The impact of managerial myopia on cybersecurity: Evidence from data breaches

Wen Chen [a], Xing Li [b,*], Haibin Wu [a], Liandong Zhang [c]

[a] City University of Hong Kong, Hong Kong, China
[b] Xi'an Jiaotong University, China
[c] Singapore Management University, Singapore

Published in Journal of Banking and Finance (2024) 166. DOI: 10.1016/j.jbankfin.2024.107254

Abstract: Using a sample of U.S. firms for the period 2005–2017, we provide evidence that managerial myopic actions contribute to corporate cybersecurity risk. Specifically, we show that abnormal cuts in discretionary expenditures, our proxy for managerial myopia, are positively associated with the likelihood of data breaches. The association is largely driven by firms that appear to cut discretionary expenditures to meet short-term earnings targets. In addition, the association is stronger for firms with greater short-term equity incentives, higher earnings response coefficients, low levels of institutional block ownership, or large market shares. Finally, firms appear to increase discretionary expenditures upon the announcement of data breaches by their industry peers.

Keywords: Cybersecurity, Data breach, Real earnings management, Managerial myopia, Discretionary expenditures, Peer effect

1. Introduction

In the past decade, companies worldwide have witnessed steady growth in both the frequency and cost of data breaches. According to the Identity Theft Resource Center (2018), the number of data breaches in the United States increased nearly eightfold between 2005 and 2018, from 157 to 1244. The Ponemon Institute (2019) estimates that the average cost of data breaches involving less than one million, more than one million, and 50 million compromised records is $8.19 million, $42 million, and $388 million, respectively, for U.S. companies in 2019. For a sample of public firms experiencing cyberattacks, Kamiya et al. (2021) show that the average loss of market value for each firm over a three-day window around the data breach announcement is approximately $495 million. Risk management professionals have recently ranked cybersecurity risk as one of the foremost business risks (Allianz, 2019). In this study, we explore myopic managerial behavior as a potential factor contributing to cybersecurity risk. We define cybersecurity risk as the risk stemming from the theft or damage of hardware, software, or electronic data, as well as from the disruption or misdirection of the services provided by a company's information technology (IT) system.[1]

Corporate competitive success increasingly depends on investments in intangible assets, such as human capital and technology capabilities (Porter, 1992; Zingales, 2000). However, classical myopia theories suggest that managers fail to invest because these investments tend to depress short-term earnings performance and thus current share prices (e.g., Stein, 1989; Edmans, 2009). In a survey of more than 400 executives, Graham et al. (2005) find that 80% reported that they would decrease discretionary spending on intangibles to meet short-term earnings targets. Several studies provide consistent empirical evidence of such myopic corporate behavior as well as their negative

[1] https://en.wikipedia.org/wiki/Computer_security

We appreciate the helpful comments of Amanda Aw Yong, Richard Crowley, Yuyan Guan, Sterling Huang, Lakshmanan Shivakumar, and seminar participants at Chinese University of Hong Kong (Shenzhen), City University of Hong Kong, Hong Kong, China, and the 2019 Boya Research Forum of Beijing University.

W. Chen and H. Wu acknowledge financial support from City University of Hong Kong, Hong Kong, China. L. Zhang acknowledges financial support from the Lee Kong Chian Professorship. X. Li acknowledges financial support from the Chinese National Natural Science Foundation (72302180). * Corresponding author. E-mail address: xings.li@xjtu.edu.cn (X. Li)

consequences (e.g., Roychowdhury, 2006; Bhojraj et al., 2009; Cohen and Zarowin, 2010; Gunny, 2010; Kothari et al., 2016). Our study extends this line of research by analyzing the impact of managerial myopia on corporate cybersecurity.

The protection of systems, networks, and data in cyberspace requires continuous investments in self-developed or third-party-procured defensive technologies, as well as the timely upgrading and maintenance of the system. It also requires investments in human capital in the form of hiring and training cybersecurity professionals and the continuous training of non-IT employees in data security principles to avoid becoming victims of social engineering[2] and accidental data leaks (Huang and Wang, 2021). Some industry reports show that a significant proportion of data breaches are caused by human error.[3] However, myopic managers can underinvest in cybersecurity expenditures such as research and development (R&D), software, and employee recruitment and training, because of their negative impact on current earnings,[4] as revealed by Graham et al. (2005). Thus, to the extent that managers engage in cybersecurity-related underinvestment, cybersecurity risks are expected to increase. Echoing our conjecture, several recent surveys of IT risk professionals suggest that lack of budget, personnel, and tools are among the major threats to cybersecurity and companies need to balance initiatives that are profit-maximizing and those that enhance cybersecurity (New York Stock Exchange, 2014; Black Hat, 2015).

To examine the impact of managerial myopia on cybersecurity risk, we obtain records of corporate data breaches from the Privacy Rights Clearinghouse (PRC) database. To capture managerial myopia (Stein, 1989; Roychowdhury et al., 2019), we focus on myopic managerial behavior and use the abnormal cuts in discretionary expenditures (Roychowdhury, 2006; Chen et al., 2015).[5] The discretionary expenditures, in this context, are defined as the sum of R&D and selling, general, and administrative (SG&A) expenses, which include employee training, maintenance expenditure, and software subscription fees, i.e., the expense items likely to be booked if firms engage in cybersecurity investment.[6]

Using a panel of 28,325 firm–year observations from 2005 to 2017, we find that abnormal cuts in discretionary expenditures are significantly and positively associated with the likelihood of data breaches. Specifically, a one-standard-deviation increase in abnormal cuts in discretionary expenditures increases the likelihood of data breaches from 1.8 %, the sample mean of the unconditional probability of data breaches for our sample, to 2.23 %. Additional tests show that more abnormal cuts in discretionary expenditures lead to more severe data breaches.

To alleviate the concern of correlated omitted variables, we examine the impact of the different components of discretionary expenditures on data breaches. We find that abnormal cuts in both R&D and SG&A increase the likelihood of future data breaches. Additional results show no evidence that abnormal levels of advertising expenses, another type of discretionary expenditure that is unlikely to affect cybersecurity directly, are related to data breaches.

The measures of abnormal cuts in discretionary expenditures, though capturing deviations from normal business practice, could still be endogenous and reflect efficient investment or operating decisions instead. To enhance our identification of managerial myopia, we perform two robustness checks. First, we employ an outcome measure for firms' short-termism to better identify the myopic firms. Specifically, we identify a group of suspect firms that have marginally met or beaten earnings targets at least once during the past three years (e.g., Bhojraj et al., 2009). Prior studies have shown that this group of firms has a higher likelihood of engaging in myopic behavior (e.g., Caskey and Ozel, 2017). We find that abnormal cuts in discretionary expenditures increase the likelihood of future data breaches only for the suspect firms. Second, we exclude internal data breaches from our analysis and continue to find a negative impact of abnormal cuts of discretionary expenditures on firm cybersecurity.

To further describe the effect of managerial myopia on cybersecurity risk, we conduct several cross-sectional analyses related to managerial benefits and the capability of engaging in myopic actions (Eldenburg et al., 2011; Roychowdhury et al., 2019). First, several studies show that equity incentives are related to myopic behavior (e.g., Bergstresser and Philippon, 2006; Peng and Roell, 2008; Kim et al., 2011; Edmans et al., 2017). We expect and find that the relation between abnormal cuts in discretionary expenditures and the likelihood of data breaches is amplified and only significant for firms with higher short-term equity incentives. Second, using the earnings response coefficient (ERC) to capture the stock market's reliance on earnings, we find that the impact of abnormal cuts in discretionary expenditures on the risk of data breaches is largely driven by firms with high ERCs. Third, prior literature suggests that the presence of institutions and blockholders mitigates the managerial myopia problem (e.g., Bushee, 1998; Edmans, 2009; Aghion et al., 2013). We find that the impact of abnormal cuts in discretionary expenditures on the likelihood of data breaches is consistently weaker for firms with greater block ownership. Lastly, we predict and find that the effect of abnormal cuts in discretionary expenditures on data breach risks is stronger for market leaders, as it is more affordable for them to behave myopically (e.g., Zang, 2011).

In a final test, we examine the potential spillover effects of data breaches on peer firms' myopic actions. We find that industry peers that engage in more myopic activities increase their abnormal expenditure related to cybersecurity after the announcement of data breaches by the focal firms, suggesting a learning effect and corrective action to avoid data breaches in the future.

Our research is related to the literature on managerial myopia.[7] Prior literature provides ample evidence that managerial myopia in the form of cutting discretionary expenditures is both pervasive and detrimental to long-run shareholder value.[8] Given that cybersecurity is increasingly critical for corporate competitiveness, our study extends this line of research by focusing on the adverse short-term consequences of managerial myopia in the form of data breaches. Data breaches not only impose a loss on shareholders but also threaten the privacy and

[2] Social engineering is the act of tricking someone into divulging information or taking action, usually through technology (https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html).

[3] https://www.tessian.com/research/the-state-of-data-loss-prevention-2020/

[4] In the U.S., most of these expenditures should be reported as part of R&D expenses or selling, general, and administrative (SG&A) expenses (e.g., labor, training, and maintenance) in the income statement. The amortization of software costs is also included in SG&A if the software is not revenue-generating.

[5] While prior studies use changes in investments to proxy myopic behavior (e.g., Bhojraj, et al., 2009; Bushee, 1998; Edmans et al., 2017), changes in firm tangible investments are unlikely to capture firms' underinvestment in cybersecurity, in contrast to the discretionary expenditure measure, which includes R&D investment and other cybersecurity-relevant items as explained in footnote 4.

[6] For example, Microsoft is reported to be investing over $1 billion annually in cybersecurity R&D in future years (https://www.reuters.com/article/us-tech-cyber-microsoft-idUSKBN15A1GA). Murphy USA Inc. stated in a press release that it includes investments in IT-related enhancements in its SG&A costs (http://ir.corporate.murphyusa.com/investor-relations/news-releases/press-release-details/2018/Murphy-USA-Inc-Reports-Preliminary-Fourth-Quarter-2017-Results/default.aspx).

[7] See Stein (2003) and Roychowdhury et al. (2019) for reviews of the theoretical and empirical literature on corporate myopia.

[8] Prior studies find that myopic operating decisions (proxied by the cutting of discretionary expenditures) lead to overvaluation around security issuance, long-term performance deterioration, and an increasing rate of employee injury or illness (Cohen and Zarowin, 2010; Kothari et al., 2016; Bhojraj et al., 2009; Caskey and Ozel, 2017).

economic well-being of other stakeholders, which makes cybersecurity a social issue and a core consideration in the environmental, social, and governance (ESG) framework.[9] Our study highlights the importance of companies engaging in cyber risk minimization, consistent with the role of firms in addressing other ESG issues, including climate change (e.g., Bolton and Kacperczyk, 2023).

