Information Systems Frontiers (2025) 27:2539–2554
https://doi.org/10.1007/s10796-025-10638-7

The Influence of Data Breach Disclosures on R&D: Firm Strategies at Play

Ashutosh Singh[1] · **Nripendra P. Rana**[2,3,4] · **Xuan Huang**[5] · **Neha Dubey**[6]

Accepted: 5 August 2025 / Published online: 17 October 2025

Abstract
R&D expenditure is crucial for firms to drive innovation, preserve competitive advantage, and guarantee long-term growth. Nevertheless, such long-term investments are susceptible to interruptions from unforeseen circumstances like mandatory disclosure of data breaches. The U.S. Government mandates all firms to publicly disclose data breach incidents, which invariably erodes stakeholder trust in a company's governance and security procedures. For the purpose of achieving immediate stability and damage management, firms tend to frequently reallocate resources away from long-term expenditures, including R&D. Based on the signalling theory and the resource-based view, we investigate the impact on firms' R&D expenditure after the mandatory disclosure of data breach incidents and identify firm-related characteristics that can affect the relationship between the post-breach disclosure phase and R&D investment. We use a unique dataset from the Audit Analytics Cybersecurity database, combined with Compustat from 2004 to 2024 for U.S. publicly traded firms, to empirically test our hypotheses. Our findings contribute to a deeper understanding of how firms navigate the tension between short-term crisis management and long-term innovation strategies in the aftermath of a data breach.

Keywords Data breach · Mandatory disclosure · R&D expenditure · Business orientation · Strategic positioning

1 Introduction

R&D spending is of paramount importance for firms to gain a competitive edge, market adaptation, increase efficiency, risk management, long-term profit and sustainability (Kim et al., 2017; Pan et al., 2021; Rahmati et al., 2021). There is more than a 50% increase in R&D expenditure from 2010 to 2022, which shows an ongoing increase in R&D spending in US industries (Fig. 4 (Appendix)). This suggests that firms recognize the importance of R&D spending; hence, they are committed to spending more on technology and innovation. This long-term investment also ensures that firms will continue to lead the technical progress of the market.

However, a data breach incident may affect firms' long-term investment strategies. Government security breach notification regulations compel firms to report data breach occurrences (D'Arcy & Basoglu, 2022; Stevens, 2012). Hence, the data breach incident comes under the category of mandatory disclosure, which is a legal mandate for firms to disclose data breach information publicly (Jayaraman & Wu, 2019). This data breach mandatory disclosure may have an impact on strategic investment decisions due to the possibility of reputational harm, regulatory scrutiny, and

✉ Nripendra P. Rana
n.p.rana@qub.ac.uk

Ashutosh Singh
a.singh1@leeds.ac.uk

Xuan Huang
Xuan.Huang@nottingham.edu.cn

Neha Dubey
N.Dubey@greenwich.ac.uk

1 Leeds University Business School, University of Leeds, 18 Lyddon Terrace, Leeds LS2 9LA, UK

2 Queen's Business School, Queen's University Belfast, Belfast BT9 5EE, UK

3 Humanities and Social Sciences Research Center (HSSRC), Imam Mohammad Ibn Saud Islamic University, Riyadh, Saudi Arabia

4 Chandragupt Institute of Management Patna, Patna, India

5 Nottingham University Business School China, University of Nottingham Ningbo China, 199 Taikang East Road, Ningbo 315100, China

6 Greenwich Business School, University of Greenwich, Old Royal Naval College, Park Row, London SE10 9LS, UK

legal repercussions. Firms may incur up-front expenditures for forensic analysis, legal counsel, and informing impacted parties (Muniz & Lakhani, 2018), which is further exacerbated due to the penalties imposed by regulatory authorities such as CCPA and GDPR for non-compliance with data protection procedures (Wolff & Atallah, 2021). Data breaches could also lead to financial liabilities for businesses, such as compensating partners or clients for the associated losses (Goode et al., 2017). Additionally, breaches can weaken customer trust, leading to client attrition and a subsequent drop in sales or subscriptions (Bachura et al., 2022; Fowler, 2016). Stakeholders grow sceptical of the firm's ability to safeguard private data. The reputation of the firms could be harmed by public uproar and media attention (Bhargava, 2020; Syed, 2019). Business alliances may file class-action lawsuits because of the data breach incident in the partner firm (Cofone, 2021). Business activities may be disrupted if systems need to be pulled offline for inspection and repair (Thaduri et al., 2019; Wang et al., 2010). Hence, a firm's operations, finances, and reputation can all suffer significantly after the mandatory disclosure of data breaches.

Prior research has found that firms adopt a range of strategies to mitigate the negative effects of data breach incidents, such as implementing cybersecurity policies (Rao and Upadhyaya, 2009; Sharma & Barua, 2023), encrypting data (Miller & Tucker, 2011), updating security systems (Mughal, 2018; Price, 2014), providing with employees training to enhance awareness of phishing scams and cybersecurity threats (Hillman et al., 2023), to show commitment to data security, regulatory requirements, and public scrutiny.

While firms take immediate action to fix the breach, mandatory disclosure of data breaches often necessitates difficult resource allocation decisions. On the one hand, signalling theory emphasises the importance of short-term risk mitigation actions (e.g., Salge et al., 2022; Spence, 1974), such as reducing R&D expenditures, to signal stability and prudence, especially in high-tech and marketing-driven industries. These measures reassure stakeholders of their commitment to crisis management and security. On the other hand, the resource-based view places a strong emphasis on the strategic use of internal resources (Alraja et al., 2022; Barney, 1991), such as technological know-how and human capital, to preserve long-term investments and competitive advantage. That said, firms may continue to invest in R&D despite the pressures of mandatory data breach disclosures, reflecting their long-term orientation, particularly in service-oriented and high-market-value sectors.

However, prior research has not specifically examined this propensity of businesses to reduce R&D expenditures following the mandatory disclosure of data breaches. Hence, this study pioneers the exploration of this under-researched area. We also propose that some firm-related factors may affect the relationship between mandatory disclosure of post-data breaches and subsequent R&D expenditure. To address the gaps, we focus on the following research questions:

RQ1: Does the mandatory disclosure of data breaches impact firms' post-incident R&D expenditure?

RQ2: How do firm-specific factors (i.e., business orientation and strategic positioning) affect the relationship between mandatory disclosure of data breaches and R&D expenditure?

We collect and merge longitudinal data from the Audit Analytics Cybersecurity database, and Compustat from 2004 to 2024 to support our hypotheses empirically. We use a fixed effects model for the analysis and a control function approach to address the endogeneity in the model. Our results document that businesses spend less on research and development after the mandatory disclosure of data breaches. We also find that the post-breach disclosure phase has a reduced negative impact on R&D expenditures for companies in the service and high-market value firms. Additionally, the results reveal that the post-breach disclosure phase more negatively impacts marketing-driven and high-tech firms in terms of their R&D expenditures.

The remaining manuscript is structured as follows: Sect. 2 discusses the conceptual framework, which also contains all the proposed hypotheses. We describe the data, analysis, results and robustness analysis in Sect. 3. We provide a discussion of the research and theoretical and managerial implications in Sect. 4. Section 5 incorporates the conclusions with research limitations and future research directions.

2 Theoretical Background, Hypotheses Development, and Proposed Conceptual Model

Signalling theory describes how firms communicate reliable information to stakeholders when there is information asymmetry (Basu et al., 2024). Firms use various signalling strategies to convey information to stakeholders (e.g., Spence, 1973). Firms disclose financial (Albarrak et al., 2020), marketing-driven (Sun et al., 2024), governance (Talmor & Wallace, 1998), operational (Chung et al., 2024), sustainability (Jabr et al., 2014) and branding actions (Agarwal et al., 2024) to reduce information asymmetry among stakeholders. Signalling enables businesses to build confidence and trust with stakeholders by exhibiting consistency and dedication (Chen et al., 2021). Businesses can impact stakeholder decisions and lower uncertainty that might otherwise impede their success by providing strategic information to improve firm performance.

A data breach is the unauthorised access and disclosure of private, sensitive, or protected data from a firm's networks (Chakraborty et al., 2016; Khan et al., 2021). It usually happens when data-protecting security mechanisms, including firewalls, encryption, or access controls, are disregarded or malfunction. Data breaches can affect proprietary, financial, or personal information, and they can have detrimental effects on the company, its partners, customers, and employees (D'Arcy et al., 2020; Lee et al., 2022). When a data breach incident happens in a firm, the firm has to disclose this information publicly as per the government guidelines of mandatory disclosure, which sends a negative signal to the market and stakeholders. It highlights weaknesses in the firm's governance, risk management, and security protocols. Stakeholders like customers, partners, and investors lose faith in the firm as a result, raising doubts about its future. Businesses frequently incur higher expenses following a breach as a result of fines, legal actions, customer compensation, and investments in enhanced cybersecurity (Furnell et al., 2020). This gives the impression that the firm is under financial strain, which could make it harder for the company to continue making discretionary investments. The mandatory disclosure of data breaches draws attention to the firm's strategic and operational risks. As a result, businesses complement risk control and short-term operational stability ahead of long-term investments, which by their very nature have uncertain returns (Rosati et al., 2017).

