of its IT systems and the robustness of security protocols (Cheng et al. 2017).

(ii) Internal data breaches, which are caused by firms' insiders (e.g., employees, collaborators, or temporary workers). While some internal breaches stem from malicious intent among insiders, the majority of breaches often result from their operational errors (Verizon 2013). Internal breaches are often attributed to employee errors. As a result, uncertainty surrounding employee actions—whether caused by inadequate training, lack of awareness, or insufficient proficiency in handling sensitive information and adhering to security protocols—can increase the likelihood of mistakes, contributing to a substantial number of internal data breaches.

Then, we analyze how the short-term and long-term effects of blockchain depend on the type of data breaches, and formulate the following predictions:

(i) In our theory, the short-term rise in data breach risks linked to blockchain

implementation is mainly driven by the *technology uncertainty effect*. Nonetheless, this effect disproportionately affects internal and external data breach risks. Specifically, this effect primarily operates on internal data breach risks by causing employees to struggle with the complexities of new technologies, making them more prone to errors or misconfigurations (D'Arcy et al. 2014; D'Arcy and Teh 2019). However, its influence on the behavior of external actors (e.g., hackers) and external data breach risks is relatively limited. Therefore, we predict that in the short term, blockchain will more significantly increase internal data breach risks than external ones.

(ii) Conversely, in the long term, the reduction in data breach risks associated with blockchain is mainly driven by the *security-enhancing design effect*. Nonetheless, the security-enhancing design effect also unequally impacts internal and external data breach risks. This effect primarily benefits firms in resisting external attacks by making firms' networks more resistant to hacking or data tampering (Kshetri 2017; Yadav et al. 2022). Therefore, we expect that the *security-enhancing design effect* could become dominant earlier for external data breach risks than for internal data breach risks. Accordingly, we predict that in the long term, blockchain will reduce external data breach risks earlier than internal ones.

To test the above predictions, we construct indicators for internal data breach risk (*Internal Breach Risk*) and external data breach risk (*External Breach Risk*). Specifically, *Internal Breach Risk* is an indicator variable equal to 1 if a firm experiences at least one internal breach in the subsequent year, and 0 otherwise. An internal breach is identified if the type of attack is categorized as "Unauthorized Access" or "Misconfiguration" according to the Audit Analytics. Similarly, *External Breach Risk* is an indicator variable equal to 1 if a firm experiences at least one external breach in the subsequent year, and 0 otherwise. An external breach is identified if the type of attack is categorized as "Phishing," "Malware," "Ransomware," "Phishing or Unauthorized," or "Malware or Phishing" according to the Audit Analytics.

Tables 11 and 12 illustrate the treatment effects across different breach types, covering short-term and long-term analyses, respectively. In Table 11, columns (1) and (2) are similar to columns (1) and (2) (Table 5), with the outcome variable being *Internal Breach Risk*. Across different specifications in columns (1) and (2), the coefficients for *Post Enactment* are consistently and significantly positive. Columns (4) and (5) (Table 11) are also analogous to columns (1) and (2) (Table 5) but with *External Breach Risk* as the outcome variable. Across different specifications in columns (4) and (5), the coefficients for *Post Enactment* are consistently insignificant. Thus, an integration of the results from Table 11 supports our prediction and suggests that in the short term, exposure to pro-blockchain laws only significantly increases firms' internal data breach risks rather than their external data breach risks. The results shown in the columns (3) and (6) of Table 11, alongside the graphical representation in sections (c) and (d) of Figure OA-4 (Online Appendix), provide strong support the fulfillment of the parallel pre-trends assumption in the DiD analyses concerning breach types.

Table 11. Effects of Blockchain Across Various Breach Types (Short-term Analysis)

Dependent variable:	*Internal Breach Risk*			*External Breach Risk*		
	(1)	(2)	(3)	(4)	(5)	(6)
Post Enactment	0.012***	0.012***		0.003	0.003	
	(2.761)	(2.756)		(0.837)	(0.844)	
Year $^{3-}$			0.000			0.000
			(0.121)			(0.011)
Year $^{-2}$			0.001			0.004
			(0.314)			(0.805)
Current			−0.000			−0.000
			(−0.064)			(−0.066)
Year $^{+1}$			0.005			0.007
			(1.046)			(1.197)
Year $^{+2}$			0.030***			0.002
			(2.952)			(0.279)
Year $^{3+}$			0.011			0.004
			(0.867)			(0.368)
Intercept	Yes	Yes	Yes	Yes	Yes	Yes
Controls	No	Yes	Yes	No	Yes	Yes
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes
N	111,361	111,361	111,361	111,361	111,361	111,361
Adjusted R^2	0.013	−0.025	0.013	−0.024	0.014	−0.024

Notes. Results of the analyses on effect heterogeneity across breach types (short-term analysis). The table provides coefficients estimated from DiD regressions examining the short-term impact of blockchain implementation on internal or external data breach risks. In columns (1) to (3), we replicate Table 5 by alternatively employing *Internal Breach Risk* as the dependent variable. In columns (4) to (6), we replicate Table 5 by alternatively employing *External Breach Risk* as the dependent variable. Definitions for all other variables can be found in Table OA-3 (Online Appendix). Standard errors are adjusted to account for heteroskedasticity. *t* statistics in parentheses, * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

In Table 12, both panels A and B, the methodology mirrors Panel B of Table 6, with alternatively utilizing the dynamic measures of *Internal Breach Risk* and *External Breach Risk* as substitutes for the dynamic measures of *Breach Risk*. Then, we compare the results from panels A and B of Table 12 to observe the varying impacts of blockchain on internal and external data breach risks. During the short-term period (Year *t* and Year *t*+1), the coefficient of *Post Enactment* is significant only when *Internal Breach Risk* (as opposed to *External Breach Risk*) is used as the outcome variable. This implies that in the short term, blockchain implementation primarily increases internal data breach risks, aligning with the findings presented in Table 11. Furthermore, in Panel A, the coefficient of *Post Enactment* begins to demonstrate negative significance starting from Year *t*+4, whereas in Panel B, the coefficient of *Post Enactment* starts to exhibit negative significance from Year *t*+3. Hence, the findings support our conjecture that in the long term, blockchain decreases external data breach risks earlier than internal data breach risks.

