Adapting to Adversity:

The Impact of Data Breaches on the Disclosure of Digital Strategic Initiatives

In the digital age, understanding the impact of data breaches on Digital Strategic Initiatives (DSIs) is crucial for organizational success. This study leverages disclosure theory and institutional theory to investigate how data breaches influence the disclosure behaviors of S&P500 firms regarding their DSIs. By examining the effects of breaches through customer, supplier, and competitor relationships, our research uncovers how proximity to breaches shapes DSI disclosure disparities of mega firms. Our findings reveal significant economic implications for megafirms: competitors of breached entities diverge more in their digital strategies, signaling robustness and innovation to stakeholders while avoiding costs associated with withholding DSI. In contrast, firms directly linked to breached suppliers and customers exhibit conservative shifts in DSI disclosures, opting for strategic silence to protect proprietary information and avoid proprietary costs associated with disclosure. Additionally, firms with historical breach experience leverage their past learnings to adjust their digital strategies more effectively, particularly in the context of supplier breaches, where information flow and interdependencies are stronger. This study extends the discourse on mandatory versus voluntary disclosures, emphasizing the role of information asymmetry and strategic considerations in shaping disclosure behaviors post-breach of megafirms. Specifically, it highlights that access to private information about breaches at suppliers or customers leads to reduced DSI disclosure, as firms strategically manage the release of sensitive information and avoid proprietary costs associated with disclosure. These findings underscore the critical need for strategic information management and robust cybersecurity practices to maintain market stability and stakeholder trust in an increasingly digital landscape.

INTRODUCTION

As organizations rely more heavily on digital strategic initiatives to drive innovation, enhance operational efficiency, and gain a competitive edge, understanding the implications of data breaches on these initiatives becomes crucial. Digital strategic initiatives encompass the actions undertaken by organizations to leverage digital technologies, including artificial intelligence (AI), and capabilities to achieve their strategic

objectives (Bharadwaj et al., 2013). Notable progress has been made in these initiatives, such as automating labor-intensive tasks and enhancing cyber resilience through advanced technologies (Siponen, 2000; Kraemer & Carayon, 2007; Werlinger, 2009; Acemoglu & Restrepo, 2018). The adoption of DSIs and the subsequent communication of this adoption to inform investors have thus become focal points for firms aiming to harness digital transformation while ensuring robust cybersecurity measures. Amidst this landscape, exploring how DSIs are influenced by the experience and knowledge gained from data breaches becomes paramount.

In this work, drawing upon the disclosure theory (Dye, 1983; Dye, 2001) and institutional theory (Meyer & Rowan, 1977; DiMaggio & Powell, 1983), we investigate firms' disclosures of DSIs following data breaches. Institutional theory posits that organizations are subject to isomorphic pressures, leading them to emulate practices of perceived successful peers to gain legitimacy (Cavusoglu et al., 2015). Such pressures are intensified in the wake of data breaches, as firms seek to reassure stakeholders by aligning their DSIs with those of non-breached firms or by proactively enhancing their cybersecurity disclosures to reflect industry best practices. The interaction between these theories informs our hypotheses regarding the disclosure behaviors of organizations in close proximity to breached entities through customer, supplier, and competitor relationships. This emphasis is justified by the significant ripple effects seen in supply chain breaches, where a breach at a key supplier can impact all customer firms reliant on its services, potentially leading to industry-wide breaches. Such that, The Kaseya ransomware attack exploited an authentication bypass vulnerability (CVE-2021-30116) within Kaseya VSA servers (Kaseya, 2022), allowing hackers to execute commands via SQL injection and deploy ransomware. The attack compromised Kaseya's customer database and impacted nearly 2,000 businesses across 17 countries, making it the largest supply chain ransomware attack on record. The ransomware spread through Managed Service Providers (MSPs), highlighting the extensive reach and impact of such vulnerabilities on global supply chains. Understanding how firms manage and disclose information about their DSIs in response to such breaches is crucial as it shapes the information asymmetry and volatility in the markets. Megafirms, especially those directly tied to a breached entity through supply chain contracts, often bear contractual liabilities for any disruptions in

deliveries. These contracts typically include clauses that make firms liable for the continuity and security of their operations, thus amplifying the stakes associated with data breaches. Consequently, these firms usually have more access to private information, which allows them to manage disclosures strategically (Goswami et al., 2011; Rai and Bush 2007). This strategic management of information is essential for mitigating market volatility and maintaining stakeholder trust, highlighting the intricate relationship between contractual obligations and information disclosure practices in the context of cybersecurity. In contrast, competitor firms with less access to detailed breach information may significantly increase their disclosures to differentiate themselves and reassure stakeholders. These firms, recognizing the competitive advantage in appearing robust and proactive, leverage heightened transparency as a strategic tool. By openly communicating their own cybersecurity measures and digital strategic initiatives, they aim to project confidence and stability in the face of their rivals' vulnerabilities. This approach not only helps mitigate any potential negative perceptions associated with industry-wide breaches but also serves to attract and retain stakeholders by demonstrating a commitment to security and innovation (Tuo et al., 2020; Leary & Roberts, 2014). For example, Target experienced a major data breach in 2013, where hackers accessed credit card information of over 40 million customers. The breach was traced back to a compromised vendor, illustrating the interconnectedness of supply chains and the ripple effects of cybersecurity vulnerabilities. Following the breach, Target invested heavily in its DSIs, implementing advanced cybersecurity technologies and protocols to prevent future incidents, such as adopting EMV chip technology for payment cards and enhancing network security. Firms face significant reputational damage from supply chain attacks, with an average cost of $1.5 million in 2022, affecting customer trust and loyalty (Intellias, 2023). Target's efforts to disclose its enhanced DSIs and commitment to cybersecurity helped rebuild its reputation. By communicating its proactive measures to stakeholders, the company demonstrated its dedication to protecting customer data and preventing similar breaches in the future. The adoption of DSIs and the subsequent communication of this adoption to inform investors have thus become focal points for firms aiming to harness digital transformation while communicating their robust cybersecurity measures. The Target breach underscores the importance of DSIs in both preventing and managing the aftermath of

cybersecurity incidents. Robust DSIs enable firms to respond quickly and effectively to breaches, minimizing damage and maintaining stakeholder trust. Furthermore, strategic disclosure of DSIs plays a crucial role in managing the narrative around a breach, helping firms to restore and maintain stakeholder confidence.

By communicating their cybersecurity initiatives, firms can reassure stakeholders and mitigate the reputational damage associated with data breaches, while also advancing their digital strategic initiatives (DSIs). However, existing research lacks a comprehensive understanding of how proximity to a breached entity influences DSI disclosure behavior and information asymmetry. Furthermore, measuring digital strategic initiatives or digital transformation itself remains a complex challenge. Our study addresses these gaps by investigating how the proximity to a breached entity—whether a customer, supplier, or competitor—shapes firms' DSI disclosure behaviors. Additionally, we introduce a novel method to measure digital strategic initiatives, leveraging state-of-the-art Natural Language Processing (NLP) models on unstructured data, specifically earnings call transcripts. This innovative approach achieves state-of-the-art level accuracy, with F1 levels reaching 94%, setting a new benchmark in the field.

By examining the proximity to breaches through customer, supplier, and competitor relationships, our study illuminates the dual role of Digital Strategic Initiatives (DSIs) as both a strategic tool and a communication mechanism. When a breach occurs within a supply chain, the interconnected nature of business ecosystems necessitates a coordinated response from all affected entities. Companies with direct ties to a breached entity often gain access to private information, enabling them to manage disclosures more strategically. This allows them to balance the need for transparency with the imperative to protect proprietary information. Conversely, competitors with limited access to breach details may increase their DSI disclosures to differentiate themselves and reassure stakeholders, using DSIs to demonstrate their robust cybersecurity posture. Our findings extend the current discourse on mandatory versus voluntary disclosures. While existing research highlights that mandatory disclosures can stimulate voluntary disclosures, our study reveals that access to private information about a breach incident can lead to reduced voluntary disclosures in the context of data breaches. This nuanced understanding provides a compelling

addition to the literature, emphasizing how information asymmetry and strategic considerations shape disclosure behaviors in the aftermath of cybersecurity incidents.

THEORETICAL FRAMEWORK AND HYPOTHESES

Disclosure Theory

The foundations of disclosure theory were laid by various accounting and finance scholars throughout the 20th century, exploring the implications of financial reporting, information asymmetry, and market efficiency. Dye (2001) defines disclosure theory as the strategic decision-making process firms use regarding the release of information to the public, considering the trade-offs between what information to disclose and what to withhold. However, research findings on factors influencing disclosure behavior vary. While many studies find a positive relationship between firm size and disclosure (Buzby, 1975; Firth, 1979; McNally et al., 1982; Cooke, 1989; Wallace et al., 1994), others show no significant evidence (Malone et al., 1993). Similar discrepancies are observed in studies on forward-looking information (Aljifri & Hussainey, 2007) and other factors like profitability, leverage, auditor type, and industry, with mixed results and no consensus on their impact on disclosure (McNally et al., 1982; Raffournier, 1995; Prencipe, 2004; Wallace et al., 1994; Chow & Wong-Boren, 1987).

Corporate executives by exercising discretion, identifies an optimal level of information to release and safeguard. Drawing on that, given the undisclosed information leads to market asymmetry, the strategic disclosure of information can be used to manage market perceptions and investor relations. The information is a signal, and the manager decides to release or withhold this signal on the basis of the information's signal on the asset's market price. Therefore, the executives by exercising discretion (Verrecchia, 1983), identifies an optimal level of information to disclose and withhold the information, which shapes the threshold level of information. Costs associated with the disclosure of the information, coined as the proprietary costs (Verrecchia, 1983), create a strategic complexity in disclosure decisions. Higher proprietary costs raise the threshold level for disclosure because they extend the range of possible favorable interpretations of withheld information, allowing managers greater discretion in their disclosure decisions.