Signalling theory posits that firms can shape stakeholder perceptions by sending strategic information as signals that lessen uncertainty and restore confidence. In line with this theory, businesses may scale back R&D expenditures following a mandatory disclosure of data breaches to indicate a concentrated effort towards immediate stability and security enhancements. An increase in R&D investment enhances firms' systematic risk due to uncertainty in successful innovation and market acceptance (Ho et al., 2004). By limiting long-term, high-risk investments like R&D, businesses show stakeholders that the firm is taking a more conservative approach to its finances, which lowers perceived risk. The reduction of R&D investment after the data breach incident suggests that the firm's goals have shifted from innovation to repairing the reputational damage and building trust with stakeholders. Although this may appear to be detrimental to long-term growth, it is in line with the firm's urgent need to restore its operational integrity and image. Therefore, we propose the below hypothesis:

H1. Firms experience a decrease in R&D expenditure following a mandatory disclosure of data breaches.

By complementing signalling theory, the resource-based view (RBV) provides a deeper understanding of how firms sustain long-term competitive advantages. RBV suggests that firms are willing to endure short-term costs or risks to protect and expand their resource base (e.g., Mahoney & Pandian, 1992). Central to this perspective is the strategic cultivation and deployment of internal resources that are valuable, rare, and inimitable to outperform competitors (Barney, 1991; Mahoney & Pandian, 1992; Newbert, 2008). These resources create conditions for achieving and maintaining superior performance in dynamic markets by limiting competition and resource substitution. Developing and protecting these resources strengthens a firm's market position, fosters innovation, and ensures long-term growth (Lockett et al., 2009). Additionally, RBV also provides a robust framework for understanding how firm-specific resources affect firm decision-making by emphasizing the role of unique resources in determining strategic decisions. These resources influence not only operational and strategic priorities, but also responses to external pressures and opportunities, such as regulatory requirements, market disruptions, or innovation demands (Teece et al., 1997).

Consequently, by incorporating signalling theory and RBV, we propose that the relationship between R&D expenditure and mandatory disclosure of data breaches is not uniform across companies. It varies based on firm-specific factors that influence how businesses view, react to, and handle the fallout from a breach. We investigate different factors that may affect the influence of data breaches on R&D expenditure and provide additional hypotheses based on those factors.

2.1 Business Orientation

2.1.1 Service-Oriented Firms

Service-oriented firms prioritize providing intangible goods or services over tangible ones to meet client demands, improve experiences, and offer solutions that do not require possession of a tangible product (Saunders & Brynjolfsson, 2016). The RBV framework suggests that firms can achieve sustainable competitive advantage with the help of valuable, rare, inimitable and non-substitutable resources (Beard & Sumner, 2004). The primary intangible resources of service-oriented firms, like human capital, client relationships, and process efficiency, are considered the types of resources that help them achieve a competitive advantage (Ferratt et al., 2005). Hence, service firms need to invest in R&D to preserve core competencies even in the face of unfavourable occurrences like mandatory disclosure of data breaches. Service firms also rely on dynamic knowledge-based capabilities, such as skills and expertise, to customized offerings because the preference for personalized products changes rapidly with time (Chuang & Lin, 2017). Thus, service firms frequently invest greater resources in R&D because of their reliance on knowledge-based capabilities and intangible

assets. Based on these arguments, we propose the below hypothesis:

H2. The negative impact of mandatory disclosure of data breaches on R&D expenditure is weakened for service firms in the post-data breach period.

2.1.2 Technology-Oriented Firms

High technology firms are companies that operate in areas where technological advancement and proficiency are major drivers to achieve a competitive advantage. The trust of external stakeholders is crucial for high-tech firms. Mandatory disclosure of data breaches raises concerns about high-tech firms' dependability and security measures. Consumers may lose faith, investors may feel less confident about investing, and partners may hesitate to collaborate if there is a compromise in the online security systems (Nikkhah & Grover, 2022). High-tech firms may perceive weakness after the data breach incident, even if they have strong internal technological capabilities. So, high-tech firms will allocate resources for this crisis management and restore the trust as quickly as possible. Formulating strategies to maintain public relations can mitigate market reactions and preserve shareholder value after the mandatory disclosure of data breaches. High-tech firms will reduce the risk associated with long-term R&D investment, which provides a positive signal to external stakeholders regarding more focus on damage control. Hence, in this scenario, signalling mitigation strategies are crucial to maintaining the trust of the external stakeholders. Therefore, we propose the below hypothesis:

H3. The negative impact of mandatory data breach disclosure on R&D expenditure is stronger for firms in high-tech industries during the post-breach period.

2.2 Strategic Positioning

2.2.1 Marketing-Driven Firms

Marketing intensity is the level of resources and effort a firm invests in promotional initiatives to improve firm performance. Because high-marketing-intensity companies frequently interact with consumers more, their reputation as a brand is a vital resource (Quelch & Jocz, 2007). In order to keep stakeholders, these businesses must promptly restore trust and demonstrate dependability following a breach. Firms with high marketing intensity are more focused on a customer-centric perspective than firms that compete solely on internal resources (Papasolomou et al., 2014). While investments in cybersecurity improvements or public communication tactics provide rapid, obvious signs of remedial action after the incident, R&D expenditures are long-term and not immediately apparent to external stakeholders. Hence, marketing-driven firms are motivated by the desire to restore stakeholder trust and rehabilitate their brand in the wake of the mandatory disclosure of data breaches by sending out quick, obvious messages. Due to the mandatory disclosure of data breaches, long-term resource investments are outweighed by short-term perception management, and marketing-driven firms give less priority to R&D investments over security updates and public relations campaigns. Therefore, we propose the following hypothesis:

H4: The negative effect of mandatory data breach disclosure on R&D expenditure is stronger for firms with high marketing intensity than for those with low marketing intensity.

2.2.2 Firm Market Value

High-market value firms have a comparatively high market capitalisation because they are seen as having substantial market and investor value (Dias, 2013). These businesses are frequently well-established, have solid financial standing, and are known for their advantages over competitors (Porter, 2008). A high-market value firm has the accumulation of valuable resources that allow it to withstand brief crises without compromising key strategic investments. High-market-value firms' abundant resources are self-evident, and stakeholders are familiar with the capabilities of high-market-value firms (Srivastava et al., 1998). As a result, high-market value firms manage crises without depending on external signalling strategies by utilising their robust internal processes and available resources. Hence, high market value firms will continue investing in long-term investments like R&D expenditure, even after the mandatory disclosure of data breaches. Therefore, we propose the following hypothesis:

H5: The negative impact of mandatory data breach disclosure on R&D expenditure diminishes for firms with high market value than for firms with low market value.

The conceptual model is presented in Fig. 1.

3 Methodology

3.1 Data

We obtain the firm's data breach information from Audit Analytics. The Audit Analytics Cybersecurity Database is a unique dataset that offers details on data breaches impacting publicly traded firms. The database primarily targets publicly traded corporations that are registered with the U.S. Securities and Exchange Commission and legally obligated to report major cybersecurity events. This guarantees that the dataset provides a representative sample for

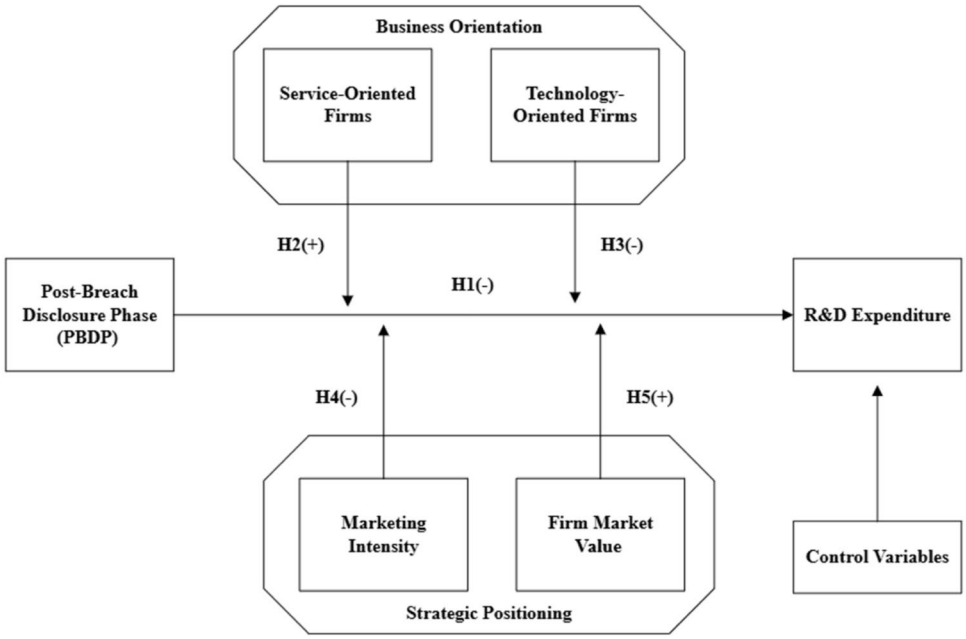

Fig. 1 Proposed Conceptual Model

study by encompassing a wide range of significant U.S. firms in different industries. Prior researchers have also used this database for research related to data breach incidents (Westland, 2022). We merge the Compustat database with this breach data to enrich the dataset with firm-level financial and operational information. This process includes all firm-specific variables required to support our hypothesis empirically. With this process, we obtain a panel dataset that includes 5,689 year-wise observations across 355 firms spanning from 2004 to 2024. Figure 2 presents a flowchart illustrating the complete methodology.