Our paper is related to Xu et al. (2019) but differs in a number of ways. First, they study the change in firm earnings management behavior *after* data breaches. We use real earnings management as a proxy for myopia and treat it as a determinant of the occurrence of data breaches. Second, while Xu et al. (2019) focus on the breached firms, we also show a spillover effect of focal firms' data breaches on the corrective actions of myopic, non-breached peer firms (Ashraf, 2022).

Our study is also related to the literature on cybersecurity and cyber risk management. Much of the literature focuses on the negative valuation effects of cybersecurity events (e.g., Johnson et al., 2017; Akey et al., 2018) and has paid relatively less attention to the determinants of cybersecurity risk. Kamiya et al. (2021) conducted a preliminary study of the factors contributing to firm cybersecurity risk. Our research supplements theirs by demonstrating managerial myopia as another potential contributing factor.

Finally, our findings have important implications for regulators and industry practitioners. In the past decade, the Securities and Exchange Commission (SEC) has expanded its Crypto Assets and Cyber Unit and has brought enforcement actions against several registrants for failing to maintain adequate cybersecurity controls and for failing to appropriately disclose cyber-related risks and incidents. Our research echoes the concern of the SEC on corporate cybersecurity risk and suggests the unneglectable role of managerial myopia in driving data breaches. More importantly, our study highlights the importance of effective corporate governance in cybersecurity risk management. Specifically, our research suggests that the board of directors should pay particular attention to the potential implications of cutting discretionary expenditures on cybersecurity risk and data breaches.

2. Background, data, and research design

2.1. Background and the PRC database

Cybersecurity risk refers to the risk stemming from the theft or damage of hardware, software, or electronic data, as well as from the disruption or misdirection of the services provided by a company's IT system. In this paper, we focus on a specific and important manifestation of cybersecurity risk: data breaches. The Ponemon Institute (2019) identifies four types of costs related to data breaches: detection costs, which include costs related to investigative and forensic activities; notification costs, which include the costs of notifying data subjects and communications with regulators; post-breach response costs, which include legal expenditure and regulatory interventions (fines), as well as costs related to the recovery of services; and costs related to the loss of business, which include the costs of the disruption of business, lost customers and business-sensitive information, reputation loss, and diminished goodwill. The Ponemon Institute (2019) suggests that lost business is the biggest contributor to data breach costs, and data breaches can affect organizations for years.

In terms of the number of lost records, the data breach of Yahoo is the largest to date. In 2013–2014, Yahoo experienced two major data breaches, affecting over one billion active user accounts and leading to a leak of sensitive information including names, telephone numbers, dates of birth, encrypted passwords, and unencrypted security questions.[10] Two years later, in 2016, Yahoo announced the data breach after Verizon agreed to acquire Yahoo. The announcement slashed $350 million off the initial offering price of the acquisition.[11] Due to the delayed disclosure, Yahoo's holding company, Altaba, agreed to pay a $35 million penalty to the SEC.[12] In 2022, Yahoo and Aabaco Small Business, the co-defendant, proposed to settle the class action lawsuit for $117.5 million.[13] The Yahoo case is certainly not the only high-profile data breach. The data breaches of Capital One, Equifax, Marriott, and Target Corporation are prominent examples of the severity and cost of mega large data breaches in recent years. For instance, for a data breach that affected nearly 150 million Americans in 2017, Equifax recently announced a settlement agreement of up to $700 million with the Federal Trade Commission, the Consumer Financial Protection Bureau, and 50 U.S. states and territories.[14]

In the U.S., firms experiencing data breaches are required by state security breach notification laws to inform affected state residents about their information being compromised. By 2018, all 50 states and Washington, D.C., Guam, Puerto Rico, and the Virgin Islands had adopted the law.[15] In addition, the SEC requires public companies to disclose "materially important" cybersecurity risks and incidents in form 8-K filings according to cybersecurity disclosure guidance. Moreover, the 1996 Privacy Rule of the Health Insurance Portability and Accountability Act requires firms to report breaches of unsecured protected health information to the Secretary of the U.S. Department of Health and Human Services. In our research, we obtained information on data breach events from the PRC database. The PRC collects information on data breaches and the number of records breached reported through either government agencies or verifiable media sources since 2005. One advantage of using the PRC data is the alleviation of the potential sample underreporting issue compared to other available data breach databases (Kamiya et al., 2021). Unlike other databases, the PRC database is limited to data breaches in which individuals in the U.S. are affected.

2.2. Sample

Our sample begins with all firm–year observations shared by Compustat and the Center for Research in Security Prices (CRSP) for the period 2005 to 2017. We start in 2005 because it is the first year in which PRC data are available. From this initial sample, we remove financial and utilities industries (with Standard Industrial Classification codes 6000–6900 and 4900–4999, respectively) because financial reporting rules, especially reporting for discretionary expenditures, are different for these regulated industries.[16] We also remove small firms with total assets below $50 million to mitigate the small denominator problem. The PRC database contains the following information regarding data breaches: the date of the breach known by the public, the name of the company breached, and the number of breached data records. We manually checked the dates when the data breach events occurred (rather than when they were known to the public) and use the occurrence dates for the event period identification.[17] Next, we match the PRC organization names with firm names reported in the Compustat database. Following Kamiya et al. (2021), a firm is also treated as a

[9] https://www.jpmorgan.com/insights/esg/governance-strategies/why-is-cybersecurity-important-to-esg

[10] *The New York Times*, December 14, 2016.

[11] *The New York Times*, February 21, 2017.

[12] SEC Press Release, 2018-71.

[13] https://yahoodatabreachsettlement.com/

[14] *The Wall Street Journal*, July 23, 2019.

[15] Appendix A of Kamiya et al. (2021) summarizes the effective dates of the law for each state.

[16] Our results are not sensitive to the inclusion of the financial and utilities industries.

[17] We use news reports and press releases to identify the dates of data breach occurrences, which could be different from the data breach announcement dates recorded in PRC database. For example, Yahoo's case was made public in December 2016 from the PRC database, and we verify by online searching that the two disclosed breaches occurred in 2013 and 2014.

breached firm if a breach event happens in its unlisted subsidiaries. After further requirements regarding the availability of financial data to calculate our independent and control variables, we are left with a final sample of 28,325 firm–year observations over the period 2005–2017.

For our final sample, we identify 507 data breach events. We retain data breaches caused by both external and internal factors for our main analysis.[18] Table 1 presents the distributions of data breaches by year (Panel A), industry (Panel B), and breach type (Panel C).[19] In Panel A, there is no obvious trend in terms of the number and the average record loss of reported data breaches over time for our Compustat firms.[20] In Panel B, the business service industry experiences the most data breaches (96 breaches) and the highest average level of lost records (198 million), followed by the health service (63 breaches) and communication (40 breaches) industries. In Panel C, we follow the PRC classification of data breach types and present the distribution by type. The most common type of data breach is hacking or malware (135 breaches, 26.63 % of all breaches), followed by the loss or theft of portable devices (102 breaches, 20.12 %). Hacking or malware results in the greatest data loss among all the breach types, with an average of 244.8 million lost records.

In Table 1, Panel D, we present the mean and median cumulative market-adjusted returns around the announcement dates of the data breaches for our sample. Using either the value- or equal-weighted CRSP index return as the market return proxy, the average abnormal return ranges from −0.2 % to −0.6 % when measured over the windows (−1, +1), (−2, +2), and (−5, +5) days. All these cumulated abnormal returns are significantly different from zero. The magnitudes of the market reactions are slightly smaller than those reported by Kamiya et al. (2021), which focus only on data breaches caused by external cyberattacks and are more likely to have extreme record losses (as shown in Panel C of Table 1).

2.3. Research design

To examine how cuts in discretionary expenditures affect the likelihood of data breaches, we estimate the following linear probability model :[21]

$$Breach_{i,t} = \alpha_0 + \beta_1 * Avg\_ADisc_{i,t-1} + \beta_2 * Avg\_AAccr_{i,t-1} + \gamma' X_{i,t} + f_i + \mu_t + \varepsilon_{i,t} \quad (1)$$

where the subscripts i and t denote the firm i and year t, respectively. The dependent variable *Breach* is an indicator variable that takes the value of one if the firm experiences data breach events in the year, and zero otherwise. The key independent variable of interest, *Avg_ADisc*, is the average abnormal cut in discretionary expenses (*ADisc*) over the three-year period from year $t-3$ to year $t-1$.[22] We use the aggregate measure over the past three years to capture the accumulated underinvestment and accommodate the theory that it takes time for the effect of myopic cuts in discretionary expenditures on cybersecurity to manifest in incidents of data breaches (Hutton et al., 2009).[23]

We estimate annual abnormal discretionary expenditures using a modified model developed by Roychowdhury (2006) to proxy for managerial myopic actions following prior studies (e.g., Asker et al., 2015; Acharya and Xu, 2017). The discretionary expenditures include R&D, SG&A, and advertising expenses. Corporate investments in cybersecurity are likely reflected in R&D and SG&A expenses. R&D expenses are direct expenditures on developing, designing, and enhancing a company's products, services, technologies, or processes. SG&A expenses comprise all direct and indirect selling costs, operational overhead costs, and administrative expenses; in particular, training, labor, software subscription fees, and amortization of non-revenue-generating software are all included. If firms develop their own technologies to deter the risk of data breaches and enhance system safety, then the related expenditure may be reported as R&D expenses. If firms choose to purchase cybersecurity services from third-party vendors, then the software purchase and employee training expenditures will be accounted as SG&A expenses. On the other hand, commercial advertising expenses are the costs of marketing and advertisement and are less likely to have any direct relation to cybersecurity investment. Therefore, we modify the model by using only the R&D and SG&A expenses and excluding advertising expenses from the estimation to better isolate the effect of managerial myopic cutting on firm data breach risk.[24] Specifically, we estimate the following equation for each industry–year, with the requirement of at least 20 observations for each regression:

$$\frac{Disc_{i,t}}{Asset_{i,t-1}} = \alpha_0 + \alpha_1 * \frac{1}{Asset_{i,t-1}} + \alpha_2 * \frac{Sales_{i,t-1}}{Assets_{i,t-1}} + \varepsilon_{i,t} \quad (2)$$

where *Disc* is discretionary expenditures, which is the sum of R&D expenses and SG&A expenses; *Assets* is total assets; and *Sales* is total sales revenue. The residuals from regression (2) are our proxy for abnormal discretionary expenditures (*ADisc*). A negative residual indicates that the actual expenditure falls short of the predicted level and represents an abnormal cut in discretionary expenditures. To facilitate interpretation, we multiply *ADisc* by −1. Consequently, we expect firms with more abnormal cuts in discretionary expenditures (i.e., high values of *ADisc*) to have a higher likelihood of data breaches, i.e., a *positive* coefficient on β_1 in Eq. (1).