Table 12. Effects of Blockchain Across Various Breach Types (Long-Term Analysis)

Panel A. Effects on Internal Data Breach Risks							
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Internal Breach Risk in	Year *t*−2	Year *t*−1	Year *t*	Year *t*+1	Year *t*+2	Year *t*+3	Year *t*+4
Post Enactment	0.000	0.002	0.012***	0.023***	0.006	−0.020	−0.092***
	(0.026)	(0.925)	(2.756)	(2.686)	(0.446)	(−0.366)	(−7.576)

Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Panel B. Effects on External Data Breach Risks							
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
External Breach Risk in	Year *t*−2	Year *t*−1	Year *t*	Year *t*+1	Year *t*+2	Year *t*+3	Year *t*+4
Post Enactment	0.001	0.001	0.003	−0.003	−0.004	−0.026***	−0.025***
	(0.455)	(0.512)	(0.844)	(−0.650)	(−0.387)	(−2.898)	(−3.284)
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Notes. Results of the analyses on effect heterogeneity across breach types (long-term analysis). The table provides coefficients estimated from DiD regressions examining the long-term impact of blockchain implementation on internal or external data breach risks. Panel A of this table replicates Panel B of Table 6 by alternatively employing *Internal Breach Risk* as the dependent variable. Panel B of this table replicates Panel B of Table 6 by alternatively employing *External Breach Risk* as the dependent variable. Definitions for all other variables can be found in Table OA-3 (Online Appendix). Standard errors are adjusted to account for heteroskedasticity. *t* statistics in parentheses, * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

6.2. Exploration of Contextual Factors

In this section, we investigate how the short-term effects of blockchain implementation vary based on different contextual factors, seeking to broaden the scope of and enhance the understanding of our research findings. In our theoretical framework, the short-term impacts of blockchain are mainly driven by the *technology uncertainty effect*. OPIT suggests that firms can mitigate technology uncertainty through robust relevant capabilities and resources (Galbraith 1973; Tatikonda and Montoya-Weiss 2001). Thus, in this section, we specifically examine two contextual factors: (1) managers' IT industry experience and (2) human resource sufficiency.

6.2.1. Contextual Factor: IT Industry Experience

According to OIPT, the divergence between technological operational needs and a firm's capabilities shapes the degree of technology uncertainty (Stock and Tatikonda 2008; Tatikonda and Montoya-Weiss 2001). Therefore, one of the primary ways to reduce the technology uncertainty brought about by blockchain is by enhancing the relevant capabilities of the firm. In this regard, managerial IT expertise is an important capability. One of the most effective ways for managers to accumulate experience with blockchain technology is through serving in the IT industry (Faleye et al. 2018; Moroney 2007). Managers with IT industry experience often have exposure to diverse cutting-edge technologies, including blockchain. They may have more opportunities to directly engage with blockchain-related projects and practices, thereby enhancing their understanding and ability to leverage blockchain. This experience often equips them to play a more proactive role in decision-making and strategy formulation related to blockchain implementation. Therefore, managers' extensive experience in the IT industry tends to be instrumental in resolving the technology uncertainty introduced by blockchain. Given that blockchain implementation's impact on increasing short-term data breach risks is mainly attributed to the *technology uncertainty effect*, we predict that managers' IT industry experience mitigates this effect.

To validate this prediction, we construct managers' *IT Industry Experience* as an indicator variable that equals 1 if a firm's CEO, CFO, or CTO has previously worked in the IT industry, and 0 otherwise.[11] Subsequently, we introduce the interaction term between *IT Industry Experience* and *Post Enactment*, along with the individual term of *IT Industry Experience*, into columns (1) and (2) of Table 5. The corresponding outcomes are presented in columns (1) and (2) of Table 13. Across various specifications, the coefficients of *Post Enactment* × *IT Industry Experience* are significantly and consistently negative, suggesting that the short-term increase in data breach risks attributable to blockchain implementation is mitigated when managers possess considerable IT industry experience. This finding supports our earlier prediction.

6.2.2. Contextual Factor: Human Resource Sufficiency

Management studies widely recognize that having extra human resources allows firms to respond more flexibly to changes and enhances adaptability (Azadegan et al. 2013; Mishina et al. 2004; Wiengarten et al. 2019). Similarly, when facing changes brought about by blockchain implementation, extra human resources often enable firms to allocate resources more flexibly to handle the challenges and technology uncertainties associated with the blockchain implementation. For example, having a sufficient number of available employees enables a firm to handle the research, training, and implementation necessary for successful blockchain implementation. Moreover, a larger pool of employees enables firms to allocate dedicated teams to address operational challenges specific to blockchain without detrimentally affecting other critical business functions. Consequently, we expect that, with a substantial pool of employees at hand, the *technology uncertainty effect* induced by blockchain will likely be alleviated, weakening the short-term effect of blockchain in increasing data breach risks.

To examine this prediction, we follow prior literature and construct *Human Resource Sufficiency* as the natural logarithm of the industry-adjusted ratio of labor to annual sales (Azadegan et al. 2013; Wiengarten et al. 2019). Increased labor to sales indicates that sufficient labor is available for operational adjustments. Subsequently, we incorporate the interaction term of *Post Enactment* × *Human Resource Sufficiency*, alongside the individual term of *Human Resource Sufficiency*, into columns (1) and (2) of Table 5. The corresponding results are shown in columns (1) and (2) of Table 13. Across different model specifications, the coefficients of the interaction term are significantly negative, suggesting that the short-term increase in data breach risks associated with blockchain implementation is alleviated when the firms possesses ample human resources. This result confirms our expectation.

[11] Following Kim et al. (2016), we define IT firms as the ones in IT industries, and we define IT industries based on the following four-digit SIC codes: 3570, 3571, 3572, 3576, 3577, 3578, 3579, 3661, 3663, 3674, 3812, 3822, 3825, 3826, 3827, 3842, 3845, 3861, 4812, 4813, 4822, 4832, 4833, 4841, 4899, 7370, 7371, 7372, 7373, or 7374.

Table 13. Exploration of Contextual Factors

	Dependent variable: *Breach Risk*			
	(1)	(2)	(3)	(4)
Post Enactment	0.015**	0.015***	0.015**	0.015***
	(2.563)	(4.218)	(2.566)	(4.254)
Post Enactment× IT Industry Experience	−0.011***		−0.011***	
	(−3.457)		(−3.392)	
Post Enactment× Human Resource Sufficiency		−0.018***		−0.018***
		(−5.530)		(−5.530)
IT Industry Experience	−0.001***		−0.001***	
	(−2.617)		(−2.710)	
Human Resource Sufficiency		−0.000		0.000
		(−0.307)		(0.020)
Intercept	Yes	Yes	Yes	Yes
Control	No	No	Yes	Yes
Firm FE	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes
N	110,585	82,392	110,585	82,392
Adjusted R^2	0.065	0.075	0.065	0.075

Notes. Results of the analyses on contextual factors (short-term analysis). This table presents coefficients from DiD regressions of the moderating effect of managers' IT industry experience and human resource sufficiency. Definitions for all other variables can be found in Table OA-3 (Online Appendix). Standard errors are adjusted to account for heteroskedasticity. *t* statistics in parentheses, * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

7. Concluding Remarks

Our study comprehensively analyzes the impact of blockchain implementation on firm cybersecurity through a quasi-natural experiment, in which we employ the staggered implementation of pro-blockchain laws across U.S. states as an external shock to encourage local firms to adopt blockchain technology. We find that blockchain implementation has a dual-edged and dynamic impact on cybersecurity. In the short term, it increases firms' data breach risks. However, as firms become more adept at managing blockchain technology, it reduces these risks in the long term. Empirical extensions reveal further nuances of these effects of blockchain implementation: the short-term rise in the risks primarily impacts internal breaches, such as those caused by employee errors and misconfigurations, whereas the long-term decrease in data breach risks occurs earlier in preventing external breaches, such as hacking. Additionally, we find that managers' IT industry experience and sufficient human resources play crucial roles in mitigating the short-term increases in data breach risks associated with blockchain implementation.