3.1.1 Dependent Variable

We use the ratio of R&D expenditure to sales as our dependent variable. This ratio considers business size variations by expressing R&D investment in relation to sales. While the ratio offers a standardized measure, it would be incorrect to compare the absolute R&D spending of firms of different sizes. Since a firm's operations usually cause sales to increase or decrease, the ratio helps account for these variations and enables insightful long-term comparisons. Prior literature also used the same ratio to measure R&D expenditure in firms (Jha & Bose, 2021).

3.1.2 Independent Variable

We consider the post-breach disclosure phase (PBDP) as a dummy variable equal to '1' for periods following the mandatory disclosure of the breach incidence, and otherwise, it is set to equal '0'. Each breach's disclosure year is obtained from Audit Analytics, guaranteeing a precise determination of the moment the breach is made public. Our sample has 928 data breach mandatory disclosures, and we examine the impact of data breach incidents on firms' R&D expenditure up to five years after the breach using our PBDP dummy variable. The PBDP dummy contains a time frame of a minimum of two years and a maximum of five years, with an average of 3.9 years, after the mandatory disclosure of the data breach. Typically, mandatory disclosures of data breaches are brief shocks that force businesses to adapt immediately. Because of this, the window of two to five years is suitable for capturing the short- and medium-term impacts. We also observe that firms typically don't experience multiple data breaches in the time frame we considered for the analysis.

3.1.3 Moderators

We also use a dummy variable for service firms based on Standard Industrial Classification (SIC) codes, following prior (Jha & Verma, 2023). It is equal to '1' if the firm is service-oriented; otherwise, '0'. We also create a dummy variable for high-technology firms using SIC codes as suggested by prior literature (Huang et al., 2020). The value of a high-tech dummy is '1' if the firm is technology-oriented; otherwise, it is equal to '0'. We measure marketing intensity by calculating the ratio of selling, general and administrative expenses, excluding research expenditures, to total sales (Bae et al., 2017). The standardised ratio can be applied uniformly across industries for the analysis. The firm market value is measured with the ratio of firm market

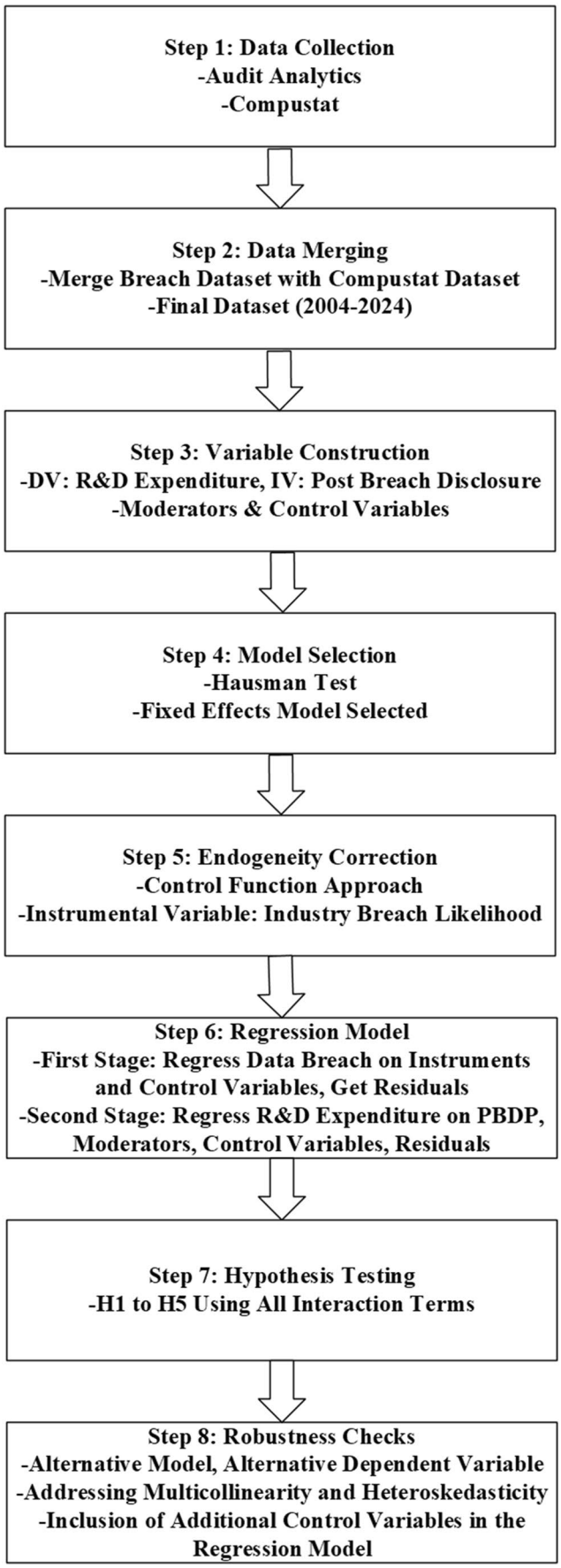

Fig. 2 Methodological Framework

value to sales (Raman et al., 2022). Even across industries with varying sizes or scales, this ratio makes it simple to compare businesses. It makes benchmarking easier by normalising market value by a key firm growth metric.

3.1.4 Control Variables

We included several control variables that could influence our study. One such variable is the firm's gross profit scaled by total assets, as higher profitability may encourage firms to allocate more resources to long-term investments. We also add the Herfindahl index as a proxy to diversification, as more diversified firms may focus more on R&D expenditure to achieve their long-term goals. In our analysis, we also add sales to asset ratio, which is a proxy for operational efficiency. High operational efficiency minimizes costs and affects R&D due to the presence of additional resources. We use a B2B dummy variable, which takes the value of '1' if the firm operates in a B2B context and '0' otherwise. We use SIC codes to define the B2B dummy variable as suggested by the prior literature (Guenther & Guenther, 2022). B2B firms typically spend money on R&D that focuses on technological innovation and collaboration with other partners (Srinivasan et al., 2011), and this may affect our study. We include all these control variables along with the primary variables in our analysis. The descriptions, descriptive statistics and correlations of these variables are given in Table 1 and Table 2.

3.2 Estimation Method

We perform the Hausman test to determine whether to employ a Fixed Effects or Random Effects model. These models are frequently employed in data analysis when observations are made for the same entities throughout a number of time periods. We perform the Hausman test by considering that the random effects model is appropriate as our null hypothesis. After performing the Hausman test, we find that the test statistic is positive and significant (Chi-square = 257.93, $p < 0.05$). Thus, the null hypothesis is rejected. The fixed effects model is more appropriate to analyse the sample (Lee et al., 2019). Hence, we use the fixed effects model to support our hypotheses empirically.

3.3 Control Function Approach for Addressing Endogeneity

There could be several factors which could affect our analysis. Measurement errors, reverse causality or omitted variables can all lead to endogeneity when examining how data

Table 1 Description of Variables

Variables	Measure	Data Source
R&D Expenditure	Ratio of R&D expenditure to sales	Compustat
PBDP	='1' if year≥Data breach mandatory disclosure year, otherwise '0'	Audit Analytics
Service Firm	='1' if the firm is a service firm, otherwise '0'	Compustat
Hightech Firm	='1' if the firm is a hightech firm, otherwise '0'	Compustat
Marketing Intensity	Ratio of (SG&A-R&D expenses) to sales	Compustat
Market Value	Ratio of firm market value to sales	Compustat
Gross Profit	Ratio of gross profit to asset	Compustat
Diversification	Herfindahl Index	Compustat
Operational Efficiency	Ratio of sales to asset	Compustat
B2B	='1' if the firm is a B2B firm, otherwise '0'	Compustat

Table 2 Correlation and Descriptive Statistics (*p<0.05)

		1	2	3	4	5	6	7	8	9	10
1	R&D Expenditure	1.00									
2	PBDP	−0.06*	1.00								
3	Service Firm	−0.14*	−0.04	1.00							
4	Hightech Firm	0.18*	0.00	−0.09*	1.00						
5	Marketing Intensity	0.02	−0.01	−0.02	0.03	1.00					
6	Market Value	0.16	−0.02	−0.04	0.02	0.09*	1.00				
7	Gross Profit	0.05	−0.03*	−0.05*	0.01	−0.00	0.07*	1.00			
8	Diversification	0.07	0.01*	−0.13*	0.16*	0.04	0.02	0.06*	1.00		
9	Operational Efficiency	0.02	0.17*	−0.02	0.07*	0.11*	−0.00	0.00	0.05*	1.00	
10	B2B	0.11*	−0.03	0.21*	0.04	0.03	0.00	−0.05*	0.04	−0.02	1.00
	Mean	0.11	0.28	0.43	0.29	0.31	0.10	0.33	0.49	0.08	0.54
	SD	0.19	0.25	0.41	0.21	0.29	0.08	0.47	0.31	0.19	0.39
	Sample Size	5689	5689	5689	5689	5689	5689	5689	5689	5689	5689

breach incidences affect R&D spending. One popular technique for dealing with endogeneity problems in regression models is the control function approach. We consider industry-level breach likelihood to be an instrumental variable in our analysis. The possibility of an industry-level breach is influenced by more general factors like rates of technological adoption and industry-standard security measures. The industry-level breach likelihood is an industry-level variable and has no direct impact on firms' decisions regarding R&D spending. However, it is highly connected with firm-level breach incidence. Therefore, our instrumental variable maintains the assumptions of exclusion restrictions.

