Journal of
Theoretical and Applied Electronic Commerce Research

MDPI

Article

The Impact of Cybersecurity Governance on Corporate Digital Marketing: Evidence from Chinese A-Share Listed Firms

Yushun Han [1] and Bing He [2,*]

[1] Northeast Asian Studies College, Jilin University, Changchun 130012, China; hanys22@mails.jlu.edu.cn
[2] School of Business, Jiangsu Ocean University, Lianyungang 222005, China
* Correspondence: binghe@jou.edu.cn

Abstract

In the digital economy era, digital marketing has become a key strategy for firms seeking competitive advantage. However, its reliance on data has heightened exposure to cybersecurity risks. While existing research highlights the importance of digital transformation, less is known about how cybersecurity governance influences firms' digital marketing activities. Drawing on signalling theory and the resource-based view, this study uses panel data from Chinese A-share listed firms during 2012–2023 to examine the impact of cybersecurity governance on digital marketing and its underlying mechanisms. The results show that effective cybersecurity governance significantly enhances firms' digital marketing engagement. Mechanism analyses identify three channels. First, by preventing data breaches and negative incidents, firms enhance corporate reputation. Second, by creating a secure operating environment, cybersecurity governance strengthens risk-taking capacity and encourages marketing innovation. Third, by improving information disclosure and stakeholder communication, it alleviates information asymmetry. Heterogeneity analyses indicate that the positive effect is more pronounced for non-state-owned enterprises, firms in eastern regions, and high-tech firms. This study fills a gap in the literature by linking cybersecurity governance path to digital marketing and contributes to research on its economic consequences. The findings also offer practical implications for strengthening internal governance to support external market activities.

Keywords: cybersecurity governance; digital marketing; corporate reputation; risk-taking; information asymmetry; China

Check for updates

Academic Editor: Hyunchul Ahn

Received: 13 February 2026
Revised: 21 March 2026
Accepted: 25 March 2026
Published: 26 March 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

In recent years, artificial intelligence, big data, and cloud computing have advanced rapidly, accelerating global digital economic change [1]. In this changing pattern, digital marketing has already become a central problem for company strategies. It is no longer just an extra tool but becomes a key part of company strategy decisions [2]. Companies increasingly use a range of digital channels—for example, social media, search engines, and e-commerce sites—to communicate with buyers, attract more customers, and strengthen brand value. Furthermore, new data science developments are delivering smart, automated solutions for digital marketing, making it a key driver of company growth in the digital economy.

However, the effectiveness of digital marketing is fundamentally dependent upon the collection, analysis, and utilization of vast amounts of user data, which inevitably exposes firms to escalating cybersecurity risks [3,4]. Cyber threats—for example, data

leaks, phishing attacks, and ransomware—may disrupt marketing work, expose private info, and, more importantly, erode buyer trust and damage the brand [5,6]. As digital business grows rapidly, recent legal developments have heightened concerns about data secrecy and protection, making compliance with the law a major challenge for companies operating in digital spaces [7,8]. So, network security risks are already a key problem in company governance, and they have a direct impact on effective digital marketing results and long-term survival.

In this context, the idea of cybersecurity governance is becoming increasingly evident. In this paper, the term "cybersecurity governance" refers to the aim of ensuring that the company's network security plan and its broader business goals remain aligned, encompassing rules, processes, team building, and technical controls [9]. Effective cybersecurity governance usually needs active boss-level involvement and oversight to make sure network dangers are fully identified, monitored, and managed [10]. Now, many studies examine network security from a tech perspective or focus on the financial outcomes of cybersecurity incidents, especially their negative impact on company value [11]. At the same time, books on digital marketing mainly focus on strategy design, selecting methods, and evaluating results [12].

Despite extensive research on network security and digital marketing, respectively, few studies have systematically examined the intrinsic link between cybersecurity governance, as an internal governance mechanism, and digital marketing, as an externally oriented market activity. Although prior scholarship has generated valuable insights into both domains, the interface between them remains largely unexplored. Specifically, much less is known about how cybersecurity governance influences firms' digital marketing strategic decisions and their ultimate performance outcomes. Existing research on IT governance has primarily focused on the efficiency of IT investment, the relationship between IT and organizational performance, or IT risk management. However, cybersecurity governance has rarely been conceptualized as an independent governance dimension and empirically linked to external market-oriented activities such as digital marketing [13–15]. Similarly, while studies on digital capabilities emphasize firms' ability to leverage digital technologies to achieve commercial objectives, they tend to concentrate on technology adoption, integration, and application. Far less attention has been paid to the foundational and enabling role of cybersecurity governance in shaping these capabilities and their market outcomes [16]. In particular, it remains unclear whether cybersecurity governance merely represents a defensive cost incurred for compliance purposes or whether it can be transformed into a strategic asset that generates distinctive value for digital marketing activities [17].

To fill this research gap, this study uses data from China A-share-listed companies from 2012 to 2023 to examine the effect of cybersecurity governance on business digital markets. Specifically, this research develops a comprehensive cybersecurity governance index and a business digital market index to test their relationship. China is a big digital economy. It provides a rich background because its listed companies spend significant money on network security and undergo rapid digital change [18]. In this framework, this research examines company reputation, risk-taking, and information asymmetry as three perspectives to investigate the hidden mechanism and show how cybersecurity governance shapes digital market outcomes. Furthermore, this research examines whether this effect differs across businesses with different ownership, locations, and technology levels.

This study makes three main contributions to the existing literature. First, this study is among the first empirical investigations to directly link internal cybersecurity governance with external digital marketing performance. By integrating these two previously distinct streams of research, this study not only extends our understanding of the economic consequences of cybersecurity governance but also introduces an important corporate

governance perspective into the digital marketing literature. In doing so, it deepens our understanding of the institutional foundations underpinning digital marketing success. Second, this study provides new theoretical explanations and empirical evidence regarding the value-creation function of cybersecurity governance. Specifically, the findings suggest that cybersecurity governance promotes firms' digital marketing activities through three primary channels: enhancing corporate reputation, strengthening risk-taking capacity, and mitigating information asymmetry. By identifying these mechanisms, this research sheds new light on how governance structures can be translated into market advantages. More importantly, it enriches the theoretical discussion of how cybersecurity governance generates strategic value, shifting the perspective from viewing it as a traditional "cost center" to recognizing it as a "value center." Finally, the findings offer important practical implications. The results indicate that investment in cybersecurity governance should not be regarded merely as a passive compliance cost. Rather, it should be considered a proactive strategic investment that can enhance firms' marketing capabilities and strengthen their market competitiveness.

2. Literature Review and Research Hypotheses

2.1. Literature Review

2.1.1. Determinants of Digital Marketing

Digital marketing, also called online marketing or internet marketing, is usually defined as using digital channels—such as the internet, social media platforms, mobile devices, and search engines—to promote products, services, and brands [19]. Compared with traditional marketing, digital marketing offers high interaction, wide market coverage, cost benefits, and measurable results [20]. By using effective digital marketing strategies, businesses can build closer customer relationships, grow brand awareness and loyalty, and ultimately drive sales growth and market share [21].

A large and growing literature from many perspectives investigates the effective factors in digital marketing. For example, some research discusses how businesses use social media platforms to spread their corporate social responsibility (CSR) plans and build long-term customer relationships [22], and other research explores how social media strategies increase brand knowledge within the industry [23]. Recent focus is on new marketing tools, such as virtual influencers (virtual stars), and their effect on company name management [24]. Furthermore, the company name itself has been shown to play a significant role in consumer risk and repeat buying behavior in digital marketing [25].

In total, these studies highlight the importance of marketing strategies and external factors in shaping digital marketing outcomes. But, for making these marketing activities happen in a safe and trusted way using governance, the focus is relatively small. Specifically, network safety governance, as a foundational system to support business digital marketing practice, has not yet been fully explored.