This means that if proprietary costs are high, managers may withhold information that could be perceived as either negative or not sufficiently positive to outweigh the costs of disclosure. This strategic withholding introduces noise into the market, as traders cannot conclusively interpret the absence of information as negative. Furthermore, Verrecchia (1983) proposes that the greater the proprietary costs, the less negatively traders react to non-disclosure. This is because higher proprietary costs expand the ambiguity surrounding withheld information, making it less likely to be interpreted negatively. Verrecchia (1983)'s model (p.192) proves two things, the proprietary cost is a continuous, decreasing function of time, and increasing function of the competition. First, the proprietary costs escalate with increased competition, positing that firms operating in highly competitive markets perceive public disclosure as potentially beneficial to competitors, thereby incurring greater proprietary costs. Conversely, in less competitive environments, firms face lower proprietary costs, facilitating more openness in disclosures. Second, new, current information carries higher proprietary costs due to its potential immediate impact on competitive advantage and market perception. However, as information ages and becomes outdated, its proprietary cost diminishes, reducing the barriers to its disclosure. This temporal decrease in proprietary costs influences the threshold level of disclosure—a critical point at which the cost of withholding information outweighs the benefits, compelling firms to disclose. An intriguing aspect of the model is the relationship between the magnitude of proprietary costs and market reactions to nondisclosure. Verrecchia (1983) finds that higher proprietary costs lead to less negative reactions from traders to withheld information. This is because when proprietary costs are high, traders expect that nondisclosure might be justified by the need to protect sensitive information rather than merely concealing poor performance or adverse conditions.

Leary and Roberts (2014) highlight that firms' financial policies and disclosure practices are significantly influenced by peer behaviors. Firms emulate the successful disclosure practices of their competitors to maintain legitimacy and reassure stakeholders. This peer influence is particularly strong following significant events, such as financial restatements or data breaches, where firms aim to mitigate investor concerns and manage market reactions through strategic disclosures (Floyd, 2016). Further, Disclosure theory (Dye, 1990) also examines the interplay between mandatory and voluntary disclosures. Mandatory

disclosures can sometimes coincide with voluntary ones when the proprietary costs of disclosing are balanced by the benefits in reducing information asymmetry. Firms disclose voluntarily when the perceived benefits (like investor confidence) outweigh the costs of giving away strategic information (Verrecchia, 1983; Dye, 1990). Mandatory disclosures provide a baseline level of transparency required by regulatory bodies, which can stimulate voluntary disclosures as firms seek to differentiate themselves and provide additional information to reduce information asymmetry further and enhance market perceptions (Healy & Palepu, 2001).

Disclosure theory contends that firms strategically manage the release of information to mitigate information asymmetry and optimize market perceptions. This strategic behavior is guided by the trade-offs between the benefits of transparency, such as increased investor confidence and market stability, and the proprietary costs associated with revealing potentially sensitive information that could be advantageous to competitors (Dye, 2001; Verrecchia, 1983). In highly competitive environments, firms are particularly attuned to the actions of their peers, often emulating successful disclosure practices to maintain legitimacy and reassure stakeholders (Leary & Roberts, 2014). This strategic emulation is crucial following significant events, as firms must carefully balance the need for transparency with the imperative to protect their competitive positioning and proprietary information. Mandatory disclosures provide a baseline level of transparency required by regulatory bodies, which can stimulate voluntary disclosures as firms seek to differentiate themselves and provide additional information to reduce information asymmetry further and enhance market perceptions (Healy & Palepu, 2001). However, if firms have access to private information related to a major event, such as a data breach, they can strategically adjust their disclosures according to proprietary costs. Higher proprietary costs lead firms to withhold information that could be perceived negatively or insufficiently positive, thus introducing noise into the market (Verrecchia, 1983). When firms gain access to both mandatory and voluntary disclosure information through their networks before it is publicly released, they can manage information asymmetry and competitive dynamics more strategically (Dye, 1986; Verrecchia, 1983). This preemptive access allows firms to decide what information to disclose to regain trust and manage perceptions, especially under heightened scrutiny following major events. This

nuanced understanding of disclosure behavior highlights the strategic interplay between timing, competition, and market expectations in corporate disclosures. In the context of data breaches, this implies that firms with preemptive access to private information about the breach can strategically decide what digital strategic initiatives (DSIs) to disclose. They may withhold certain details to protect their competitive advantage while selectively disclosing information to manage investor perceptions and maintain stakeholder trust. Conversely, firms without such access are more likely to increase their transparency regarding DSIs to signal robustness and proactive management, thereby differentiating themselves from peers and mitigating the negative impact on their market value.

Institutional Theory

The institutional theory, as introduced by Meyer and Rowan (1977), proposes that organizations are embedded within broader institutional environments that shape their behavior and practices. The institutional theory emphasizes that organizational decisions are motivated by the desire to attain greater legitimacy from stakeholders within their specific environment (Cavusoglu et al., 2015). Legitimacy is attained by adopting processes, structures, and strategies that align with established practices of other organizations in the same environment. This quest for legitimacy exposes organizations to isomorphic pressures, which result in increasing similarity among peer organizations over time (DiMaggio & Powell, 1983). To achieve this legitimacy, organizations respond to three distinct types of institutional pressures: mimetic, coercive, and normative (Cavusoglu et al., 2015). Mimetic pressure arises when organizations face uncertainty about the outcomes of a specific course of action. In such situations, organizations seek legitimacy by imitating the actions of early movers who have been successful. By following the lead of these organizations, they aim to reduce uncertainty and gain acceptance from stakeholders. Coercive pressure refers to the influence exerted on organizations by external forces and cultural expectations. Organizations face pressures to conform to specific practices, regulations, or standards set by external entities, such as government agencies, industry associations, or influential market players. Failure to comply with these pressures can result in negative consequences, including penalties, reputational damage, or

exclusion from important networks. Normative pressure operates based on the beliefs and perceptions of what is considered appropriate and acceptable within a particular organizational network or community. Organizations tend to adjust their behavior and conform to prevailing norms to maintain positive relationships with network members. This pressure is driven by the desire for acceptance, trust, and social approval within their respective communities. By conforming to institutional pressures, organizations aim to gain legitimacy and improve their position by increasing their similarity to other successful entities in their environment. In the context of a data breach event occurring at partner or peer firms, we propose that firms compare themselves to their counterparts and connected partners in their network. They would seek to incorporate best practices and align with the prevailing industry standards through non-breached firms. This benchmarking process in their strategic disclosure helps organizations ensure that their actions and approaches regarding data security align with what is considered appropriate and acceptable within their industry. By doing so, they not only enhance their legitimacy but also demonstrate their commitment to safeguarding sensitive information and maintaining the trust of their stakeholders.

Digital Strategic Initiatives

Digital strategic initiatives (DSIs) encompass the deliberate actions undertaken by organizations to harness the potential of digital technologies and capabilities in pursuit of their strategic goals. These initiatives necessitate the effective and efficient allocation of organizational resources to actualize their DSIs and initiate a profound journey towards digital transformation (Bharadwaj et al., 2013; Al-Ali et al., 2020; Jackson, 2015; Freitas Junior et al., 2016). Digital strategic initiatives are defined as specific actions undertaken by organizations to gain a competitive advantage through the utilization of digital resources in order to generate and capture economic value (Piccoli & Rodriguez, 2020; Piccoli et al., 2022, p.290). The success of organizations' digital strategic initiatives (DSI) is contingent upon their ability to recognize and adapt to the changing industry dynamics and competitive landscape. For example, a company might implement a DSI by adopting advanced analytics to improve decision-making processes, enhancing customer experiences through personalized digital interfaces, or optimizing supply chain operations using

Internet of Things (IoT) technologies. Such initiatives can significantly impact an organization's efficiency, customer satisfaction, and overall market competitiveness. The implementation and effectiveness of DSIs are profoundly influenced by the environmental context in which they are introduced. For instance, regulatory environments, technological infrastructure, and market conditions can either facilitate or hinder the success of these initiatives (Sambamurthy et al., 2003). A supportive regulatory framework and advanced technological infrastructure can enable smoother implementation and higher efficacy of DSIs. For instance, Deloitte (2023) highlights how a leading technology company helped a global industrial supplier deploy an integrated set of managed security services that use AI to provide 100% visibility and the ability to process millions of events per day. This deployment resulted in improved detection and prevention of cyberattacks, reduced response and remediation times, enhanced visibility and control over IT infrastructure, optimized security operations, and reduced costs, ultimately increasing the efficiency and productivity of security analysts (Deloitte, 2023). Effective DSIs enable firms to respond quickly and effectively to breaches, minimizing damage and maintaining stakeholder trust. Furthermore, the strategic disclosure of DSIs is essential in managing perceptions and reassuring stakeholders about a firm's commitment to cybersecurity and innovation. Drawing on the institutional theory (Cavusoglu et al., 2015), we expect that firms analyze the digital strategic initiatives of their competitors in their industry and incorporate best practices to align their own initiatives with the competitor firms. Furthermore, drawing on disclosure theory, we propose that disclosing digital strategic initiatives is a strategic decision used to manage market perceptions and investor relations, enhancing transparency and demonstrating commitment to innovation and regulatory compliance.

Proximity to Data Breaches and Access to Private Information

Malicious attacks targeting vulnerabilities persist and often become more aggressive after a successful attempt. For instance, Blackbaud, a cloud computing provider for non-profit organizations, fell victim to a sophisticated double extortion ransomware attack (RiskRecon, 2020). This attack encrypted the systems running its clients' environments and exfiltrated sensitive records from 550 organizations, severely

impacting Inova Health Systems by compromising 1 million patient records (RiskRecon, 2021). In 2023, the SEC charged Blackbaud $3 million to settle charges related to this ransomware attack. In response, organizations, including Inova Health Systems, actively detect and correct errors, question and modify existing norms, procedures, policies, and objectives (Dodgson, 1993; Chiva et al., 2010). The actions and responses of each party involved in the breach impact the evolution of others, particularly when operating at the edge of chaos due to a massive data breach.

This interconnectedness and interdependence within the broader cybersecurity ecosystem, influenced by mimetic pressures (Cavusoglu et al., 2015; Visser, 2017), lead to indirect impacts on organizations like Inova Health Systems, potentially driving them to reconfigure their digital strategic initiatives. The interactions between organizations underscore the critical role of transparency in maintaining agility and resilience within supply networks. Such as, value network transparency encompasses the sharing of transactional, strategic, and operational information, enabling network members to make informed decisions (Goswami et al., 2011; Rai and Bush 2007). This transparency is vital for synchronizing production and delivery schedules and mitigating the impact of breaches on the supply chain (Goswami et al., 2011). Proximity to a breached organization impacts both the digital strategic initiatives and the disclosure of these initiatives by other organizations, signifying a commitment to proactive cybersecurity measures such as investing in new technologies and implementing stronger security controls. Organizations strategically disclose these initiatives to manage market perceptions and investor relations, aligning their strategies with non-breached organizations due to mimetic pressures.

