The Impacts of Layoffs Announcement on Cybersecurity Breaches

Thi Tran  
*Binghamton University, SUNY, ttran9@binghamton.edu*

Bao Gia Do  
*University of Information Technology, Vietnam National University, Ho Chi Minh City, baogiado1305@gmail.com*

Anh Ngo  
*Liverpool John Moores University, tuananhsteven@gmail.com*

Sathwik Krishtipati  
*Binghamton University, skrisht1@binghamton.edu*

Nhat Anh Dang  
*Texas Woman's University, ndang5@twu.edu*

*See next page for additional authors*

Follow this and additional works at: https://aisel.aisnet.org/pacis2024

**Recommended Citation**  
Tran, Thi; Do, Bao Gia; Ngo, Anh; Krishtipati, Sathwik; Dang, Nhat Anh; and Sarkar, Sumantra, "The Impacts of Layoffs Announcement on Cybersecurity Breaches" (2024). *PACIS 2024 Proceedings*. 10.  
https://aisel.aisnet.org/pacis2024/track07_secprivacy/track07_secprivacy/10

This material is brought to you by the Pacific Asia Conference on Information Systems (PACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in PACIS 2024 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Presenter Information
Thi Tran, Bao Gia Do, Anh Ngo, Sathwik Krishtipati, Nhat Anh Dang, and Sumantra Sarkar

This event is available at AIS Electronic Library (AISeL): https://aisel.aisnet.org/pacis2024/track07_secprivacy/track07_secprivacy/10
The Impacts of Layoffs Announcement on Cybersecurity Breaches

Short Paper

Anh Ngo
Liverpool John Moores University
Liverpool, England, United Kingdom
UPLTNGO@ljmu.ac.uk

Nhat Anh Dang
Texas Woman’s University
Denton, Texas, United States
ndang5@twu.edu

Bao Gia Do
Vietnam National University
Ho Chi Minh City, Ho Chi Minh, Viet Nam
18520482@gm.uit.edu.vn

Sathwik Krishtipati
Binghamton University
Binghamton, New York, United States
skrisht1@binghamton.edu

Thi Tran
Binghamton University
Binghamton, New York, United States
ttran9@binghamton.edu

Sumantra Sarkar
Binghamton University
Binghamton, New York, United States
ssarkar@binghamton.edu

Abstract

The recent economic situations worldwide and particularly in the United States (US) have witnessed widespread waves of corporation layoffs. Simultaneously, we have also experienced much more severe issues of cybersecurity violations, such as harmful data breaches and cyberattacks. This paper attempts to examine the possible connections of corporate decisions and the severity of possible cybersecurity in the lenses of four established hypotheses surrounding the likelihood and severity of data breaches as the social reactions facing the announcements of corporate layoffs. It also expands the consideration to the effectiveness of corporate social responsibility in triggering these reactions. Various theoretical contributions, practical implications, and managerial implications, together with suggestions for future research, have been extracted accordingly.

Keywords: data breach, cyberattack, layoff, corporate social responsibility, reactions
Introduction

In the first quarter of 2023, a staggering number of more than 136,000 employees were let go in layoffs in the United States at the end of September, according to Forbes’ 2023 Layoff Tracker (Bushard, 2023). This figure surpasses the total number of layoffs from the previous two fiscal quarters and is based on data compiled by Forbes. Notably, prominent companies such as Amazon, Google, IBM, Salesforce and Goldman Sachs were substantial reductions in their workforce. A wave of job cuts spanning tech, banks, media and manufacturing continues. Revealed by CNN in the third quarter of 2023, Amazon, Alphabet, Dell, Boeing and hundreds other firms, have collectively disclosed their decisions to implement workforce reductions, impacting a significant number of employees in the United States. Most recently, it has been reported to have more than 270,000 laid off positions in the entire 2023, and nearly 25,000 positions within just over a month at the beginning of 2024 (Chan, 2024), indicating a dramatic increasing trend of layoffs in the current market.