2.1.2. Research on Cybersecurity Governance

Cybersecurity governance is usually defined as a set of processes, policies, and structural frameworks that aim to ensure the organization's network security plan aligns with its business goals and complies with relevant laws [15]. It goes beyond pure tech defense measures, covering planning, organization design, leadership power, and accountability structures [26]. Effective cybersecurity governance aims to systematically mitigate cyber risks by establishing clear lines of responsibility, implementing comprehensive risk management procedures, and fostering organization-wide security awareness [27].

In recent years, literature on cybersecurity governance has been growing. Early research tends to focus on law and the following levels, examining information security

law changes and trends in information security law across different jurisdictions [28]. As network threats become more complex, the academic world's focus has already slowly shifted to governance frameworks and models. For example, some scholars put forward moving and fitting cybersecurity governance frames to address changing threats [29], and other scholars explore the development of many accountability system models within the cybersecurity governance structure [30].

Regarding the governance theme, the role of the board of directors gets special focus. Previous research shows that directors' IT knowledge and experience are important for lifting the company's web security state [31]. Likewise, companies with board members with IT expertise tend to exhibit stronger web security governance, which, in turn, affects their risk management decisions [32]. In summary, this research provides financial results as proof of web security governance; however, it focuses heavily on internal controls and reducing risk. The hidden strategic value of web security governance for a company's outside market activities has not yet been fully tested.

2.2. Research Hypotheses

Building on the resource-based view and signalling theory, this study conceptualizes cybersecurity governance as both a strategic resource that enhances firms' digital capability base and a credible signal that conveys data protection commitment to diverse stakeholders. Furthermore, considering the institutional and cultural embeddedness of the Chinese context, we incorporate insights from dynamic capability and institutional perspectives to capture how regulatory pressures and organizational learning jointly shape the effectiveness of cybersecurity governance. From the resource-based view perspective, a company's ability to compete comes from having resources and power that are valuable, rare, difficult to copy, and not easy to change. In the digital economy, data has already become an important plan asset. So, the power to protect these data assets—which is network security governance power—makes one key group capability. A strong network security governance system ensures the company's digital foundation runs stably, protects customer data privacy, and keeps it whole and usable, providing a safe, trustworthy foundation for digital marketing activities [13]. Furthermore, this governance power enables the company to use new digital technologies—such as the Internet of Things and artificial intelligence—to run marketing in new ways and not be overly constrained by concerns about hidden security risks [33]. In this sense, network security governance shows an internal, hard-to-copy group power. It directly powers digital marketing efforts and provides the company with a distinct advantage in an increasingly competitive market.

From a signaling theory perspective, in a market where information is asymmetric, one side (e.g., a company) can use trust signals to convey to the other side (e.g., a buyer) the quality it cannot see. A company's network security governance level is naturally hard for outside people to see directly. So, a company may take a set of visible actions to show its promise and power in network security. These signals include obtaining international security standards (such as ISO/IEC 27001), showing network security plans and financial support for security in annual reports, naming a high-level security leader (such as a Chief Information Security Officer, CISO), and speaking clearly and responsibly when security incidents occur [34]. These positive signals can effectively reduce the privacy and security risks buyers feel when engaging in digital marketing activities (such as signing up for accounts, making online payments, and sharing personal data), thereby fostering trust [11]. Trust is widely thought to be the foundation of digital marketing success. High trust leads to more user participation, higher conversion rates, and stronger customer loyalty. All in all, as discussed above, whether it is seen as an internal strategic power or an external

market signal, good network security governance provides a solid foundation for digital marketing success. Accordingly, we propose the following hypothesis:

H1: *Cybersecurity governance has a significantly positive impact on firms' digital marketing performance.*

Integrating the resource-based view and signalling theory, cybersecurity governance functions not only as a firm-specific strategic capability that secures and leverages data assets for digital marketing (RBV), but also as an observable and credible signal that reduces stakeholder uncertainty regarding data security practices (signalling theory). This dual role links internal capability formation with external trust building, thereby jointly underpinning our hypotheses and empirical design on how cybersecurity governance enhances digital marketing outcomes. To further elucidate the underlying mechanisms through which cybersecurity governance influences digital marketing, we next examine three potential mediating channels—corporate reputation, risk-taking, and information asymmetry—as illustrated in Figure 1.

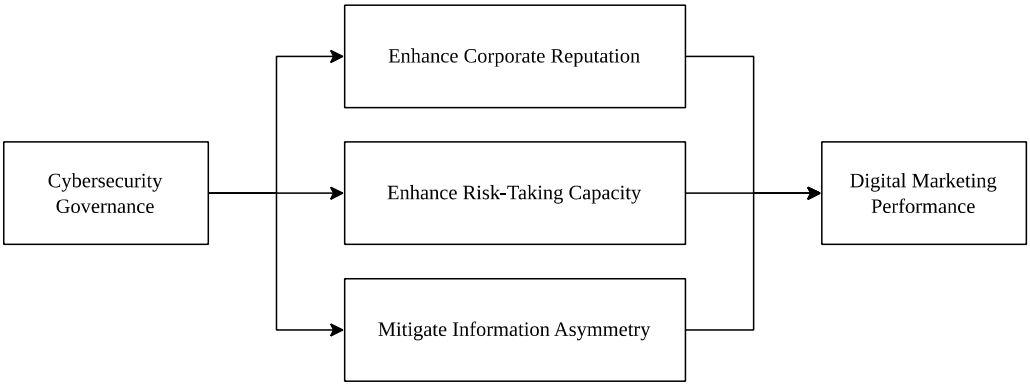

Figure 1. Theoretical framework of the impact of cybersecurity governance on digital marketing performance.

2.2.1. Enhancing Corporate Reputation

Enterprise reputation means the evaluation and feelings the public collects about an organization over time, and it is widely seen as one of its most valuable invisible assets. However, in the digital age, enterprise reputation becomes particularly vulnerable; a single big data leak can severely undermine the brand trust built over many years [35]. Good internet safety governance, by building strong defense systems and effective incident response mechanisms, can prevent or mitigate internet safety incidents and their adverse consequences, thereby preserving enterprise reputation [36].

More importantly, proactive cybersecurity governance practices—such as the adoption of Corporate Digital Responsibility (CDR) principles—may themselves function as positive drivers of corporate reputation [37,38]. When consumers perceive that a firm takes data protection seriously and can safeguard their personal information, their trust and favorable attitudes towards the firm are likely to increase significantly. Such reputational capital has direct conversion value in digital marketing contexts. Firms with stronger reputations are more likely to elicit positive consumer responses to marketing campaigns; their advertising messages tend to be perceived as more persuasive, and users are more willing to share branded content, thereby facilitating electronic word-of-mouth diffusion [39]. Taken together, these arguments suggest that cybersecurity governance may enhance digital marketing performance by strengthening corporate reputation. Accordingly, we propose the following hypothesis:

H2a: *Cybersecurity governance enhances digital marketing performance through the mediating effect of corporate reputation.*

2.2.2. Strengthening Risk-Taking Capacity

Digital marketing is inherently characterized by continuous experimentation and innovation. Whether firms attempt to engage with new social media platforms, adopt artificial intelligence–driven personalized recommendation algorithms, or launch novel online interactive campaigns, such initiatives inevitably involve technological, operational, and compliance-related risks [40]. A robust cybersecurity governance system can provide a "safety net" for marketing innovation. Through systematic security assessments of new technologies and applications, effective vulnerability management, and continuous monitoring mechanisms, firms are better able to control the cybersecurity risks associated with innovative activities and reduce the potential costs of failure [32].