Firms with greater access to private information are likely to reduce the amount of digital strategic initiatives disclosed with respect to non-breached organizations to avoid proprietary costs of disclosure, signaling shareholders about their cybersecurity governance. Digital strategic initiatives reflect an organization's efforts to leverage advanced technologies and enhance its strategic position in the face of evolving cyber threats. Based on these assumptions, firms with direct ties to breached entities through supplier or customer relationships are more likely to have access to private information about breach incidents, which can influence their strategic disclosure behaviors to align closely with non-breached

competitors. Conversely, companies in the same industry face competitive pressures and limited information about competitors' breaches, enhancing the mimetic pressure to exceed the initiatives of non-breached organizations. Therefore, competitive firms with limited access to private information are likely to increase the amount of digital strategic initiatives disclosed with respect to non-breached organizations to avoid proprietary costs of withholding, signaling shareholders about their cybersecurity governance. This competitive dynamic could stem from a desire to differentiate themselves by demonstrating a stronger commitment to cybersecurity or leveraging perceived weaknesses in competitors' security postures to gain a competitive advantage. Additionally, the lack of information about competitors' breaches may lead organizations to adopt a more cautious approach, potentially overcompensating with additional cybersecurity measures to protect against unknown threats.

Suppliers to breached customers face significant upstream pressure. If a customer experiences a data breach, the supplier must adapt quickly to potential changes in demand and operational disruptions. The breach might hinder the customer's ability to receive and process supplies, necessitating adjustments from the supplier. Additionally, suppliers might need to disclose more information about their operational status and contingency plans to reassure their customers and maintain trust. Effective governance and information sharing are critical in such scenarios to synchronize production and delivery schedules and mitigate the impact of the breach on the supply chain (Goswami et al., 2011). Conversely, customers of breached suppliers experience downstream pressure. A breached supplier might face challenges in fulfilling orders, disrupting the customer's supply chain and production processes. In such cases, customers need timely and accurate information from their suppliers to adjust their operations and manage potential disruptions. The concept of absorptive capacity highlights the importance of a firm's ability to recognize, assimilate, and apply valuable external knowledge (Lane and Lubatkin, 1998). In the context of a breach, customers with higher absorptive capacity can better leverage shared information from suppliers to adapt their strategies and maintain operational continuity.

Overall, the nuanced dynamics of these relationships highlight the importance of strategic disclosure management. Organizations must balance transparency with the protection of proprietary information,

leveraging DSIs as both a strategic tool and a communication mechanism in response to cybersecurity incidents within their industry. In essence, proximity to breaches and resultant access to private information shape the strategic disclosure behaviors of firms. Those with direct ties to breached entities manage their information disclosure cautiously particularly such disclosures might also inform existing vulnerabilities, whereas industry competitors adopt more aggressive cybersecurity enhancements to navigate the complex landscape of digital strategic initiatives. This interplay of competitive pressures and strategic information management underscores the critical role of transparency and proactive cybersecurity practices in maintaining organizational resilience and stakeholder trust.

Therefore, we hypothesize that:

H1: A data breach at a competitor will lead to an increase in the Digital Strategic Initiative Disparity (DSID) with respect to non-breached competitors.

H2: A data breach at one of the suppliers will lead to a decrease in the Digital Strategic Initiative Disparity (DSID) with respect to non-breached competitors.

H3: A data breach at one of the customers will lead to a decrease in the Digital Strategic Initiative Disparity (DSID) with respect to non-breached competitors.

Historical Breach Experience

In addition to the external pressures discussed within the context of institutional theory, firms also face internal pressures that significantly shape their decision-making processes and reconfiguration of their digital strategic initiatives. These internal pressures arise from within the firm itself. In our study, we operationalize this internal pressure by examining the occurrence of recent data breaches within the firm, as well as subsequent breaches at partner organizations as external pressures. Historical breach experience refers to past instances where a firm has faced data breaches. Such experiences prompt firms to prioritize internal pressures, which involve internally driven actions and initiatives aimed at enhancing security and resilience (Kwon et al., 2013). These internal pressures compel firms to reflect on their own breach events, identify underlying causes, and areas for improvement. It reinforces the significance of benchmarking

against industry standards and assimilating the insights gained from both internal and external breach incidents. Therefore, we propose that when firms are confronted with both external pressures caused by breaches in their supplier, customer, or competitor firms and internal pressures stemming from their own breach events, firms effectively leverage insights from various sources and adapt their digital strategic initiatives accordingly (Visser, 2012). Firms with a history of breaches are expected to be more reactive to the associated risks at their competitors and their network, aligning their strategic initiatives more closely with non-breached firms to mitigate these risks. Moreover, these firms are likely to have implemented stringent cybersecurity measures, which might reduce the extent of strategic deviation in response to a competitor's breach.

Based on these insights, we propose the following hypotheses:

H1a. A data breach at a competitor will lead to an increase in the Digital Strategic Initiative Disparity (DSID) with respect to non-breached competitors, positively moderated by the firm's breach history.

H2a. A data breach at one of the suppliers will lead to a decrease in the Digital Strategic Initiative Disparity (DSID) with respect to non-breached competitors, positively moderated by the firm's breach history.

H3a. A data breach at one of the customers will lead to a decrease in the Digital Strategic Initiative Disparity (DSID) with respect to non-breached competitors, positively moderated by the firm's breach history.

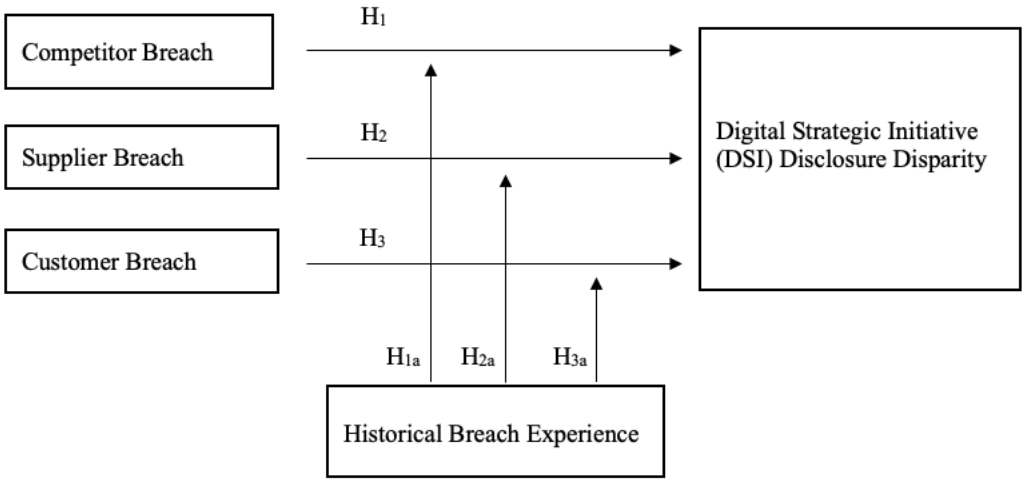


Figure 1. Research Model

RESEARCH METHODOLOGY

Data

In our study, our analysis is conducted at the firm-year level, focusing on S&P 500 firms from 2014. to 2019. We retrospectively utilized the 2019 S&P 500 firm list to collect earnings calls for these companies, deliberately selecting this list to avoid the significant shift in disclosures related to the COVID-19 pandemic. The pandemic led to a major focus on COVID-19-related issues, which could potentially skew the disclosure data According to data from the Privacy Rights Clearinghouse (PRC), the total number of breached S&P 500 companies between 2014 and 2019 was 95. The PRC data is a reputable source and has been widely used in several cybersecurity research studies to provide comprehensive insights into data breach incidents and their impacts (Say & Vasudeva, 2020; Kim & Kwon, 2019; Haislip et al., 2021). These companies were removed from our dataset, as our focus is on examining the roles of competitors, customers, and suppliers of breached companies. Our initial dataset comprised 3,284 data points, resulting from missing earnings call transcripts and breached company removal. After accounting for missing variables, such as R&D expenditures, the dataset was further reduced to 2,838 observations. Consequently, we have a panel data set with 307 firm-year level, totaling 2,838 observations. To measure the digital strategy initiatives of these firms, we used companies' quarterly earnings call disclosures, which are publicly

available on SeekingAlpha. Additionally, we examined the proximity to breached firms by analyzing supply chain relations from FactSet data. All other control variables were sourced from the Compustat database.

Measurement

Independent Variable: Proximity to Data Breaches

Competitor Breach (Independent Variable 1): Binary variable. To capture the impact of being a competitor, we used industry peers as a proxy for competitor breaches. Specifically, we defined industry peers of breached organizations, as organizations within the same 3-digit Standard Industrial Classification (SIC) code of breached companies. By utilizing the 3-digit SIC code classification, we ensure a more accurate representation of industry peers. This process resulted in identifying 690 company-year instances of S&P 500 companies being competitors of a breached company. However, our analysis was also supported by an analysis using the 2-digit SIC code classification as a part of our robustness checks. This additional analysis provides a broader industry grouping, which serves as a robustness check for our primary analysis and helps to validate the consistency of our findings across different levels of industry granularity.

Supplier Breaches (Independent Variable 2): Binary variable. To identify organizations that were customers of a breached supplier, we utilized FactSet data. We first merged FactSet data with Compustat data through CUSIPs to obtain public companies at both the supplier and customer levels. This selection was necessary to control for industry information of customers, which would not be possible for private firms. We then selected any deals that were active between 2014 and 2019. By merging supplier information with PRC data, we identified breached suppliers by checking if the deal was active during the breach period. This process resulted in identifying 169 firm-year instances of S&P 500 firms being customers of a breached supplier. By identifying S&P 500 firms that were customers of a breached supplier, we aimed to capture the potential ripple effects and the broader impact of breaches on interconnected organizations within the supply chain.