7.1. Theoretical Contributions and Implications

Our research makes several noteworthy contributions to the literature. First, it builds on and advances prior cybersecurity research, especially empirical studies investigating the determinants of data breach risks. These empirical studies have previously yielded mixed findings on the impact of IT on cybersecurity, generally suggesting that such an impact is dual-edged and can be both beneficial and

detrimental (Angst et al. 2017; Kwon and Johnson 2014; Sen and Borle 2015; Wang et al. 2023). By offering empirical evidence specific to blockchain, our research not only supports these earlier findings but also adds greater depth and specificity. Specifically, we show the temporal nature of the risks and benefits of technology implementation change over time. Additionally, we address a gap in this strand of research, where studies frequently use aggregated IT measures but fail to consider the effects of any individual IT component on cybersecurity. By examining blockchain specifically, our study offers a more nuanced perspective on IT's impact on cybersecurity, thereby extending the previous research.

Second, our study adds to the existing blockchain literature. Although the literature on blockchain is diverse, it is primarily conceptual (e.g., Nowiński and Kozma 2017), descriptive (e.g., Fabian et al. 2018; Tapscott and Tapscott 2016), or model-based (e.g., Hafid et al. 2019). However, empirical investigations of blockchain's impact on organizations, especially theory-driven ones, are notably scarce. Our study addresses this gap by offering a new theoretical framework and empirical evidence on the impact of blockchain on firms' cybersecurity, making significant strides in expanding the existing blockchain research. Moreover, while theoretical studies have examined the cybersecurity implications of blockchain (e.g., Hasanova et al. 2019; Mahmood et al. 2022; Toufaily et al. 2021), we contribute to the literature by providing the groundbreaking empirical evidence to measure this effect, which has only been theorized so far.

Third, our study extends the application of OIPT by exploring its relevance in the context of blockchain implementation. This application demonstrates that OIPT can be a valuable framework for understanding how organizations manage the complexities and uncertainties introduced by emerging technologies. In addition, our study provides empirical evidence supporting OIPT's view that aligning information processing capabilities with organizational needs is crucial for reducing the uncertainties associated with technology adoption (Galbraith 1973; Srinivasan and Swink 2018; Tatikonda and Montoya-Weiss 2001).

7.2. Practical Contributions

Our research has significant practical implications for firms considering or currently adopting blockchain technology. First, our research shows that firms face heightened data breach risks, particularly those originating from insiders, during the initial phase of blockchain implementation. This highlights the importance of developing comprehensive risk management plans and strengthening security measures when adopting the technology. For example, firms may consider enhancing security measures by updating policies, providing specialized employee training, and hiring blockchain and cybersecurity experts to manage short-term data breach risks and early challenges of blockchain implementation.

Second, our findings indicate that blockchain implementation leads to a reduction in data breach risks in the long term, particularly by enhancing protection against external threats such as hacking. This demonstrates that investing in blockchain implementation, despite initial challenges, is a strategic

move that offers substantial long-term cybersecurity benefits. Firms can capitalize on the long-term security advantages of blockchain technology, effectively reducing data breach risks and strengthening their overall cybersecurity framework.

Third, our study underscores the crucial role of organizational capabilities, particularly managerial IT industry experience and sufficient human resources, in mitigating short-term data breach risks from blockchain implementation. Therefore, firms should consider hiring managers with extensive IT experience to manage blockchain-related complexities and risks. Additionally, ensuring adequate human resources to support the blockchain implementation process is essential.

7.3. Conclusions

To conclude, our study provides an empirical analysis of the polarized opinions among practitioners regarding blockchain's impact on cybersecurity. Our findings, derived from robust empirical analyses, shed light on the dual-edged and dynamic influence of blockchain on cybersecurity—detrimental initially but beneficial in the long run. Specifically, on the one hand, blockchain implementation poses a short term threat to cybersecurity, and on the other hand, blockchain implementation improves cybersecurity over time. We also explore how these effects depend on breach types and a range of contextual factors, enriching the research and supporting our proposed theoretical mechanisms. Our findings help reconcile the polarized views of practitioners on blockchain's cybersecurity impact, offering valuable insights for both researchers and practitioners.

References

Angst CM, Block ES, D'Arcy J, and Kelley K. 2017. When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. *MIS Quarterly*. 41(3): 893-A898.

Azadegan A, Patel PC, and Parida V. 2013. Operational Slack and Venture Survival. *Production and Operations Management*. 22(1): 1-18.

Bansal P, Panchal R, Bassi S, and Kumar A. 2020. "Blockchain for Cybersecurity: A Comprehensive Survey," *2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT)*: IEEE, pp. 260-265.

Bulgurcu B, Cavusoglu H, and Benbasat I. 2010. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS quarterly*. 34(3): 523-548.

Burtch G, Carnahan S, and Greenwood BN. 2018. Can You Gig It? An Empirical Examination of the Gig Economy and Entrepreneurial Activity. *Management Science*. 64(12): 5497-5520.

Callaway B, and Sant'Anna PH. 2021. Difference-in-Differences with Multiple Time Periods. *Journal of Econometrics*. 225(2): 200-230.

Cavusoglu H, Mishra B, and Raghunathan S. 2004. 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*. 9(1): 70-104.

Cengiz D, Dube A, Lindner A, and Zipperer B. 2019. The Effect of Minimum Wages on Low-Wage Jobs. *The Quarterly Journal of Economics*. 134(3): 1405-1454.

Chen MA, Hu SS, Wang J, and Wu Q. 2023. Can Blockchain Technology Help Overcome Contractual Incompleteness? Evidence from State Laws. *Management Science*. 69(11): 6540-6567.

Cheng L, Liu F, and Yao D. 2017. Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*. 7(5): e1211.

Chu Y, Tian X, and Wang W. 2019. Corporate Innovation Along the Supply Chain. *Management Science*. 65(6): 2445-2466.