When an enterprise fills its heart with trust in its risk management, high-level managers are more likely to allow and support the exploration of digital market projects, thereby raising the enterprise's overall risk-taking capacity. This kind of risk-taking ability from safety protection is important for keeping market life and winning the competition. On the contrary, when an enterprise's internet security foundation is weak, management decision-makers might take a more conservative stance because they worry about potential security holes, so they limit future market expansion. To sum up, these points show that internet safety governance builds a safe new-creation environment, strengthens the enterprise's will and ability to take risks, and, as a result, encourages them to participate more actively in digital market activities. Accordingly, we propose the following hypothesis:

H2b: *Cybersecurity governance enhances digital marketing performance through the mediating effect of firms' risk-taking capacity.*

2.2.3. Mitigating Information Asymmetry

Information asymmetry is a common phenomenon in market economies, referring to one party in a trade having more or better information than the other. In the digital marketing context, significant information asymmetry exists between the business and the consumer: the business fully understands its products, services, and data processes, but the consumer typically knows little about these details. This imbalance may lead to a lack of trust and back-choice problems. For example, because they worry that personal data may be misused, consumers may provide false information or avoid digital services altogether, thereby reducing the usefulness of marketing.

Effective cybersecurity governance constitutes an important mechanism for mitigating information asymmetry. As noted earlier, through transparent disclosures—such as publishing privacy policies, security white papers, and periodic security audit reports—firms can proactively communicate their data protection practices and commitments to external stakeholders [41]. Such transparency reduces uncertainty regarding how consumer data is collected, stored, and utilized, enabling consumers to make more informed decisions. Similarly, recent research on AI finds that the technology can reduce information asymmetry and lower the risk of stock price falls through stronger company governance and greater information clarity [42]. By using this push, net safety governance, as a major part of IT governance, can reduce consumers' sense of "marketing risk" through greater information clarity and growing trust based on specific information. As information asymmetry decreases, consumers want deeper contact with the business and are more willing to provide accurate personal data, so digital marketing tactics become much more effective and useful. To summarize, these points show that net safety governance can strengthen

digital marketing by reducing information asymmetry between businesses and consumers. Accordingly, we propose the following hypothesis:

H2c: *Cybersecurity governance enhances digital marketing performance by mitigating information asymmetry between firms and consumers.*

3. Materials and Methods

3.1. Model Specification

To test Hypothesis H1, namely the direct effect of cybersecurity governance on digital marketing, the following baseline regression model was constructed:

$$DM_{i,t} = \beta_0 + \beta_1 CSG_{i,t} + X'_{i,t}\theta + \mu_i + \lambda_t + \varepsilon_{i,t} \quad (1)$$

where i and t denote firm and year, respectively. $DM_{i,t}$ represents the dependent variable, measuring the level of digital marketing of firm i in year t. $CSG_{i,t}$ is the core explanatory variable, capturing the level of cybersecurity governance. $X'_{i,t}$ denotes a vector of control variables. μ_i represents firm fixed effects, controlling for time-invariant firm-specific characteristics, and λ_t denotes year fixed effects, capturing common macroeconomic shocks. $\varepsilon_{i,t}$ is the error term. The coefficient of primary interest is β_1. A significantly positive estimate of β_1 would indicate that stronger cybersecurity governance contributes to a higher level of digital marketing. To mitigate potential heteroskedasticity and other estimation concerns, robust standard errors were employed in all regression analyses.

3.2. Variable Selection

3.2.1. Dependent Variable

Following prior studies [43,44], the present study employs a textual analysis approach to measure firms' digital marketing level. Text-based measures have been widely adopted in recent research to capture firms' strategic orientation and managerial emphasis. A digital marketing keyword dictionary was constructed, including terms such as "digital marketing," "social media marketing," "search engine optimization (SEO)," "content marketing," "online advertising," "e-commerce," "O2O," "live-streaming commerce," and "private traffic." These keywords were identified based on their relevance to digital marketing practices in the Chinese context. For measurement, the total frequency of these keywords was calculated within the "Management Discussion and Analysis" (MD&A) section of each firm's annual report. To reduce skewness and ensure comparability across firms, the natural logarithm of one plus the total keyword frequency was taken to construct the digital marketing variable (DM).

3.2.2. Independent Variable

To enhance measurement validity, this study employs text-mining techniques based on annual reports to construct proxies for both cybersecurity governance and digital marketing engagement, which are widely used in recent literature to capture firms' strategic orientation and disclosure behavior. Drawing on prior studies [45–47], the measurement of firms' cybersecurity risk governance was conducted using the following procedure. First, to ensure that the textual measurement reflects the institutional and regulatory characteristics of the Chinese context, we developed a cybersecurity risk dictionary grounded in multiple authoritative sources. Specifically, 68 cybersecurity-related keywords were identified based on (i) China's national cybersecurity laws and regulations (e.g., Cybersecurity Law, Data Security Law), (ii) policy documents and industry guidelines issued by relevant government agencies, (iii) authoritative industry reports, and (iv) prior academic literature. These keywords include terms such as "data security," "information protection," "network

security governance," and "risk monitoring," which are widely used in Chinese corporate disclosures. This dictionary-based approach helps ensure contextual relevance while reducing the risk of omitted content bias [48]. Second, the annual report texts to be labeled were segmented into sentences using full stops as delimiters, thereby forming an initial corpus. A fixed-number random sampling procedure was then conducted at the firm–year level. A total of 13,000 sentences were randomly selected to construct the sentence pool for subsequent analysis. From this pool, approximately 1% of the sentences were further randomly drawn and manually annotated, and these manually labeled sentences served as the training set for model prediction [49]. Third, the manually selected sentences were carefully reviewed to determine (i) whether the content was related to cybersecurity and (ii) whether it reflected corporate cybersecurity governance activities. Each sentence was assigned a binary label (1 or 0) accordingly. Specifically, sentences were displayed sequentially, and labels were assigned based on human judgment. Fourth, a machine learning model was trained on the annotated dataset. The present study employed the RoBERTa model to learn from the training set. Model performance was evaluated using a validation set, and once an accuracy rate of 80% or higher was achieved, the fine-tuned RoBERTa model was used to predict the remaining unlabeled sentences [50]. This procedure enabled the identification of whether the textual content in annual reports genuinely reflected firms' cybersecurity risk governance behavior. Finally, based on the classification results, we constructed a firm-level dummy variable (CSG). If at least one sentence in a firm's annual report in a given year was identified as reflecting cybersecurity governance practices, the firm was coded as 1 for that year. Consistent with the persistence of governance structures, once a firm adopts cybersecurity governance practices, the CSG variable remains equal to 1 in subsequent years. Otherwise, it is coded as 0.

3.2.3. Control Variables

In line with prior research [51], a set of control variables was included to account for other factors that may influence firms' digital marketing activities. AGE is the natural logarithm of the firm's operating years, calculated as the statistical year minus the year of establishment plus one. The natural logarithm of total assets measures firm size (SIZE). ROE measures corporate profitability by dividing net profit by net assets. Liabilities to assets is the financial leverage (LEV) ratio. The book-to-market ratio (BM) is obtained by dividing a firm's book value by its market value. The ownership structure is further characterized by an ownership balance indicator (BALANCE), calculated as the ratio of the combined shareholdings of the second through fifth-largest shareholders to those of the largest shareholder. In addition, firm growth (GROWTH) is measured as the year-on-year growth rate of operating revenue, while cash flow (CASHFLOW) is defined as net cash flows from operating activities scaled by total assets.

3.3. Data Sources

The present study uses a firm-level panel dataset of Chinese A-share-listed companies from 2012 to 2023 as the initial research sample. Financial and corporate governance data were obtained from the China Stock Market and Accounting Research (CSMAR). Data on cybersecurity governance and digital marketing were derived from textual analysis of firms' annual reports using Python-based programming techniques. To ensure data reliability, the sample was screened according to the following criteria. First, firms in the financial industry were excluded. Second, firms designated as ST, *ST, or PT were removed from the sample. Third, firms that were listed or delisted during the sample period were excluded to maintain consistency in observations. Fourth, observations with missing values for key variables were deleted. After applying these screening procedures, the final

sample comprised 4530 firms and 35,063 firm–year observations, forming an unbalanced panel dataset. To mitigate the influence of extreme values, all continuous variables were winsorized at the 1% and 99% levels.