By definition, layoffs are organizational decisions made for several reasons, including cost-cutting, strategic restructuring, or response to economic challenges (Budd & Na, 2017). While it is expected that layoffs are based on necessary business decisions (Richter and König, 2017), such behaviors can significantly stir the social statuses of those impacted and involved stakeholders, which needs serious consideration to minimize unwanted social damages (Rajnikant, 2023).

After a series of layoffs announcements from companies, the consequences of these staff reductions extend beyond monetary and operational deliberations. The responses of the employees varied from surprise and disillusionment to anxiety and animosity (Wiesenfeld, 2001). These sentiments, intensified by the feeling of job uncertainty that frequently accompanies downsizing, fostered an atmosphere of increased internal conflicts within the organization (Dutta et al., 2009). While the companies cited financial restructuring as the primary motivation behind this difficult decision, the aftermath revealed a complex relationship between human emotions, organizational security, and the ever-present threat of cybersecurity breaches (Oladapo et al., 2018).

The effect of layoffs can exert a noteworthy influence on the all-encompassing work environment, contributing to increased stress and distraction among remaining employees (Friedman et al., 2020). The weight of witnessing colleagues leaving and the uncertainty surrounding their own job security can result in increased feelings of anxiety and decreased morale. Within this context, employees may encounter difficulties in sustaining their attention and focus on their daily tasks. This state of distraction can also extend to their responsibilities in adhering to cybersecurity best practices. Experts in the field of cybersecurity caution that this lack of vigilance can create vulnerabilities, rendering it easier for malicious individuals to exploit weaknesses in security protocols and increasing the likelihood of employees falling prey to social engineering attacks, such as phishing or pretexting schemes (Kemper, 2019).

Despite the possibility of backfired reactions from (former) employees or even the public toward firms that annonce layoffs due to sentimental reactions such as anger and disappointment, research on potential cyber threats as public reactions toward layoff announcements are scarce. Such an examination is vital to prevent forthcoming cybersecurity harmful events such as data breaches and cyber-attacks, as well as to aid efforts minimizing informational harms towards potential victims of those events. Particularly, while existing research has extensively investigated various factors contributing to cybersecurity breaches, there is a notable gap concerning the influence of workforce reductions, particularly layoffs, on cybersecurity risks. Despite studies addressing security culture, overall staffing levels, and economic pressures, the emotional and psychological impact of layoffs on employees, and its subsequent effect on cybersecurity, remains undere xplored.

To fill the research gap and to answer the aforementioned necessary research need, in this study, we aim to explore and statistically examine the answer to the overall research question, as “How announcements of layoffs can lead to cybersecurity breaches?”. There are several channels for which employee layoffs could post a threat on firms’ cybersecurity. First, layoffs can result in increased levels of former employees’ dissatisfaction, thus increasing the potential for internal threats (Oladapo et al., 2018). Disgruntled ex-employees might perceive their former company as vulnerable entities for potential cyberattacks (Choi and Shin, 2019; Nikolova & Devinney, 2019). They may demonstrate a greater tendency to exploit their knowledge of the organization’s information systems and procedures to provoke or assist stealing,
destroying or manipulating valuable, highly sensitively classified and business-related vital information packages. Particularly, this situation can motivate various types of threats to cyber security toward the financial and strategic information systems, including but not limited to cyber-attacks, data breaches, data theft, system disruption, or the introduction of malware (Williams et al., 2013). Second, mass layoffs have the potential to result in the withdrawal of professionals specialized in cybersecurity, thereby causing a deficiency in the organization's cybersecurity proficiency (Kohli et al., 2020). This deficiency can impair an organization's capacity to preemptively safeguard itself against emerging cyber risks, particularly those originating from former employees (McNurlin & Sprague, 2019).