Customer Breaches (Independent Variable 3): Binary variable. To identify firms that were suppliers to a breached customer, we utilized FactSet data. Initially, we merged FactSet data with Compustat data through

CUSIPs to identify public companies at both the supplier and customer levels. This step was essential to ensure we could control for industry information of suppliers, which is often unavailable for private firms. We then selected deals that were active between 2014 and 2019. By integrating customer information with PRC data, we identified breached firms by verifying if the deal was active during the breach period. This process resulted with 275 firm-year instances of S&P firms being suppliers of a breached customer. By selecting only S&P 500 firms that were suppliers to a breached customer, we aimed to capture the potential ripple effects and the broader impact of breaches on interconnected organizations within the supply chain.

Dependent Variable: Digital Strategic Initiative (DSI) Disclosure Disparity

To measure the digital strategic initiatives within the industry, we exclude all breached S&P 500 firms from our sample and calculate the average digital strategic initiatives for each firm by only considering its non-breached peers within the same 3-digit SIC code. We assess the aspect and maturity of the digital strategies of S&P 500 companies using transformer-based language models with domain-specific knowledge, leveraging earnings call disclosures. Various studies have attempted to measure digital strategy and maturity (Thordsen et al., 2020; Gurbaxani and Dunkle, 2019; Kane et al., 2017). Our approach builds on the state-of-the-art (SOTA) transformer-based model DigiCall (Pataci et al., 2022), expanding it to cover the period from 2014 to 2019. This extends the work of Al-Ali et al. (2020) by providing a more comprehensive measurement of digital strategic initiative disclosures over a broader timeframe. We first use the DigiCall method and data to obtain the aspect and maturity of digital strategic initiatives at the company level for each quarter and then calculate an average digital strategic initiative at the industry level for each industry and quarter by aggregating the firm-level data.

Prediction of the aspects of the digital strategic initiatives: For aspect prediction, previous research created a dictionary of 350 terms organized into 17 topics and 3 groups in digital transformation (Pataci et al., 2022; Al-Ali et al., 2020). In our work, we used this dictionary in a bag-of-words fashion to identify sentences containing aspects of digital strategic initiatives; the complete list of this dictionary is available in Appendix A.2.

Prediction of the maturity of the digital strategic initiatives: In the case of maturity prediction, we utilized annotated data and fine-tuned language models, as outlined in the work of Pataci et al. (2022). They trained several transformer-based models, both domain-agnostic and domain-specific, by fine-tuning them with data annotated by linguists. Among the domain-agnostic models, they employed BERT (Devlin et al., 2018), RoBERTa (Liu et al., 2019), which are pre-trained on general corpora and designed for various language understanding tasks. Additionally, they considered FinBERT (Araci, 2019), a BERT-based model pre-trained on financial documents, to address the specific nature of their task. The researchers found that the domain-agnostic models, particularly BERT base-uncased, outperformed the domain-specific models, exhibiting the highest F-1 weighted level for their task, See Appendix A.3. This suggests that the general-purpose language models trained on diverse data sources provided superior performance in predicting the maturity of digital strategic initiatives in corporate disclosures. We use the pre-trained and fine-tuned BERT base-uncased model to predict the maturity of the digital strategic initiatives with the expanded dataset to calculate (X_{it}). In the next stage, by using 3-digit SIC codes, we calculated average strategic initiatives in the industry ($\overline{ISI}_{pt}$) by excluding the focal firm *i* for each label *L*. This industry-level analysis measure ($\overline{ISI}_{pt}$) allows us to assess how firm *i* is distant to their industry peers in terms of digital strategic initiatives for each label.

$$(\mathrm{DSI}_{\mathrm{it,\ L1}}) = (\mathrm{X}_{\mathrm{it,\ L1}}) - (\overline{ISI}_{\mathrm{pt,\ L1}})$$

Once we obtained $\mathrm{DSI}_{\mathrm{it,\ L1,\ \ldots}}\ \mathrm{DSI}_{\mathrm{it,\ L17}}$ for each of the 17 categories, we then calculated the Euclidean distance with the below formula at the company level for each label. Hence, we operationalize digital strategic initiative distance through:

$$(\mathrm{DSI}_{i,t}) = \sqrt{\frac{[(X_{i,t,\mathrm{L1}}) - (\overline{DSI}_{p,t,\mathrm{L1}})]^2 + \cdots + [(X_{i,t,\mathrm{L17}}) - (\overline{DSI}_{p,t,\mathrm{L17}})]^2}{17}}$$

Further, we also operationalize the Digital Strategic Initiative (DSI) as a change in distance from the previous quarters to avoid bias, denoted as $\overline{(DSI)}$. This helps to mitigate any seasonal or temporal biases that might affect DSI measurements in any single quarter. To calculate this change, we first take the average of the DSI values from the two previous quarters:

$$(\overline{DSI}_{i,t-1}) = ((\text{DSI}_{i,t-1}) + (\text{DSI}_{i,t-2})) / 2$$

Then, we calculate the difference between the average ($\overline{DSI}_{i,t-1}$) and the post-breach ($\text{DSI}_{i,t}$) digital strategic initiatives. So, the DSI disparity (ΔDSI_{it}) would be:

$$(\Delta\text{DSI}_{it}) = (\overline{DSI}_{i,t-1}) - (\text{DSI}_{i,t})$$

This approach ensures that the measurement of the change in DSI accounts for potential fluctuations and biases by averaging prior values, thus providing a more stable and accurate reflection of strategic shifts post-breach.

Control Variables

Research and Development (R&D) intensity is crucial because it reflects a firm's commitment to advancing its technological capabilities, which can significantly impact its digital strategic initiatives. Profitability included as a control because financially robust companies are more likely to invest in and successfully implement digital strategic initiatives. Log of assets included as a control because financially robust companies are more likely to invest in and successfully implement digital strategic initiatives. Industry classification, based on the 3-digit SIC code, accounts for industry-specific factors that might influence digital strategic initiatives. Different industries have varying levels of digital adoption and regulatory requirements, which can affect how companies approach their digital strategies. Quarter-year controls for temporal effects, capturing any time-specific factors that might influence digital strategic initiatives. By accounting for quarter-year, we control for seasonal variations and broader economic trends that could impact digital strategy disclosures. Summary of our variables and the sources are also available in the Appendix A.1., while summary statistics and pairwise correlations are presented here.

Variables	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
(1) DSI Disclosure Disparity	1.000							
(2) Competitor Breach	0.028 (0.113)	1.000						
(3) Supplier Breach	-0.040* (0.023)	0.084* (0.000)	1.000					
(4) Customer Breach	-0.049* (0.006)	0.132* (0.000)	0.055* (0.002)	1.000				
(5) Log of Assets	0.004 (0.843)	0.004 0.831)	0.057* (0.001)	0.044* (0.012)	1.000			
(6) R&D Intensity	-0.009 (0.619)	-0.025 (0.169)	0.049* (0.008)	-0.033 (0.078)	0.000 (0.987)	1.000		
(7) Profitability (ROA)	0.010 (0.589)	0.043* (0.014)	0.035* (0.047)	0.001 (0.942)	-0.263* (0.000)	-0.088* (0.000)	1.000	
(8)Historical Breach Experience	0.001 (0.935)	0.051* (0.003)	0.081* (0.000)	0.023 (0.196)	0.124* (0.000)	0.060* (0.001)	0.097* (0.000)	1.000
*** p<0.01, ** p<0.05, * p<0.1								

Table 1. Pairwise correlations

Variable	Obs	Mean	Std. Dev.	Min	Max
DSI Disclosure Disparity	3187	-.033	1.938	-18.098	12.899
Competitor Breach	3284	.141	.348	0	1
Supplier Breach	3284	.028	.166	0	1
Customer Breach	3284	.055	.229	0	1
Log of Assets	3272	0	1	-3.128	3.287
R&D Intensity	2937	0	1	-.488	7.676
Profitability (ROA)	3272	0	1	-15.571	9.071
Historical Breach Experience	3285	.084	.278	0	1

Table 2. Summary Statistics

Estimation

The main hypotheses in our study examine the relationship between DSI Disparity (Digital Strategic Initiative Disparity) and breaches experienced by competitors, suppliers, and customers. Specifically, the Model 1 used for the main hypotheses is:

$$Model\ 1:\ DSI\ Disclosure\ Disparity_{it} = \beta 0 + \beta 1\ Breach_{it} + ui + \gamma t + \epsilon it$$

In Model 1, ui represents the random effects at the organizational level, capturing unobserved heterogeneity that varies across organizations but is constant over time. The term γt represents time-fixed effects,

accounting for time-specific factors that might affect DSI Disparity. The error term ϵit captures idiosyncratic shocks. The moderating hypotheses explore the interaction between breaches and historical breach experience. Model 2 used for the moderating hypotheses is:

Model 2: DSI Disc. Disparity $_{it}$ = $\beta 0+\beta 1($ *Breach* $_{it}$ *X Historical Breach Experience* $_{it}$ $) + ui + \gamma t + \epsilon it$

Historical Breach Experience$_{it}$ allows us to assess whether the effect of a breach on DSI Disparity is moderated by the organization's historical experience with breaches. This interaction term helps to understand if organizations with more breach experience react differently to breaches if it is a competitor, supplier, or customer of a breached company.

We employed random effects in our analysis. By employing a random effects model, we effectively account for both time-varying and time-invariant unobserved heterogeneity. The selection of the random effects model is substantiated by the Hausman test results for each hypothesis. For Hypothesis 1 (DSI Disparity and Competitor Breach), the Hausman test yielded a $\chi^2(21) = 4.58$ with a p-value of 0.9999, indicating no significant difference and supporting the random effects model. Similarly, Hypothesis 2 (DSI Disparity and Supplier Breach) presented a $\chi^2(21) = 6.11$ with a p-value of 0.9993, and Hypothesis 3 (DSI Disparity and Customer Breach) showed a $\chi^2(21) = 8.98$ with a p-value of 0.9894, both favoring the random effects model. For the moderating hypotheses, the results were consistent: Hypothesis 1a (Competitor Breach and Historical Breach Experience) had a $\chi^2(22) = 4.40$ with a p-value of 1.0000, Hypothesis 2a (Supplier Breach and Historical Breach Experience) showed a $\chi^2(22) = 5.61$ with a p-value of 0.9998, and Hypothesis 3a (Customer Breach and Historical Breach Experience) had a $\chi^2(22) = 9.27$ with a p-value of 0.9918. These high p-values across all hypotheses confirm that the random effects model is the most appropriate choice for our analysis. Furthermore, we included fixed effects models as part of our robustness checks in supplemental tests, enhancing the robustness and validity of our findings by controlling for unobserved, time-invariant factors at the firm level. To account for endogeneity issues, we employed dynamic panel data models. These models allow us to control for potential endogeneity by incorporating lagged dependent variables as regressors, thereby addressing the potential reverse causality and omitted variable bias. For robustness, the same analysis was conducted at the SIC 2-digit industry level using both

random and fixed effects models. This approach further controls for unobserved, time-invariant factors at the organizational level, enhancing the robustness and validity of our findings.