Table 1 shows the main variable descriptive statistics. Digital marketing (DM) average value is 3.342 and standard deviation is 2.327. This table highlights that DM min and max values have a wide range, showing that companies in digital marketing put in different value levels. Cybersecurity governance (CSG) average value is 0.245, standard deviation is 0.430. This variable has a relatively big scatter, showing that company cybersecurity governance practices have different natures, giving enough cross-sectional change for real analysis. Other control variables stay in a good range and are similar to variables in the current research. Taken together, these descriptive statistics provide preliminary support for the suitability and reliability of the sample used in this study.

Table 1. Descriptive statistics.

Variable	Obs	Mean	Std.	Min	Max
DM	35,063	3.34	2.327	0	7.53
CSG	35,063	0.246	0.431	0	1
AGE	35,063	2.983	0.307	2.079	3.611
SIZE	35,063	22.3	1.292	19.91	26.31
ROE	35,063	0.0469	0.142	−0.787	0.306
LEV	35,063	0.42	0.2	0.0549	0.875
BM	35,063	0.625	0.253	0.118	1.201
BALANCE	35,063	0.756	0.61	0.0322	2.832
GROWTH	35,063	0.143	0.373	−0.582	2.204
CASHFLOW	35,063	0.0479	0.0674	−0.154	0.242

4. Results

4.1. Benchmark Regression Results

Table 2 reports the effect of cybersecurity governance on the company's digital marketing, based on regression results. Column (1) shows results without control variables. The coefficient for CSG is positive and statistically significant at the 1% level. Column (2) adds firm-level control variables. As shown in Table 2, the coefficient for CSG is 0.302 and remains statistically significant at the 1% level. Column (3) further reports the results using robust standard errors. The estimated coefficient for CSG remains 0.332 and is still significant at the 1% level. These results show that, after controlling for other factors, company cybersecurity governance significantly improves its digital marketing performance. This finding gives strong support for hypothesis H1.

Table 2. Benchmark regression results.

	(1)	(2)	(3)
	DM	DM	DM
CSG	0.318 ***	0.302 ***	0.302 ***
	(8.444)	(7.981)	(8.215)
AGE		−0.167	−0.167
		(−0.857)	(−0.791)
SIZE		0.150 ***	0.150 ***
		(5.974)	(5.484)
ROE		−0.070	−0.070
		(−0.915)	(−0.908)

Table 2. *Cont.*

	(1)	(2)	(3)
	DM	**DM**	**DM**
LEV		−0.167 *	−0.167 *
		(−1.747)	(−1.654)
BM		−0.035	−0.035
		(−0.515)	(−0.497)
BALANCE		0.020	0.020
		(0.673)	(0.622)
GROWTH		0.001	0.001
		(0.049)	(0.046)
CASHFLOW		−0.460 ***	−0.460 ***
		(−2.964)	(−2.860)
Constant	3.263 ***	0.519	0.519
	(270.367)	(0.690)	(0.637)
Id FE	YES	YES	YES
Year FE	YES	YES	YES
N	35,044	35,044	35,044
R2	0.663	0.663	0.663

Note: *, *** indicate significance at the 10%, and 1% levels, respectively.

4.2. Robustness Tests

To ensure the reliability of the empirical findings, a series of robustness checks was conducted.

First, the dependent variable was replaced with an alternative proxy measure. Specifically, the logarithm of the frequency of digital marketing-related terms was used as an alternative indicator of firms' digital marketing activities (DM2). As shown in Column (1) of Table 3, the coefficient of cybersecurity governance remains significantly positive. These results are consistent with the baseline findings and suggest that the positive relationship between cybersecurity governance and digital marketing is not sensitive to alternative variable specifications.

Table 3. Robustness tests.

	(1)	(2)	(3)	(4)
	DM2	**DM**	**DM**	**DM**
CSG	0.167 ***		0.320 ***	1.017 ***
	(11.246)		(8.530)	(2.268)
L.CSG		0.080 *		
		(1.934)		
Constant	−0.851 ***	−0.261	0.341	11.814 **
	(−2.704)	(−0.264)	(0.402)	(2.342)
Id FE	YES	YES	YES	YES
Year FE	YES	YES	YES	YES
High-Dimensional Fixed Effects	NO	NO	YES	NO
N	35,044	28,959	34,986	35,063
R2	0.759	0.679	0.681	-

Note: *, **, *** indicate significance at the 10%, 5%, and 1% levels, respectively.

Second, the key explanatory variable lagged by one period. Given that cybersecurity governance is a long-term, systematic investment, its impact on digital marketing may exhibit a time-lagged effect. Moreover, lagging the explanatory variable helps mitigate potential reverse causality and endogeneity concerns. The results reported in Column (2) of

Table 3 show that the lagged cybersecurity governance variable (L.CSG) remains positively and significantly associated with digital marketing. This finding provides further support for the robustness of the main results.

Third, high-dimensional fixed effects were incorporated to control for industry-level heterogeneity and potential omitted variable bias. Specifically, industry–year interaction fixed effects were included in the baseline model to account for time-varying industry-specific shocks. As reported in Column (3) of Table 3, the positive effect of cybersecurity governance on firms' digital marketing remains statistically significant after controlling for cross-industry heterogeneity. This result further confirms the robustness of the main findings.

Fourth, a double machine learning (DML) approach was employed. Compared with traditional linear regression models, the DML method is better suited to addressing the "curse of dimensionality" arising from a large set of control variables, thereby allowing for more reliable estimation of causal effects. The results presented in Column (4) of Table 3 indicate that the estimated coefficient of cybersecurity governance remains significantly positive. These results are consistent with the baseline regression estimates and further support the validity of the empirical conclusions.

Given that key variables are constructed using text-based proxies derived from annual reports, measurement bias related to disclosure incentives and reporting heterogeneity may arise. To address this concern, we conducted multiple robustness checks using alternative variable specifications and estimation methods, and the results remain qualitatively unchanged, thereby supporting the reliability of our findings.

4.3. Mechanism Analysis

To examine the mediating mechanisms proposed above—namely, reputation, risk-taking, and information asymmetry—this study follows the approach of prior research [52] and constructs the following mediation models:

$$Med_{i,t} = \beta_0 + \beta_1 CSG_{i,t} + X'_{i,t}\theta + \mu_i + \lambda_t + \varepsilon_{i,t} \quad (2)$$

$$DM_{i,t} = \beta_0 + \beta_1 CSG_{i,t} + \beta_2 Med_{i,t} + X'_{i,t}\theta + \mu_i + \lambda_t + \varepsilon_{i,t} \quad (3)$$

In Equations (2) and (3), $Med_{i,t}$ denotes the mediating variables, including firm reputation (Reputation), risk-taking (Risk), and information asymmetry (InfoAsym). Equation (2) examines the impact of cybersecurity governance on the mediators, while Equation (3) incorporates both CSG and the mediating variables to assess whether the indirect effect operates through these channels. The estimation results of the mediation analysis are presented in Table 4.

Table 4. Mechanism Test.