We use the first two digits of SIC codes to define the industries as prior literature suggests (Germann et al., 2015). We use the below formula to calculate industry breach likelihood:

$$BreachLikelihood_{j,t} = \frac{\sum_{i=1toN_j,t} Breach_{i,t}}{N_{j,t}} \quad (1)$$

where,

$BreachLikelihood_{j,t} =$ Breach likelihood of industry j at time t

$\sum_{i=1toN_j,t} Breach_{i,t} =$

Sum of all data breach incidents for all firms i in industry j at time$t$

$N_{j,t} =$ Total number of firms in industry j at time t

3.4 First and Second-Stage Regressions

In the first-stage regression, we regress data breach incidence on industry breach likelihood using the fixed effects model. We use all control variables for the first-stage regression, which are reported in Table 1 and Table 2. The estimation equation for the first-stage regression is given below:

$$DataBreachIncident_{it} = \lambda_0 + \lambda_1 * BreachLikelihood_{it} + \lambda_2 * W_{it} + \varepsilon \quad (2)$$

The list of all control variables in Eq. (2) is denoted by W_{it}. After running the regression given in the estimation Eq. (2), we obtain the fitted values of the data breach incident for the *i*th firm at time *t,* along with residuals. We use these residuals in the second stage of regression. The equation of the second-stage regression is given below:

$$
\begin{aligned}
R\&DExpenditure_{it} &= \beta_0 + \beta_1 * PBDP_{it} \\
&+ \beta_2 * PBDP_{it} * ServiceFirm_{it} \\
&+ \beta_3 * PBDP_{it} * HightechFirm_{it} \\
&+ \beta_4 * PBDP_{it} * MarketingIntensity_{it} \\
&+ \beta_5 * PBDP_{it} * FirmMarketValue_{it} \\
&+ \beta_6 * ServiceFirm_{it} \\
&+ \beta_7 * HightechFirm_{it} \\
&+ \beta_8 * MarketingIntensity_{it} \\
&+ \beta_9 * FirmMarketValue_{it} \\
&+ \beta_{10} * GrossProfit_{it} \\
&+ \beta_{11} * Diversification_{it} \\
&+ \beta_{12} * OperationalEfficiency_{it} \\
&+ \beta_{13} * B2B_{it} \\
&+ \beta_{14} * Residual_{it} + \varepsilon
\end{aligned} \tag{3}
$$

3.5 Results

We run the fixed effects model to estimate Eq. (3). The results are reported in Table 3. Model 1 investigates the primary impact of the post breach variable on R&D expenditure without incorporating any control variables and interactions. Model 2 includes control variables along with the primary effect. Model 3 incorporates interactions and control variables to test the hypotheses. We check the results to find out if they empirically support our hypotheses.

3.5.1 Empirical Support for H1

The coefficient of the PBDP variable is negative and significant ($\beta = -0.03$, $p < 0.05$). Hence, Hypothesis H1 is supported, suggesting that firms spend less on R&D after a mandatory disclosure of data breaches.

3.5.2 Empirical Support for H2

The coefficient of the interaction of the PBDP variable with service firms is positive and significant ($\beta = 0.05$, $p < 0.05$). Hence, Hypothesis H2 is also supported. Therefore, the impact of mandatory disclosure of data breaches on R&D

Table 3 Main Results – DV-R&D Expenditure

Independent Variables	Model 1: Main Effect Only	Model 2: Main Effect with Controls	Model 3: Full Model Results (FE)
PBDP	**−0.03*** (0.01)**	**−0.02*** (0.01)**	**−0.03** (0.01)**
PBDP *Service Firm			**0.05** (0.02)**
PBDP *Hightech Firm			**−0.13*** (0.02)**
PBDP *Marketing Intensity			**−0.65*** (0.06)**
PBDP *Firm Market Value			**0.04** (0.02)**
Service Firm		−0.14 (0.04)	−0.22 (0.06)
Hightech Firm		0.23* (0.04)	0.19* (0.05)
Marketing Intensity		0.02 (0.01)	0.03 (0.01)
Firm Market Value		0.09 (0.02)	0.10 (0.02)
Gross Profit		0.06* (0.03)	0.07** (0.03)
Diversification		0.05 (0.02)	0.05 (0.03)
Operational Efficiency		0.08 (0.01)	0.36 (0.06)
B2B		0.13 (0.04)	0.16 (0.07)
Residual Control Variable	Present	Present	Present
Industry fixed effects	Present	Present	Present
Year fixed effects	Present	Present	Present
R^2	0.01	0.22	0.24
_cons	0.11* (0.04)	0.04 (0.06)	0.05 (0.06)

[Note: *p<0.1, **p<0.05, ***p<0.01]

expenditure is less unfavourable for service firms in the post-data breach period.

3.5.3 Empirical Support for H3

The coefficient of the interaction of the PBDP variable with high technology firms is negative and significant ($\beta = -0.13$, $p < 0.01$). Thus, Hypothesis H3 is also supported, suggesting that mandatory data breach disclosure has a greater detrimental effect on R&D spending in the post-breach phase for high-tech companies.

3.5.4 Empirical Support for H4

The coefficient of the interaction of the PBDP variable with marketing intensity is negative and significant ($\beta = -0.65$, $p < 0.01$). Thus, the results support Hypothesis H4. Hence, following mandated data breach disclosure, firms with higher marketing intensity spend less on research and development.

3.5.5 Empirical Support for H5

The coefficient of the interaction of the PBDP variable with firm market value is positive and significant ($\beta = 0.04$, $p < 0.05$). Thus, Hypothesis H5 is also supported. Hence, for firms with high market value, the effect of mandatory data breach disclosure on R&D spending decreases during the post-breach period.

Overall, all of our hypotheses are empirically supported. We present the moderation plots in Fig. 3 to complement the statistical moderation analysis. We also find that firms' gross profit is positive and significant, suggesting that additional slack resources due to higher profitability allow firms to invest in R&D for long-term growth (Du et al., 2022). However, other control variables- diversification, operational efficiency and B2B firm type are not significant. These results imply that firms may place a greater emphasis on risk management after the data breach incident, irrespective of firm-level characteristics. We also perform some robustness analysis to strengthen the results further.

3.6 Robustness Analysis

3.6.1 Alternative Model

We also use the random effects model to analyze our sample for the robustness check. The random effects model assumes that the firm-specific factors are not correlated