RESULTS

In examining the impact of data breaches on digital strategic initiative disclosures, our study uncovers several significant findings (Table 3). Competitors of breached entities diverge more in their digital strategies, potentially exploiting the breach to differentiate themselves by overreacting (H1: 0.243, *p<0.1). Furthermore, firms directly linked to a breached entity, such as customers or suppliers, are likely to adjust their digital strategic initiatives significantly. For example, customers of breached suppliers show a notable decrease in digital strategic initiative disparity (H2: -0.641, *p<0.05), indicating a conservative shift post-breach. Similarly, suppliers of breached customers exhibit a significant reduction in their digital strategic initiative disparity (H3: -0.597, *p<0.05).

The analysis of moderating effects reveals interesting dynamics. Historical breach experience appears to have a significant moderating effect for customers of breached supplier firms (H2a: 1.102, *p<0.05). This suggests that firms with historical breach experience are better able to adapt their digital strategies, drawing on past experiences and unique information obtained through their supplier relationships. However, the moderation effect of historical breach experience on the behavior of competitors and suppliers of breached entities was found to be insignificant (H1a: 0.588, p>0.1; H3a: 0.528, p>0.1). This suggests that historical breach experience does not significantly influence how competitors and suppliers adjust their digital strategic initiative disclosures in response to breaches.

Dependent variable: DSI Disclosure Disparity	M1	M2	M3	M4	M5	M6
	H1	H2	H3	H1a	H2a	H3a
Main Hypotheses						
Competitor Breach	**0.243+** (1.94)			0.184 (1.50)		
Supplier Breach		**-0.641*** (-1.97)			-0.895* (-2.26)	
Customer Breach			**-0.597*** (-2.25)			-0.655* (-2.23)
Moderation						
Competitor Breach * Historical Breach Experience				0.588 (1.21)		
Supplier Breach * Historical Breach Experience					**1.102*** (2.04)	
Customer Breach * Historical Breach Experience						0.528 (1.30)
Historical Breach Experience				-0.119 (-1.36)	-0.0715 (-0.66)	-0.0374 (-0.34)
Control Variables						
Log of Assets	0.0198 (0.82)	0.0288 (1.12)	0.0290 (1.11)	0.0233 (0.88)	0.0301 (1.09)	0.0287 (1.02)
R&D Intensity	-0.0091 (-0.42)	0.0002 (0.01)	-0.013 (-0.63)	-0.0068 (-0.32)	-0.0031 (-0.14)	-0.0131 (-0.60)
Profitability (ROA)	0.0157 (0.44)	0.0230 (0.66)	0.0180 (0.52)	0.0170 (0.48)	0.0255 (0.72)	0.0184 (0.53)
Industry Control	Y	Y	Y	Y	Y	Y
Quarter, Year Control	Y	Y	Y	Y	Y	Y
N	2838	2838	2838	2838	2838	2838
χ^2	795.8	779.0	778.4	836.0	798.1	783.8
**** p<0.01, ** p<0.05, * p<0.1,* t statistics in parentheses						

Table 3. Random Effects Results at SIC-3 Level

The fixed effects regression results, presented in Table 4, reinforce our earlier findings. Competitors of breached entities continue to exhibit a significant increase in digital strategic initiative disparity (H1: 0.248, *p<0.1), highlighting their tendency to overreact to breaches by differentiating their strategies. Additionally, both customers and suppliers of breached firms maintain a significant reduction in digital strategic initiative disparity (H2: -0.790, *p<0.1; H3: -0.821, *p<0.1 and -1.023, *p<0.05; -0.897, *p<0.05,

respectively), indicating a conservative strategic shift in response to breaches. The moderating effects of historical breach experience remain consistent, further substantiating the robustness of our results across different model specifications.

Dependent variable: DSI Disclosure Disparity	M7	M8	M9	M10	M11	M12
	H1	H2	H3	H1a	H2a	H3a
Main Hypotheses						
Competitor Breach	**0.248+ (1.76)**			0.140 (0.98)		
Supplier Breach		**-0.790* (-2.12)**			-1.023* (-2.30)	
Customer Breach			**-0.821* (-2.49)**			-0.897* (-2.47)
Moderation						
Competitor Breach * Historical Breach Experience				0.447 (0.87)		
Supplier Breach * Historical Breach Experience					**1.042+ (1.70)**	
Customer Breach * Historical Breach Experience						0.664 (1.34)
Control Variables						
Log of Assets	0.27 (1.18)	0.295 (1.24)	0.292 (1.21)	0.257 (1.06)	0.263 (1.12)	0.291 (1.20)
R&D Intensity	0.22 (1.09)	0.250 (1.24)	0.239 (1.20)	0.219 (1.08)	0.253 (1.27)	0.239 (1.20)
Profitability (ROA)	0.0019 (0.04)	0.0123 (0.27)	0.0018 (0.04)	0.0038 (0.08)	0.0150 (0.32)	0.0011 (0.02)
Industry Control	Y	Y	Y	Y	Y	Y
Quarter, Year Control	Y	Y	Y	Y	Y	Y
N	2838	2838	2838	2838	2838	2838
*** p<0.01, ** p<0.05, * p<0.1, t statistics in parentheses						

Table 4. Fixed Effects Results at SIC-3 Level

Supplemental Tests

To ensure the robustness of our findings, we conducted additional analyses at the SIC-2 level, employing both random and fixed effects models. This approach helps to validate our results across

different industry classifications and provides a more comprehensive understanding of the impact of data breaches on digital strategic initiative disclosures.

The random effects models at the SIC-2 level confirm our main findings (Table 5). Competitor breaches continue to be positively associated with digital strategic initiative disparity (H1: 0.247, *p<0.1), indicating that competitors of breached entities diverge more in their digital strategies. The impact of supplier breaches remains significant and negative (H2: -0.572, +p<0.1), as well as for customers (H3: -0.538, *p<0.1), indicating a negative disparity in their digital strategic initiative disclosures. The moderating effect of historical breach experience remains significant for customers of breached suppliers (H2a: 1.303, **p<0.01), but remains less pronounced for competitors (H1a: 0.602, +p<0.1) and is insignificant for customers (H3a: 0.502, p>0.1).

The fixed effects models at the SIC-2 level also reinforce our main findings (Table 6). The impact of competitor breaches on digital strategic initiative disclosure disparity is still positive and significant (H1: 0.280, *p<0.05). The effects of supplier breaches (H2: -0.737, +p<0.1) and customer breaches (H3: -0.778, *p<0.05) remain significant and negative. The moderating effect of historical breach experience is significant for customers of breached suppliers (H2a: 1.356, *p<0.05), but not for competitors (H1a: 0.573, p>0.1) or suppliers of breached customers (H3a: 0.608, p>0.1).

These robustness checks, conducted at the SIC-2 level with both random and fixed effects models, confirm the validity of our main findings and highlight the consistent patterns observed across different industry classifications. The consistency of results across these different models and industry levels provides strong evidence supporting our conclusions about the impact of data breaches on digital strategic initiative disclosures at competitor, supplier, and customer level.

Dependent variable: DSI Disclosure Disparity	M13	M14	M15	M16	M17	M18
	H1	H2	H3	H1a	H2a	H3a
Main Hypotheses						
Competitor Breach	**0.247* (2.06)**			0.195+ (1.65)		
Supplier Breach		**-0.572+ (-1.80)**			-0.824* (-2.20)	
Customer Breach			**-0.538* (-2.19)**			-0.596* (-2.19)
Moderation						
Competitor Breach * Historical Breach Experience				**0.602+ (1.69)**		
Supplier Breach * Historical Breach Experience					**1.303** (2.64)**	
Customer Breach * Historical Breach Experience						0.502 (1.30)
Historical Breach Experience				-0.153+ (-1.74)	-0.063 (-0.67)	-0.012 (-0.14)
Control Variables						
Log of Assets	0.0175 (0.73)	0.0291 (1.19)	0.0305 (1.21)	0.0170 (0.67)	0.0304 (1.18)	0.0286 (1.09)
R&D Intensity	-0.0138 (-0.80)	-0.0045 (-0.26)	-0.0169 (-0.96)	-0.0102 (-0.58)	-0.009 (-0.52)	-0.016 (-0.95)
Profitability (ROA)	0.00612 (0.21)	0.0156 (0.53)	0.0116 (0.39)	0.00665 (0.22)	0.0178 (0.59)	0.0115 (0.39)
Industry Control	Y	Y	Y	Y	Y	Y
Quarter, Year Control	Y	Y	Y	Y	Y	Y
N	2868	2868	2868	2868	2868	2868
χ^2	1006.7	996.5	981.4	1018.8	1004.8	1002.7
*** *p<0.01, ** p<0.05, * p<0.1,* t statistics in parentheses						