Cram WA, D'arcy J, and Proudfoot JG. 2019. Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS quarterly*. 43(2): 525-554.

D'Arcy J, Adjerid I, Angst CM, and Glavas A. 2020. Too Good to Be True: Firm Social Performance and the Risk of Data Breach. *Information Systems Research*. 31(4): 1-45.

D'Arcy J, Herath T, and Shoss MK. 2014. Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*. 31(2): 285-318.

D'Arcy J, and Teh P-L. 2019. Predicting Employee Information Security Policy Compliance on a Daily Basis: The Interplay of Security-Related Stress, Emotions, and Neutralization. *Information & Management*. 56(7): 103151.

Dai Y, Rau PR, Stouraitis A, and Tan W. 2020. An Ill Wind? Terrorist Attacks and CEO Compensation. *Journal of Financial Economics*. 135(2): 379-398.

De Chaisemartin C, and d'Haultfoeuille X. 2020. Two-Way Fixed Effects Estimators with Heterogeneous Treatment Effects. *American Economic Review*. 110(9): 2964-2996.

Deshpande M, and Li Y. 2019. Who Is Screened Out? Application Costs and the Targeting of Disability Programs. *American Economic Journal: Economic Policy*. 11(4): 213-248.

Fabian B, Ermakova T, Krah J, Lando E, and Ahrary N. 2018. Adoption of Security and Privacy Measures in Bitcoin–Stated and Actual Behavior. *working paper*.

Faleye O, Hoitash R, and Hoitash U. 2018. Industry Expertise on Corporate Boards. *Review of Quantitative Finance and Accounting*. 50 441-479.

Ferrara EL, Chong A, and Duryea S. 2012. Soap Operas and Fertility: Evidence from Brazil. *American Economic Journal: Applied Economics*. 4(4): 1-31.

Foerderer J, and Schuetz SW. 2022. Data Breach Announcements and Stock Market Reactions: A Matter of Timing? *Management Science*. 68(10): 7298-7322.

Galbraith J. 1973. Designing Complex Organizations. *Reading, Mass*.

Gimenez-Aguilar M, De Fuentes JM, Gonzalez-Manzano L, and Arroyo D. 2021. Achieving Cybersecurity in Blockchain-Based Systems: A Survey. *Future Generation Computer Systems*. 124 91-118.

Goldfarb A, and Tucker CE. 2014. Conducting Research with Quasi-Experiments: A Guide for Marketers. *Toronto, ON, Canada: Rotman School of Management*.

Goodman-Bacon A. 2021. Difference-in-Differences with Variation in Treatment Timing. *Journal of Econometrics*. 225(2): 254-277.

Gupta S. 2018. Organizational Barriers to Digital Transformation.

Gwebu KL, Wang J, and Wang L. 2018. The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management. *Journal of Management Information Systems*. 35(2): 683-714.

Hafid A, Hafid AS, and Samih M. 2019. New Mathematical Model to Analyze Security of Sharding-Based Blockchain Protocols. *IEEE Access*. 7 185447-185457.

Hainmueller J. 2012. Entropy Balancing for Causal Effects: A Multivariate Reweighting Method to Produce Balanced Samples in Observational Studies. *Political Analysis*. 20(1): 25-46.

Haislip J, Lim J-H, and Pinsker R. 2021. The Impact of Executives' IT Expertise on Reported Data Security Breaches. *Information Systems Research*. 32(2): 318-334.

Hart M, Manadhata P, and Johnson R. 2011. "Text Classification for Data Loss Prevention," *International Symposium on Privacy Enhancing Technologies Symposium*: Springer, pp. 18-37.

Hasanova H, Baek Uj, Shin Mg, Cho K, and Kim MS. 2019. A Survey on Blockchain Cybersecurity Vulnerabilities and Possible Countermeasures. *International Journal of Network Management*. 29(2): e2060.

He S, Ficke E, Pritom MMA, Chen H, Tang Q, Chen Q, Pendleton M, Njilla L, and Xu S. 2022. Blockchain-Based Automated and Robust Cyber Security Management. *Journal of Parallel and Distributed Computing*. 163 62-82.

Hendricks B, Howell T, and Bingham C. 2019. How Much Do Top Management Teams Matter in Founder-Led Firms? *Strategic Management Journal*. 40(6): 959-986.

Higgs JL, Pinsker RE, Smith TJ, and Young GR. 2016. The Relationship between Board-Level Technology Committees and Reported Security Breaches. *Journal of Information Systems*. 30(3): 79-98.

Hilary G, Segal B, and Zhang MH. 2016. Cyber-Risk Disclosure: Who Cares? *Georgetown McDonough School of Business Research Paper*. (2852519).

Huang HH, and Wang C. 2021. Do Banks Price Firms' Data Breaches? . *The Accounting Review*. 96(3): 261-286.

Huang J, Cao J, Hasan T, and Zhao J. 2021. Low-Carbon City Initiatives and Firm Risk: A Quasi-Natural Experiment in China. *Journal of Financial Stability*. 57 100949.

Janakiraman R, Lim JH, and Rishika R. 2018. The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer. *Journal of Marketing*. 82(2): 85-105.

Jaradat A, Ali O, and AlAhmad A. 2022. Blockchain Technology: A Fundamental Overview. *Blockchain Technologies for Sustainability*. 1-24.

Kamiya S, Kang J-K, Kim J, Milidonis A, and Stulz RM. 2021. Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms. *Journal of Financial Economics*. 139(3): 719-749.

Khalil M, Khawaja KF, and Sarfraz M. 2022. The Adoption of Blockchain Technology in the Financial Sector During the Era of Fourth Industrial Revolution: A Moderated Mediated Model. *Quality & Quantity*. 56(4): 2435-2452.

Kshetri N. 2017. Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy. *Telecommunications Policy*. 41(10): 1027-1038.

Kwon J, and Johnson ME. 2014. Proactive Versus Reactive Security Investments in the Healthcare Sector. *MIS Quarterly*. 38(2): 451-A453.

Kwon J, and Johnson ME. 2018. Meaningful Healthcare Security: Does "Meaningful-Use" Attestation Improve Information Security Performance? *MIS quarterly*. 42(4): 1043-1067.

Li H, Yoo S, and Kettinger WJ. 2021. The Roles of IT Strategies and Security Investments in Reducing Organizational Security Breaches. *Journal of Management Information Systems*. 38(1): 222-245.

Lind MR, and Zmud RW. 1991. The Influence of a Convergence in Understanding between Technology Providers and Users on Information Technology Innovativeness. *Organization Science*. 2(2): 195-217.

Liu C-W, Huang P, and Lucas HC. 2020. Centralized IT Decision Making and Cybersecurity Breaches: Evidence from Us Higher Education Institutions. *Journal of Management Information Systems*. 37(3): 758–787.