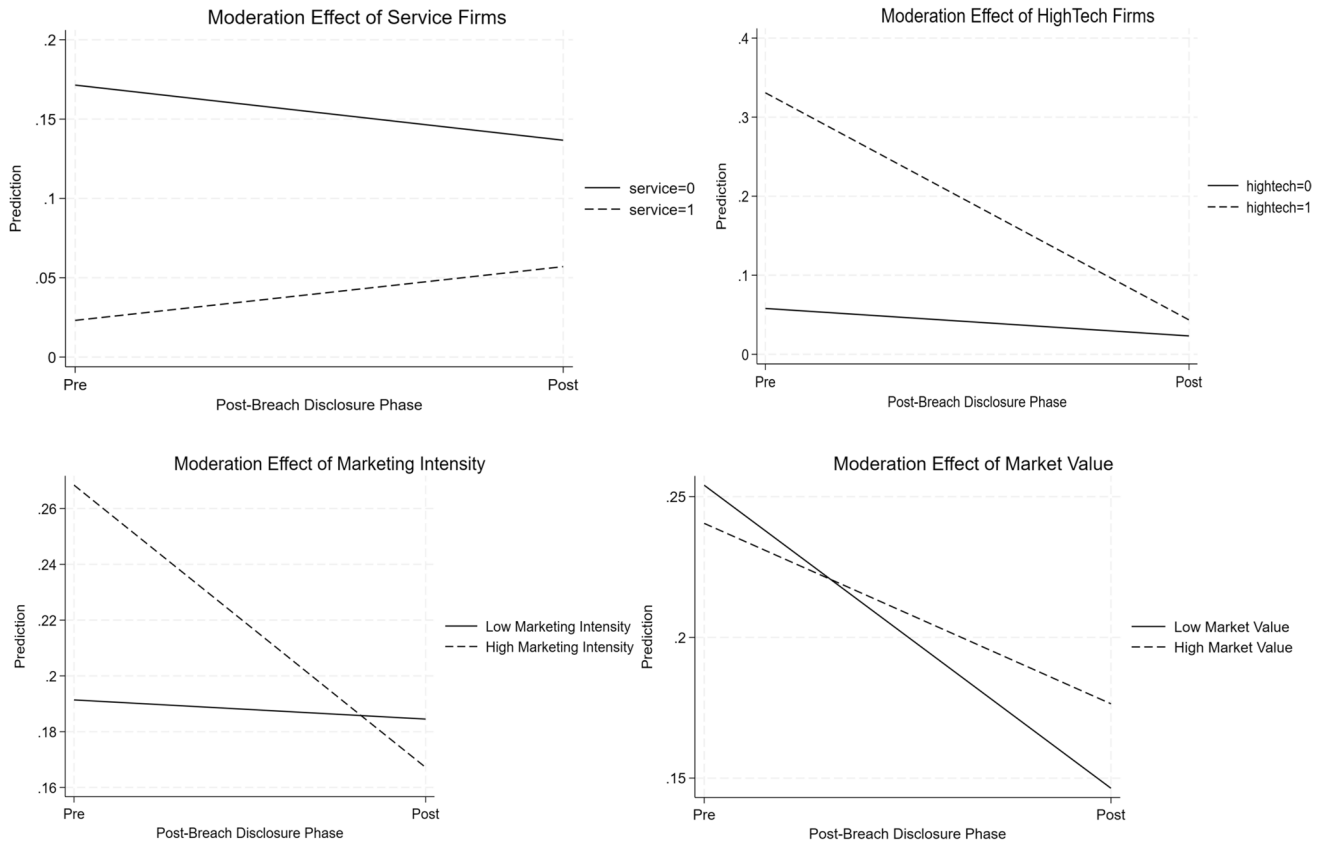

Fig. 3 Visualization of Moderation Effects

with independent variables (Baumann et al., 2022). This may preserve the capacity to generalize results while permitting firm-specific heterogeneity. We run the analysis, and the results are reported in Table 4 (Model 1). We find that businesses spend less on R&D following a mandatory disclosure of data breaches. However, this effect is less evident for service firms and those with high market value, while it is more pronounced for high-tech firms and those with greater marketing intensity. Hence, all of our hypotheses are also supported using the random effects model.

3.6.2 Alternative Dependent Variable

We also use an alternative dependent variable, which is R&D capital stock, as a proxy for firms' innovation investments. Lev and Sougiannis (1996) use R&D capital stock by combining the delayed effects of lagged R&D investments with a constant depreciation rate. They use a complex formula to calculate the R&D capital stock. We use an easier version of that equation by simplifying the time-varying depreciation to a constant depreciation rate. The equation for calculating R&D capital stock is given below:

Table 4 Robustness Model Results

Independent Variables	Model 1: Random Effects Model	Model 2: R&D Capital Stock as DV	Model 3: Additional Control Variables
PBDP	**−0.03*** (0.01)**	**−0.33*** (0.09)**	**−0.04*** (0.01)**
PBDP *Service Firm	**0.04*** (0.01)**	**0.34** (0.15)**	**0.05*** (0.01)**
PBDP *Hightech Firm	**−0.14*** (0.03)**	**−0.83* (0.48)**	**−0.13*** (0.03)**
PBDP *Marketing Intensity	**−0.66*** (0.11)**	**−6.21*** (1.34)**	**−0.64*** (0.10)**
PBDP *Firm Market Value	**0.06*** (0.01)**	**5.18*** (1.01)**	**0.04*** (0.01)**
Service Firm	−0.15** (0.05)	−0.66* (0.39)	−0.15 (0.04)
Hightech Firm	0.25* (0.05)	0.64 (0.49)	0.26** (0.04)
Marketing Intensity	0.02 (0.01)	−0.16 (0.13)	0.02 (0.01)
Firm Market Value	0.09 (0.03)	3.53** (0.62)	0.09 (0.01)
Gross Profit	0.01 (0.01)	0.02 (0.12)	0.01 (0.01)
Diversification	0.05* (0.02)	0.12 (0.09)	0.04 (0.02)
Operational Efficiency	0.64 (0.11)	5.82* (1.68)	0.63 (0.11)
B2B	0.14 (0.05)	0.59 (0.38)	0.13 (0.05)
Inflation			0.04 (0.02)
GDP Growth			−0.08 (0.02)
Recession			−0.07 (0.02)
Pandemic			−0.01 (0.01)
Residual Control Variable	Present	Present	Present
Industry fixed effects		Present	Present
Year fixed effects		Present	Present
R^2	0.27	0.46	0.25
_cons	0.03 (0.02)	0.15 (0.31)	0.04 (0.03)

[Note: *p<0.1, **p<0.05, ***p<0.01]

$$R\&DCapitalStock_{it} = \sum_{k=0}^{N} R\&D_{i,t-k} * (1-\delta)^{k} \quad (4)$$

where,

$R\&DCapitalStock_{it}$= R&D capital stock for ith firm at time t.

$R\&D_{i,t-k}$= R&D capital stock for ith firm at time t-k.

N = Number of considered lag years.

δ= Depreciation rate.

k = Lag index.

$(1-\delta)^{k}$= Retention factor, suggesting lagged R&D effects fade over time.

In order to construct R&D capital stock, we aggregate the R&D expenditures over five years, and then we weigh the contribution of each year based on its retention rate. We consider a depreciation rate of 15% as suggested by prior literature (Mazzucato & Tancioni, 2012). We use R&D capital stock in our analysis as a dependent variable, and the results are reported in Table 4 (Model 2). All five hypotheses are empirically supported with R&D capital stock as a dependent variable, reinforcing the robustness of our study.

3.6.3 Additional Control Variables

We also consider some macroeconomic variables which can affect our analysis. A high inflation rate may increase firms' capital costs, which can limit investment in R&D expenditure (Davig et al., 2011). A high growth in GDP makes firms more optimistic, encouraging more investment in firms' R&D expenditure (Rashid & Saeed, 2017). The inflation and GDP growth datasets for the United States are available on the World Bank website. We collect the data for the years 2004–2024 and merge it with our original dataset for analysis. Economic downturns or major disruptions affect market demand, which may negatively affect the R&D expenditure of firms (Barnichon et al., 2022). Hence, we include dummy variables for the US recession and Covid-19 pandemic events. The recession dummy variable is equal to '1' for the years 2008 and 2009. Otherwise, it is equal to '0'. The pandemic dummy variable is equal to '1' for the years 2020 and 2021; otherwise, '0'. We include these additional control variables in the analysis. The results are reported in Table 4 (Model 3). The additional control variables don't affect our results, confirming the robustness of our study.

3.6.4 Multicollinearity and Heteroskedasticity

We also check the multicollinearity within our model. The variance inflation factor has a value of 7.16, which is below 10 (Kapoor et al., 2015). Therefore, multicollinearity is not present in our model. We also use robust standard errors in our analysis to address the issue of heteroskedasticity (Kim et al., 2023). Consequently, our results show no multicollinearity or heteroskedasticity. Hence, the chances of Type I and Type II errors in our analysis are low, and estimates are more reliable.

4 Discussion

This study advances the scholarly discourse on cybersecurity and firm resilience (Baatwah et al., 2025); problematic trade-offs between immediate remediation and long-term R&D investment (He et al., 2020) by revealing how R&D allocation is affected by data breach and its mandatory disclosure by investigating cross-industry differences, particularly in sectors where R&D is the main source of competitive advantage. It uses an RBV framework and signalling theory to examine how mandatory disclosure of data breaches affects businesses' R&D spending. Our results offer strong empirical backing for the theories put forth, illuminating how companies strategically modify their R&D expenditures in reaction to mandatory disclosure of data breach events and how firm-specific variables mitigate these impacts. The PBDP variable's negative and significant coefficient indicates that our data support Hypothesis H1. This implies that following a mandatory disclosure of data breaches, businesses curtail their R&D spending, perhaps putting short-term stability and security enhancements ahead of long-term innovation. Businesses adopt a cautious approach to resource allocation to restore stakeholder trust and operational integrity after a mandatory data breach disclosure conveys an unfavourable impression to stakeholders about the company's governance and risk management. Hypothesis H2 is supported by the PBDP variable and service firms' positive and significant interaction coefficient. Intangible assets, including client relationships, human capital, and process efficiency, are crucial for service-oriented businesses. According to the RBV framework, these businesses need to keep investing in R&D in order to retain their competitive edge, even in times of crisis. R&D is essential to the recovery and survival of service organisations because of their reliance on knowledge-based capabilities and customised service offerings, which demand constant innovation. Hypothesis H3 is supported by the negative and significant interaction between the PBDP variable and high-technology enterprises. Due to their reliance on technical innovation, high-tech companies are especially susceptible to mandatory disclosure of data breaches, which can undermine shareholder trust in their security protocols. Instead of maintaining high-risk, long-term R&D investments, many companies are likely to redirect their resources to damage