Table 5. Random Effects Results at SIC-2 Level

Dependent variable: DSI Disclosure Disparity	M19	M20	M21	M22	M23	M24
	H1	H2	H3	H1a	H2a	H3a
Main Hypotheses						
Competitor Breach	**0.280* (2.03)**			0.230+ (1.68)		
Supplier Breach		**-0.737+ (-1.96)**			-0.987* (-2.29)	
Customer Breach			**-0.778* (-2.51)**			-0.849* (-2.48)
Moderation						
Competitor Breach * Historical Breach Experience				0.573 (1.53)		
Supplier Breach * Historical Breach Experience					**1.356* (2.47)**	
Customer Breach * Historical Breach Experience						0.608 (1.34)
Control Variables						
Log of Assets	0.222 (1.05)	0.253 (1.19)	0.253 (1.18)	0.200 (0.93)	0.217 (1.05)	0.252 (1.17)
R&D Intensity	0.244 (1.46)	0.276+ (1.69)	0.266+ (1.67)	0.240 (1.46)	0.278+ (1.72)	0.266+ (1.67)
Profitability (ROA)	-0.0008 (-0.02)	0.0115 (0.29)	0.0016 (0.04)	-0.0003 (-0.01)	0.0141 (0.36)	0.0009 (0.02)
Industry Control	Y	Y	Y	Y	Y	Y
Quarter, Year Control	Y	Y	Y	Y	Y	Y
N	2868	2868	2868	2868	2868	2868
*** p<0.01, ** p<0.05, * p<0.1, t statistics in parentheses						

Table 6. Fixed Effects Results at SIC-2 Level

Endogeneity and Dynamic Panel Data Analysis

To address potential endogeneity concerns and provide more robust estimates, we employed dynamic panel data models. Endogeneity can arise due to omitted variable bias, measurement errors, or reverse causality, which can lead to biased and inconsistent estimates. To mitigate these issues, we used the System Generalized Method of Moments (System GMM) estimator, which is well-suited for handling endogeneity in panel data settings. The System GMM approach helps mitigate these issues by using lagged levels as instruments for differenced equations and lagged differences as instruments for level equations. The results

of this analysis, presented in Table 7 provide further insights into the impact of data breaches on digital strategic initiative (DSI) disparity. Our Dynamic Panel Data Analysis at SIC 3 level provide consistent results with our Random Effects results at SIC 3 level.

The dynamic panel data analysis using the System GMM estimator supports our main hypotheses regarding the impact of competitor, supplier, and customer breaches on DSI disclosure disparity. For the main hypotheses, the coefficient for competitor breaches (H1) is positive and marginally significant, indicating that competitors of breached firms tend to diverge more in their DSI disclosure post-breach, with a coefficient of 0.440 ($p < 0.1$). The effect of supplier breaches on DSI disclosure (H2) is notably significant and negative, with a coefficient of -1.782 ($p < 0.05$), implying that customers of breached suppliers align their DSI disclosures more conservatively post-breach. Similarly, the coefficient for customer breaches (H3) is significantly negative, with a value of -1.389 ($p < 0.1$), indicating that suppliers of breached customers tend to reduce their DSI disclosure disparity, reflecting a more conservative approach following a breach.

Regarding the moderating hypotheses, the interaction term for competitor breach and historical breach experience (H1a) is not significant, with a coefficient of 0.286, suggesting that historical breach experience does not significantly moderate the impact of competitor breaches on DSI disclosure disparity. Conversely, the interaction term for supplier breach and historical breach experience (H2a) is significantly negative, with a coefficient of -0.436 ($p < 0.05$), indicating that historical breach experience exacerbates the conservative shift in digital strategies among customers of breached suppliers. Finally, the interaction term for customer breach and historical breach experience (H3a) is not significant, with a coefficient of 0.549, suggesting that historical breach experience does not significantly moderate the impact of customer breaches on DSI disparity of supplier companies.

Dependent variable: DSI Disclosure Disparity	M25	M26	M27	M28	M29	M30
	H1	H2	H3	H1a	H2a	H3a
Main Hypotheses						
Competitor Breach	**0.440+ (1.85)**					
Supplier Breach		**-1.782* (-2.45)**				
Customer Breach			**-1.389* (-1.98)**			
Moderation						
Competitor Breach * Historical Breach Experience				0.286 (1.00)		
Supplier Breach * Historical Breach Experience					**-0.436* (-2.49)**	
Customer Breach * Historical Breach Experience						0.549 (0.55)
Control Variables						
Log of Assets	1.062 (0.89)	1.148 (0.97)	0.901 (0.79)	1.039 (0.89)	1.100 (0.94)	1.073 (0.93)
R&D Intensity	0.679* (1.96)	0.734* (2.24)	0.748* (2.42)	0.679* (2.02)	0.686* (2.02)	0.687* (2.04)
Profitability (ROA)	0.0579 (0.57)	0.0820 (0.84)	0.0609 (0.60)	0.0656 (0.65)	0.0626 (0.63)	0.0654 (0.65)
Industry Control	Y	Y	Y	Y	Y	Y
Quarter, Year Control	Y	Y	Y	Y	Y	Y
N	1179	1179	1179	1179	1179	1179
$\chi 2$	217.5	198.0	184.9	193.1	185.7	209.9
*** p<0.01, ** p<0.05, * p<0.1, t statistics in parentheses						

Table 7. Dynamic Panel Data Analysis Results at SIC-3 Level

DISCUSSION

Our study offers several insights into how data breaches shape the disclosure behaviors of firms concerning their Digital Strategic Initiatives (DSIs). Utilizing disclosure theory and institutional theory as our theoretical lenses, we investigate how proximity to breaches—through customer, supplier, and competitor relationships—affects these disclosure behaviors. Our findings elucidate the nuanced dynamics at play and contribute to the broader discourse on corporate strategy and cybersecurity management.

Our analysis reveals that competitors of breached entities tend to diverge more in their digital strategies. This divergence is indicative of an overreaction, as firms aim to capitalize on the competitive advantage by enhancing their digital initiatives to differentiate themselves. The significant coefficient for competitor breaches (0.243, *p<0.1) underscores this behavior. This response aligns with the principles of disclosure theory, where firms strategically manage information to gain a competitive edge in the market.

Firms directly linked to a breached supplier, exhibit a notable decrease in DSI disclosure disparity (-0.641, *p<0.05). This conservative shift suggests that these firms, having access to more private information about the breach, choose to disclose less, possibly to avoid revealing vulnerabilities or strategic weaknesses. The supplier breach impact highlights the critical role of information asymmetry in shaping disclosure behaviors, as firms with more information may opt for strategic silence to protect proprietary details.

Similar to suppliers, firms that are suppliers of breached customers also show a significant reduction in DSI disparity (-0.597, *p<0.05). This finding reinforces the notion that closer proximity to the breach, and thus better access to detailed information, leads to more conservative disclosure strategies. These firms likely aim to minimize uncertainty and reassure stakeholders by avoiding over-disclosure of their strategic responses.

Overall, our findings extend the current discourse on mandatory versus voluntary disclosures. While existing research highlights that mandatory disclosures can stimulate voluntary disclosures, our study reveals that access to private information about an incident can lead to reduced voluntary disclosures in the context of data breaches. This nuanced understanding provides a compelling addition to the literature, emphasizing how information asymmetry and strategic considerations shape disclosure behaviors in the aftermath of cybersecurity incidents. The interplay between timing, competitive pressures, and the strategic management of information underscores the complexity of corporate disclosure decisions.

Our investigation into the moderating effects of historical breach experience provides additional layers of understanding. Interestingly, historical breach experience does not significantly moderate the impact for competitors (0.588, p>0.1) or suppliers (0.528, p>0.1) of breached customers. This suggests that while past breach experience is valuable, its influence may be more pronounced in direct supplier-customer

relationships, where information flow and strategic interdependencies are stronger. Historical breach experience significantly moderates the relationship between supplier breaches and DSI disclosure disparity (1.102, *p<0.05), this might be due to the fact that ripple breach events are more likely to cascade upstream. Customer firms with prior breach experience leverage their knowledge and past learnings to adjust their digital strategies more effectively. This adaptive behavior underscores the importance of experiential learning in cybersecurity management. Customer firms with historical breach experience are likely to have developed robust mechanisms for interpreting and responding to breach-related information, allowing them to adjust their DSIs in a manner that both protects their interests and communicates their proactive stance to stakeholders. This capability is less pronounced in competitor relationships, where access to detailed breach information is limited, leading to less effective adaptation and disclosure strategies.

CONCLUSION

Our study provides critical insights into how data breaches influence the strategic disclosure behaviors of firms concerning their Digital Strategic Initiatives (DSIs). Drawing upon disclosure theory and institutional theory, we examine the nuanced effects of proximity to breaches through customer, supplier, and competitor relationships. The findings underscore the significant impact of these relationships on firms' disclosure strategies, revealing the complex interplay between information asymmetry, competitive pressures, and market expectations.

First, our research highlights that competitors of breached entities tend to diverge more in their digital strategies, likely as a response to capitalize on the competitive advantage and differentiate themselves in the market. This behavior aligns with the principles of disclosure theory, where firms manage information strategically to enhance their market position. The significant coefficient for competitor breaches underscores this dynamic, indicating a deliberate overreaction to breaches as a means to signal robustness and innovation to stakeholders. Competitor firms avoid costs associated with the withholding of DSI-related disclosures.

Second, firms directly linked to a breached supplier exhibit a notable decrease in DSI disclosure disparity. This conservative shift suggests that these firms, having access to more private information about the breach, opt for strategic silence to protect proprietary information and avoid proprietary costs associated with the disclosure.

Third, our analysis of historical breach experience as a moderating factor reveals that it significantly influences the relationship between supplier breaches and DSI disclosure disparity. Firms with historical breach experience leverage their past learnings to adjust their digital strategies more effectively, underscoring the importance of experiential learning in cybersecurity management. This adaptive behavior is particularly pronounced in breaches at suppliers, where information flow and strategic interdependencies are stronger, given that these types of breaches are often the source of ripple effects.

Overall, our study extends the current discourse on mandatory versus voluntary disclosures, demonstrating that access to private information about a breach can lead to reduced voluntary disclosures in the context of data breaches. This nuanced understanding provides a compelling addition to the literature, highlighting how strategic considerations and information asymmetry shape disclosure behaviors in the aftermath of cybersecurity incidents.

In conclusion, our research contributes valuable insights into the intersection of cybersecurity, corporate strategy, and stakeholder communication for megafirms. By examining the proximity to breaches and the role of historical breach experience, we offer a deeper understanding of how these large firms navigate the complexities of digital strategic initiative disclosures in response to cyber threats. These findings have important implications for managers and policymakers, emphasizing the need for strategic information management and robust cybersecurity practices to sustain organizational resilience and stakeholder trust in an increasingly digital landscape.