	(1)	(2)	(3)	(4)	(5)	(6)
	Reputation	**DM**	**RiskTaking**	**DM**	**InfoAsym**	**DM**
CSG	0.014 **	0.302 ***	0.004 ***	0.299 ***	−0.063 ***	0.296 ***
	(2.179)	(8.237)	(3.520)	(8.152)	(−12.515)	(8.025)
Reputation		0.109 ***				
		(2.992)				
RiskTaking				0.828 ***		
				(5.263)		
InfoAsym						−0.079 **
						(−2.167)
Sobel test	0.014 ** (z = 2.28)		0.000 *** (z = 2.78)		−0.00 *** (z = −7.7)	
Constant	−6.229 ***	1.220	−0.095 ***	0.578	−0.286 **	0.438
	(−39.376)	(1.439)	(−3.024)	(0.709)	(−2.052)	(0.537)

Table 4. *Cont.*

	(1)	(2)	(3)	(4)	(5)	(6)
	Reputation	**DM**	**RiskTaking**	**DM**	**InfoAsym**	**DM**
Id FE	YES	YES	YES	YES	YES	YES
Year FE	YES	YES	YES	YES	YES	YES
N	34,831	34,831	35,028	35,028	34,890	34,890
R2	0.970	0.663	0.503	0.664	0.638	0.663

Note: **, *** indicate significance at the 5%, and 1% levels, respectively.

4.3.1. Reputation Channel

Following prior research [53], firm reputation is measured using the principal component analysis (PCA) method. The variables included in the PCA are Market Capitalization, Debt Ratio, Listing Years, Sustainable Growth Ability, Advertising Expense, Auditor Tenure, Nature of Firm, Return on Assets, and High-Tech Firm status. Columns (1) and (2) of Table 4 examine the mediating role of firm reputation (Reputation). Column (1) reports the estimation results of Equation (2), where Reputation is the dependent variable. As shown in Table 4, the coefficient on cybersecurity governance (CSG) is positive and statistically significant, indicating that higher levels of cybersecurity governance are associated with better firm reputation. Column (2) reports the results of Equation (3), where both CSG and Reputation are included in the regression of digital marketing (DM). The results indicate that the coefficient for Reputation is positive and statistically significant. Meanwhile, although the coefficient on CSG remains positive, its magnitude decreases compared with the baseline regression. In addition, Sobel tests were conducted to further validate the mediation effects, and the corresponding Z-statistics are significant at the 5% level for all three channels, confirming the robustness of the indirect effects. Taken together, these findings suggest that firm reputation partially mediates the relationship between cybersecurity governance and digital marketing, thereby supporting Hypothesis H2a.

4.3.2. Risk-Taking Channel

In line with prior research [54], this study measures risk-taking by the volatility of return on invested capital (ROIC). Specifically, risk-taking is defined as the standard deviation of seasonally adjusted quarterly pre-tax ROIC over a three-year window from year t to t + 2. ROIC is calculated as operating income after depreciation divided by the sum of debt, minority interest, preferred stock, and common equity.

Columns (3) and (4) of Table 4 examine the mediating role of risk-taking (RiskTaking). Column (3) reports the results of Equation (2), where RiskTaking is the dependent variable. As shown in Table 4, the coefficient on cybersecurity governance (CSG) is positive and statistically significant, indicating that improved cybersecurity governance significantly increases firms' risk-taking levels. Column (4) presents the results of Equation (3), in which both CSG and Risk are included in the regression of digital marketing. The coefficient on Risk is positive and statistically significant, suggesting that firms with higher risk-taking capacity tend to exhibit higher levels of digital marketing. Meanwhile, the coefficient on CSG remains positive but decreases in magnitude compared with the baseline regression. What stands out in Table 4 is the attenuation of the CSG coefficient after controlling for Risk. Taken together, these findings suggest that risk-taking serves as another important mediating channel through which cybersecurity governance promotes digital marketing, thereby supporting Hypothesis H2b.

4.3.3. Information Asymmetry Channel

Firms with higher levels of discretionary accruals are generally considered to face more severe information asymmetry. Following Cao et al. [55], this study measures information asymmetry (InfoAsym) as the absolute value of the sum of discretionary accruals in the current and the previous two fiscal years. Columns (5) and (6) of Table 4 examine the mediating role of information asymmetry. Column (5) reports the results of Equation (2), where InfoAsym is the dependent variable. As shown in Table 4, the coefficient on CSG is negative and statistically significant, indicating that improvements in cybersecurity governance significantly reduce information asymmetry. Column (6) presents the results of Equation (3), in which both CSG and InfoAsym are included in the regression of digital marketing. The coefficient on InfoAsym is negative and statistically significant, suggesting that lower levels of information asymmetry are associated with higher levels of digital marketing. Meanwhile, although the coefficient on CSG remains statistically significant, its magnitude decreases compared with the baseline regression. What stands out in Table 4 is the attenuation of the CSG coefficient after controlling for InfoAsym. Taken together, these findings suggest that cybersecurity governance enhances digital marketing by alleviating information asymmetry and creating a more favorable external environment, thereby supporting Hypothesis H2c.

4.4. Endogeneity Analysis

Given the potential dynamic persistence in firms' digital marketing activities—where firms with higher levels of digital marketing engagement tend to maintain or further strengthen such engagement over time—and the possible bidirectional causality between cybersecurity governance and digital marketing, this study incorporates the lagged dependent variable and employs both system GMM and difference GMM estimations to address endogeneity concerns. As reported in Table 5, the estimated coefficients of cybersecurity governance are 0.378 and 0.430, respectively, both statistically significant at conventional levels. These results indicate that the positive impact of cybersecurity governance on firms' digital marketing remains robust after controlling for dynamic effects and mitigating potential reverse causality and omitted variable bias.

Table 5. Endogeneity Analysis.

	(1)	**(2)**
	System-GMM	**Difference GMM**
L.DM	0.378 ***	0.430 ***
	(5.278)	(3.695)
CSG	3.560 ***	0.773 **
	(4.140)	(2.044)
Control variables	YES	YES
AR (1)	0.000	0.000
AR (2)	0.807	0.116
Observations	12,833	24,133

Note: **, *** indicate significance at the 5%, and 1% levels, respectively.

4.5. Heterogeneity Analysis

Given differences in resources, strategies, and environments, the effect of net safety governance may vary across company types. To discuss this possibility, this study conducts a heterogeneity analysis across three domains: ownership structure, technology strength, and region.

4.5.1. Ownership Heterogeneity

To examine whether the effect differs by ownership type, the sample was divided into state-owned enterprises (SOEs) and non-state-owned enterprises (Non-SOEs), and separate regressions were performed for each subsample. As reported in Table 6, the results indicate that the coefficient on CSG is 0.35 for Non-SOEs, which is substantially larger than that for SOEs (0.229), with both coefficients being statistically significant at the 1% level. These findings suggest that the positive effect of cybersecurity governance on digital marketing is more pronounced among non-state-owned firms. One possible explanation is that Non-SOEs face more intense market competition and therefore have stronger incentives to improve marketing performance by enhancing governance practices.

Table 6. Heterogeneity Analysis by Ownership Type.

	(1)	(2)
	DM (SOEs)	**DM (Non-SOEs)**
CSG	0.229 ***	0.350 ***
	(3.713)	(7.524)
Constant	0.516	3.768 ***
	(0.317)	(5.134)
Id FE	YES	YES
Year FE	YES	YES
N	11,433	10,642
R2	0.638	0.690

Note: *** indicate significance at the 1% level.

4.5.2. Technological Intensity Heterogeneity

Based on the industry classification of the China Securities Regulatory Commission (CSRC), firms were categorized into high-technology and non-high-technology industries. As reported in Table 7, the regression results show that the coefficient on CSG for high-technology firms (0.352) is significantly larger than that for non-high-technology firms (0.223). This may be because high-technology firms rely more heavily on data and digital technologies in their business models. Their digital marketing activities tend to be more sophisticated and technology-driven, making effective cybersecurity governance particularly important for supporting marketing performance.

Table 7. Heterogeneity Analysis by Technological Characteristics.