control and faith restoration in the wake of data compromise. High-tech companies must put urgent risk mitigation ahead of innovation because of the bad signal that mandatory disclosure of a data breach sends. Hypothesis H4 is supported by the significant and negative interaction between marketing intensity and the PBDP variable. Following a mandatory data breach disclosure, marketing-driven companies that mostly depend on consumer trust and brand reputation give priority to short-term measures to repair their reputation. These companies prioritise short-term, visible initiatives like security updates and public relations efforts over long-term R&D expenditures. This strategy enables them to control stakeholder perceptions while effectively exhibiting a prompt response to a crisis. Hypothesis H5 is supported by the PBDP variable and firm market value, which have a positive and significant relationship. High-market-value companies can withstand crises without drastically changing their long-term investment strategy since they have enormous resources and established credibility. Stakeholders acknowledge these companies' capacity to handle transient shocks, which enables them to continue investing in R&D even in the face of mandatory disclosure of data breaches. These companies continue to innovate while tackling current issues by utilising their strong internal procedures and financial position. We also discuss the theoretical and managerial implications in the next two sections.

4.1 Theoretical Implications

Using the lens of signalling theory and RBV, this study makes two key contributions from a theoretical perspective. First, it extends the signalling theory into the domain of post-data breach resource allocation. Unlike the prevailing use of signalling theory as a means to focus on proactive reputation-building behaviours (Bergh et al., 2014; Guest et al., 2021; Connelly et al., 2025), our findings reveal that firms also use it to signal a shift towards stability and security through reactive resource adjustments, such as reductions in R&D expenditure. This expands the conceptualization of signals beyond communication and transparency to include resource reallocation as a form of non-verbal signalling. To reduce information gaps, businesses strategically convey information to stakeholders, as per signalling theory. Firms restore trust after a data breach by considering noticeable steps, like cutting R&D spending, for signalling stability and risk aversion. Cutting R&D spending after a mandatory data breach disclosure helps address urgent worries about the company's stability and highlights a cautious financial approach. The signalling strategy helps in some industries after the mandatory data breach disclosure. Due to their dependence on technological reliability, high-tech companies place a high priority on security signalling and crisis management to preserve investor and customer confidence. Marketing-driven businesses prioritize obvious remedial measures to preserve consumer confidence and brand reputation, both of which are critical to their competitive edge. Businesses that have experienced a data breach use signals to communicate operational stability and reduce risk in order to lessen the unfavourable impressions of uncertainty. This may result in a strategic decision to prioritize short-term risk-control measures above long-term investments like R&D.

Second, our research enhances RBV by analysing how resource allocation priorities are adjusted under threat conditions. According to the RBV, companies' valuable, rare, unique, and non-substitutable resources give them a competitive edge. A firm's internal resources can handle the challenges along with long-term strategic spending. A service-oriented firm's unique resources (e.g., skilled workforce team) can manage data breach crises without affecting R&D spending. Companies with high market value maintain well-established market positions and ample resources. RBV emphasizes the thoughtful utilization of internal capabilities to manage data breach impacts while preserving R&D spending. RBV allows businesses to prioritize long-term advantages by using internal strengths, even when external pressures imply otherwise, whereas signalling theory emphasizes external perceptions. The dynamic of maintaining internal and external resources is reflected in the decision to continue R&D to leverage resources or reduce R&D to signal stability. When businesses prioritize stakeholder confidence and external perceptions first, signalling theory takes centre stage. When businesses rely on their internal strengths to weather a crisis without changing their long-term strategies, RBV takes the stage.

Researchers can incorporate signalling theory and the RBV into post-breach decision-making frameworks to explore how firms strategically navigate crises. By demonstrating firms' use of resource reallocation as a non-verbal cue of stability, this study opens new avenues for research into reactive signalling. Future studies can extend this work by examining how diverse non-verbal signals can shape stakeholder views and aid in firm recovery. Furthermore, the RBV lens enables scholars to examine how a firm's capacity to absorb shocks and maintain long-term investment strategies. This dual-theory framework encourages researchers to investigate the push and pull between maintaining long-term competitive advantages and responding to short-term stakeholder expectations. The framework also promotes in-depth, industry-tailored studies to evaluate how the comparative impact of signalling versus internal resource management changes across sectors with distinct technological intensities and stakeholder sensitivities.

4.2 Managerial Implications

Our research also contains several managerial recommendations. Managers need to understand that a data breach disclosure frequently necessitates concentrating on operational stability and short-term risk reduction. We find that a reduction in R&D spending after the data breach incident may signal the stakeholders' need to manage the issues and lower risk. Firms should be transparent in their resource allocation strategies and maintain trust by openly connecting these strategies to improvements in security and stability. The formulation of a step-by-step plan to reinvest in R&D to prevent long-term competitive disadvantages, even when short-term R&D reductions may be required.

Even in the wake of a mandatory data breach disclosure such as Marriott's $52 million settlement with U.S. states and the FTC over cybersecurity failures (Kelleher, 2024), managers of service-oriented companies should prioritize safeguarding intangible assets such as human capital and client relationships by continuing R&D expenditures such as developing sustainable service models, workflow automation, digital transformation projects or the development of AI-driven anomaly detection tools to reduce breach detection time. They should prioritize innovation and continual improvement to keep their competitive edge because service companies mostly rely on dynamic knowledge-based capabilities. They should proactively convey to stakeholders that the company's continuous investment in R&D demonstrates its dedication to maintaining individualized services and quality, hence boosting trust in the company's flexibility. On the contrary, in high-tech firms, managers should give priority to crisis management and security enhancements to rebuild stakeholder faith swiftly. They should use well-thought-out PR campaigns to reassure partners, investors, and clients of the company's dedication to operational recovery and security. The temporary cutting of R&D spending and prioritizing urgent security measures communicates a positive message of risk management, which can boost stakeholder trust during that time.

The recent cyberattack on Marks & Spencer (M&S) highlights critical lessons for managers in adjusting R&D investments to mitigate reputational damage and restore customer trust (BBC News, 2025). In order to swiftly win back customer trust, managers of marketing-driven companies should prioritize brand rehabilitation by concentrating on cybersecurity enhancements and public outreach. They should draw attention to short-term remedial actions that stakeholders and customers can see right away, including enhanced security features or restitution for impacted parties. They should also prevent reputational harm and maintain market positioning, temporarily reallocating funds from long-term R&D to public relations and consumer engagement projects. In the case of high market value firms, managers should use their market leadership position to sustain R&D expenditures despite a data breach disclosure. They should assure stakeholders of the company's resilience and long-term foresight by explaining that its robust resource base enables it to handle crises without sacrificing long-term innovation. They should show confidence in the company's capacity to bounce back and expand by keeping a dual focus on fixing the breach and making strategic investments.

5 Conclusions

We investigate the impact of post-data breach disclosure phase data on firms' R&D spending. We find that firms spend less on research and development after a data breach disclosure. For businesses in the service sector, the effect of a data breach on R&D spending is less detrimental. A post-breach disclosure phase has a more detrimental effect on R&D spending for businesses in high-tech sectors. After a mandatory disclosure of a data breach, R&D spending decreases for companies with increased marketing intensity. For companies with substantial market value, the after-effect of a data leak on R&D spending is lessened.

Our research also has some limitations. We use a merged longitudinal database to support our hypotheses empirically. Researchers can conduct C-suite officers' interviews to gain more insight and provide a mixed-method study to expand this data breach-related research. Our focal firms are U.S. publicly traded firms. Researchers can collect data from privately held firms and expand the reach of this study. They can also collect data from emerging markets and extend this study by comparing developed economies with emerging markets. We integrate signalling theory and RBV framework to draw our conceptualization. Researchers can look for other frameworks that may provide a more nuanced understanding and help extend this research, which is crucial in the field of cybersecurity and management. We use the breach dataset of the U.S. publicly traded firms to provide empirical evidence for our hypotheses. Hence, this work can be extended by investigating the same effect on privately held firms or firms in different geographical regions, which can provide a deeper insight into the impact of mandatory data breach disclosures on innovation investments.