Broadly speaking, managerial myopia also includes efforts to manage earnings using the flexibility embedded in accounting standards (Healy and Wahlen, 1999). However, the manipulation of reported earnings using accounting accruals is unlikely to affect a firm's cybersecurity. In our regression, we include a measure of accrual manipulation to determine whether this is the case. In addition, a nil effect of accrual manipulation on cybersecurity risk can serve as a falsification test, which helps rule out the possibility that our results are directly driven by some underlying cause of managerial myopia and not the myopic actions themselves (i.e., cutting discretionary expenditures).

To capture accrual manipulation, we use average abnormal accruals over the past three years (*Avg_AAccr*), where annual abnormal accruals are estimated using the modified Jones model (Dechow et al., 1995). Again, we require at least 20 observations for each industry–year for the regression:

[18] Managers' myopic cuts in discretionary expenditures, such as employee training, could lead to an increase in the likelihood of data breaches caused by internal failures (Huang and Wang, 2021).

[19] Appendix B provides detailed descriptions of the different types of data breaches.

[20] In 2016, there are four large data breaches, i.e., breaches with more than 100 million records loss, compared to one or two large data breaches in other years.

[21] The asymptotic properties and flexibility of linear models produce more robust results than nonlinear models (e.g., Angrist and Pischke, 2010). In addition, linear models can easily accommodate large numbers of firm and year fixed effects. Nonetheless, our results are robust to using a logit model.

[22] In the untabulated results, we use abnormal discretionary expenditures in the previous year and consistently find an increase in the likelihood of data breaches in the subsequent year.

[23] To the extent that firms' discretionary expenditures and (cybersecurity) risk management are simultaneously determined by firm fundamentals, our results are potentially endogenously driven. In addition to a set of time-varying control variables and firm and year fixed effects in the main tests and a lead-lag specification of Eq. (1) to help mitigate this concern, we conduct a robustness test in Section 3.3.

[24] All of our results hold if we include advertising expenses when estimating abnormal discretionary expenditures.

Table 1
Distribution of data breach events.

Panel A: Data breach events distributed by year

Year	Number of Breaches	Average Number of Records Lost
2005	15	177,674.67
2006	33	3,749,380.60
2007	46	58,190.15
2008	29	3,248,800.30
2009	31	6,175,707.20
2010	36	3,864,623.90
2011	50	371,112.50
2012	57	8,709,987.20
2013	45	2,782,658.70
2014	62	3,828,004.50
2015	23	3,460,814.90
2016	32	46,370,052.00
2017	48	177,674.67
Total	507	

Panel B: Data breach events distributed by industry

Industry	Number of Breaches	Average Number of Records Lost
Business Services	96	19,814,548.00
Health Services	63	2,702.21
Communications	40	15,253,299.00
Miscellaneous Retail	35	968,309.62
Insurance Carriers	28	192,208.50
Chemical & Allied Products	25	12,731.14
Eating & Drinking Places	20	40,097.00
Electronic & Other Electric Equipment	17	227,803.00
Instruments & Related Products	16	11,005.33
Transportation Equipment	15	43,772.00
Others	152	6,779,425.90
Total	507	

Panel C: Data breach events distributed by type

Type	Number of Breaches	Average Number of Records Lost
Hacking or Malware	135	24,479,609.00
Portable Device	102	34,842.39
Unintended Disclosure	89	1,883,617.20
Physical Loss	85	67,460.89
Insider	49	2,920.26
Unknown	32	3,250,794.79
Stationary Device	11	18,617.50
Payment Card Fraud	4	7,000,000.00
Total	507	

Panel D: Market reaction to breach announcements

	Value Weighted		Equal Weighted	
Window (days)	Mean	Median	Mean	Median
CAR (−1, +1)	−0.003*	−0.003***	−0.003*	−0.003***
	(0.054)	(0.003)	(0.056)	(0.005)
CAR (−2, +2)	−0.004**	−0.002**	−0.003**	−0.002**
	(0.047)	(0.049)	(0.047)	(0.050)
CAR (−5, +5)	−0.004*	−0.006**	−0.005*	−0.005**
	(0.088)	(0.033)	(0.061)	(0.039)

Panel D presents the market reactions to breach announcements. *CAR* is the cumulated abnormal returns over different windows (in days) around the breach event. The abnormal returns are calculated using the market model. Parameters of the market model are estimated using the return data over 220 trading days beginning 280 days before and ending 61 days before the breach announcements, using the CRSP value-weighted or equal-weighted return as a proxy for the market return.

$$\frac{TA_{i,t}}{Assets_{i,t-1}} = \alpha_0 + \alpha_1 * \frac{1}{Assets_{i,t-1}} + \alpha_2 * \frac{\Delta Sales_{i,t}}{Assets_{i,t-1}} + \alpha_3 * \frac{PPE_{i,t}}{Assets_{i,t-1}} + \varepsilon_{i,t} \quad (3)$$

where total accruals (*TA*) are defined as the difference between income before extraordinary items and operating cash flow net of extraordinary items (e.g., Barton and Simko, 2002); *PPE* is property, plant, and equipment; and *Assets* and *Sales* are as defined in Eq. (2). Abnormal accruals (*AAccr*) are the residuals from the regression in Eq. (3). Higher values of *AAccr* indicate more income-increasing accrual manipulations.

In Eq. (1), the vector *X* is a set of control variables from prior studies (e.g., Akey et al., 2018; Kamiya et al., 2021), including firm size (*Size*), the Tobin Q ratio (*TobinQ*), leverage (*LEV*), asset intangibility (*Intangibility*), profitability (*ROA*), sales growth (*SalesGrowth*), financial constraint (*FinancialCons*), institutional block ownership (*BlockOwner*), and being listed as a Fortune 500 company (*FT500*). The variable *Size* is the logarithm of the market value of total assets; *TobinQ* is the ratio of the market value of total assets to the book value of total assets; *LEV* is calculated as the book value of long-term debt plus debt in current liabilities, divided by total assets; *Intangibility* is the ratio of intangible assets to total assets; *ROA* is net income divided by total assets; *SalesGrowth* is the firm's sales growth; *FinancialCons* is a dummy variable that takes the value of one if a firm's Whited–Wu score (Whited and Gu, 2006) is ranked in the top tercile of the sample, and zero otherwise; *BlockOwner* is the percentage of shares held by institutional block shareholders, which are defined as institutional investor who owns at least 5 % of the outstanding shares; and *FT500* is a dummy variable that takes the value of one if the firm is included in the Fortune 500 list, and zero otherwise. In all regressions, we include firm and year fixed effects to control for time-invariant unobserved firm-level characteristics and economy-wide factors that potentially influence cybersecurity risk. We cluster standard errors at the firm level. All continuous variables are winsorized at the top and bottom one percentile to mitigate the undue influence of outliers. Appendix A presents detailed definitions of all the variables in our regression model.

2.4. Descriptive statistics

Table 2 reports the descriptive statistics (Panel A) and the correlation matrix (Panel B) for the main variables. In Panel A, the fraction of firm–years with data breaches in our sample is 1.8 %, which is higher than the result of Kamiya et al. (2021), since we also include data breaches caused by internal factors (e.g., failure to follow internal data security principles). The three-year average abnormal cuts in discretionary expenditures and average abnormal accruals have mean values of 0.086 and 0.042, respectively. The distributions of the other control variables are generally consistent with studies focusing on a similar sample period (e.g., Lo et al., 2017). In Panel B, the correlation between data breaches and abnormal cuts in discretionary expenditures is positive and significant at 1 %, which is consistent with our prediction. Firm size, asset intangibility, *ROA*, sales growth, the status of financial constraint, and inclusion on the Fortune 500 list are all correlated with data breaches in the expected directions. For example, Kamiya et al. (2021) show that larger and more visible firms, firms with less growth opportunity, more profitable firms, and firms with more intangible assets are more likely to experience data breaches.

3. Main results

3.1. Relation between managerial myopia and the likelihood of data breaches

Table 3 presents the regression results of estimating Eq. (1) regarding the relation between managerial myopic actions of cutting discretionary expenditures and the likelihood of data breaches. Column (1) reports the results without control variables and column (2) reports the results with the full set of control variables (except for accrual manipulation). In both columns (1) and (2), the coefficients on *Avg_ADisc* (i.e., average abnormal cuts in discretionary expenditures over the past three years) are positive and statistically significant (column (1), coefficient = 0.013, *t*-value = 2.46; column (2), coefficient = 0.012, *t*-value = 2.26). The magnitude of the coefficients indicates that a one-standard-deviation

Table 2
Summary statistics.

Panel A: Descriptive statistics

Variable	Mean	S.D.	Q1	Median	Q3
Breach	0.018	0.133	0.000	0.000	0.000
Avg_ADisc	0.086	0.354	−0.029	0.087	0.249
Avg_AAccr	0.042	0.168	−0.009	0.042	0.100
Size	6.748	1.678	5.444	6.598	7.839
TobinQ	1.970	1.272	1.177	1.562	2.285
LEV	0.229	0.223	0.020	0.189	0.353
Intangibility	0.749	0.234	0.639	0.835	0.928
ROA	0.002	0.160	−0.016	0.039	0.079
SalesGrowth	0.123	0.365	−0.023	0.068	0.184
FinancialCons	0.333	0.471	0.000	0.000	1.000
BlockOwner	0.161	0.173	0.000	0.121	0.279
FT500	0.038	0.191	0.000	0.000	0.000

Panel B: Correlation matrix

		(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
(1)	*Breach*	1.000										
(2)	*Avg_ADisc*	0.028***	1.000									
(3)	*Avg_AAccr*	0.006	0.424***	1.000								
(4)	*Size*	0.177***	0.150***	0.046***	1.000							
(5)	*TobinQ*	0.006	−0.163***	−0.033***	−0.085***	1.000						
(6)	*LEV*	0.039***	0.077***	0.011*	0.277***	−0.124***	1.000					
(7)	*Intangibility*	0.013**	0.002	−0.003	−0.176***	0.184***	−0.297***	1.000				
(8)	*ROA*	0.037***	0.074***	0.103***	0.276***	0.032***	−0.130***	−0.043***	1.000			
(9)	*SalesGrowth*	−0.011*	−0.075***	−0.051***	−0.070*	0.209***	−0.021***	0.030***	−0.002	1.000		
(10)	*FinancialCons*	−0.059***	−0.121***	−0.044***	−0.604***	0.993***	−0.037***	0.122***	−0.270***	0.104***	1.000	
(11)	*BlockOwner*	−0.022***	0.024***	0.010	−0.009	−0.021***	0.035***	0.027***	−0.042***	−0.047***	−0.021***	1.000
(12)	*FT500*	0.176***	0.054***	0.011*	0.426***	−0.023***	0.019***	−0.039***	0.073***	−0.048***	−0.042***	−0.074***

Panel B presents the correlation between variables in the baseline regression model. All the variable definitions are summarized in Appendix A. The superscripts ***, **, and * indicate significance at the 1%, 5%, and 10% confidence levels, respectively.