Liu F, Shu X, Yao D, and Butt AR. 2015. "Privacy-Preserving Scanning of Big Content for Sensitive Data Exposure with Mapreduce," *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*: ACM, pp. 195-206.

Mackelprang AW, Habermann M, and Swink M. 2015. How Firm Innovativeness and Unexpected Product Reliability Failures Affect Profitability. *Journal of Operations Management*. 38 71-86.

Mahmood S, Chadhar M, and Firmin S. 2022. Cybersecurity Challenges in Blockchain Technology: A Scoping Review. *Human Behavior and Emerging Technologies*. 2022(1): 7384000.

McLeod A, and Dolezel D. 2018. Cyber-Analytics: Modeling Factors Associated with Healthcare Data Breaches. *Decision Support Systems*. 108 57-68.

Mishina Y, Pollock TG, and Porac JF. 2004. Are More Resources Always Better for Growth? Resource Stickiness in Market and Product Expansion. *Strategic Management Journal*. 25(12): 1179–1197.

Modi SB, and Mishra S. 2011. What Drives Financial Performance–Resource Efficiency or Resource Slack?: Evidence from Us Based Manufacturing Firms from 1991 to 2006. *Journal of Operations Management*. 29(3): 254-273.

Moroney R. 2007. Does Industry Expertise Improve the Efficiency of Audit Judgment? *Auditing: A Journal of Practice & Theory*. 26(2): 69-94.

Nowiński W, and Kozma M. 2017. How Can Blockchain Technology Disrupt the Existing Business Models? *Entrepreneurial Business and Economics Review*. 5(3): 173-188.

Papadimitriou P, and Garcia-Molina H. 2011. Data Leakage Detection. *IEEE Transactions on knowledge and data engineering*. 23(1): 51-63.

Romanosky S. 2016. Examining the Costs and Causes of Cyber Incidents. *Journal of Cybersecurity*. 2(2): 121-135.

Romanosky S, Hoffman D, and Acquisti A. 2014. Empirical Analysis of Data Breach Litigation. *Journal of Empirical Legal Studies*. 11(1): 74-104.

Rosenbaum PR, and Rubin DB. 1983. The Central Role of the Propensity Score in Observational Studies for Causal Effects. *Biometrika*. 70(1): 41-55.

Schneier B. 2015. Secrets and Lies: Digital Security in a Networked World. John Wiley & Sons.

Sen R, and Borle S. 2015. Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems*. 32(2): 314-341.

Shu X, Yao D, and Bertino E. 2015. Privacy-Preserving Detection of Sensitive Data Exposure. *IEEE transactions on information forensics and security*. 10(5): 1092-1103.

Srinivasan R, and Swink M. 2018. An Investigation of Visibility and Flexibility as Complements to Supply Chain Analytics: An Organizational Information Processing Theory Perspective. *Production and Operations Management*. 27(10): 1849-1867.

Sriram V, Sanyal S, Laddunuri MM, Subramanian M, Bose V, Booshan B, Shivaram C, Bettaswamy M, Booshan S, and Thangam D. 2023. Enhancing Cybersecurity through Blockchain Technology. IGI Global.

Stock GN, and Tatikonda MV. 2000. A Typology of Project-Level Technology Transfer Processes. *Journal of Operations Management*. 18(6): 719-737.

Stock GN, and Tatikonda MV. 2008. The Joint Influence of Technology Uncertainty and Interorganizational Interaction on External Technology Integration Success. *Journal of Operations Management*. 26(1): 65-80.

Sun T, Viswanathan S, and Zheleva E. 2021. Creating Social Contagion through Firm-Mediated Message Design: Evidence from a Randomized Field Experiment. *Management Science*. 67(2): 808-827.

Swanson EB, and Ramiller NC. 2004. Innovating Mindfully with Information Technology. *MIS Quarterly*. 553-583.

Tapscott D, and Tapscott A. 2016. The Impact of the Blockchain Goes Beyond Financial Services. *Harvard Business Review*. 10(7): 2-5.

Tatikonda MV, and Montoya-Weiss MM. 2001. Integrating Operations and Marketing Perspectives of Product Innovation: The Influence of Organizational Process Factors and Capabilities on Development Performance. *Management Science*. 47(1): 151-172.

Tatikonda MV, and Rosenthal SR. 2000. Successful Execution of Product Development Projects: Balancing Firmness and Flexibility in the Innovation Process. *Journal of Operations Management*. 18(4): 401-425.

Toufaily E, Zalan T, and Dhaou SB. 2021. A Framework of Blockchain Technology Adoption: An Investigation of Challenges and Expected Value. *Information & Management*. 58(3): 103444.

Verizon. 2013. "2013 Verizon Data Breach Investigations Report."

Wang J, Gupta M, and Rao HR. 2015. Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications. *MIS Quarterly*. 39(1): 91-112.

Wang Q, Ngai EW, Pienta D, and Thatcher JB. 2023. Information Technology Innovativeness and Data-Breach Risk: A Longitudinal Study. *Journal of Management Information Systems*. 40(4): 1139-1170.

Wiengarten F, Fan D, Pagell M, and Lo CK. 2019. Deviations from Aspirational Target Levels and Environmental and Safety Performance: Implications for Operations Managers Acting Irresponsibly. *Journal of Operations Management*. 65(6): 490-516.

Wing C, Yozwiak M, Hollingsworth A, Freedman S, and Simon K. 2024. Designing Difference-in-Difference Studies with Staggered Treatment Adoption: Key Concepts and Practical Guidelines. *Annual Review of Public Health*. 45.

Wylde V, Rawindaran N, Lawrence J, Balasubramanian R, Prakash E, Jayal A, Khan I, Hewage C, and Platts J. 2022. Cybersecurity, Data Privacy and Blockchain: A Review. *SN Computer Science*. 3(2): 127.

Yadav SK, Sharma K, Kumar C, and Arora A. 2022. Blockchain-Based Synergistic Solution to Current Cybersecurity Frameworks. *Multimedia Tools and Applications*. 81(25): 36623-36644.

Yaga D, Mell P, Roby N, and Scarfone K. 2019. Blockchain Technology Overview. *arXiv preprint arXiv:1906.11078*.

Zhang L, Xie L, and Zheng X. 2023. Across a Few Prohibitive Miles: The Impact of the Anti-Poverty Relocation Program in China. *Journal of Development Economics*. 160 102945.

Zhuang P, Zamir T, and Liang H. 2020. Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey. *IEEE Transactions on Industrial Informatics*. 17(1): 3-19.

Is Blockchain the Ultimate Cybersecurity Weapon?: Evidence from a Quasi-Natural Experiment in the U.S.