Appendix A1

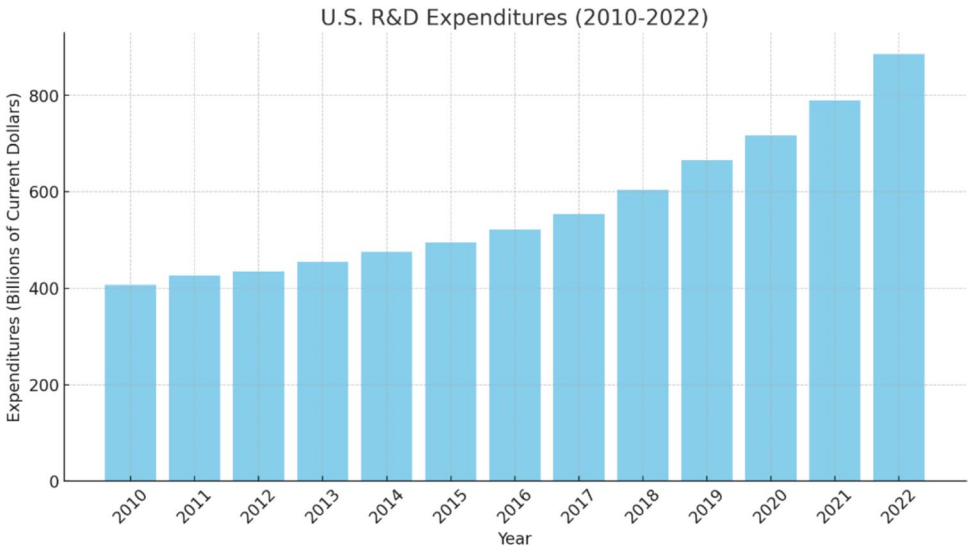

Fig. 4 Trend of U.S. R&D expenditures across all sectors (2010–2022) (https://ncses.nsf.gov/pubs/nsf24317)

Acknowledgements The authors would like to thank editors and anonymous reviewers for their contributions.

Authors' Contributions Each of the listed co-authors has contributed to this research paper meaningfully.

Funding There is no funding to report for this research.

Data Availability Requests for anonymised data and material can be made to the correspondence author.

Declarations

Ethics Approval and Consent to Participate This research has received full ethics approval and consent of participants.

Consent for Publication The authors give full consent for publication.

Competing interests The authors declare that they have no competing interests.

References

Agarwal, A., Lee, S. Y., & Whinston, A. B. (2024). The effect of popularity cues and peer endorsements on assertive social media ads. *Information Systems Research*. https://doi.org/10.1287/isre.2021.0606

Albarrak, M. S., Elnahass, M., Papagiannidis, S., & Salama, A. (2020). The effect of Twitter dissemination on cost of equity: A big data approach. *International Journal of Information Management,50*, 1–16.

Alraja, M. N., Imran, R., Khashab, B. M., & Shah, M. (2022). Technological innovation, sustainable green practices and SMEs sustainable performance in times of crisis (COVID-19 pandemic). *Information Systems Frontiers, 24*(4), 1081–1105.

Bachura, E., Valecha, R., Chen, R., & Rao, H. R. (2022). The OPM data breach: An investigation of shared emotional reactions on Twitter. *MIS Quarterly, 46*(2), 881–910.

Bae, J., Kim, S. J., & Oh, H. (2017). Taming polysemous signals: The role of marketing intensity on the relationship between financial leverage and firm performance. *Review Of Financial Economics,33*, 29–40.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99–120.

Barnichon, R., Matthes, C., & Ziegenbein, A. (2022). Are the effects of financial market disruptions big or small? *Review Of Economics And Statistics,104*(3), 557–570.

Baumann, E., Kern, J., & Lessmann, S. (2022). Usage continuance in software-as-a-service. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-020-10065-w

Beard, J. W., & Sumner, M. (2004). Seeking strategic advantage in the post-net era: Viewing ERP systems from the resource-based perspective. *The Journal of Strategic Information Systems, 13*(2), 129–150.

Bergh, D. D., Connelly, B. L., Ketchen, D. J., Jr., & Shannon, L. M. (2014). Signalling theory and equilibrium in strategic management research: An assessment and a research agenda. *Journal of Management Studies, 51*(8), 1334–1360.

Bhargava, V. R. (2020). Firm responses to mass outrage: Technology, blame, and employment. *Journal of Business Ethics, 163*(3), 379–400.

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Rao, H. R. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems, 83*, 47–56.

Chen, K., Li, X., Luo, P., & Zhao, J. L. (2021). News-induced dynamic networks for market signaling: Understanding the impact of news on firm equity value. *Information Systems Research, 32*(2), 356–377.

Chuang, S. H., & Lin, H. N. (2017). Performance implications of information-value offering in e-service systems: Examining the resource-based perspective and innovation strategy. *The Journal of Strategic Information Systems, 26*(1), 22–38.

Chung, S., Han, K., Animesh, A., & Pinsonneault, A. (2024). Strategic utilization of software patents to counteract rival penetration in the IT industry. *The Journal of Strategic Information Systems, 33*(1), Article 101820.

Connelly, B. L., Certo, S. T., Reutzel, C. R., DesJardine, M. R., & Zhou, Y. S. (2025). Signaling theory: State of the theory and its future. *Journal of Management, 51*(1), 24–61.

D'Arcy, J., & Basoglu, A. (2022). The influences of public and institutional pressure on firms' cybersecurity disclosures. *Journal of the Association for Information Systems,23*(3), 779–805.

D'Arcy, J., Adjerid, I., Angst, C. M., & Glavas, A. (2020). Too good to be true: Firm social performance and the risk of data breach. *Information Systems Research, 31*(4), 1200–1223.

Fowler, K. (2016). *Data breach preparation and response: Breaches are certain, impact is not*. Syngress.

Stevens, G. M. (2012). *Data security breach notification laws*. Congressional Research Service.

Davig, T., Leeper, E. M., & Walker, T. B. (2011). Inflation and the fiscal limit. *European Economic Review, 55*(1), 31–47.

Dias, A. (2013). Market capitalization and value-at-risk. *Journal of Banking & Finance,37*(12), 5248–5260.

Du, Y., Kim, P. H., Fourné, S. P., & Wang, X. (2022). In times of plenty: Slack resources, R&d investment, and entrepreneurial firms in challenging institutional environments. *Journal of Business Research, 145*, 360–376.

Ferratt, T. W., Agarwal, R., Brown, C. V., & Moore, J. E. (2005). It human resource management configurations and IT turnover: Theoretical synthesis and empirical analysis. *Information Systems Research, 16*(3), 237–255.

Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020). Understanding the full cost of cyber security breaches. *Computer Fraud & Security,2020*(12), 6–12.

Germann, F., Ebbes, P., & Grewal, R. (2015). The chief marketing officer matters! *Journal of Marketing, 79*(3), 1–22.

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action. *MIS Quarterly, 41*(3), 703-A16.

Guenther, P., & Guenther, M. (2022). Can B2B firms benefit from competitors' advertising? A dynamic business environment perspective on an emerging communication form. *Industrial Marketing Management, 102*, 252–265.

Guest, D. E., Sanders, K., Rodrigues, R., & Oliveira, T. (2021). Signalling theory as a framework for analysing human resource management processes and integrating human resource attribution theories: A conceptual analysis and empirical exploration. *Human Resource Management Journal, 31*(3), 796–818.

He, C. Z., Frost, T., & Pinsker, R. E. (2020). The impact of reported cybersecurity breaches on firm innovation. *Journal of Information Systems, 34*(2), 187–209.

Hillman, D., Harel, Y., & Toch, E. (2023). Evaluating organizational phishing awareness training on an enterprise scale. *Computers & Security,132*, Article 103364.

Ho, Y. K., Xu, Z., & Yap, C. M. (2004). R&D investment and systematic risk. *Accounting & Finance,44*(3), 393–418.

Huang, C. K., Wang, T., & Huang, T. Y. (2020). Initial evidence on the impact of big data implementation on firm performance. *Information Systems Frontiers, 22*(2), 475–487.

Jabr, W., Mookerjee, R., Tan, Y., & Mookerjee, V. S. (2014). Leveraging philanthropic behavior for customer support: The case of user support forums. *MIS Quarterly, 38*(1), 187–208.

Jayaraman, S., & Wu, J. S. (2019). Is silence golden? Real effects of mandatory disclosure. *The Review of Financial Studies, 32*(6), 2225–2259.

Jha, A. K., & Bose, I. (2021). Linking drivers and outcomes of innovation in IT firms: The role of partnerships. *Information Systems Frontiers, 23*(6), 1593–1607.

Jha, A. K., & Verma, N. K. (2023). Social media sustainability communication: An analysis of firm behaviour and stakeholder responses. *Information Systems Frontiers, 25*(2), 723–742.

Kapoor, K. K., Dwivedi, Y. K., & Williams, M. D. (2015). Examining the role of three sets of innovation attributes for determining adoption of the interbank mobile payment service. *Information Systems Frontiers, 17*, 1039–1056.

Khan, F., Kim, J. H., Mathiassen, L., & Moore, R. (2021). Data breach management: An integrated risk model. *Information and ManagemeNt, 58*(1), Article 103392.

Kim, K., Mithas, S., & Kimbrough, M. (2017). Information technology investments and firm risk across industries. *MIS Quarterly, 41*(4), 1347–1368.

Kim, J. Y., Sim, J., & Cho, D. (2023). Identity and status: When counterspeech increases hate speech reporting and why. *Information Systems Frontiers, 25*(5), 1683–1694.