To answer the aforementioned research question and expectedly fill the emerging research gap, our research model and hypotheses are tested on various databases. Specifically, we gather data from different sources related to cybersecurity breach incidents, including their frequency, severity, and specific details of each incident that have been widely adopted by cybersecurity experts such as Privacy Rights Clearinghouse (PRC) website, SEC EDGAR, Nexus Uni (Smith and Vincent, 2021; Li and Walton, 2022). More details on the methodology of this study will be further explained in the following sections.

In this research endeavor, we embark upon a comprehensive statistical investigation into the intricate relationship between layoffs and cybersecurity breach. Our research focuses on three aspects. First, our aim is to establish whether there is a discernible association between the disclosure of workforce cutbacks by firms and their probability of encountering a cybersecurity breach. Second, we examine if the level of severity in the publicly announced layoffs plan has impacts on the seriousness of subsequent cybersecurity infractions. Third, we examine the mitigating effect of corporate social responsibility in the connection between layoffs and cybersecurity breach. Our research thus encompasses a thorough analysis of the intricate connections that exist among layoffs, CSR, and cybersecurity incidents. It is then expected to significantly contribute to the literature of information consumption and the efforts of understanding and controlling online public reactions facing such breakthrough and impactful events as layoff announcements, and later sheds lights for future research expansions.

Apart from the theoretical contribution to the current literature of examining information consumption and reactions, this study has several expected practical contributions. We contribute to a growing area of research by being one of the frontrunners in examining the diverse effects of layoffs on companies. Our particular emphasis lies in exploring the intricate connection between layoffs and cybersecurity breaches. By bringing attention to this unexplored interplay, we broaden the understanding of internal organizational incidents and their impact on cybersecurity breaches. Furthermore, our research offers business leaders a deeper understanding of the intricate relationship between employee relations practices and cybersecurity outcomes. Equipped with this knowledge, decision-makers can make more informed decisions regarding workforce management, communication strategies, and cybersecurity protocols, ultimately bolstering their ability to navigate the challenges posed by cybersecurity threats while maintaining workforce.

**Theoretical Background**

In this section, we discuss the concerned contexts of layoffs and cyber threats of data breaches, and form the theoretical basis for our study.

**Layoffs impacts on companies**

In the face of economic challenges, mass layoffs profoundly impact companies, affecting not only their financial health but also their perceived image and reputation. Research by Abraham et al. (2013) highlights the wide-ranging implications of such strategic decisions, emphasizing the need for a comprehensive understanding of their ramifications. These studies reveal a complex relationship between layoffs and long-term firm performance, indicating that the aftermath of layoffs intertwines with a company's financial trajectory over time (Abraham et al., 2013).

Beyond financial metrics, the repercussions of layoffs extend to corporate reputation and investor sentiments. Scholars like Gatzert (2015) and Collins et al. (2018) delve into the interplay between reputation and events that may damage it, underscoring their influence on financial performance and broader perceptions of the company's image. Moreover, research on disclosure strategies and investor reactions
emphasizes the importance of how layoffs are communicated and justified, as it significantly impacts the preservation of the company's perceived image (Nègre et al., 2017; Bachura et al., 2022).

However, amid these considerations, an unexplored dimension emerges—the psychological impact of layoffs on the remaining workforce. Sarvesh & Nitin (2022) suggest that understanding this aspect is crucial, as it may influence employee engagement and productivity. Furthermore, while existing studies shed light on critical dimensions, there remains uncharted territory—the potential influence of layoffs on organizational trust and subsequent cascading effects on stakeholder relationships (Wiesenfeld et al., 2001). By exploring these facets comprehensively, companies can better navigate the multifaceted impacts of layoffs on both their financial standing and their broader image and relationships.