PRACTICAL CONTRIBUTION

Our study offers several practical contributions that are crucial for managers, policymakers, and practitioners involved in corporate strategy, cybersecurity, and digital transformation.

One of the key takeaways from our research is the importance of strategically managing the disclosure of Digital Strategic Initiatives (DSIs) in the wake of data breaches. Managers must recognize the dual role of DSIs as both a strategic tool and a communication mechanism. Firms that are directly linked to breached entities, such as suppliers and customers, should carefully assess the extent of their disclosures to balance transparency with the protection of proprietary information. This strategic management can help firms mitigate potential risks associated with over-disclosure while maintaining stakeholder trust. By carefully calibrating their disclosure strategies, managers can protect their competitive advantage and ensure that stakeholders remain confident in the firm's resilience and strategic direction.

For policymakers, our study underscores the need for regulatory frameworks that support transparency and accountability in cybersecurity practices. Regulatory bodies should consider guidelines that encourage firms to disclose relevant cybersecurity information while providing protections against the risks of over-disclosure. Policies that promote information sharing and collaboration among firms can also enhance the overall security posture of the industry, reducing the likelihood of widespread breaches. Policymakers must strike a balance between fostering an environment of transparency and ensuring that firms are not unduly penalized for sharing critical information that could enhance collective security.

Finally, our study introduces a novel method for measuring digital strategic initiatives using state-of-the-art Natural Language Processing (NLP) models on unstructured data. Practitioners can adopt this approach to gain deeper insights into their digital transformation efforts and benchmark their progress against industry standards. This innovative measurement technique can support more informed decision-making and help firms optimize their digital strategies for better performance and resilience. By leveraging advanced NLP models, firms can more accurately assess their strategic positioning and identify areas for improvement, thereby enhancing their overall digital capabilities and competitive standing.

In summary, our research provides actionable insights for managers aiming to navigate the complexities of DSI disclosures post-breach, policymakers tasked with crafting effective cybersecurity regulations, and practitioners seeking to leverage advanced analytical techniques for strategic assessment. These contributions are pivotal in fostering a more secure, transparent, and strategically aligned business environment in the digital age.

LIMITATIONS AND FUTURE RESEARCH

This study does not deeply explore the role of varying regulatory environments in shaping disclosure behaviors post-breach. Different regulatory landscapes could impose distinct pressures and incentives for disclosure, and this variation is not adequately addressed, potentially limiting the generalizability of the findings across different regions and regulatory frameworks.

Our study opens several avenues for future research that could further deepen the understanding of strategic disclosure behaviors in the context of data breaches. First, future work could delve deeper into the mechanisms underlying the strategic disclosure of DSIs in the context of varying types of breaches. While our study focuses on breaches within customer, supplier, and competitor networks, other relational contexts, such as joint ventures, alliances, and mergers and acquisitions, could be explored to understand how these relationships influence disclosure behavior. Investigating these additional contexts could reveal new insights into the strategic considerations firms weigh when deciding how much information to disclose. Second, investigating the role of regulatory environments in shaping DSI disclosures post-breach could provide valuable insights. Different regulatory landscapes might impose distinct pressures and incentives for disclosure, impacting how firms navigate their strategic communication in the wake of a breach. Comparative studies across regions with varying regulatory frameworks could illuminate these dynamics, helping policymakers design more effective regulations that balance the need for transparency with the protection of proprietary information. Third, the interplay between digital strategic initiatives and other forms of strategic disclosures, such as environmental, social, and governance (ESG) disclosures, could be an intriguing area of research. Understanding how firms balance and integrate multiple dimensions of disclosure in response to breaches could offer a more holistic view of corporate disclosure strategies. This

line of inquiry could uncover whether firms prioritize certain types of disclosures over others and how these priorities shift in response to different types of crises.

By addressing these areas, future research can build on our findings, offering deeper insights into the complex interplay between data breaches, strategic disclosures, and organizational behavior in the digital age. These investigations could not only advance academic knowledge but also provide practical guidance for managers and policymakers striving to enhance corporate transparency and resilience.

REFERENCES

Acemoglu, D., & Restrepo, P. (2018). The race between man and machine: Implications of technology for growth, factor shares, and employment. *American Economic Review*, *108*(6), 1488-1542.

Al-Ali, A. G., Phaal, R., & Sull, D. (2020). Deep learning framework for measuring the digital strategy of companies from earnings calls. *arXiv preprint arXiv:2010.12418*.

Aljifri, K., & Hussainey, K. (2007). The determinants of forward-looking information in annual reports of UAE companies. *Managerial Auditing Journal*, *22*(9), 881-894.

Araci, D. (2019). Finbert: Financial sentiment analysis with pre-trained language models. *arXiv preprint arXiv:1908.10063*.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. V. (2013). Digital business strategy: toward a next generation of insights. *MIS Quarterly*, 471-482.

Buzby, S. L. (1975). Company size, listed versus unlisted stocks, and the extent of financial disclosure. *Journal of Accounting Research*, 16-37.

Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management*, *52*(4), 385-400.

Chiva, R., Grandío, A., & Alegre, J. (2010). Adaptive and generative learning: Implications from complexity theories. *International Journal of Management Reviews*, *12*(2), 114-129.

Chow, C. W., & Wong-Boren, A. (1987). Voluntary financial disclosure by Mexican corporations. *Accounting Review,* 533-541.

Cooke, T. E. (1989). Disclosure in the corporate annual reports of Swedish companies. *Accounting and Business Research*, *19*(74), 113-124.

Deloitte. (2023AI in cybersecurity: A double-edged sword. Deloitte | A Middle East Point of View.

Depoers, F. (2000). A cost benefit study of voluntary disclosure: Some empirical evidence from French listed companies. *European Accounting Review*, *9*(2), 245-263.

Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2018). Bert: Pre-training of deep bidirectional transformers for language understanding. *arXiv preprint arXiv:1810.04805*.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 147-160.

Dodgson, M. (1993). Organizational learning: a review of some literatures. *Organization Studies*, *14*(3), 375-394.

Dye, R. A. (1983). Communication and post-decision information. *Journal of Accounting Research*, 514-533.

Dye, R. A. (2001). An evaluation of "essays on disclosure" and the disclosure literature in accounting. *Journal of Accounting and Economics*, *32*(1-3), 181-235.

Firth, M. (1979). The impact of size, stock market listing, and auditors on voluntary disclosure in corporate annual reports. *Accounting and Business Research*, *9*(36), 273-280.

Floyd, W. F. (2016). *Financial Reporting Quality and Voluntary Disclosure*. Stanford University.

Ghazawneh, A., & Henfridsson, O. (2013). Balancing platform control and external contribution in third-party development: the boundary resources model. *Information Systems Journal*, *23*(2), 173-192.

Goswami, S., Ravichandran, T., Teo, H.-H., & Krcmar, H. (2011). Achieving high performing supply networks through value network transparency. *PACIS 2011 Proceedings,* 68. https://aisel.aisnet.org/pacis2011/68

Gurbaxani, V., & Dunkle, D. (2019). Gearing up for successful digital transformation. *MIS Q. Executive*, *18*(3), 6.

Haislip, J., Lim, J. H., & Pinsker, R. (2021). The impact of executives' IT expertise on reported data security breaches. *Information Systems Research*, *32*(2), 318-334.

Healy, P. M., & Palepu, K. G. (2001). Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature. *Journal of Accounting and Economics*, *31*(1-3), 405-440.

Intellias. (2023). Supply chain attacks: Reputational damage. https://intellias.com/supply-chain-attacks/#:~:text=Reputational%20damage.,reputational%20damage%20from%20a%20cyberattack.

Kane, G. C., Palmer, D., & Phillips, A. N. (2017). Achieving digital maturity. *MIT Sloan Management Review.*

Kaseya. (2022) *Kaseya responds swiftly to sophisticated cyberattack - Kaseya. https://www.kaseya.com/press-release/kaseya-responds-swiftly-to-sophisticated-cyberattack-mitigating-global-disruption-to-customers/*

Kim, S. H., & Kwon, J. (2019). How do EHRs and a meaningful use initiative affect breaches of patient information?. *Information Systems Research,* 30(4), 1184-1202.

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, *38*(2), 143-154.

Kwon, J., & Johnson, M. E. (2013). Security practices and regulatory compliance in the healthcare industry. *Journal of the American Medical Informatics Association*, 20(1), 44-51. https://doi.org/10.1136/amiajnl-2012-000906

Leary, M. T., & Roberts, M. R. (2014). Do peer firms affect corporate financial policy?. *The Journal of Finance*, *69*(1), 139-178.

Liu, Y., Ott, M., Goyal, N., Du, J., Joshi, M., Chen, D., ... & Stoyanov, V. (2019). Roberta: A robustly optimized bert pretraining approach. *arXiv preprint arXiv:1907.11692*.

Malone, T. W., Crowston, K., Lee, J., & Pentland, B. (1993). Tools for inventing organizations: Toward a handbook of organizational processes. In *[1993] Proceedings Second Workshop on Enabling Technologies-Infrastructure for Collaborative Enterprises*, 72-82.

McNally, G. M., Eng, L. H., & Hasseldine, C. R. (1982). Corporate financial reporting in New Zealand: An analysis of user preferences, corporate characteristics and disclosure practices for discretionary information. *Accounting and Business Research*, *13*(49), 11-20.

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*, *83*(2), 340-363.

Pataci, H., Sun, K., & Ravichandran, T. (2022). DigiCall: A Benchmark for Measuring the Maturity of Digital Strategy through Company Earning Calls. In *Proceedings of the Fourth Workshop on Financial Technology and Natural Language Processing (FinNLP)*, 58-67.

Piccoli, G., Rodriguez, J., & Grover, V. (2022). Digital strategic initiatives and digital resources: construct definition and future research directions. *MIS Quarterly*, *46*(4).

Piccoli, Gabriele and Rodriguez, Joaquin, "Digital Strategic Initiatives: Conceptualization and Illustration" (2020). *BLED 2020 Proceedings.* 39. https://aisel.aisnet.org/bled2020/39.

Prencipe, A. (2004). Proprietary costs and determinants of voluntary segment disclosure: evidence from Italian listed companies. *European Accounting Review*, *13*(2), 319-340.