Lee, Y. J., Keeling, K. B., & Urbaczewski, A. (2019). The economic value of online user reviews with ad spending on movie box-office sales. *Information Systems Frontiers, 21*, 829–844.

Lee, J., de Guzman, M. C., Wang, J., Gupta, M., & Rao, H. R. (2022). Investigating perceptions about risk of data breaches in financial institutions: A routine activity-approach. *Computers & Security,121*, Article 102832.

Lev, B., & Sougiannis, T. (1996). The capitalization, amortization, and value-relevance of R&D. *Journal of Accounting and Economics,21*(1), 107–138.

Lockett, A., Thompson, S., & Morgenstern, U. (2009). The development of the resource-based view of the firm: A critical appraisal. *International Journal of Management Reviews, 11*(1), 9–28.

Mahoney, J. T., & Pandian, J. R. (1992). The resource-based view within the conversation of strategic management. *Strategic Management Journal, 13*(5), 363–380.

Mazzucato, M., & Tancioni, M. (2012). R&D, patents and stock return volatility. *Journal of Evolutionary Economics,22*(4), 811–832.

Miller, A. R., & Tucker, C. E. (2011). Encryption and the loss of patient data. *Journal of Policy Analysis and Management, 30*(3), 534–556.

Mughal, A. A. (2018). The Art of Cybersecurity: Defense in Depth Strategy for Robust Protection. *International Journal of Intelligent Automation and Computing, 1*(1), 1–20.

Muniz, J., & Lakhani, A. (2018). *Investigating the cyber breach: the digital forensics guide for the network engineer*. Cisco Press.

Newbert, S. L. (2008). Value, rareness, competitive advantage, and performance: A conceptual-level empirical investigation of the resource-based view of the firm. *Strategic Management Journal,29*(7), 745–768.

Nikkhah, H. R., & Grover, V. (2022). An empirical investigation of company response to data breaches. *MIS Quarterly,46*(4), 2163–2196.

Pan, X., Guo, S., & Chu, J. (2021). P2P supply chain financing, R&d investment and companies' innovation efficiency. *Journal of Enterprise Information Management,34*(1), 578–597.

Papasolomou, I., Thrassou, A., Vrontis, D., & Sabova, M. (2014). Marketing public relations: A consumer-focused strategic perspective. *Journal of Customer Behaviour, 13*(1), 5–24.

Porter, M. E. (2008). *Competitive Advantage: Creating and Sustaining Superior Performance*. Simon and Schuster.
Price, J. D. (2014). *Reducing the risk of a data breach using effective compliance programs*. Walden University.
Quelch, J. A., & Jocz, K. E. (2007). *Greater good: How good marketing makes for better democracy*. Harvard Business Press.
Rahmati, P., Tafti, A., Mithas, S., & Sachdev, V. (2021). How does the positioning of information technology firms in strategic alliances influence returns to R&D investments? *Journal of the Association for Information Systems, 22*(2), 6.
Raman, R., Aljafari, R., Venkatesh, V., & Richardson, V. (2022). Mixed-methods research in the age of analytics, an exemplar leveraging sentiments from news articles to predict firm performance. *International Journal of Information Management, 64*, Article 102451.
Rao, H. R., & Upadhyaya, S. (2009). *Information assurance, security and privacy services*. Emerald Group Publishing.
Rashid, A., & Saeed, M. (2017). Firms' investment decisions-explaining the role of uncertainty. *Journal of Economic Studies, 44*(5), 833–860.
Rosati, P., Cummins, M., Deeney, P., Gogolin, F., Van der Werff, L., & Lynn, T. (2017). The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis,49*, 146–154.
Salge, T. O., Antons, D., Barrett, M., Kohli, R., Oborn, E., & Polykarpou, S. (2022). How IT investments help hospitals gain and sustain reputation in the media: The role of signaling and framing. *Information Systems Research, 33*(1), 110–130.
Saunders, A., & Brynjolfsson, E. (2016). Valuing information technology related intangible assets. *MIS Quarterly, 40*(1), 83–110.
Sharma, P., & Barua, S. (2023). From data breach to data shield: The crucial role of big data analytics in modern cybersecurity strategies. *International Journal of Information and Cybersecurity, 7*(9), 31–59.
Spence, M. (1973). Job market signaling. *Quarterly Journal of Economics, 87*, 355–374.
Spence, M. (1974). Competitive and optimal responses to signals: An analysis of efficiency and distribution. *Journal of Economic Theory, 7*(3), 296–332.
Srinivasan, R., Lilien, G. L., & Sridhar, S. (2011). Should firms spend more on research and development and advertising during recessions? *Journal of Marketing, 75*(3), 49–65.
Srivastava, R. K., Shervani, T. A., & Fahey, L. (1998). Market-based assets and shareholder value: A framework for analysis. *Journal of Marketing, 62*(1), 2–18.
Sun, X., Zhang, Y., & Feng, J. (2024). Impact of online information on the pricing and profits of firms with different levels of brand reputation. *Information and ManageMeNt, 61*(1), Article 103882.
Syed, R. (2019). Enterprise reputation threats on social media: A case of data breach framing. *The Journal of Strategic Information Systems, 28*(3), 257–274.
Talmor, E., & Wallace, J. S. (1998). Computer industry executives: An analysis of the new barons' compensation. *Information Systems Research, 9*(4), 398–414.
Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal, 18*(7), 509–533.
Thaduri, A., Aljumaili, M., Kour, R., & Karim, R. (2019). Cybersecurity for emaintenance in railway infrastructure: Risks and consequences. *International Journal of System Assurance Engineering and Management, 10*, 149–159.
Wang, J., Xiao, N., & Rao, H. R. (2010). Drivers of information security search behavior: An investigation of network attacks and vulnerability disclosures. *ACM Transactions on Management Information Systems, 1*(1), 1–23.
Westland, J. C. (2022). Assessing privacy and security of information systems from audit data. *Information Systems Frontiers, 24*(5), 1417–1434.
Wolff, J., & Atallah, N. (2021). Early GDPR penalties: Analysis of implementation and fines through May 2020. *Journal of Information Policy, 11*, 63–103.
Baatwah, S. R., Asiri, M., Bajaher, M. S., Alyafai, A., & Baajajah, S. (2025). Thriving post-cyberattacks: the power of control, disclosure, and IT maturity. *Electronic Commerce Research*, 1–39.
Basu, B., Sebastian, M. P., & Kar, A. K. (2024). What Affects User Experience of Shared Mobility Services? Insights from Integrating Signaling Theory and Value Framework. *Information Systems Frontiers*, 1–23.
Cofone, I. N. (Ed.). (2021). *Class Actions in Privacy Law*. Routledge.
Kelleher, S. R. (2024). Marriott gets $52 million slap on wrist for breaches due to 'lax security'. Forbes, Accessed from the web link [29th April 2025] https://www.forbes.com/sites/suzannerowankelleher/2024/10/10/marriott-52-million-slap-wrist-cybersecurity-breaches-lax-security/
BBC News. (2025). Why is the M&S cyber-attack chaos taking so long to resolve? https://www.bbc.co.uk/news/articles/cz79547nywno, Accessed on 29th April 2025.

Ashutosh Singh is a Lecturer in Marketing at Leeds University Business School. He holds a PhD in Marketing from the University of Central Florida (USA). He has BSc and MSc degrees in Economics from the Indian Institute of Technology Kanpur (India). His broad research focus is in the area of Marketing Strategy, where he uses analytical and empirical models to solve relevant marketing problems and eventually provide actionable guidance to managers. His substantive research interests lie in the areas of designing strategies for a marketing executive's job and digital platforms.

Nripendra P. Rana is a Professor of Digital Marketing and Systems at the Queen's Business School, Queen's University Belfast, UK. His current research interests focus primarily on adoption and diffusion of emerging ICTs, e-commerce, m-commerce, digital and social media marketing and the role of artificial intelligence on the consumer decision-making and behaviour. He has published more than 400 papers in a range of leading academic journals, conference proceedings, books, etc. Some of such journals where his papers got published include British Journal of Management, European Journal of Information Systems, Annals of Tourism Research, Public Management Review, European Journal of Marketing, Journal of Sustainable Tourism, and International Journal of Information Management to name a few.

Xuan Huang is an Assistant Professor in Marketing and Innovation at the Nottingham University Business School China. Prior to this, she was a Lecturer in Marketing at University of Leeds. She obtained a PhD degree in Marketing from University of Leeds. She has publications in journals such as Journal of International Marketing and Journal of Business Research. She also serves as a reviewer for many academic journals, including Journal of Business Research, Psychology & Marketing, and Technovation.

Neha Dubey is currently doing her PhD at the Department of Management and Marketing in the Greenwich Business School at University of Greenwich. After exploring the nuances of English Literature in her first master's degree, she transitioned into the dynamic realm of Marketing. She is primarily interested in Services Marketing, Consumer Behaviour and Digital Transformation.