**Cybersecurity Breach**

**The impacts of cybersecurity breach on companies**

In their 2022 survey of 722 chief financial officers, PricewaterhouseCoopers (PwC) reports that top company executives rank cyber-attacks as the number risk that businesses are facing. Despite the fact that businesses have implemented several data protection techniques (i.e., system authentication, encryption, and user access control) along with risk mitigation measures (i.e., employee training, user education), perpetrators are becoming more organized and complex (Juma’h and Alnsour, 2020). In recent years, there have been numerous severe data loss instances, leaving business organizations with massive losses. For instance, in 2019, Capital One Financial reported a serious breach incident, which affected nearly one hundred million customers in the United States and caused a $190 million settlement (Avery, 2022). The attackers gained access to sensitive information such as credit scores, credit limits, balances, payment history, and contact information. Additionally, 140,000 Social Security numbers and 80,000 connected bank account details were leaked. Capital One is not the only one who suffers from the negative impact of a cybersecurity breach. According to IBM's 2023 Cost of Data Breach Report¹, the global average cost of a data breach in 2023 is $4.45 million, up 15% in the past three years, indicating that this is an increasingly serious issue. As a result, 51% of firms intend to boost cybersecurity investment this year, which includes incident response (IR) planning and testing, staff training, and threat detection and response systems.

Prior studies have examined the impacts of cybersecurity breach on firms’ performance. From the operation perspective, cybersecurity breach is documented to devastatingly reduce a firm production volume and increase cost (Bai et al., 2015). Firms who experience cybersecurity breaches are also associated with higher CIO and CEO turnover rates (Banker and Feng, 2019). Financially, cybersecurity breaches are documented to negatively impact firms’ stock performance (Acquisti et al., 2006; Richardson et al., 2019). Lenders are found to be more critical over firms who experience cybersecurity breach (Huang and Wang, 2021). Additionally, firms who suffer from cybersecurity breach also experience higher perceived risk (Gwebu et al., 2014), resulting in higher audit fees (Li et al., 2017; Smith et al., 2019).

**Determinants of Cybersecurity Breach**

It is crucial to understand the factors that contribute to cybersecurity breaches. Many prior studies have explored the determinants of firms’ cybersecurity breach and what factors would mitigate/enhance the risk. IT expertise within the top management team plays a significant role in minimizing the frequency of reported cybersecurity data breaches. Specifically, a CEO/CFO with a background in IT or the presence of a CIO within the top management team can support establishing and implementing strong IT policies and controls to reduce the risk of data breaches (Haislip et al., 2021). The establishment of a board-level technology committee or internal cybersecurity audit committee as part of the company’s IT governance significantly mitigates data breaches incidents (Higgs et al., 2016; Islam et al., 2018). Besides that, firms that invest in digitalization, network security control systems (i.e., antivirus and intrusion detection systems), identity and access management security systems (i.e., biometric scanning and user authentication), and innovation tend to experience reduced risks of data breach occurrences (Li et al., 2021; Sen et al., 2023).

¹ https://www.ibm.com/reports/data-breach
Prior research has also explored various other possible determinants of data breaches. First, some studies focus on economic factors, such as financial constraints, budgetary limitations, and resource allocation decisions within organizations (Campbell et al., 2003; Chai et al., 2011). Then, organizational factors affecting the likelihood of breaches are considered, such as organizational culture, employee training programs, incident response protocols, and the commitment of leadership to cybersecurity practices (Haislip et al., 2021; Kemper, 2019). Importantly, technological factors play a critical role in triggering the likelihood and susceptibility of facing data breaches, including outdated systems, insecure configurations, and emerging cyber threats, contribute to an organization’s susceptibility to breaches (West and Zentner, 2019). All of these possible determinants of breaches will further help our study to better form the following considerations of hypotheses and research models.