Raffournier, B. (1995). The determinants of voluntary financial disclosure by Swiss listed companies. *European Accounting Review*, *4*(2), 261-280.

Rai, A. and Bush, A. (2007). Recalibrating Demand and Supply Chain for the Digital Economy. *Systèmes d'Information et Management* 12(2), 21- 52.

RiskRecon. (2021). New 2020 ripple event examples in action. https://blog.riskrecon.com/new-2020-ripple-event-examples-in-action.

Sambamurthy, V., Bharadwaj, A., & Grover, V. (2003). Shaping agility through digital options: Reconceptualizing the role of information technology in contemporary firms. *MIS Quarterly*, 237-263.

Say, G., & Vasudeva, G. (2020). Learning from digital failures? The effectiveness of firms' divestiture and management turnover responses to data breaches. *Strategy Science*, 5(2), 117-142. https://doi.org/10.1287/stsc.2020.0106

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31-41.

Thordsen, T., Murawski, M., & Bick, M. (2020). How to measure digitalization? A critical evaluation of digital maturity models. In Responsible Design, Implementation and Use of Information and Communication Technology: *19th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2020, Skukuza, South Africa, April 6–8, 2020, Proceedings*, Part I 19 (pp. 358-369). Springer International Publishing.

Tuo, L., Yu, J., & Zhang, Y. (2020). How do industry peers influence individual firms' voluntary disclosure strategies?. *Review of Quantitative Finance and Accounting*, *54*, 911-956.

Verrecchia, R. E. (1983). Discretionary disclosure. *Journal of Accounting and Economics,* 5, 179-194.

Visser, W. (2012), The Age of Responsibility: CSR 2.0 and the New DNA of Business, Willey, London.

Wallace, R. O., Naser, K., & Mora, A. (1994). The relationship between the comprehensiveness of corporate annual reports and firm characteristics in Spain. *Accounting and Business Research*, *25*(97), 41-53.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, *17*(1), 4-19.

APPENDIX

A.1. Variable Overview and Data Sources

Variables		Description	Data Sources
Dependent Variable DSI Disclosure Disparity (DSID)		The difference in (DSI) between firm and their non-breached industry peers' average (SIC-3 level)	Earning call transcripts, SeekinAlpha. (2015-2019)
Independent Variable (I) Competitor Breach		Binary variable. A firm's competitor experienced a data breach. (SIC-3 level)	Privacy Rights Clearing House (PRC)
Independent Variable (II) Supplier Breach		Binary variable. A firm's supplier experienced a data breach.	Privacy Rights Clearing House (PRC Data) FactSet Data
Independent Variable (III) Customer Breach		Binary variable. A firm's customer experienced a data breach.	
Moderating Variable Historical Breach Experience		Binary variable. A firm's experienced a data breach in the past. (2010-2014).	Privacy Rights Clearing House (PRC Data)
Controls	Log of Assets	Control variable for firm size.	Company financial statements, Compustat
	R&D Intensity	Control variable for the firm's investment in innovation.	
	Profitability (ROA)	Control variable for the firm's profitability.	

A.2. Digital Strategy Aspect

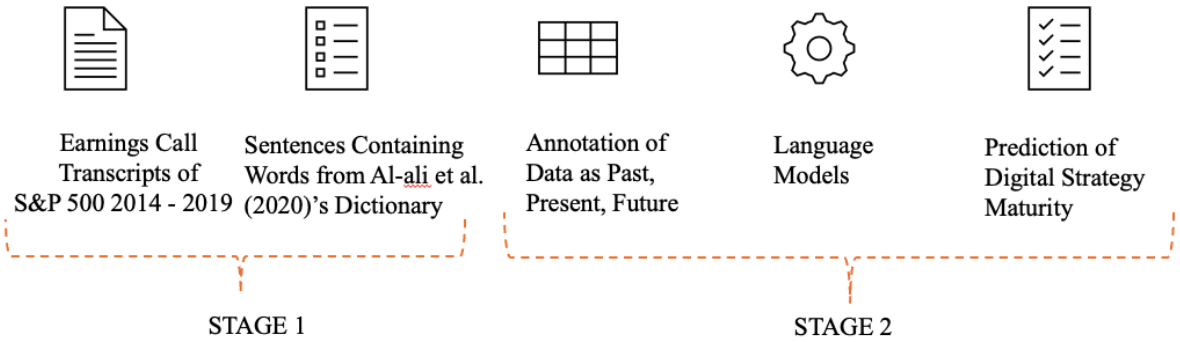
This list presents 17 topics of interest detailed by 350 definitional terms obtained from Al-Ali et al. (2020), Pataci et al., (2022).

Topic	Labels	Label Terms
Business Value	**Digital Product**	smart product*, connected product*, software as a service, Saas, platform as a service, Paas, platform, product as a service
	Digital Customer Experience	digital experience, customer experience, CX, user experience, UX, user journey, customer journey, digital engagement, customer engagement, personalization, personalisation, digital marketing, recommendation, market place, marketplace, e-commerce platform, digital service, digital services, e-service, online chat, chatbot, \bapp\b, digital channel, omnichannel
	Digital Operations	process automation, process mining, process analytics, process optimization, efficiency, cost saving, cost reduction, reduce cost, reducing cost, automation, predictive maintenance, ERP, supply chain, logistics, operations
	Digital Business Model	business model, new market, new segment, monetization, Saas, software as a service, on-demand, product as a service, value proposition, freemium, subscription, marketplace, ad-revenue, ads, peer-to-peer, two-sided, double-sided
Strategy Management	**Enablers**	digital strategy, digital business strategy, digital transformation strategy, governance, prioritization, digital vision, digital leadership, leadership support, leadership buy-in, communication, digital goals, data scientist, data analyst, machine learning engineer, developer, coder, programmer, chief digital officer, CDO, head of digital transformation, head of digital, product manager, product owner, cross-functional, scrum master, agile coach, innovation manager, data lake, data warehouse, middleware, enterprise architecture, digital tools, digital workplace, digital integration, chat, video call, CRM, ERP, service-oriented architecture, \bSOA\b
	Practices	Agile, scrum, MVP, minimum viable product, sprint, design thinking, business experiment, DevOps, \bepic\b, feature, user story, product owner, product manager, collaboration, cross-functional, cross-functional, A/B testing, exploratory data analysis, data analysis, decision support system, dashboard, hypothesis testing, experimental design, product metrics, user metrics, usage metrics, click-through rate, conversion rate, click stream, digital marketing, customer segmentation, risk modeling, simulation, decision analytics, decision support system, project management, digital skills, digital leadership, transformation, data analysis, social media management, social listening, user

		research, UX research, UX design, UI design, programming, coding, lean startup, experimentation, incubator, accelerator, innovation lab, digital lab, digital transformation, open innovation, design thinking, design sprint, digitalization, digitization, digital technolog[a-z]*
Digital Technology	**AI**	\bAI\b, artificial intelligence, NLP, natural language processing, natural language understanding, NLU, natural language generation, NLG, speech recognition, sentiment analysis, speech to text, text to speech, deep learning, machine learning, \bML\b, neural network, algorithm, generative adversarial network, GANs, supervised learning, unsupervised learning, reinforcement learning, semi-supervised learning, active learning, self-learning, transfer learning, back propagation, tensorflow, Salesforce Einstein, IBM Watson, Kaggle, AI as a service, Microsoft Azure ML, AutoML, autonomous vehicles, computer vision, image recognition, pattern recognition, cognitive computing, predictive analytics, predictive maintenance, algorithmic trading, clustering, dimensionality reduction, t-SNE, PCA, principal component analysis, chatbot, \bbot\b, RPA, robotic process automation, matrix factorization, collaborative filtering, recommender system, recommendation engine, graph mining, graph theory, Cortana, Alexa, Google Assistant
	Cloud Computing	cloud computing, cloud native, cloudless, distributed cloud, distributed computing, clustered computing, hybrid cloud, platform as a service, edge computing, cloud API, Google Cloud, Azure Cloud, AWS Cloud, software as a service, cloud applications, cloud, GPU, HPC management, cloud storage, elasticity, elastic computing, the cloud, data platform
	IoT	Internet of things, \bIoT\b, industrial internet, IIoT, embedded device, embedded sensor, digital twin, digital thread, building information modelling, BIM, connected devices, connected sensors, IoE, internet of everything, smart machines, connected machines, wearable, cyber-physical systems, machine to machine, connected factory, model-based definition
	Virtual Reality	\bVR\b, virtual reality, immersive technologies, mixed reality
	Augmented Reality	\bAR\b, augmented reality, immersive technologies, mixed reality
	Robotics	robots, humanoid, drone, drones, smart robots, smart warehouse, smart spaces, Lidar, computer vision, UAV, autonomous vehicles, swarm robots, industrial robot, robotics, automation
	Analytics	analytics, business intelligence, optimization, exploratory data analysis, data science, augmented analytics, descriptive analytics, descriptive statistics, prescriptive analytics, predictive, inference, inferential, customer segmentation, correlation, data visualization, data

		storytelling, text analytics, data lake, data warehouse, big data, social analytics, network analytics, network mining, network analysis
	Mobile	mobile, smartphone, mobile app, mobile application, mobile platform, mobile solution, mobile technology
	Social	social media, social network, content marketing
	3D Printing	3D print[a-z]*, additive manufacturing, 3D scan, material jetting, stereolithography, bioprint, bioprinted organ, fused deposition modeling, digital light processing, selective laser sintering, selective laser melting, laminated object manufacturing, digital beam melting
	Blockchain	blockchain, distributed ledger, decentralized, smart contracts, cryptocurrency, \bICO\b, initial coin offering, asset tokenization

A.3. DigiCall Pipeline



Stage 1: Aspect	Business Value, Strategy Management, Digital Technologies
Stage 2: Maturity	Past, Present, Future

A.4. DigiCall Benchmarks

	F1	**Accuracy**		
		PAST	PRESENT	FUTURE
Domain Agnostic				
BERT-base-cased	0.91	0.87	0.88	0.92
BERT-base-uncased	**0.94**	**0.88**	**0.98**	**0.92**
ALBERT base-v2	0.89	0.84	0.87	0.92
RoBERTa base	0.79	0.79	0.86	0.75
Domain-Specific				
FinBERT	0.90	0.91	0.91	0.83