	(1)	(2)
	DM (Non-High-Technology)	**DM (High-Technology)**
CSG	0.223 ***	0.352 ***
	(4.162)	(6.463)
Constant	0.225	1.562
	(0.178)	(1.254)
Id FE	YES	YES
Year FE	YES	YES
Region FE	YES	YES
N	16,631	18,144
R2	0.694	0.663

Note: *** indicate significance at the 1% level.

4.5.3. Regional Heterogeneity

To examine regional heterogeneity, the sample was divided into eastern, central, and western regions according to firms' registered locations. As reported in Table 8, the results show that the coefficient on CSG is significantly positive for firms located in the eastern region (0.33) and the central region (0.289), while it is statistically insignificant for firms in the western region. These findings suggest that cybersecurity governance plays a more prominent role in enhancing digital marketing performance in regions with relatively more developed digital infrastructure and market environments. In contrast, its effect is less evident in the western region.

Table 8. Heterogeneity Analysis by Geographic Region.

	(1)	(2)	(3)
	DM (Eastern City)	**DM (Central City)**	**DM (Western City)**
CSG	0.330 ***	0.289 ***	0.176
	(7.760)	(2.974)	(1.625)
Constant	0.213	4.953 **	−0.624
	(0.226)	(2.249)	(−0.244)
Id FE	YES	YES	YES
Year FE	YES	YES	YES
N	25,164	5425	4424
R2	0.671	0.648	0.633

Note: **, *** indicate significance at the 5%, and 1% levels, respectively.

5. Discussion

This study uses 2012–2023 China A-share listed company data. It examines how cybersecurity governance affects a company's digital markets and discusses the ins and outs of this topic. Research results show that strong cybersecurity governance significantly improves a company's digital market position. Perhaps the biggest finding is that this positive influence operates through three middle paths: enhancing corporate reputation, strengthening firms' risk-taking capacity, and mitigating information asymmetry. Another important finding is that this help is greater in non-state companies, companies in the east, and high-tech companies. These results show that cybersecurity governance works differently depending on a company's structure, the local environment, and the level of technology.

5.1. Theoretical Contributions

First, these findings provide further support for applying signaling theory to cybersecurity governance. Prior studies have noted that, in digital marketing activities, consumers and business partners are increasingly concerned about data privacy and security issues [20,40]. In this regard, firms that strengthen cybersecurity governance and disclose related information effectively transmit a strong positive signal to the market [46]. This signal may indicate that the firm possesses the capability to safeguard user data, maintain system stability, and act as a responsible and trustworthy partner. These findings suggest that such signaling mechanisms can reduce stakeholder uncertainty, thereby enhancing corporate reputation. The present study found that improvements in corporate reputation constitute one of the key mediating channels through which cybersecurity governance promotes digital marketing. This finding is consistent with previous research showing that proactive corporate behaviors, such as green innovation, can enhance firm reputation and, in turn, improve market performance [53].

Second, from the perspective of the resource-based view, this study reconceptualizes cybersecurity governance as a strategic resource and core capability rather than merely a compliance cost. In the digital economy, a safe and stable digital environment provides a foundation for value creation [13]. Strong cybersecurity rules may work like a "digital firewall." It is valuable, rare, and hard to copy. This ability not only protects the business from external threats but also strengthens its internal risk management. This study's results show that this ability strengthens business risk-taking, leading the business to try more in digital sales, for example, by using advanced data tools or exploring new sales channels. These results are the same as those of the Xu (2025) [46] study, which found that cybersecurity rules can strengthen business risk-taking to spark business innovation.

Finally, the study's biggest theoretical contribution is the integration of two traditionally separate areas: internal company rules and external market performance. Previous studies mainly examined the immediate effect of internal IT rules or external market digital sales results. By contrast, the present findings suggest that internal governance—particularly cybersecurity governance—can be directly translated into improved external market activities. These results provide support for the idea that, in the digital era, the boundary between internal management and external market performance is becoming increasingly blurred. It may therefore be the case that a firm's market competitiveness increasingly depends on the strength of its internal technological and governance capabilities.

In addition, the heterogeneous effects across ownership types, regions, and technological intensity also suggest that the impact of cybersecurity governance is contingent upon firms' resource endowments and external environments, reflecting important boundary conditions such as market competition, uncertainty, and industry digitalization. Future research may further explore these mechanisms by incorporating additional moderating factors and adopting longitudinal designs to examine how firms' transitions in cybersecurity governance shape the dynamic evolution of digital marketing.

5.2. Practical Implications

These findings for company managers, investors, and policymakers have important practical implications. First, for corporate managers, the results highlight the strategic value of cybersecurity governance. This finding implies that cybersecurity should no longer be regarded as an isolated technical issue confined to the IT department, but rather elevated to the core level of corporate governance and strategic planning [31,32]. Investment in cybersecurity governance may therefore be viewed not merely as a defensive measure to prevent potential attacks and losses, but as a proactive strategic investment aimed at strengthening brand trust, empowering digital marketing, and creating long-term business value. These results show that the connection between the sales and IT/safety parts is important. Data-driven sales depend on building a strong safety base. If there is no base, keeping and using new sales may be negatively impacted.

Second, for investors, this study offers a new perspective on company value. Study results show that cybersecurity rules can be used for investment decisions in non-financial areas. This is because it has a strong link with a running company name, guest loyalty, and final financial results. This view aligns with the daily stress on ESG (environmental, social, and governance) investment rules. In these rules, the "rule" side can be understood to include cybersecurity and data rule practices [56].

Lastly, for policymakers, the findings suggest that the rule frame should balance the "hurt" and "encourage" ways. Punishment for data leaks is still needed, but the government can also consider encouraging greater transparency around cybersecurity rules. For example, through required or recommended standards, the market can identify

and reward businesses with strong cybersecurity practices [57]. These results show that a good design for a rule frame to deal with digital money in a time of growing network risk fear is important.

5.3. Limitations and Future Research

Although there are these value findings, we should admit some limits. This points to future study ways. First, there are limitations related to variable measurement. This study employed textual analysis of annual reports to quantify the levels of cybersecurity governance and digital marketing among listed firms. Although this approach is widely used in the existing literature, it is highly dependent on firms' disclosure incentives and reporting quality and may not fully capture undisclosed or informal practices. These findings, therefore, need to be interpreted with caution. Future research is needed to develop more diversified data sources. For example, subsequent studies could conduct surveys of chief information officers (CIOs) or chief marketing officers (CMOs), utilize cybersecurity rating data published by third-party agencies, or obtain more detailed information on marketing budget allocations. Such approaches may help provide a more comprehensive assessment of firms' cybersecurity governance and digital marketing activities. Second, identifying causal relationships remains challenging. Although this study used lagged variables, instrumental variables, and difference-in-differences models to mitigate endogeneity concerns, establishing definitive causality is inherently difficult in observational research. It is possible that an underlying forward-looking corporate culture simultaneously encourages both cybersecurity investment and digital marketing innovation, thereby influencing the observed relationship. Further work is needed to identify more rigorous quasi-natural experimental settings. Future studies might also collaborate directly with firms to conduct field experiments, thereby enabling clearer identification of the causal mechanisms at play. Third, the generalizability of the findings warrants careful consideration. The sample consists of Chinese A-share listed firms, whose unique institutional background and market environment may shape the observed effects. The generalisability of our findings may be influenced by cross-country institutional differences, particularly in regulatory frameworks governing data protection and the maturity of digital market architectures. These institutional variations may shape both the signalling effectiveness and resource value of cybersecurity governance, thereby affecting the strength and transmission mechanisms identified in this study. These results may be context-specific and not fully generalizable to other institutional settings. Future studies are therefore recommended to extend this analytical framework to other countries and markets, including developed economies and other emerging markets. Comparative research across different institutional environments would help assess the robustness of the present findings and examine whether the role of cybersecurity governance varies across contexts. As a result, the findings of this study may be context-specific and should be generalized with caution. Future research is encouraged to extend this analytical framework to other institutional settings and conduct cross-country comparative analyses. Such studies would help assess whether the observed relationships hold under different regulatory environments and digital market conditions, and whether the role of cybersecurity governance varies across contexts.