Online Appendix (OA)

This appendix provides more detailed information about the data, regression results, and analyses.

OA-1. Data Breach Descriptions

Table OA-1 presents the distribution of data breach in the data breach sample by cause, and Figure OA-1 displays the frequency of these breaches by state.

Table OA-1. Data Breach Distribution by Source

Data Breach Cause	Frequency	Percent
Malware	172	15.13
Misconfiguration	90	7.92
Phishing	143	12.58
Ransomware	120	10.55
Unauthorized Access	285	25.07
Not Disclosed	327	28.76
Total	1,137	100

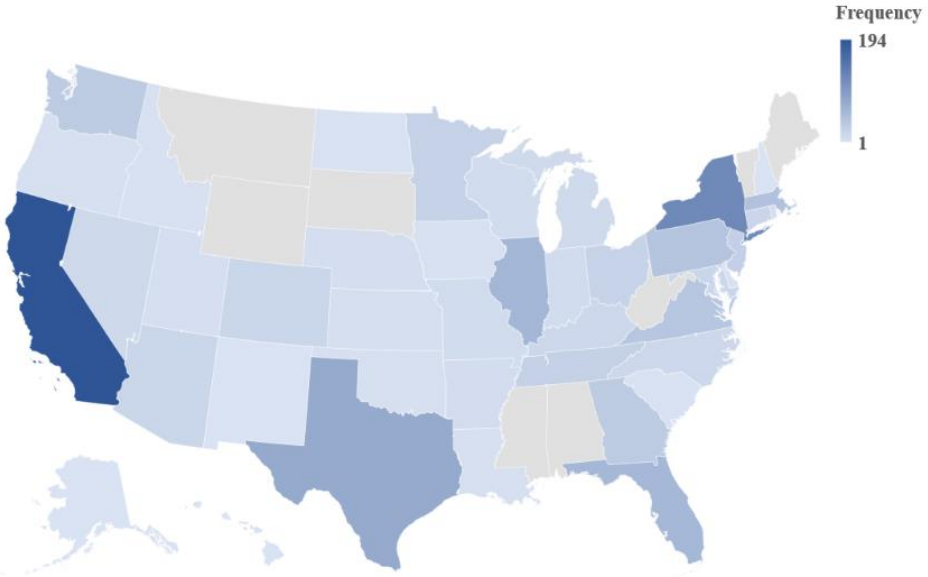


Figure OA-1. Distribution of Data Breaches by State

OA-2. Pro-Blockchain Legislation Descriptions

Table OA-2 shows the specifics of the pro-blockchain laws examined in our study, encompassing details like the enacting state, bill number, initial introduction and enactment years, and key provisions. This data is sourced from Chen et al. (2023). To enhance comprehension of the context surrounding blockchain implementation in our research, we have appended this information.

Table OA-2. Description of Pro-Blockchain Legislation

State	Bill no.	Introduced year	Enacted year	Core provisions
AR	HB 1944	2019	2019	Provides that a signature or contract on blockchain is electronic form; provides that a smart contract shall be a commercial contract
AZ	HB 2417	2017	2017	Recognizes smart contracts in commerce (certain exceptions for cases where terms of transaction expressly transfer ownership or use of information secured by blockchain technology)
AZ	HB 2602	2018	2018	Provides that running a blockchain node in a residence is a state concern; prohibits cities, towns, or counties from impeding a person running a node on blockchain technology in a residence
IL	HB 3575	2019	2019	Creates the Blockchain Technology Act; provides for permitted uses and limitations to blockchain technology; prohibits local governments from restricting blockchain use
ND	HB 1045	2019	2019	Legitimizes blockchain, smart contracts, and electronic signatures in commerce
NV	SB 398	2017	2017	Recognizes blockchain as a type of electronic record for UETA; prohibits local government from taxing or restricting use of a blockchain
NV	SB 162	2019	2019	Affirms blockchain as a type of electronic record for the UETA; provides that user of a public blockchain does not relinquish any right of ownership; prohibits local government from taxing or imposing restrictions upon use of a public blockchain
NV	SB 163	2019	2019	Revises the definition of electronic transmission for certain businesses to include blockchain; allows certain business entities to store records and carry out their duties with blockchain
OH	SB 220	2017	2018	Allows transactions recorded by blockchain technology under the UETA
OK	SB 700	2019	2019	Relates blockchain to the definition of electronic records and the UETA
SD	HB 1196	2019	2019	Revises definitions of electronic transmission and contracting to include blockchain
TN	HB 1507/SB 1662	2018	2018	Recognizes the legal authority to use blockchain technology and smart contracts in conducting electronic transactions; protects ownership rights with respect to information secured by blockchain
UT	SB 213	2019	2019	Defines and clarifies terms related to blockchain technology. Exempts a person who exchanges, sells certain blockchain products from the Money Transmitter Act
VT	HB 868	2016	2016	Creates statutory presumptions of authenticity for records using blockchain technology
WA	SB 5638	2019	2019	Recognizes the validity of distributed ledger technology; affirms that electronic records may not be denied legal effect or enforceability solely because they are related to distributed ledger technology
WY	HB 70	2018	2018	Affirms that a person who develops, sells, or exchanges an open blockchain token is not subject to specified securities and money transmission laws

OA-3. Variable Descriptions

Table OA-3 provides descriptions of the variables employed in the study, including those used for the primary and exploratory analyses.