Table 3
Abnormal cuts in discretionary expenditures and data breaches.

Dependent	(1) *Breach*	(2) *Breach*	(3) *Breach*
Avg_ADisc	0.013**	0.012**	0.012**
	(2.46)	(2.26)	(2.32)
Avg_AAccr			−0.000
			(−0.08)
Size		0.003	0.003
		(1.27)	(1.28)
TobinQ		−0.001	−0.001
		(−1.14)	(−1.13)
LEV		−0.003	−0.003
		(−0.44)	(−0.44)
Intangibility		0.026**	0.026**
		(2.22)	(2.22)
ROA		−0.005	−0.005
		(−0.88)	(−0.88)
SalesGrowth		−0.002	−0.002
		(−1.08)	(−1.08)
FinancialCons		−0.001	−0.001
		(−0.47)	(−0.47)
BlockOwner		0.007	0.007
		(1.20)	(1.20)
FT500		0.018	0.018
		(0.95)	(0.95)
Constant	0.017***	−0.021	−0.021
	(36.83)	(−1.11)	(−1.12)
Firm Fixed Effects	Yes	Yes	Yes
Year Fixed Effects	Yes	Yes	Yes
Observations	28,325	28,325	28,325
Adjusted R^2	0.1372	0.1373	0.1373

This table presents the results of the impact of abnormal cuts in discretionary expenditures on the likelihood of data breaches. Columns (1), (2) and (3) present the estimation results with different control sets. The variable *Breach* is a dummy variable that takes the value of one if a firm experiences a data breach in year *t*, and zero otherwise. *Avg_ADisc* is the three-year average (years *t−1, t−2*, and *t−3*) abnormal cut in discretionary R&D and SG&A expenditures using the residuals estimated from the model of Roychowdhury (2006) and multiplied by −1. *Avg_AAccr* is the three-year average (years *t−1, t−2*, and *t−3*) abnormal accruals estimated from the modified Jones model (Dechow et al., 1995). All the variable definitions are summarized in Appendix A. Firm-clustered heteroskedasticity-robust *t*-statistics are reported in parentheses. The superscripts ***, **, and * indicate significance at the 1%, 5%, and 10% confidence levels, respectively.

increase in abnormal cuts in discretionary expenditures increases the probability from 1.8 %, the sample mean of the likelihood of data breaches, to 2.23 %.

In column (3), we further include the average abnormal accrual for the past three years, *Avg_AAccr*, in the regression. The coefficient on abnormal cuts in discretionary expenditures continues to be positive and significant. However, the coefficient on *Avg_AAccr* is not significant, which partially alleviates the endogeneity concern. Most of the control variables are not significant, which may be an artifact of firm fixed effects subsuming the variation in variables that are sticky over time.[25]

Overall, the results in Table 3 support our prediction that managerial myopia, in the form of abnormal cuts in discretionary expenditures, is positively related to the risk of data breaches.

3.2. Real earnings management and data breaches: robustness test

In our main test, we use the sum of abnormal cuts in R&D and SG&A expenditures to capture managerial myopic actions. In this section, we employ the Kothari et al. (2016) model to individually estimate the magnitudes of abnormal R&D, SG&A, and advertising expenses. This serves to validate the robustness of our findings in Section 3.1 and as a falsification test. While myopic managers could cut advertising expenses to meet short-term goals, any abnormal cut in advertising expenses is less likely to induce future data breaches. A nonsignificant relation would help mitigate the concern that our baseline results are driven by underlying factors that impact managerial myopic actions and firm cybersecurity risk at the same time. Specifically, Kothari et al. (2016) developed the following fixed-effect first-order autoregressive models to estimate components of discretionary expenditures:

$$\frac{RD_{i,t}}{Assets_{i,t-1}} = \alpha_{rd,i} + \Delta_{rd,t} + \varnothing_{rd} * \frac{RD_{i,t-1}}{Assets_{i,t-2}} + \gamma_{rd} * \frac{Sales_{i,t-1}}{Assets_{i,t-2}} + \varepsilon_{rd,i,t} \quad (4)$$

$$\frac{SGA_{i,t}}{Assets_{i,t-1}} = \alpha_{sga,i} + \Delta_{sga,t} + \varnothing_{sga} * \frac{SGA_{i,t-1}}{Assets_{i,t-2}} + \gamma_{sga} * \frac{Sales_{i,t-1}}{Assets_{i,t-2}} + \varepsilon_{sga,i,t} \quad (5)$$

$$\frac{AD_{i,t}}{Assets_{i,t-1}} = \alpha_{ad,i} + \Delta_{ad,t} + \varnothing_{ad} * \frac{AD_{i,t-1}}{Assets_{i,t-2}} + \gamma_{ad} * \frac{Sales_{i,t-1}}{Assets_{i,t-2}} + \varepsilon_{ad,i,t} \quad (6)$$

where for firm *i* and year *t*, *RD*, *SGA*, and *AD* are annual R&D expenses, SG&A expenses, and advertising expenses, respectively; *Sales* and *Assets* are defined in the same way as in Eq. (2).

Following Kothari et al. (2016), to control for year- and firm-specific effects that induce model misspecification, we first subtract the cross-sectional mean of each discretionary expenditure component (i.e., R&D, SG&A, or advertising) from each firm's annual expenditure for that year. Then, for each firm, the annual deviation of each discretionary expenditure component from the cross-sectional mean is differenced from the firm's mean across the sample period. The explanatory variable *Sales* is differenced twice in the same manner. We then estimate models (4) to (6) using panel data, yielding a time series of residuals for each discretionary expenditure component for each firm. Finally, we subtract from each firm–year residual the mean value of the residual across all years for the corresponding firm to obtain the abnormal R&D, SG&A, and advertising expenditures.

Similar to our main test, we first multiply each abnormal component by −1 and calculate the three-year average abnormal R&D expenses (*Avg_ARD*), SG&A expenses (*Avg_ASGA*), and advertising expenses (*Avg_AAD*). We re-estimate Eq. (1) by replacing *Avg_ADisc* with *Avg_ARD*, *Avg_ASGA*, and *Avg_AAD*, respectively. Table 4 reports the results of how myopic cuts in different components of discretionary expenditure affect the likelihood of data breaches. Consistent with our prediction and the results reported in Table 3, both myopic R&D cuts and SG&A cuts are associated with an increased risk of data breaches. In contrast, the effect of myopic cuts in advertising expenses on data breaches is nonsignificant.

3.3. Alternatives: efficient investment and endogeneity

The results thus far are consistent with our prediction that managerial myopic actions are associated with an increase in cybersecurity risk. However, our interpretation is subject to alternatives. For example, the cut in discretionary expenditures is calculated after factoring in the increased cybersecurity risk or the relation we document in Section 3.1 may be endogenously driven. In this section, we conduct additional analyses to further understand the relation between managerial myopia and data breaches.

First, to rule out the efficient investment decision alternative, we identify a subsample of firms suspected of taking myopic actions to meet or beat short-term earnings targets. We expect that the relation between abnormal cuts in discretionary expenditures and data breaches to be more pronounced for these suspect firms. We define suspect firms as those that marginally met or beat the prior year's earnings or analyst

[25] If we follow Kamiya et al. (2021) and use industry fixed effects instead, the coefficient estimations for the control variables are comparable to Kamiya et al. (2021).

Table 4
Abnormal cuts in discretionary expenditures and data breaches: R&D, SG&A, and advertising.

Dependent	(1) *Breach*	(2) *Breach*	(3) *Breach*
Avg_ARD	0.089**		
	(2.57)		
Avg_ASGA		0.036**	
		(2.16)	
Avg_AAD			0.197
			(0.72)
Avg_AAccr	0.007	0.008	0.008
	(0.73)	(0.84)	(0.84)
Size	0.002	0.002	0.002
	(0.69)	(0.53)	(0.75)
TobinQ	−0.001	−0.001	−0.002
	(−1.01)	(−1.07)	(−1.16)
LEV	−0.008	−0.007	−0.008
	(−0.96)	(−0.87)	(−0.92)
Intangibility	0.031**	0.031**	0.031**
	(2.16)	(2.12)	(2.16)
ROA	−0.007	−0.005	−0.007
	(−1.01)	(−0.78)	(−1.01)
SalesGrowth	−0.001	−0.001	−0.001
	(−0.52)	(−0.46)	(−0.57)
FinancialCons	0.000	0.000	0.000
	(0.08)	(0.00)	(0.02)
BlockOwner	0.008	0.008	0.008
	(1.20)	(1.15)	(1.21)
FT500	0.019	0.019	0.018
	(0.97)	(0.97)	(0.96)
Constant	−0.016	−0.012	−0.017
	(−0.65)	(−0.49)	(−0.69)
Firm Fixed Effects	Yes	Yes	Yes
Year Fixed Effects	Yes	Yes	Yes
Observations	23,101	23,101	23,101
Adjusted R^2	0.1496	0.1496	0.1495

This table reports the results of the impact of abnormal cuts in discretionary expenditures on the likelihood of data breaches for each component of discretionary expenses (R&D expenses, SG&A expenses, and advertising expenses), as tabulated in Columns (1), (2) and (3) respectively. The variable *Breach* is a dummy variable that takes the value of one if a firm experiences a data breach in year *t*, and zero otherwise. *Avg_ARD* (*Avg_ASGA* and *Avg_AAD*) is the three-year average (years *t−1, t−2*, and *t−3*) abnormal cut in R&D expenses (SG&A expenses and advertising expenses), estimated using the model of Kothari et al. (2016) and multiplied by −1. *Avg_AAccr* is the three-year average (years *t−1, t−2*, and *t−3*) abnormal accruals estimated from the modified Jones model (Dechow et al., 1995). All the variable definitions are summarized in Appendix A. Firm-clustered heteroskedasticity-robust *t*-statistics are reported in parentheses. The superscripts ***, **, and * indicate significance at the 1%, 5%, and 10% confidence levels, respectively.

forecasts ;[26] specifically, those that just met or beat consensus earnings-per-share forecasts by one cent or firms that had zero earnings changes (defined as income before extraordinary items scaled by total assets) or earnings changes of less than 0.01. Firms that failed to meet earnings targets or that safely beat them by more than five cents (more than 0.05 in the case of the prior year's earnings benchmark) are non-suspect firms. For alignment with our measurement of myopic cuts in discretionary expenditures, we identify suspect firms as firms that marginally met or beat earnings targets at least once during the past three years and non-suspect firms as those that never met or always safely beat earnings targets in the past three years.