6. Conclusions

In the context of the rapidly evolving digital economy, this study provides systematic evidence that cybersecurity governance plays a critical and value-creating role in shaping firms' digital marketing activities. Using panel data from Chinese A-share listed firms, we demonstrate that cybersecurity governance is not merely a defensive mechanism but a strategic enabler that significantly enhances digital marketing engagement. More im-

portantly, this study moves beyond documenting a direct relationship and uncovers the underlying mechanisms through which cybersecurity governance generates marketing value. The findings reveal that effective cybersecurity governance strengthens corporate reputation, fosters a greater willingness to undertake innovation-related risks, and reduces information asymmetry between firms and stakeholders. Together, these mechanisms illustrate how internal governance structures can be transformed into external market advantages, highlighting the increasingly blurred boundary between organizational governance and market-facing capabilities in the digital era.

Several key lessons can be drawn from these findings. First, cybersecurity governance should be reinterpreted as a strategic resource that supports value creation rather than as a compliance-driven cost center. Second, firms seeking to enhance digital marketing performance must recognize the foundational role of secure and trustworthy data environments in enabling customer engagement and innovation. Third, the effectiveness of cybersecurity governance is context-dependent, being more pronounced in competitive, technology-intensive, and institutionally developed environments, suggesting that governance investments should be aligned with firm characteristics and external conditions. Overall, this study contributes to a more integrated understanding of how governance mechanisms shape market outcomes and offers a new perspective on the strategic role of cybersecurity in the digital economy.

Author Contributions: Conceptualization, Y.H.; Methodology, Y.H.; Formal analysis, Y.H.; software, Y.H.; validation, Y.H.; Investigation, B.H.; Writing—original draft preparation, Y.H.; Writing—review and editing, Y.H.; visualization, B.H. and Y.H.; Supervision, Y.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Davies, P.; Fritzsche, A.; Parry, G.; Wood, Z. Data, Resilience, and Identity in the Digital Age. *Strateg. Change* **2023**, *32*, 169–174. [CrossRef]
2. Li, J. Research on Corporate Brand Marketing Strategies in the Context of the Digital Economy. *FBEM* **2024**, *15*, 240–243. [CrossRef]
3. Saura, J.R.; Škare, V.; Dosen, D.O. Is AI-Based Digital Marketing Ethical? Assessing a New Data Privacy Paradox. *J. Innov. Knowl.* **2024**, *9*, 100597. [CrossRef]
4. Wang, X.; Qiu, X. The Positive Effect of Artificial Intelligence Technology Transparency on Digital Endorsers: Based on the Theory of Mind Perception. *J. Retail. Consum. Serv.* **2024**, *78*, 103777. [CrossRef]
5. Adejumo, A.P.; Ogburie, C.P. Strengthening Finance with Cybersecurity: Ensuring Safer Digital Transactions. *World J. Adv. Res. Rev.* **2025**, *25*, 1527–1541. [CrossRef]
6. Sathyadevi, R.; Ramesh, M.; Metilda, V.P.; Cyriac, J. Quantification of Cybersecurity Risk and Economic Impact Modeling. In *AI in Industry 5.0: Revolutionizing Business and Technology*; Royal Book Publishing: Tamil Nadu, India, 2025; pp. 173–177.
7. Farhad, M.A. Consumer Data Protection Laws and Their Impact on Business Models in the Tech Industry. *Telecommun. Policy* **2024**, *48*, 102836. [CrossRef]
8. Bakare, S.S.; Adeniyi, A.O.; Akpuokwe, C.U.; Eneh, N.E. Data Privacy Laws and Compliance: A Comparative Review of the EU GDPR and USA Regulations. *Comput. Sci. IT Res. J.* **2024**, *5*, 528–543. [CrossRef]
9. Cheng, S.; Li, J.; Luo, L.; Zhu, Y. Cybersecurity Governance and Digital Finance: Evidence from Sovereign States. *Financ. Res. Lett.* **2024**, *65*, 105533. [CrossRef]

10. Galle, A.; Vletter-van Dort, H. From Cybersecurity to Cyber Resilience in the Board Room: Key Steps for Supervisory Board Members and Non-Executives. *Int. Cybersecur. Law Rev.* **2025**, *6*, 221–237. [CrossRef]
11. Tan, W.; Guo, B.; Zhang, Q. Cybersecurity Governance and Corporate Market Value: Perspectives from Investor Trust and Supply Chain Trust. *Pac.-Basin Financ. J.* **2025**, *90*, 102646. [CrossRef]
12. Yasmin, A.; Tasneem, S.; Fatema, K. Effectiveness of Digital Marketing in the Challenging Age: An Empirical Study. *Int. J. Manag. Sci. Bus. Adm.* **2015**, *1*, 69–80. [CrossRef]
13. Ali, C.S.M.; Zeebaree, S.R.M. Cloud-Based Web Applications for Enterprise Systems: A Review of AI and Marketing Innovations. *Asian J. Res. Comput. Sci.* **2025**, *18*, 427–451. [CrossRef]
14. Wu, S.P.-J.; Straub, D.W.; Liang, T.-P. How Information Technology Governance Mechanisms and Strategic Alignment Influence Organizational Performance: Insights from a Matched Survey of Business and IT Managers1. *MIS Q.* **2015**, *39*, 497–518. [CrossRef]
15. Savaş, S.; Karataş, S. Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance. *Int. Cybersecur. Law Rev.* **2022**, *3*, 7–34. [CrossRef]
16. Saeed, S.; Jhanjhi, N.Z.; Khan, M.A.; Yadav, D.K. Editorial: Digital Transformation and Cybersecurity Challenges. *Front. Comput. Sci.* **2025**, *7*, 1631362. [CrossRef]
17. Barlow, E. Cybersecurity as a Brand Differentiator: Building Trust in the Age of AI. *Zenodo* **2025**. [CrossRef]
18. Li, L.; Hsu, C.; Mao, J.; Zhang, W. Contextualising Digital Innovation in Today's China: Local Practices and Global Contributions. *Inf. Syst. J.* **2022**, *32*, 623–629. [CrossRef]
19. Okazaki, S. (Ed.) *Handbook of Research on International Advertising; Elgar Original Reference*; Edward Elgar: Cheltenham, UK; Northampton, MA, USA, 2012; ISBN 978-1-78100-104-2.
20. Al Prince, A.; Siddiqui, H.A.; Lakho, M.B.; Ahmad, S.; Asghar, A. Leveraging Artificial Intelligence for Hyper-Personalized Marketing: Opportunities and Challenges in the Digital Era. *Inverge J. Soc. Sci.* **2025**, *4*, 274–287. [CrossRef]
21. Xu, Y. Strategic Engagement and Brand Perception: An Analysis of Social Media Marketing in the Luxury Automobile Industry. *Adv. Econ. Manag. Political Sci.* **2024**, *105*, 56–63. [CrossRef]
22. Dan Ioan, T.; Silvia Stefania, M.; Carmen Adina, P.; Irina Bogdana, P.; Mircea Stefan, S. Using CSR Communication through Social Media for Developing Long-Term Customer Relationships. The Case of Romanian Consumers. *Econ. Comput. Econ. Cybern. Stud. Res.* **2022**, *56*, 255–272. [CrossRef]
23. Capitello, R.; Agnoli, L.; Begalli, D.; Codurri, S. Social Media Strategies and Corporate Brand Visibility in the Wine Industry: Lessons from an Italian Case Study. *EuroMed J. Bus.* **2014**, *9*, 129–148. [CrossRef]
24. Xin, B.; Hao, Y.; Xie, L. Virtual Influencers and Corporate Reputation: From Marketing Game to Empirical Analysis. *J. Res. Interact. Mark.* **2024**, *18*, 759–786. [CrossRef]
25. Oğuz, G.; Karaca, Y. The Effect of Corporate Reputation on Perceived Risk and Repurchase Behavior in Digital Marketing. *J. Bus. Res.-Turk* **2023**, *15*, 3029–3047. [CrossRef]
26. Gilbert, C.; Gilbert, M.A. Organizational and Leadership Aspects of Cybersecurity Governance. *Int. J. Res. Publ. Rev.* **2024**, *5*, 1174–1191. [CrossRef]
27. Yusif, S.; Hafeez-Baig, A. A Conceptual Model for Cybersecurity Governance. *J. Appl. Secur. Res.* **2021**, *16*, 490–513. [CrossRef]
28. Smedinghoff, T.J. The State of Information Security Law: A Focus on the Key Legal Trends. *EDPACS* **2008**, *37*, 1–52. [CrossRef]
29. Melaku, H.M. A Dynamic and Adaptive Cybersecurity Governance Framework. *J. Cybersecur. Priv.* **2023**, *3*, 327–350. [CrossRef]
30. Slapničar, S.; Axelsen, M.; Bongiovanni, I.; Stockdale, D. A Pathway Model to Five Lines of Accountability in Cybersecurity Governance. *Int. J. Account. Inf. Syst.* **2023**, *51*, 100642. [CrossRef]
31. Al-Sartawi, A.M.A.M. Information Technology Governance and Cybersecurity at the Board Level. *Int. J. Crit. Infrastruct.* **2020**, *16*, 150. [CrossRef]
32. Ling, S.; Liu, Z.; Xia, H. Code, Control and Cybersecurity: How Board IT Expertise Shapes Corporate Risk Management. *J. Account. Lit.* **2025**, 1–23. [CrossRef]
33. Liantifa, M.; Hendra; Sekianti, A. The Role of Internet of Things in Smart Business Decision-Making: A Narrative Review. *Novatio J. Manag. Technol. Innov.* **2025**, *3*, 66–79. [CrossRef]
34. Pokhidnia, B. Ethics in Information Management: Personal Data Protection. *Econ. Scope* **2025**, *197*, 212–216. [CrossRef]
35. Lupion Garcia, R.; Hackmann, E.O. Cibersegurança e Dever de Diligência Do Administrador. *Rev. Direito Empres.* **2024**, *2*, 21. [CrossRef]
36. Blue, G.; Faraji, O.; Khotanlou, M.; Rezaee, Z. A Corporate Risk Assessment and Reporting Model in Emerging Economies. *J. Appl. Account. Res.* **2023**, *25*, 783–811. [CrossRef]
37. Santoso, R.A.; Harefa, T.; Fuadah, L.L. Corporate Social Responsibility: A Literature Review on Practices, Implications, and Future Directions. *Int. J. Econ. Account. Manag.* **2024**, *1*, 209–214. [CrossRef]