**Theory Development and Research Hypotheses**

**The relationship between layoffs and cybersecurity breach**

There are several mechanisms in which layoffs can potentially influence the state of cybersecurity within an organization. First, layoffs can create negative emotions such as uncertainty, anxiety, and stress among remaining employees (Mujtaba, 2022). Employees who are worried about their job security may not prioritize security best practices. Besides that, layoffs can lead to dissatisfied former staff members who could potentially access sensitive data or systems, presenting an internal security risk, whether it’s intentional or unintentional (Shavell, 2020). Second, layoffs frequently lead to diminished human resources which reduce an organization’s capability to monitor and respond to security threats (Mujtaba and Senathip, 2020). Moreover, layoffs may loss of experienced cybersecurity experts who were in charge of establishing and maintaining security measures. The absence of these experts can undermine an organization’s capacity to protect against cyber threats efficiently (Hartmann and Carmenate, 2021). Third, layoffs not only lead to a reduced workforce but also lead to a decrease in the available budget. As a consequence of these layoffs, organizations might postpone or terminate cybersecurity projects and plans due to financial limitations stemming from the spending reductions. This can lead to outdated or inadequate security systems, which could expose the organization to potential security breaches (Sen et al., 2023). Furthermore, in response to layoffs, some organizations may opt to delegate specific IT and security tasks to external outsourcing service providers (Li et al. 2021). This decision could potentially introduce additional risks if the security practices of these providers do not meet the same standards as those of the organization. Finally, a company often faces negative publicity when it announces layoffs (Stabler et al., 2023). These layoffs might be interpreted as an indication of financial problems or poor leadership, resulting in disapproval from the public. Certain individuals with hacking skills are driven by social or political motivations. If they perceive a company’s actions as unjust or irresponsible, they might select it as a target for hacktivist activities. Their actions could involve damaging the company’s website, unveiling confidential information, or disrupting its activities in order to bring attention to their cause (Schneider, 2012). From the above discussion, we formally form our hypotheses as below:

**Hypothesis H1a:** Companies who announce their layoffs plan are more likely to face a cybersecurity breach.

**Hypothesis H1b:** The severity of the layoffs plan positively influences the severity of the cybersecurity breach.

**The mitigating impact of Corporate Social Responsibility (CSR)**

Corporate Social Responsibility (CSR) entails a firm’s dedication to fostering sustainable economic development. This involves collaborative efforts with employees, their families, the local community, and society as a whole, with the aim of enhancing overall quality of life. Corporate social responsibility (CSR) is a topic which has attracted academia attention since the 1960s. Spending money on CSR efforts helps build a positive public image for firms, which could result in potential future benefits associated with that image. Guidry and Patten (2010) indicates that a CSR efforts could help establish the company reputation and create a good basis for stakeholders (i.e., employees, customers) communications. Lins et al. (2017) find that during the 2008 financial crisis, firms with higher CSR experienced higher stock returns and significantly outperformed their peers. D’Arcy et al. (2020) examine how companies implement CSR through the lens of corporate social performance (CSP) and suggest that a firm’s level of social engagement,
as measured by CSP, may impact its risk of cyber attacks leading to data breaches. Furthermore, they argue that applying stakeholder theory at a fundamental level shows that robust CSP can improve a company’s relationships with its stakeholders. A robust corporate social performance (CSP) can enhance trust with stakeholders by demonstrating the organization’s commitment to social and environmental responsibilities. Due to the benefit of CSR, we want to explore the mitigating effects of CSR on the impact of layoffs on cybersecurity breach. We argue that firms who have a higher level of CSR will either (a) be less likely to experience a cybersecurity breach when they announce their layoffs plans, or (b) suffer less severe cybersecurity breach. We formalize our prediction under the two hypotheses below:

**Hypothesis H2a:** Companies with a higher level of corporate social responsibility (who announce their layoffs plan) will be less likely to face a cybersecurity breach.

**Hypothesis H2b:** Companies with a higher level of corporate social responsibility (who announce their layoffs plan) will suffer from less severe cybersecurity breaches.

### Methodology

In this section, details about the methodology of the study are presented.