We re-estimate Eq. (1) separately for the suspect and non-suspect

[26] The literature uses three common earnings thresholds: zero earnings, the prior year's earnings, and analyst consensus forecasts (e.g., Roychowdhury, 2006; Bhojraj et al., 2009; Zang, 2011; Caskey and Ozel, 2017). Given that our sample starts in 2005 and zero earnings discontinuity disappears in the period after the implementation of the Sarbanes–Oxley Act (e.g., Gilliam et al., 2015), we only use the prior year's earnings and analyst forecasts as earnings targets.

Table 5
Alternatives: Efficient investment and endogeneity.

Panel A: Alternative of efficient investment: Suspect versus non-suspect firms

Dependent	(1) Suspect *Breach*	(2) Non-suspect *Breach*
Avg_ADisc	0.042***	−0.007
	(2.64)	(−1.18)
Avg_AAccr	−0.021	0.001
	(−1.15)	(0.17)
Size	0.008	−0.007*
	(1.44)	(−1.75)
TobinQ	−0.002	−0.002
	(−0.82)	(−1.45)
LEV	−0.002	−0.005
	(−0.12)	(−0.57)
Intangibility	0.056*	−0.017
	(1.68)	(−0.97)
ROA	−0.032*	0.008
	(−1.83)	(1.32)
SalesGrowth	0.002	0.001
	(0.38)	(0.67)
FinancialCons	−0.003	−0.002
	(−0.61)	(−0.56)
BlockOwner	0.010	0.013
	(0.98)	(1.33)
FT500	−0.010	−0.068
	(−0.53)	(−1.00)
Constant	−0.074	0.068**
	(−1.53)	(2.13)
Firm Fixed Effects	Yes	Yes
Year Fixed Effects	Yes	Yes
Observations	11,221	3,960
Adjusted R^2	0.1364	0.1469

Panel B: Alternative of endogeneity: External hacks

Dependent	(1) *Breach*	(2) *Breach*	(3) *Breach*
Avg_ADisc	0.003*	0.003*	0.004**
	(1.78)	(1.65)	(1.98)
Avg_AAccr			0.005
			(1.48)
Size		−0.001	−0.002
		(−0.98)	(−1.04)
TobinQ		0.000	0.000
		(0.33)	(0.30)
LEV		−0.001	−0.000
		(−0.11)	(−0.08)
Intangibility		0.012*	0.012*
		(1.92)	(1.94)
ROA		0.001	0.001
		(0.29)	(0.32)
SalesGrowth		−0.000	−0.000
		(−0.25)	(−0.24)
FinancialCons		−0.002	−0.002
		(−0.97)	(−0.97)
BlockOwner		0.002	0.002
		(0.66)	(0.67)
FT500		0.010	0.010
		(0.89)	(0.90)
Constant	0.006***	0.007	0.007
	(25.01)	(0.64)	(0.67)
Firm Fixed Effects	Yes	Yes	Yes
Year Fixed Effects	Yes	Yes	Yes
Observations	28,325	28,325	28,325
Adjusted R^2	0.0490	0.0489	0.0489

Panel A presents the results of the impact of abnormal cuts in discretionary expenditures on the likelihood of data breaches for suspect and non-suspect firms. The variable *Breach* is a dummy variable that takes the value of one if a firm experiences a data breach in year *t*, and zero otherwise. *Avg_ADisc* is the three-year average (years *t−1, t−2*, and *t−3*) abnormal cut in discretionary R&D and SG&A expenditures using the residuals estimated from the model of Roychowdhury (2006) and multiplied by −1. *Avg_AAccr* is the three-year average (years *t−1, t−2*, and *t−3*) abnormal accruals estimated from the modified Jones model (Dechow et al., 1995). Columns (1) and (2) present the results for the

suspect and non-suspect groups, respectively. A firm is considered suspect if it marginally met or beat analysts' consensus within one cent or met or beat last year's return on assets by one cent at least once in the last three years. A firm is considered non-suspect if it failed to attain the analyst consensus or last year's earnings or if it beat the analyst consensus (last year's return on assets) by more than five cents in the last three years. All variable definitions are summarized in Appendix A. Firm-clustered heteroskedasticity-robust *t*-statistics are reported in parentheses. The superscripts ***, **, and * indicate significance at the 1%, 5%, and 10% confidence levels, respectively.

Panel B presents the results of the impact of abnormal cuts in discretionary expenditures on the likelihood of external data breaches. Columns (1), (2) and (3) present the estimation results with different control sets. The variable *Breach* is a dummy variable that takes the value of one if a firm experiences an external hacking event in year *t,* and zero otherwise. *Avg_ADisc* is the three-year average abnormal cut in discretionary R&D and SG&A expenditures using the residuals estimated from the model of Roychowdhury (2006) and multiplied by −1. *Avg_AAccr* is the three-year average abnormal accruals estimated from the modified Jones model (Dechow et al., 1995). All the variable definitions are summarized in Appendix A. Firm-clustered heteroskedasticity-robust *t*-statistics are reported in parentheses. The superscripts ***, **, and * indicate significance at the 1%, 5%, and 10% confidence levels, respectively.

firms and report the results in Table 5 Panel A. In column (1), we find that the abnormal cuts in discretionary expenditures are positively and significantly associated with the likelihood of data breaches for the sample of suspect firms. For the sample of non-suspect firms in column (2), the coefficient on abnormal discretionary expenditures is negative but nonsignificant.

Second, we focus on the occurrence of external data breaches only, i.e., those by hacking or malware. To the extent that external data breaches are less likely affected by the optimal cutting of discretionary expenditures or impacted by unobservable firm characteristics or actions, it alleviates the endogeneity concern if the positive relation between the abnormal discretionary expenditure cuts and external data breaches still exists in the external data breaches subsample. We replicate Table 3 by assigning a value of one to *Breach* if the firm experiences an external data breach, and zero otherwise. We report the results in Table 5 Panel B and the coefficients on *Avg_ADisc* are still positive and significant.

Overall, the results in this section are consistent with the interpretation that the relation between abnormal cuts in discretionary expenditures and data breaches is driven by managerial myopia, rather than by efficient investment decisions or endogeneity.

3.4. Severity of data breaches

In this section, we examine the economic losses of data breaches caused by managerial myopia. Specifically, we re-estimate Eq. (1) by replacing the dependent variable with the three-day market-adjusted abnormal returns around the announcements of data breaches. The abnormal return is calculated using a market model whose parameters are estimated using the return data over 220 trading days beginning 280 days before and ending 61 days before the breach announcements. The results are reported in Table 6. We find similar coefficients on *Avg_ADisc* for the univariate regression and different specifications of multivariate regressions, suggesting that the magnitude of the abnormal cut in firm expenditure is related to not only the likelihood of data breaches but also the severity of data breaches.

Table 6
Abnormal cuts in discretionary expenditures and magnitude of loss

Dependent	(1) *CAR* (−1, +1)	(2) *CAR* (−1, +1)	(3) *CAR* (−1, +1)
Avg_ADisc	−0.0004**	−0.0003**	−0.0003**
	(−2.52)	(−2.39)	(−2.15)
Avg_AAccr			−0.0001
			(−0.27)
Size		0.0000	0.0000
		(0.69)	(0.71)
TobinQ		0.0000	0.0000
		(0.27)	(0.28)
LEV		−0.0000	−0.0000
		(−0.05)	(−0.06)
Intangibility		−0.0004	−0.0004
		(−0.88)	(−0.89)
ROA		0.0003	0.0003
		(1.48)	(1.47)
SalesGrowth		0.0001	0.0001
		(1.33)	(1.33)
FinancialCons		0.0001	0.0001
		(0.69)	(0.69)
BlockOwner		−0.0002	−0.0002
		(−1.24)	(−1.24)
FT500		0.0003	0.0003
		(0.88)	(0.87)
Constant	−0.0002***	−0.0003	−0.0003
	(−7.89)	(−0.48)	(−0.49)
Firm Fixed Effects	Yes	Yes	Yes
Year Fixed Effects	Yes	Yes	Yes
Observations	28,325	28,325	28,325
Adjusted R^2	0.0270	0.0270	0.0270

This table presents the results of the impact of abnormal cuts in discretionary expenditures on the severity of data breaches. Columns (1), (2) and (3) present the estimation results with different control sets. The variable *CAR* is the cumulated abnormal returns over the three-day window around the breach event. The abnormal returns are calculated using the market model. Parameters of the market model are estimated on the return data over 220 trading days beginning 280 days before and ending 61 days before the breach announcements, using the CRSP value-weighted return as a proxy for the market return. *Avg_ADisc* is the three-year average (years *t−1, t−2,* and *t−3*) abnormal cut in discretionary R&D and SG&A expenditures using the residuals estimated from the model of Roychowdhury (2006) and multiplied by −1. *Avg_AAccr* is the three-year average (years *t−1, t−2,* and *t−3*) abnormal accruals estimated from the modified Jones model (Dechow et al., 1995). All the variable definitions are summarized in Appendix A. Firm-clustered heteroskedasticity-robust *t*-statistics are reported in parentheses. The superscripts ***, **, and * indicate significance at the 1%, 5%, and 10% confidence levels, respectively.

4. Cross-sectional analysis

In this section, we conduct several additional cross-sectional analyses to further support the effect of managerial myopia on data breaches.

4.1. Managerial equity incentives

In this section, we examine the impact of abnormal cuts in discretionary expenditures on the likelihood of data breaches, conditioning on managerial equity incentives. The prior theoretical and empirical literature suggests that managerial equity incentives motivate managers to take myopic actions, such as earnings manipulation (e.g., Bergstresser and Philippon, 2006; Burns and Kedia, 2006; Efendi et al., 2007; Benmelech et al., 2010; Kim et al., 2011). Therefore, if the impact of abnormal cuts in discretionary expenditures on data breaches is driven by managerial myopia, we expect the effect to be stronger for firms with stronger incentives to take myopic actions.