38. Chaudhary, H.K.; Singh, M.; Ghosh, P. Influence of Corporate Digital Responsibility, Responsible Marketing, Green Technology and Responsible Practices on Green Brand Equity in Star-Rated Hotels. *Int. J. Contemp. Hosp. Manag.* **2025**, *37*, 3632–3656. [CrossRef]
39. Peng, H.; Zhang, Q.; Zhang, Z. Does Information Source Matter? Corporate Reputation Management during Negative Social Responsibility Events. *J. Theor. Appl. Electron. Commer. Res.* **2024**, *19*, 2747–2764. [CrossRef]
40. Catayoc, R.B. Privacy, Promotion, and Platform Pitfalls: The Case of How Telegram's Marketing Approach Inadvertently Attracted Illicit Actors. *Randwick Int. Soc. Sci. J.* **2025**, *6*, 60–78. [CrossRef]
41. Razinkin, N.; Fedosiuk, D. Business Intelligence in the Digital Environment: Legal and Analytical Aspects. *Bus. Navig.* **2025**, *3*, 243–248. [CrossRef]
42. Zhang, J.; Cui, C.; Zheng, C.; Taylor, G. Artificial Intelligence Innovation and Stock Price Crash Risk. *J. Financ. Res.* **2025**, *48*, 503–543. [CrossRef]
43. Herhausen, D.; Miočević, D.; Morgan, R.E.; Kleijnen, M.H.P. The Digital Marketing Capabilities Gap. *Ind. Mark. Manag.* **2020**, *90*, 276–290. [CrossRef]
44. Zhang, Y.; Jiang, M. Digital Marketing, Social Media Sentiment, and Corporate Cash Flow. *Financ. Res. Lett.* **2026**, *92*, 109538. [CrossRef]
45. Wang, D.; Hu, Y.; Li, Y. Cybersecurity Risk and Corporate Maturity Mismatch. *Int. Rev. Financ. Anal.* **2026**, *109*, 104757. [CrossRef]
46. Xu, J. Cybersecurity Governance and Corporate Innovation: Evidence from China. *Financ. Res. Lett.* **2025**, *82*, 107619. [CrossRef]
47. Florackis, C.; Louca, C.; Michaely, R.; Weber, M. Cybersecurity Risk. *Rev. Financ. Stud.* **2022**, *36*, 351–407. [CrossRef]
48. Geng, Y.; Xiang, X.; Wan, P. Supply Chain Trust Decline: Cybersecurity Risks and Corporate Trade Credit. *China Ind. Econ.* **2024**, *5*, 135–154. [CrossRef]
49. Lu, Y.; Shi, H.; Zhou, X. Impact of Digital Technology Risk Exposure on Corporate Value in Chinese Firms: Evidence from Text Analysis Using Large Language Models. *Econ. Res. J.* **2025**, *60*, 73–89.
50. Liu, Y.; Ott, M.; Goyal, N.; Du, J.; Joshi, M.; Chen, D.; Levy, O.; Lewis, M.; Zettlemoyer, L.; Stoyanov, V. RoBERTa: A Robustly Optimized BERT Pretraining Approach. *arXiv* **2019**, arXiv:1907.11692.
51. Quintino, J.P. The Impact of Artificial Intelligence (AI) on Digital Marketing. In *Next Generation Entrepreneurship*; Springer Nature: Cham, Switzerland, 2026; pp. 317–333.
52. Baron, R.M.; Kenny, D.A. The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations. *J. Personal. Soc. Psychol.* **1986**, *51*, 1173–1182. [CrossRef]
53. Iftikhar, K.; Bagh, T.; Shabbir, M.N. Corporate Reputation Gains from Green Innovation: Moderating Effects of Subsidies and Eco-Friendly Products. *Res. Int. Bus. Financ.* **2025**, *80*, 103108. [CrossRef]
54. Ljungqvist, A.; Zhang, L.; Zuo, L. Sharing Risk with the Government: How Taxes Affect Corporate Risk Taking. *J. Account. Res.* **2016**, *55*, 669–707. [CrossRef]
55. Cao, F.; Li, H.; Zhang, X.; Zou, H. Preventive Regulatory Enforcement and Access to Trade Credit: Evidence from a Quasi-Natural Experiment. *J. Corp. Financ.* **2026**, *96*, 102855. [CrossRef]
56. Shackelford, S.J.; Raymond, A.; McCrory, M.A.; Bonime-Blanc, A. Cyber Silent Spring: Leveraging ESG+T Frameworks and Trustmarks to Better Inform Investors and Consumers about the Sustainability, Cybersecurity, and Privacy of Internet-Connected Devices. *SSRN Electron. J.* **2022**, *55*, 669–707. [CrossRef]
57. Qudus, L. Cybersecurity Governance: Strengthening Policy Frameworks to Address Global Cybercrime and Data Privacy Challenges. *Int. J. Sci. Res. Arch.* **2025**, *14*, 1146–1163. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.