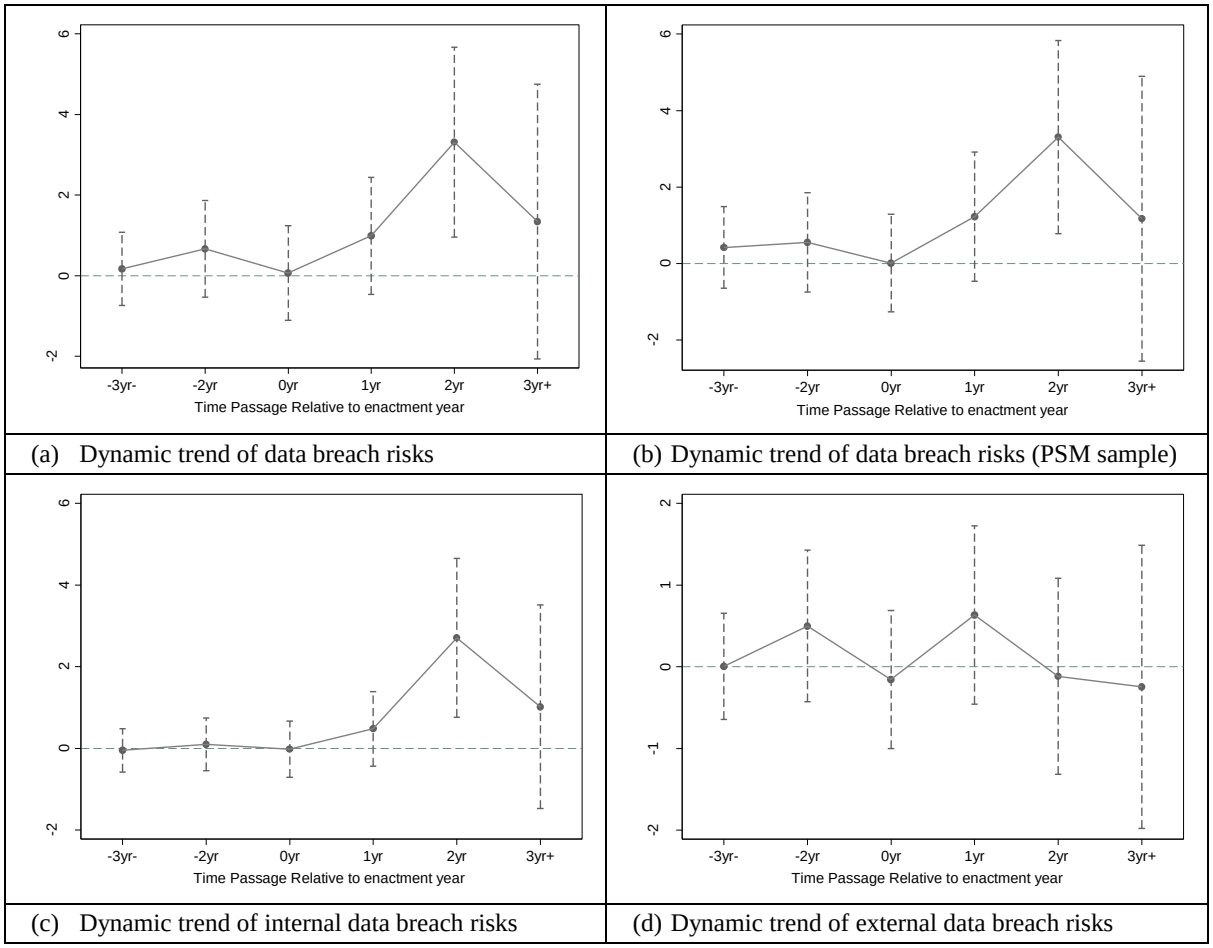
Table OA-3. Variable Descriptions

Variable	Description	Source
Dependent Variable		
Breach Risk	A binary variable that equals 1 if a firm experiences at least one breach in the subsequent year, and 0 otherwise, following Liu et al. (2015) and Wang et al. (2023)	Audit Analytics cybersecurity database
Treatment Dummy		
Post Enactment	A binary variable that equals 1 if at least one pro-blockchain legislation has been passed in the past in states where a firm operates, and 0 otherwise	NCSL[12]
Control Variables		
Firm Size	The natural logarithm of total assets	Compustat
Leverage	The ratio of the beginning total liabilities divided by the beginning total assets	
ROA	The ratio of net income before extraordinary items divided by the total assets	Compustat
Loss Position	An indicator variable that equals 1 if the firm reports negative net income in the current year, 0 otherwise	Compustat
R&D	The natural logarithm of R&D expenses	Compustat
IT governance	A dummy variable equals 1 if a firm has at least an IT executive in its top management team, and 0 otherwise, following Kwon et al. (2013)	Compustat
Different Breach Types		
Internal Breach Risk	A binary variable that equals 1 if a firm experiences at least one internal data breach in the subsequent year; otherwise, it equals 0. An internal data breach is identified if the type of attack is categorized as "Unauthorized Access" or "Misconfiguration" according to WRDS.	Audit Analytics cybersecurity database
External Breach Risk	A binary variable that equals 1 if a firm experiences at least one external data breach in the subsequent year; otherwise, it equals 0. An external data breach is identified if the type of attack is categorized as "Phishing," "Malware," "Ransomware," "Phishing or Unauthorized," or "Malware or Phishing" according to WRDS.	Audit Analytics cybersecurity database
Contextual Factors		
IT Industry Experience	An indicator variable that equals 1 if a firm's CEO, CFO, or CTO has previously worked in the IT industry, and 0 otherwise	BoardEx
Human Resource Sufficiency	The natural logarithm of the industry-adjusted ratio of labor to annual sales, following Azadegan et al. (2013)	Compustat

[12] The full name of NCSL is the National Conference of State Legislatures.

OA-4. Parallel Trends Plot

Figure OA-4 presents parallel trends plots to enhance the visualization of the dynamic trends in the outcome variables across analyses. Section (a) corresponds to the results of column (3) in Table 5. Section (b) corresponds to column (3) in Table 7. Section (c) corresponds to the results of column (3) in Table 11. Lastly, section (d) corresponds to column (6) in Table 11.



(a) Dynamic trend of data breach risks

(b) Dynamic trend of data breach risks (PSM sample)

(c) Dynamic trend of internal data breach risks

(d) Dynamic trend of external data breach risks

Figure OA-4. Parallel Trends Plot

OA-5. Results of Propensity Score Matching

We conduct a series of diagnostic tests for PSM. First, in Panel A, Table OA-5, we present univariate comparisons between the pre-breach characteristics of treatment and control firms, along with their respective *t*-statistics. Notably, the observed differences are largely and statistically insignificant, suggesting a similarity in the characteristics of both treatment and control firm groups. Second, we test the differences between the propensity scores of the treatment firms and those of the matched control firms. Panel B reveals that the differences are substantially trivial.

Table OA-5. The Results of Propensity Score Matching (PSM)

Panel A: Comparison of Firm Characteristics Prior To Enactment of Pro-Blockchain Laws

Characteristics	Treatment firms	Matched control firms	%bias	*t*-test
Size	5.905	5.945	−1.3	−1.18
Leverage	1.444	1.392	1.1	1.07
ROA	−0.585	−0.543	−1.4	−1.37
Loss Position	0.053	0.056	−2.1	−1.88
R&D	0.374	0.363	2.2	2.03
IT Governance	0.048	0.050	−1	−0.88

Panel B. Estimated Propensity Score Distributions

Propensity Score	No. of Obs	Min	P25	Median	Mean	S.D.	P75	Max
Treatment	14,251	0.029	0.115	0.138	0.138	0.040	0.165	0.353
Control	23,626	0.028	0.117	0.140	0.140	0.039	0.167	0.353
Difference	–	0.001	−0.002	−0.002	−0.001	0.001	−0.002	0.000

OA-6. Entropy Balancing Matching

In the entropy balancing matching process, all continuous control variables are utilized as covariates. The balancing method is then applied to ensure that the balanced control group and treatment group have similar means and skewness for these variables. Table OA-6 provides the results of entropy balancing diagnostics. Columns (1) and (2) present the means and skewness of covariates in the treatment group, and columns (3) and (4) show the corresponding values for the control group. Pre-balancing, there are notable disparities in these statistics. However, post-balancing, the statistics for the control group closely resemble those of the treatment group. We also conduct regression analysis of the group indicator on these variables and display the outcomes for both the unbalanced and balanced samples in column (5). This analysis aims to determine whether these variables can predict the treatment allocation. The results indicate that the coefficients of these variables decrease in magnitude, lose statistical significance, and the *pseudo* R^2 drops from 0.011 to 0.000. This suggests that post-balancing, these variables no longer serve as predictors for the treatment allocation.