We use the sensitivity of managerial wealth to changes in stock prices and the total unearned options and restricted stock holdings to gauge managers' short-term incentives (Lee et al., 2018).[27] Columns (1) and (2) of Table 7 present the results of estimating Eq. (1) using the two

[27] In addition, we use vega for CEOs, i.e., the CEO risk-taking incentive, as an alternative measure of managerial equity incentives for this cross-sectional test (e.g., Core and Guay). We find consistent results that the coefficient on abnormal cuts in discretionary expenditures is significant only for the subsample of firms with higher vega. The differences in the two coefficients from the two subsamples are statistically significant.

Table 7
Abnormal cuts in discretionary expenditures and data breaches: Cross-sectional tests.

	(1) High WPS	(2) Low WPS	(3) High–Unearned Compensation	(4) Low–Unearned Compensation	(5) High ERC	(6) Low ERC	(7) High BLK	(8) Low BLK	(9) High MKT Share	(10) Low MKT Share
Dependent	*Breach*	*Breach*	*Breach*	*Breach*	*Breach*	*Breach*	*Breach*	*Breach*	*Breach*	*Breach*
Avg_ADisc	0.052***	−0.008	0.009	0.042***	0.026**	0.001	0.007	0.021***	0.020**	−0.001
	(2.83)	(−0.45)	(0.73)	(2.72)	(2.33)	(0.09)	(0.88)	(2.70)	(2.36)	(−0.09)
Avg_AAccr	−0.036	0.022	−0.013	−0.013	−0.012	0.007	−0.012	−0.002	−0.002	−0.008
	(−1.36)	(0.77)	(−0.87)	(−0.61)	(−0.75)	(0.62)	(−1.29)	(−0.26)	(−0.17)	(−0.91)
Size	0.008	0.000	0.007	−0.001	0.002	−0.000	0.003	0.004	0.010**	−0.004
	(1.12)	(0.01)	(1.08)	(−0.15)	(0.41)	(−0.07)	(0.76)	(1.01)	(2.04)	(−1.38)
TobinQ	−0.002	−0.003	−0.003	0.002	−0.003*	−0.001	0.001	−0.004**	−0.000	−0.001
	(−0.46)	(−0.88)	(−0.98)	(0.78)	(−1.73)	(−0.97)	(0.39)	(−2.13)	(−0.26)	(−1.14)
LEV	−0.033	0.004	0.010	−0.002	−0.002	0.001	−0.000	−0.006	−0.007	−0.001
	(−1.53)	(0.21)	(0.40)	(−0.11)	(−0.12)	(0.09)	(−0.04)	(−0.57)	(−0.56)	(−0.07)
Intangibility	0.097**	0.008	0.060	0.025	0.032	0.012	0.031*	0.020	0.008	0.041**
	(2.53)	(0.20)	(1.32)	(0.87)	(1.45)	(0.55)	(1.83)	(1.10)	(0.43)	(2.45)
ROA	−0.015	0.006	−0.017	0.012	0.005	−0.004	−0.004	−0.010	0.000	−0.009
	(−0.63)	(0.35)	(−0.63)	(0.97)	(0.56)	(−0.33)	(−0.50)	(−1.16)	(0.04)	(−1.21)
SalesGrowth	0.003	0.006	0.001	−0.005	−0.003	−0.002	−0.001	−0.003	−0.004	−0.000
	(0.33)	(0.89)	(0.09)	(−0.88)	(−1.01)	(−0.66)	(−0.48)	(−1.26)	(−1.40)	(−0.08)
FinancialCons	−0.003	0.002	0.005	−0.007	−0.006	−0.010**	−0.001	−0.002	0.000	−0.003
	(−0.31)	(0.21)	(0.52)	(−1.15)	(−1.36)	(−1.99)	(−0.20)	(−0.52)	(0.09)	(−0.75)
BlockOwner	−0.009	0.026*	−0.000	0.020*	−0.001	0.012	0.008	0.003	0.009	0.006
	(−0.67)	(1.73)	(−0.03)	(1.68)	(−0.06)	(1.14)	(1.07)	(0.28)	(0.82)	(0.89)
FT500	0.036	0.076*	0.031	−0.011	0.054*	−0.015	−0.007	0.018	0.018	−0.002
	(1.58)	(1.90)	(1.22)	(−0.31)	(1.83)	(−0.54)	(−0.30)	(0.62)	(0.88)	(−0.59)
Constant	−0.103*	0.016	−0.071	0.005	−0.014	0.016	−0.032	−0.012	−0.048	0.012
	(−1.76)	(0.26)	(−1.11)	(0.10)	(−0.40)	(0.45)	(−1.04)	(−0.39)	(−1.33)	(0.49)
Firm Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	7,544	6,280	6,682	9,330	13,283	9,254	13,695	14,145	14,315	12,823
Adjusted R^2	0.1533	0.1582	0.1679	0.1585	0.1413	0.1611	0.1233	0.1466	0.1456	0.0716
Difference: p-value	0.011		0.061		0.043		0.080		0.036	

This table presents the cross-sectional results of the impact of abnormal cuts in discretionary expenditures on the likelihood of data breaches. The variable *Breach* is a dummy variable that takes the value of one if a firm experiences a data breach in year *t*, and zero otherwise. *Avg_ADisc* is the three-year average (years *t−1, t−2*, and *t−3*) abnormal cut in discretionary R&D and SG&A expenditures using the residuals estimated from the model of Roychowdhury (2006) and multiplied by −1. *Avg_AAccr* is the three-year average (years *t−1, t−2*, and *t−3*) abnormal accruals estimated from the modified Jones model (Dechow et al., 1995). Columns (1) and (2) report the results using subsamples split by CEO wealth-performance sensitivity (WPS). A firm–year is assigned to the high-WPS (low-WPS) group if the past three-year average CEO WPS is ranked above (below) the sample median. Columns (3) and (4) report the results using subsamples split by CEO total unearned options and restricted stock holdings. A firm–year is assigned to the high–unearned compensation (low–unearned compensation) group if the past three-year average unearned options and stocks is ranked above (below) the sample median. Columns (5) and (6) report the results using subsamples split by the firm earnings response coefficient (ERC). We assign firms into high- and low-ERC groups using the three-year average median ERC. Columns (7) and (8) report the results using subsamples split by blockholder ownership. We classify firm–years into groups with high (low) levels of blockholder ownership if the average level of blockholder ownership over the past three years is ranked above (below) the sample median. A blockholder is defined as an investor who owns at least 5% of the outstanding shares. Columns (9) and (10) report the results using subsamples split by market share. We classify firm–years into the group with a high (low) market share if the average market share over the past three years is ranked above (below) the sample median. All variable definitions are summarized in Appendix A. Firm-clustered heteroskedasticity-robust *t*-statistics are reported in parentheses. The superscripts ***, **, and * indicate significance at the 1%, 5%, and 10% confidence levels, respectively.

subsamples split at the median of managerial wealth sensitivity to stock prices (e.g., Edmans et al., 2008)[28] and Columns (3) and (4) report the results using the sample median of total unearned options and restricted stock holdings. To be consistent with the measurement of abnormal cuts in discretionary expenditures, we use the average equity incentive over the past three years as the splitting variable. We find that the coefficient on abnormal cuts in discretionary expenditures is significant only for the subsample of firms with higher short-term equity incentives, i.e., the subsample with higher sensitivity to wealth and lower unearned value options and restricted stock holding. The differences in the two coefficients from the two subsamples are statistically significant, as reported at the bottom of Table 7.[29]

4.2. Market reaction to earnings news

Most formal models of myopia start with the assumption that the stock market uses earnings to make a rational forecast of firm value and managers pump up earnings to raise the forecasted value (e.g., Stein, 1989). Thus, managers' incentives to pump up earnings are stronger if the stock market relies more heavily on earnings in making its decisions (Matsumoto, 2002). Thus, the impact of abnormal cuts in discretionary expenditures on cybersecurity risk is more likely driven by managerial myopia for firms with stronger market reactions to earnings news.

We use the ERC to capture the stock market's reliance on firm earnings in making its decisions. Specifically, for each year, we estimate the firm-specific ERC using quarterly earnings data in the past 20 quarters. Then, we calculate the three-year average of firm-specific ERC, the median value of which is employed to classify firms into high- and low-ERC groups. We separately estimate Eq. (1) for the two subgroups and present the results in columns (5) and (6) of Table 7. We find that the positive relation between abnormal cuts in discretionary expenditures and the occurrence of data breaches is significant only for firms in the high-ERC group, whereas the relation is nonsignificant in the low-ERC group. The difference between these two coefficients is

[28] We thank Alex Edmans for sharing the wealth–performance sensitivity data on his website (http://alexedmans.com/data).

[29] We acknowledge that there is also evidence that equity incentives might not be related to myopic reporting behavior (e.g., Erickson et al., 2006). To the extent that equity incentives do not induce myopia, the results here should be interpreted with caution.

Table 8
Peer firm reactions to the announcement of data breaches.

Dependent	(1) *ADisc*	(2) *ADisc*
Post	0.052***	0.049***
	(3.26)	(3.00)
*HighRisk*Post*	−0.078***	−0.076***
	(−5.40)	(−5.25)
Size		−0.044
		(−1.37)
TobinQ		−0.025**
		(−2.35)
LEV		−0.017
		(−0.24)
Intangibility		0.165
		(1.03)
ROA		0.050
		(1.35)
Age		−0.031
		(−0.95)
CFO		−0.070
		(−0.89)
Suspect		0.001
		(0.27)
INDGrowth		0.082**
		(2.08)
GDPGrowth		0.077
		(0.27)
BlockOwner		0.005
		(0.25)
Constant	0.069***	0.315
	(16.32)	(1.35)
Firm Fixed Effect	Yes	Yes
Year Fixed Effect	Yes	Yes
Observations	10,445	10,445
Adjusted R^2	0.5599	0.5633

This table presents the results of peer firms' reaction to data breaches. Columns (1) and (2) present the estimation results with different control sets. *ADisc* is the abnormal cut in discretionary R&D and SG&A expenditures using the residuals estimated from the model of Roychowdhury (2006) and multiplied by −1. Peers are firms in the same industry as the breached firms but with no data breaches. *HighRisk* is a dummy variable that takes the value of one for peer firms with more abnormal cutting of the three-year average discretionary expenditure compared to the sample median, and zero otherwise. The regression is estimated over a five-year period around the breach announcements. *Post* is a dummy variable that takes the value of one for the two-year period following the data breaches of the focal firms (i.e., years 1 and 2), and zero otherwise. Variable definitions are summarized in Appendix A. Firm-clustered heteroskedasticity-robust *t*-statistics are reported in parentheses. The superscripts ***, **, and * indicate significance at the 1%, 5%, and 10% confidence levels, respectively.

significant at the 5 % level.