#### Data Sources

We gather data from different sources. First, data regarding firms’ cybersecurity breach incidents are from Privacy Rights Clearinghouse (Privacyrights.org). Privacyrights.org is an established nonprofit organization which has been tracking data breaches incidents since 1992. Their database has been widely adopted by cybersecurity researchers (Smith and Vincent, 2021, Li and Walton, 2022). Second, we also follow Calderon and Gao (2023) method to generate a novel dataset of cybersecurity breaches from firms’ annual reports. Data of firms’ annual reports are from the SEC EDGAR database. Under Calderon and Gao (2023) method, data regarding firms’ cybersecurity breaches incidents are directly scraped from Item 1A of their 10-K reports. Third, data regarding firms’ layoffs announcements are manually collected from news sources. We use Nexis Uni to search through companies within the list of S&P 500 and identify (1) the date and time of the layoffs announcements, (2) the number of employees being laid off. We restrict our sample to just announcements from 2021 and forward to alleviate the spill-over effect of COVID-19. Fourth, data regarding companies’ CSR levels are from MSCI ESG database. In addition to the above main data sources, we also gather data from COMPUSTAT, BoardEx, and Audit Analytics to generate control variables.

#### Measurement of Dependent Variable (DV)

The main dependent variable of interest in this study is $BREACH$, which is an indicator variable equal 1 if a firm $i$ suffer from a cybersecurity breach in year $t$, 0 otherwise. Additionally, we also estimate the severity of the cybersecurity risk by using the number of words and the number of uncertainty words within the cybersecurity breach disclosure in firms’ 10-k reports. This results in the variable $BREACHSEVERITY$.

#### Measurement of main Independent Variables (IVs)

The main independent variable of interest in this study is $LAYOFFS$, which is an indicator variable equal 1 if a firm announces their layoffs plans in year $t$, 0 otherwise. Moreover, we estimate the severity of the layoffs announcement by using the total number of employees being laid off in the year $t$. This results in the variable $LAYOFFSEVERITY$. Additionally, to explore the mitigating impact of firms’ past ethical efforts and corporate social responsibility level, we adopt the variable CSR, which is constructed using MSCI ESG database. CSR is a composite variable, calculated by adding/subtracting the score from 5 stakeholder-oriented categories of employee relations, community, diversity, environment, and human rights.

### Research Models

At the current stage, our studies are in-progress, while some preliminary efforts have obtained results. We have collected data for both layoff announcements and data breaches incidents from different sources and started several data analyses, which are expected to yield coming preliminary results. Accordingly, based
on the aforementioned hypotheses in the previous sections, we formulate the following statistical models for testing.

To test H1a, we adopt the following Logistic Regression model:

$$\text{Prob}(\text{BREACHRISK}_{i,t+1} = 1) = \beta_0 + \beta_1 \text{LAYOFF}_{i,t+1} + \beta_2 \text{LNASSET}_{i,t} + \beta_3 \text{LNFIRMAGE}_{i,t} + \beta_4 \text{LEVERAGE}_{i,t} + \beta_5 \text{ROA}_{i,t} + \beta_6 \text{GROWTH}_{i,t} + \beta_7 \text{MB}_{i,t} + \beta_8 \text{GROWTH}_{i,t} + \beta_9 \text{Industry FE} + \beta_{10} \text{Year} + \epsilon$$  (1)

In that, BREACHRISK is the main DV of interest, indicating if firm i suffer from cybersecurity breach in year t. Layoffs is the main independent variable of interest, capturing if a firm i announces any layoffs plans in year t. Following prior studies (Li and Walton, 2023, Brown et. al., 2018), we control for a variety of factors which have been documented to impact the likelihood of a firm facing a cybersecurity breach. We control for firm size (LNASSET), age (LNFIRMAGE), leverage (LEVERAGE), profitable company (LOSS) and yearly growth (ROA, GROWTH, MB) because larger, expanding organizations may face heightened cybersecurity risk and disclosure incentives. All control variables (which are based on firm’s financial data) are lagged 1 year compared to the main DV to control for the timing gap in financial reports. The main coefficient of interest is $\beta_1$. If H1a is supported, then $\beta_1$ is positive and significant.