Table OA-6. Balancing Test Results of Entropy Balancing Method

	Treatment		**Control**		
	Mean	Skewness	Mean	Skewness	Logit
	(1)	(2)	(3)	(4)	(5)
Before Balancing					
Firm Size	6.389	9.839	5.404	8.964	0.061***
					(16.58)
Leverage	1.594	22.670	1.263	15.350	0.022***
					(6.75)
ROA	−0.630	8.513	−0.542	6.079	−0.035***
					(−6.23)
Firm Loss	0.051	0.035	0.071	0.045	−0.321***
					(−6.43)
R&D	0.391	0.238	0.459	0.248	−0.253***
					(−12.37)
IT Governance	0.054	0.051	0.036	0.035	0.179***
					(4.39)
pseudo R^2					*0.011*
After Balancing					
Firm Size	6.389	9.839	6.389	9.839	0.006
					(0.72)
Leverage	1.594	22.670	1.594	22.670	0.003
					(0.48)
ROA	−0.630	8.513	−0.630	8.513	−0.005
					(−0.43)
Firm Loss	0.051	0.035	0.051	0.035	−0.082
					(−0.72)
R&D	0.391	0.238	0.391	0.238	−0.060
					(−1.28)
pseudo R^2					*0.000*

Notes. This table presents the results of the diagnostic analyses related to entropy balancing. Columns (1) and (2) present the means and skewness of the covariates in the treatment groups, while columns (3) and (4) provide the same statistics for the control group. Column (5) reports the logit regression results of regressing the group indicator on the covariates before and after balancing. *t* statistics in parentheses, * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

OA-7. Placebo Test

We employ a placebo test proposed by Ferrara et al. (2012) and Burtch et al. (2018). This involves randomly cselecting firms involved in pro-blockchain enactment within their state and assigning random treatment timings to mimic a randomized experiment. We then conduct regression analysis following Equation (1). To ensure the reliability of this placebo test, we repeat the process 500 times, generating a distribution plot of estimated coefficients for the placebo DiD term. The purpose of this test is to determine if data breach risks in firms are substantially influenced by variables other than the enactment of pro-blockchain laws. A placebo DiD term with estimated coefficients approaching zero would indicate the absence of significant omitted variables, validating that the observed impacts in the baseline analysis are indeed due to the pro-blockchain enactment within firms' states.

Figure OA-7 displays the distribution plot of estimated coefficients obtained from the placebo test. It indicates that the estimated coefficients for the pseudo-treatment dummies are primarily clustered around zero. The dashed line represents the coefficient of the real treatment dummy. Across all 500 random experiments, the estimates do not exceed this real value, suggesting a minimal probability of the actual baseline coefficient occurring randomly. These findings affirm that our main effect results remain robust against randomness or other potential time series factors.

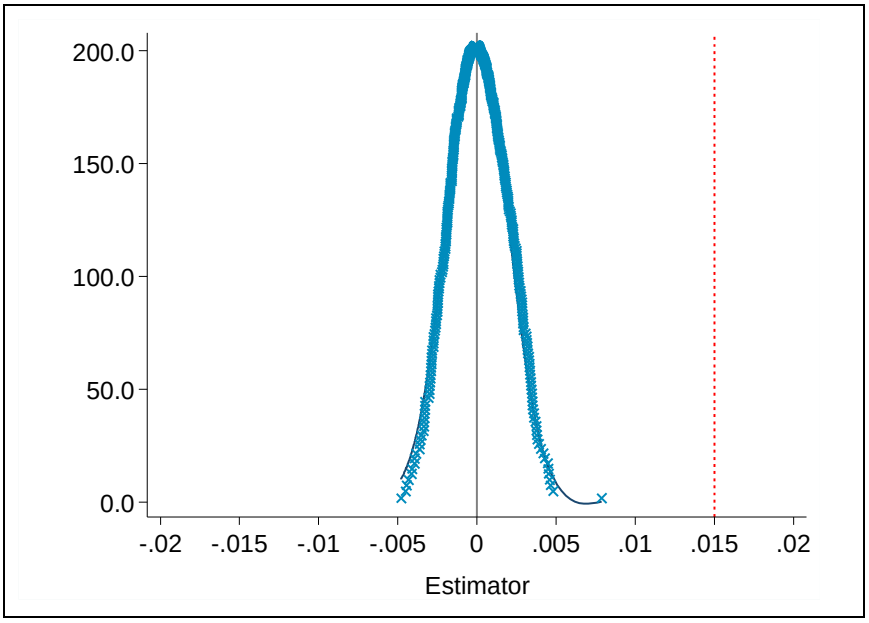


Figure OA-7. Placebo Test

References

Azadegan A, Patel PC, and Parida V. 2013. Operational Slack and Venture Survival. *Production and Operations Management*. 22(1): 1-18.

Burtch G, Carnahan S, and Greenwood BN. 2018. Can You Gig It? An Empirical Examination of the Gig Economy and Entrepreneurial Activity. *Management Science*. 64(12): 5497-5520.

Chen MA, Hu SS, Wang J, and Wu Q. 2023. Can Blockchain Technology Help Overcome Contractual Incompleteness? Evidence from State Laws. *Management Science*. 69(11): 6540-6567.

Ferrara EL, Chong A, and Duryea S. 2012. Soap Operas and Fertility: Evidence from Brazil. *American Economic Journal: Applied Economics*. 4(4): 1-31.

Kwon J, Ulmer JR, and Wang T. 2013. The Association between Top Management Involvement and Compensation and Information Security Breaches. *Journal of Information Systems*. 27(1): 219-236.

Liu F, Shu X, Yao D, and Butt AR. 2015. "Privacy-Preserving Scanning of Big Content for Sensitive Data Exposure with Mapreduce," *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*: ACM, pp. 195-206.

Wang Q, Ngai EW, Pienta D, and Thatcher JB. 2023. Information Technology Innovativeness and Data-Breach Risk: A Longitudinal Study. *Journal of Management Information Systems*. 40(4): 1139-1170.