4.3. Block ownership

Next, we examine the effect of abnormal cuts in discretionary expenditures on data breaches, conditioning on levels of institutional block ownership. Prior research suggests that sophisticated investors, such as blockholders, place greater weight on long-run value than on short-term earnings performance (Edmans, 2009). Therefore, managers have weaker incentives to conduct myopic cuts in discretionary expenditures to increase short-term earnings if their firms have greater block ownership. In addition, to the extent that these sophisticated investors actively monitor management, managers should also have less freedom to engage in myopic actions. For example, Edmans et al. (2017) find that short-term incentives induce stronger investment cuts in firms with low institutional and block ownership. Thus, we expect the effect of the abnormal cutting in discretionary expenditures on the likelihood of data breaches to be more pronounced for firms with a low level of block ownership.

Columns (7) and (8) of Table 7 present the results of estimating Eq. (1) using subsamples split at the sample median based on the block ownership. We define a blockholder as an investor who owns at least 5 % of the outstanding shares. Again, we use the average level of block ownership over the past three years as the splitting variable. Consistent with our expectation, the effect of abnormal cuts in discretionary expenditures on the likelihood of data breaches is significant only for the subsamples of firms with low block ownership and the magnitudes of the coefficients in the two columns are significantly different at the 10 % level.

4.4. Cost of myopic actions: market leaders

In the final cross-sectional analysis, we examine how the expected costs of myopic actions affect the relation between abnormal cuts in discretionary expenditures and the risk of data breaches. Prior literature suggests that competitive pressure from the product market can force firms out of business and ruin managerial careers if managers take myopic actions at the expense of long-term value (e.g., Machlup, 1967). Consistent with this argument, Zang (2011) shows that market leaders are more likely to cut discretionary expenditures to meet earnings targets because these firms can better afford myopic actions that lead to losses in long-term value.

We measure a firm's market leader status using the three-year average market share and split the sample into groups with high and low market shares based on the industry-year median. Columns (9) and (10) of Table 7 report the regression results estimating Eq. (1) separately for the two subsamples. Consistent with our expectation, the effect of abnormal cuts in discretionary expenditures on the likelihood of data breaches is significant only for the subsample of firms with high market share and the difference in the coefficients in the two columns is significant at the 5 % level.

Overall, the cross-sectional results based on managerial equity incentives, the ERC, block ownership, and market shares are all consistent with the managerial myopia interpretation of our main findings.

5. Peer effect

In this section, we examine the potential spillover effect of data breach announcements in terms of industry peers' subsequent myopic actions. There is extensive evidence that firms learn from the experiences of their peers and respond accordingly (e.g., Beatty et al., 2013). If firms learn that managerial myopia, e.g., abnormal cuts in discretionary expenditures, contributes to the occurrence of data breaches of their peers, they are expected to correct such myopic behavior, e.g., by increasing their discretionary expenditures, upon the announcement of data breaches of their peers. To test this conjecture, we identify peer firms (without data breaches) as those in the same industry as the focal firm. We use the previous three-year accumulated abnormal discretionary expenditures to rank the peer firms into high (more abnormal cutting of discretionary expenditures) and low (less abnormal cutting of discretionary expenditures) risk groups using the industry–year median. We interpret more aggressive cutting of discretionary expenditures as high-risk peers that face a higher cybersecurity risk. Then, we estimate the following difference-in-differences regression for the industry peer sample:

$$ADisc_{i,t} = \alpha_0 + \beta_1 * Post_{i,t} + \beta_2 * HighRisk_i * Post_{i,t} + \gamma' X + f_i + f_t + \varepsilon_{it} \quad (7)$$

where *ADisc* is the residual estimated from Eq. (2) to capture abnormal discretionary expenditures. We focus on a five-year period around the announcement of each breach, and *Post* is the dummy variable that takes the value of one for the two-year period following the data breaches of the focal firms (i.e., years 1 and 2), and zero otherwise. *HighRisk* takes the value of one for the high-risk subsample and zero for the low-risk group. Since we multiply the residual in Eq. (2) by −1 to obtain *ADisc*

(i.e., a higher value of *ADisc* indicates a larger cut in discretionary expenditures), we expect the coefficient estimate on *HighRisk*Post* to be significantly negative.

The control variables are taken from prior studies (e.g., Healy and Wahlen, 1999; Fields et al., 2001). In addition to the vector of controls identified in Section 2.3, we include firm age, *Age* (the number of years since a firm's first appearance in Compustat), and operating cash flow, *CFO* (operating cash flow divided by total assets). We also control for managers' incentives to meet or beat earnings benchmarks, *Suspect* (e.g., Burgstahler and Dichev, 1997; Frankel et al., 2002; Kasznik and McNichols, 2002). We include industry growth rate and state GDP growth rate to control for industry-wide and statewide factors. Finally, we include firm and year fixed effects to control for unobserved firm-level characteristics and macroeconomic conditions that may affect real expenditures.

Table 8 presents the regression results. As expected, we find a negative and significant coefficient estimate on the interaction item, *HighRisk*Post*, supporting the conjecture that data breaches have spillover effects and peer firms respond to the data breaches of the focal firms by increasing discretionary expenditures, i.e., they reduce myopic actions. This finding is consistent with Ashraf (2022), who shows that non-breached firms take real actions to reduce their cybersecurity risk exposure.

6. Conclusion

This paper explores managerial myopia as one potential factor contributing to cybersecurity risk. Using abnormal cuts in discretionary expenditures as a proxy of managerial myopia, we show that it is significantly and positively associated with the likelihood and severity of data breaches. Our multivariate regression tests suggest that the impact of myopia on cybersecurity risk is driven by abnormal cuts in R&D and SG&A expenditures, which are more likely to involve investments in cybersecurity. To buttress the conclusion that our main results reflect myopic manipulation rather than efficient decision-making or endogeneity, we show that abnormal cuts in discretionary expenditures are related to cybersecurity risk only if managers appear to take actions to marginally meet or beat short-term earnings targets and our results are not sensitive to the exclusion of internal data breaches. In addition, we find that the impact of myopic cuts in discretionary expenditure on cybersecurity risk is largely driven by firms with greater short-term managerial equity incentives, higher ERCs, and lower levels of block ownership and by firms that are market leaders. Finally, in an additional analysis, we show that firms appear to respond to the data breaches of their industry peers by increasing discretionary expenditures. Taken together, the results support the conclusion that managerial myopic actions threaten corporate cybersecurity.

Our research contributes to the literature on corporate myopia and cybersecurity risk. A large body of prior literature has examined the sources of managerial myopia, and several studies have examined the consequences of myopia in terms of firms' financial performance and stock performance. Our study adds to the literature by documenting one potential real effect of managerial myopia, namely, its impact on cybersecurity risk. Our paper adds to the nascent corporate finance literature on cyber risk management (e.g., Kamiya et al., 2021). Our results suggest that cyber risk is not only driven by managerial risk-taking incentives but can also be influenced by managerial myopic actions and highlight the potential impact of effective corporate governance on preventing data breaches.

CRediT authorship contribution statement

Wen Chen: Writing – review & editing, Writing – original draft, Project administration, Methodology, Conceptualization. **Xing Li:** Writing – review & editing, Methodology, Formal analysis, Conceptualization. **Haibin Wu:** Writing – review & editing, Methodology, Formal analysis, Conceptualization. **Liandong Zhang:** Writing – review & editing, Supervision, Methodology, Conceptualization.

Data availability

Data will be made available on request.

Appendix A. Variable definitions

Variable	Definition
Data Breach	
Breach	Dummy variable that takes the value of one if a firm experiences a data breach in year *t*, and zero otherwise.
Managerial Myopia	
Avg_ADisc	The average value of abnormal discretionary R&D and SG&A expenditures over the three-year period (years $t-1$, $t-2$, and $t-3$), computed using the residuals estimated from the model of Roychowdhury (2006), multiplied by −1.
Avg_AAccr	The average value of abnormal accruals over the three-year period (years $t-1$, $t-2$, and $t-3$), computed using the residuals estimated from the modified Jones model (Dechow et al., 1995).
Control Variables	
Size	The logarithmic value of the market value of total assets, calculated as $\ln(PRCC\_F_t*CSHO_t + AT_t - CEQ_t)$.
TobinQ	Market value of total assets divided by the book value of total assets, calculated as $(PRCC\_F_t*CSHO_t + AT_t - CEQ_t)/AT_t$.
LEV	Book value of long-term debt plus debt in current liabilities, divided by total assets, calculated as $(DLTT_t + DLC_t)/AT_t$.
Intangibility	Intangible assets divided by total assets, calculated as $INTAN_t/AT_t$.
ROA	Net income divided by total assets, calculated as NI_t/AT_t.
SalesGrowth	Sales growth is calculated as $(SALE_t - SALE_{t-1})/SALE_{t-1}$.
FinancialCons	Dummy variable that takes the value of one if a firm's Whited–Wu score (Whited and Gu, 2006) is in the top tercile of the sample in the given year, and zero otherwise, where the Whited–Wu score (Whited and Gu, 2006) is calculated as $-0.091*(IB_t + DP_t)/AT_{t-1} - 0.062*DIV_t + 0.021*DLTT_t/AT_{t-1} - 0.044*ln(AT_t) + 0.102*industry\ SalesGrowth_t - 0.035*firm\ SalesGrowth_t$.
BlockOwner	Percentage of shares held by block holders. A block holder is defined as an institutional investor who owns at least 5 % of the outstanding shares.
FT500	Dummy variable that takes the value of one if a firm is included in the Fortune 500 list in the year, and zero otherwise. The Fortune 500 membership information is obtained from the Fortune website.
Other Variables	
Avg_ARD	The average value of abnormal R&D expenses over the three-year period (years $t-1$, $t-2$, and $t-3$), computed using the residuals estimated from the model of Kothari et al. (2016), multiplied by −1.
Avg_ASGA	The average value of abnormal SG&A expenses over the three-year period (years $t-1$, $t-2$, and $t-3$), computed using the residuals estimated from the model of Kothari et al. (2016), multiplied by −1.
Avg_AAD	The average value of abnormal advertising expenses over the three-year period (years $t-1$, $t-2$, and $t-3$), computed using the residuals estimated from the model of Kothari et al. (2016), multiplied by −1.