To test H1b, we adopt the following Ordinary Least Squares (OLS) regression model:

$$\text{BREACHSEVERITY}_{i,t+1} = \theta_0 + \theta_1 \text{LAYOFFSEVERITY}_{i,t+1} + \theta_2 \text{LNASSET}_{i,t} + \theta_3 \text{LNFIRMAGE}_{i,t} + \theta_4 \text{LEVERAGE}_{i,t} + \theta_5 \text{ROA}_{i,t} + \theta_6 \text{GROWTH}_{i,t} + \theta_7 \text{MB}_{i,t} + \theta_8 \text{GROWTH}_{i,t} + \theta_9 \text{Industry FE} + \theta_{10} \text{Year} + \epsilon$$  (2)

Most variables in (2) are similar to those of (1), except for BREACHSEVERITY, which captures the severity level of the cybersecurity breach affected by the layoffs in the year, and LAYOFFSEVERITY, which captures the severity of the layoff’s announcement. Our main coefficient of interest is $\theta_1$. If H1b is supported, then we will expect $\theta_1$ to be positive and significant.

To test H2a and H2b, we adopt the following regression models:

$$\text{Prob}(\text{BREACHRISK}_{i,t+1} = y_0 + y_1 \text{LAYOFF}_{i,t+1} + y_2 \text{LAYOFF*CSR}_{i,t+1} + y_3 \text{CSR}_{i,t} + y_4 \text{LNASSET}_{i,t} + y_5 \text{LNFIRMAGE}_{i,t} + y_6 \text{LEVERAGE}_{i,t} + y_7 \text{ROA}_{i,t} + y_8 \text{GROWTH}_{i,t} + y_9 \text{MB}_{i,t} + y_{10} \text{GROWTH}_{i,t} + y_{11} \text{Industry FE} + y_{12} \text{Year} + \epsilon$$  (3)

$$\text{BREACHSEVERITY}_{i,t+1} = \partial_0 + \partial_1 \text{LAYOFFSEVERITY}_{i,t+1} + \partial_2 \text{LAYOFF*CSR}_{i,t+1} + \partial_3 \text{CSR}_{i,t} + \partial_4 \text{LNASSET}_{i,t} + \partial_5 \text{LNFIRMAGE}_{i,t} + \partial_6 \text{LEVERAGE}_{i,t} + \partial_7 \text{ROA}_{i,t} + \partial_8 \text{GROWTH}_{i,t} + \partial_9 \text{MB}_{i,t} + \partial_{10} \text{LOSS}_{i,t} + \partial_{11} \text{Industry FE} + \partial_{12} \text{Year} + \epsilon$$  (4)

CSR is the variable which captures firms’ level of corporate social responsibility. All other variables are similarly defined above. If H2 is supported, then we will expect $y_1$ and $\partial_1$ to be negative.

**Discussion**

From the expected results of the proposed research models, we have the following extracted potential contributions, spanning across various perspectives.

Our study has several expected theoretical contributions to the body of knowledge for the current literature. First, it enriches the understanding of economic cost and market reactions (Campbell et al., 2003; Chan, 2011) by examining stock market evidence, investigating investors’ responses to firms’ information security investment decisions, and examining the importance of proactive cybersecurity measures in maintaining market value. Second, it explores the impact of corporate reputation on financial performance (Gatzerl, 2015) in the aftermath of reputation-damaging events, such as data breaches, and the effects on firms’ financial performance, emphasizing the interconnectedness of cybersecurity and corporate reputation management. Third, it examines the issues of employee layoffs and organizational downsizing (Collins et al., 2018), such as psychological distress among employees and survivors' trust issues in re-employment opportunities, which in turn lead to harmful reactions and events like cyberattacks and data breaches.
In addition to the theoretical contributions, our work also signals practical implications to better safeguard the information systems facing possible data breaches. First, for cybersecurity investment and risk mitigation, enlightened by the work of Avery (2022) and Bachura et al. (2022), our analysis underscores the importance of strategic cybersecurity investments in mitigating the risks of data breaches. Second, considering stakeholder communication and brand management, our research extends the findings of Stäbler et al. (2023) and emphasizes the role of effective stakeholder communication in managing the aftermath of data breaches. Timely and transparent communication strategies can help organizations minimize reputational damage and maintain brand strength over time, mitigating the long-term impact of security incidents. Finally, about the consideration of employee training and cybersecurity awareness: Building on the insights of Kemper (2019), we advocate for robust employee training programs to enhance cybersecurity awareness within organizations. By empowering employees with the knowledge and skills to identify and respond to security threats, companies can fortify their defense mechanisms against internal and external breaches.