(*continued on next page*)

(*continued*)

Variable	Definition
Age	The logarithmic value of the number of years since a firm's first appearance in Compustat.
CFO	Operating cash flow divided by total assets, calculated as $OANCF_t/AT_t$.
Suspect	A dummy variable that takes the value of one if either of the following two criteria are met: the change in income before extraordinary items (*IB*) scaled by total assets (*AT*) lies in the range [0, 0.01] or earnings beats analyst forecasts by one cent or less.
INDGrowth	Industry sales growth is the median of firm sales growth in an industry.
GDPGrowth	GDP growth in the state where firms are headquartered.

Appendix B. Definitions of breach types

Breach Type	Description
Payment Card Fraud	Fraud involving debit and credit cards that is not accomplished via hacking, e.g., skimming devices at point-of-service terminals.
Hacking or Malware	Hacked by outside party or infected by malware.
Insider	Insider (someone with legitimate access intentionally breaches information).
Physical Loss	Includes paper documents that are lost, discarded, or stolen (non-electronic).
Portable Device	Lost, discarded, or stolen laptop, PDA, smartphone, memory stick, hard drive, data tape, etc.
Stationary Device	Stationary computer loss (lost, inappropriately accessed, discarded, or stolen computer or server not designed for mobility).
Unintended Disclosure	Unintended disclosure (not involving hacking, intentional breach, or physical loss, e.g., sensitive information posted publicly, mishandled, or sent to the wrong party by publishing it online or sending it in an email, mail, or fax).
Unknown	All others.

Definitions of these breach types are reproduced from the PRC website: https://privacyrights.org/data-breaches.

References

Acharya, V., Xu, Z., 2017. Financial dependence and innovation: the case of public versus private firms. J. Financ. Econ. 124 (2), 223–243.

Aghion, P., Van Reenen, J., Zingales, L., 2013. Innovation and institutional ownership. Am. Econ. Rev. 103 (1), 277–304.

Akey, P., Lewellen, S., Liskovich, I., 2018. Hacking corporate reputations. Working paper no. 3143740, Rotman School of Management. Available at https://ssrn.com/abstract=3143740 or 10.2139/ssrn.3143740.

Allianz Global Corporate & Specialty, 2019. Allianz risk barometer. Available at: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf.

Angrist, J.D., Pischke, J.S., 2010. The credibility revolution in empirical economics: how better research design is taking the con out of econometrics. J. Econ. Perspect. 24 (2), 3–30.

Ashraf, M., 2022. The role of peer events in corporate governance: evidence from data breaches. Account. Rev. 97 (2), 1–24.

Asker, J., Farre-Mensa, J., Ljungqvist, A., 2015. Corporate investment and stock market listing: a puzzle? Rev. Financ. Stud. 28 (2), 342–390.

Barton, J., Simko, P.J., 2002. The balance sheet as an earnings management constraint. Account. Rev. 77 (s–1), 1–27.

Beatty, A., Liao, S., Yu, J.J., 2013. The spillover effect of fraudulent financial reporting on peer firms' investments. J. Account. Econ. 55, 183–205.

Benmelech, E., Kandel, E., Veronesi, P., 2010. Stock-based compensation and CEO (dis) incentives. Q. J. Econ. 125 (4), 1769–1820.

Bergstresser, D., Philippon, T., 2006. CEO incentives and earnings management. J. Financ. Econ. 80 (3), 511–529.

Bhojraj, S., Hribar, P., Picconi, M., McInnis, J., 2009. Making sense of cents: an examination of firms that marginally miss or beat analyst forecasts. J. Financ. 64 (5), 2361–2388.

Black Hat, 2015. Black Hat attendee survey. Available at: https://www.blackhat.com/docs/us-15/2015-Black-Hat-Attendee-Survey.pdf.

Bolton, P., Kacperczyk, M., 2023. Firm Commitments. National Bureau of Economic Research. Working paper no. w31244.

Burgstahler, D., Dichev, I., 1997. Earnings management to avoid earnings decreases and losses. J. Account. Econ. 24 (1), 99–126.

Burns, N., Kedia, S., 2006. The impact of performance-based compensation on misreporting. J. Financ. Econ. 79 (1), 35–67.

Bushee, B.J., 1998. The influence of institutional investors on myopic R&D investment behavior. Account. Rev. 73 (3), 305–333.

Caskey, J., Ozel, N.B., 2017. Earnings expectations and employee safety. J. Account. Econ. 63 (1), 121–141.

Chen, Y., Rhee, S.G., Veeraraghavan, M., Zolotoy, L., 2015. Stock liquidity and managerial short-termism. J. Bank. Financ. 60, 44–59.

Cohen, D.A., Zarowin, P., 2010. Accrual-based and real earnings management activities around seasoned equity offerings. J. Account. Econ. 50 (1), 2–19.

Dechow, P.M., Sloan, R.G., Sweeney, A.P., 1995. Detecting earnings management. Account. Rev. 70 (2), 193–225.

Edmans, A., 2009. Blockholder trading, market efficiency, and managerial myopia. J. Financ. 64 (6), 2481–2513.

Edmans, A., Fang, V.W., Lewellen, K.A., 2017. Equity vesting and investment. Rev. Financ. Stud. 30 (7), 2229–2271.

Edmans, A., Gabaix, X., Landier, A., 2008. A multiplicative model of optimal CEO incentives in market equilibrium. Rev. Financ. Stud. 22 (12), 4881–4917.

Efendi, J., Srivastava, A., Swanson, E.P., 2007. Why do corporate managers misstate financial statements? The role of option compensation and other factors. J. Financ. Econ. 85 (3), 667–708.

Eldenburg, L.G., Gunny, K.A., Hee, K.W., Soderstrom, N., 2011. Earnings management using real activities: evidence from nonprofit hospitals. Account. Rev. 86 (5), 1605–1630.

Erickson, M., Hanlon, M., Maydew, E.L., 2006. Is there a link between executive equity incentives and accounting fraud? J. Account. Res. 44 (1), 113–143.

Fields, T.D., Lys, T.Z., Vincent, L., 2001. Empirical research on accounting choice. J. Account. Econ. 31, 255–307.

Frankel, R.M., Johnson, M.F., Nelson, K.K., 2002. The relation between auditors' fees for nonaudit services and earnings management. Account. Rev. 77, 71–105.

Gilliam, T.A., Heflin, F., Paterson, J.S., 2015. Evidence that the zero-earnings discontinuity has disappeared. J. Account. Econ. 60 (1), 117–132.

Graham, J.R., Harvey, C.R., Rajgopal, S., 2005. The economic implications of corporate financial reporting. J. Account. Econ. 40 (1–3), 3–73.

Gunny, K.A., 2010. The relation between earnings management using real activities manipulation and future performance: evidence from meeting earnings benchmarks. Contemp. Account. Res. 27 (3), 855–888.

Healy, P.M., Wahlen, J.M., 1999. A review of the earnings management literature and its implications for standard setting. Account. Horiz. 13 (4), 365–383.

Huang, H.H., Wang, C., 2021. Do banks price firms' data breaches? Account. Rev. 96 (3), 261–286.

Hutton, A.P., Marcus, A.J., Tehranian, H., 2009. Opaque financial reports, R^2, and crash risk. J. Financ. Econ. 94 (1), 67–86.

Identity Theft Resource Center, 2018. End-of-year data breach report. Available at: https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/.

Johnson, M., Kang, M.J., Lawson, T., 2017. Stock price reaction to data breaches. J. Financ. Issues 16, 1–13.

Kamiya, S., Kang, J.K., Kim, J., Milidonis, A., Stulz, R.M., 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. J. Financ. Econ. 139 (3), 719–749.

Kasznik, R., McNichols, M.F., 2002. Does meeting earnings expectations matter? Evidence from analyst forecast revisions and share prices. J. Account. Res. 40 (3), 727–759.

Kim, J.B., Li, Y., Zhang, L., 2011. CFOs versus CEOs: equity incentives and crashes. J. Financ. Econ. 101 (3), 713–730.

Kothari, S.P., Mizik, N., Roychowdhury, S., 2016. Managing for the moment: the role of earnings management via real activities versus accruals in SEO valuation. Account. Rev. 91 (2), 559–586.

Lee, J.M., Park, J.C., Folta, T.B., 2018. CEO career horizon, corporate governance, and real options: the role of economic short-termism. Strateg. Manag. J. 39 (10), 2703–2725.

Lo, K., Ramos, F., Rogo, R., 2017. Earnings management and annual report readability. J. Account. Econ. 63 (1), 1–25.

Machlup, F., 1967. Theories of the firm: marginalist, behavioral, managerial. Am. Econ. Rev. 57 (1), 1–33.

Matsumoto, D.A., 2002. Management's incentives to avoid negative earnings surprises. Account. Rev. 77 (3), 483–514.

New York Stock Exchange, 2014. Managing cyber risk: are companies safeguarding their assets? Available at: https://www.nyse.com/publicdocs/nyse/listing/NYSE_Governance_Services_Managing_Cyber_Risk.pdf.
Peng, L., Roell, A., 2008. Manipulation and equity-based compensation. Am. Econ. Rev. 98 (2), 285–290.
Ponemon Institute, 2019. Cost of a data breach report. Available at: https://www.ibm.com/downloads/cas/RDEQK07R.
Porter, M.E., 1992. Capital disadvantage: America's failing capital investment system. Harv. Bus. Rev. 70 (5), 65–82.
Roychowdhury, S., 2006. Earnings management through real activities manipulation. J. Account. Econ. 42 (3), 335–370.
Roychowdhury, S., Shroff, N., Verdi, R.S., 2019. The effects of financial reporting and disclosure on corporate investment: a review. J. Account. Econ. 68 (2), 101246.
Stein, J.C., 1989. Efficient capital markets, inefficient firms: a model of myopic corporate behavior. Q. J. Econ. 104 (4), 655–669.
Stein, J.C., 2003. Agency, information and corporate investment. Handbook of the Economics of Finance. Elsevier, pp. 111–165.
Whited, T.M., Wu, G., 2006. Financial constraints risk. Rev. Financ. Stud. 19 (2), 531–559.
Xu, H., Savannah, G., Haislip, J.Z., Pinsker, R.E., 2019. Earnings management in firms with data security breaches. J. Inf. Syst. 33 (3), 267–284.
Zang, A.Y., 2011. Evidence on the trade-off between real activities manipulation and accrual-based earnings management. Account. Rev. 87 (2), 675–703.
Zingales, L., 2000. In search of new foundations. J. Financ. 55 (4), 1623–1653.