Along the line, our work also has several managerial implications. First, it suggests open and transparent communication throughout the layoff process can help mitigate feelings of anger and resentment among employees. This could reduce the likelihood of disgruntled employees intentionally causing cybersecurity breaches (Avery, 2022). Second, it aids the information security efforts during layoffs by maintaining robust cybersecurity protocols, which might involve stricter access controls, data encryption, and close monitoring of employee activity, particularly for those with high-level access (Haislip et al., 2021; West & Zentner, 2019). Third, it helps developing well-defined exit strategies that ensure a smooth handover of responsibilities and minimize disruption to security protocols can be beneficial (Richter & König, 2017). Fourth, the research could also inform corporate social responsibility (CSR) investments and stakeholder relationship management by focus on Cybersecurity in CSR Efforts in different ways. Companies might consider incorporating cybersecurity measures into their CSR initiatives by providing severance packages that emphasize ethical behavior and data security, or offering outplacement services that include cybersecurity awareness training (Collins et al., 2018). Finally, it helps strengthen stakeholder relationships through proactive communication with stakeholders, including employees, investors, and customers, about cybersecurity measures taken during layoffs can help maintain trust and confidence (Stäbler et al., 2023).

Our research therefore can shed lights on directions for related future research. Future studies can conduct case studies of companies that have experienced layoffs and cybersecurity breaches to understand how they managed the situation and identify best practices (Rajnikant, 2023). They can also have surveys targeting managers who have overseen layoffs to gather insights into their experiences and the challenges they faced regarding cybersecurity (Shavell, 2020).

To conclude, by exploring these managerial implications, our research can not only contribute to the academic understanding of cybersecurity risks associated with layoffs but also provide valuable practical guidance to companies navigating this complex situation.

**Conclusion**

Even rooted in the necessity of restructuring and optimizing costs from firms, layoff announcements have caused serious social concerns, public attentions and worriesome, as well as unwanted reactions toward the involved corporates. In lights of possible cyber threats as the reactions toward these events, our study examines how such announcements can lead to possible data breaches and the severity of the forthcoming breaches, which then cause even much bigger harms than the layoffs themselves to the public.

Our study aims to bridge this gap by examining the relationship between layoffs, corporate social responsibility (CSR) efforts, and cybersecurity breaches. We hypothesize that layoffs can create conditions where disgruntled employees, facing stress or job insecurity, are more inclined towards risky behaviors that heighten vulnerability to breaches. Additionally, we propose that CSR initiatives emphasizing ethical conduct and data security during layoffs could potentially mitigate these risks.

Extracting insights from various data sources, our research is expected to significantly contribute to the body of knowledge about information consumption and reaction in times of (financial) crises, as well as to the efforts controlling cybersecurity issues, particularly facing the severity of possible data breaches. This is expected to shed lights on future research expansions and related research directions in examining the
The Impacts of Layoffs Announcement on Cybersecurity Breaches

social impacts of both business restructuring and data breaches, as well as the unique roles of social media conversation in exaggerating the social issues and shaping public's attitudes and reactions.

By addressing this under-researched area, our study seeks to contribute to a deeper understanding of the multifaceted factors influencing cybersecurity breaches. Moreover, it offers practical insights for organizations navigating the complexities of workforce reductions, thereby aiding in the development of more effective cybersecurity strategies and risk mitigation measures.

References


Shavell, R. (2020). ePrevent data theft by disgruntled employees. HR Future, 2020(7), 36-37. https://hdl.handle.net/10520/EJC-1ef806b6e0

