Journal of the Association for Information Systems

Volume 26 | Issue 1 Article 5

2025

Do Good and Do No Harm Too: Employee-Related Corporate Social (Ir)responsibility and Information Security Performance

Qian Wang
University of Macau, qianwang@um.edu.mo

Dan Pienta
University of Tennesee, Knoxville, dpienta@utk.edu

Shenyang Jiang
Tongji University, shenyangjiang@tongji.edu.cn

Eric W. T. Ngai
The Hong Kong Polytechnic University, eric.ngai@polyu.edu.hk

Jason Bennett Thatcher
University of Colorado Boulder / University of Manchester, jason.thatcher@colorado.edu

Journal of the Association for Information Systems (2025) **26**(1), 171-204
doi: 10.17705/1jais.00908

RESEARCH ARTICLE

ISSN 1536-9323

Do Good and Do No Harm Too: Employee-Related Corporate Social (Ir)responsibility and Information Security Performance

Qian Wang,[1] Daniel Pienta,[2] Shenyang Jiang,[3] Eric W. T. Ngai,[4] Jason Bennett Thatcher,[5]

[1]Faculty of Business Administration, University of Macau, Macau, China, qianwang@um.edu.mo
[2]Dept. of Accounting and Information Management, University of Tennesee, Knoxville, USA, dpienta@utk.edu
[3]Advanced Institute of Business, Tongji University, China, shenyangjiang@tongji.edu.cn
[4]Dept. of Management & Marketing, The Hong Kong Polytechnic University, Hong Kong, China, eric.ngai@polyu.edu.hk
[5]University of Colorado Boulder, USA / University of Manchester, UK, jason.thatcher@colorado.edu

Abstract

This study draws upon the principal-agent theory to investigate the relationship between employee-related social performance and information security. This exploration encompasses both positive and negative dimensions of such performance: employee-related socially responsible activities (employee-related CSR) and employee-related socially irresponsible activities (employee-related CSiR). We employed a multistudy approach. First, we analyzed an eight-year sample of publicly listed firms, revealing a negative association between firms' engagement in employee-related CSR and information security risks, while their involvement in employee-related CSiR is positively linked to such risks. Our exploratory analysis uncovered additional intriguing findings, demonstrating that the uniqueness of employee-related social performance can amplify its impact on security. In a subsequent study, we conducted a scenario-based experiment to provide empirical evidence for our proposed principal-agent-based theory.

Keywords: Information Security, Data Breach, Employee-Related Social Performance, Employee-Related Corporate Social (Ir)responsibility, Agency Theory, Principal-Agent Framework

Yulin Fang was the accepting senior editor. This research article was submitted on March 16, 2023, and underwent two revisions.

1 Introduction

"He that does good for good's sake seeks neither paradise nor reward but is sure to find both in the end"[1] (William Penn)

In today's digital era, firms heavily rely on information systems (IS) to conduct business, necessitating stringent management of information security risks.[2] To counter these risks, firms employ a layered approach involving risk management planning, advanced technologies, and security compliance policies. Despite these efforts, security threats remain unpredictable and pose a significant danger to business operations (IBM, 2022), with experts noting that many come from employees—the actual people who work in firms (Bulgurcu et al., 2010; Cram et al., 2019). Verizon's Data Breaches Investigations Report (2022) reveals that 82% of data breaches involve human error and negligence. Consequently, the imperative to enhance information security measures from a human-centric perspective has become undeniable.

[1] https://www.brainyquote.com/authors/william-penn-quotes

[2] Hereafter, we abbreviate "information security risks" as "security risks."

Employees have emerged as significant contributors to security risks, largely driven by a misalignment between their objectives and their firms' security goals. Specifically, while employees' efforts toward security are crucial for firms, these efforts often lack immediate personal benefits, likely leading to employees' reduced engagement in security learning and adherence to protocols (Zhou et al., 2022). Furthermore, the intricate nature of network interconnectivity poses challenges in accurately detecting employees' suboptimal security behaviors, thereby frequently contributing to employees' insufficient compliance with security policies (Shim, 2015). This *misalignment* between employee and firm security goals is linked to considerable data breaches, as exemplified by the 2017 "WannaCry" ransomware attack that exploited an already patched vulnerability due to employees' disengagement and failure to install security updates timely.[3]

In light of this context, firms can potentially boost information security performance by strategically aligning employees' goals. Therefore, we focus on employee-related social performance, a corporate practice that effectively shapes employees' goal-aligned behaviors. Effective employee-related social performance, which includes activities that directly impact employees' interests (Barber, 2004; Garel & Petit-Romec, 2020), often influence employees' goal-aligned behaviors effectively. For instance, according to a 2010 report from the Workplace Foundation, inadequate workplace health and safety performance is a crucial predictor of diminished employee engagement.[4] Furthermore, a 2009 report from Right Management indicates that organizations are four times more likely to experience talent loss when they fail to effectively manage health and well-being.[5] Past research also shows that various forms of employee-related socially responsible activities—such as providing training (Madhavan et al., 2023; Yoon & Sengupta, 2019), fostering well-being initiatives (Ungureanu et al., 2019), implementing incentive schemes (Colvin & Boswell, 2007; Pendleton, 2006), offering employee support (Lee et al., 2008), and promoting work-life balance (Parkes & Langford, 2008)—contribute to aligning employees' goals with those of the firm. Therefore, employee-related social performance will likely impact firms' information security performance by shaping the alignment of employees' goals. With this in mind, we ask: *How does a firm's employee-related social performance influence its security risks?*

Our study specifically centers on employee-related social performance within firms due to the following reasons. Other facets of corporate social performance, particularly those oriented externally (e.g., community and environmental social performance), are often utilized for signaling or greenwashing (Wu et al., 2020; Zerbini, 2017). Research has extensively highlighted employees' hesitance toward their firms' externally oriented social initiatives (D'Arcy et al., 2020; Donia et al., 2019). In contrast, employee-related social performance is designed to directly enhance employee well-being, effectively bridging the gap between employees' goals and organizational goals (Flammer & Luo, 2017). This positioning makes employee-related social performance a pertinent focus for our research investigation.

To analyze the relationship between employee-related social performance and security risks, we adopted the principal-agent perspective (Eisenhardt, 1989; Fama, 1980), which posits that principals can use incentives to motivate agents to align their behavior with the firm's interests. We applied this view to the context of information security, where, as previously mentioned, conflicts often arise between employee and firm goals regarding security. By integrating this principal-agent perspective, we propose that employee-related social performance has the potential to shape the alignment of employees' behavior with the security goals of a firm, thus influencing the firm's information security performance.

However, the landscape of employee-related social performance is intricate, encompassing both positive and negative dimensions: employee-related socially responsible activities (employee-related CSR) and employee-related socially irresponsible activities (employee-related CSiR) (Kang et al., 2016; Tang et al., 2015). Employee-related CSR involves responsible actions that enhance employee well-being across areas like work-life balance, growth, compensation, health, safety, and active engagement (Barber, 2004). On the other hand, employee-related CSiR encompasses detrimental behaviors that compromise employee interests, including rights violations, wage withholding, contribution to safety incidents, and punitive measures (Barber, 2004). These two dimensions differ conceptually and dynamically, leading to diverse implications (Fu et al., 2020; Tang et al., 2015). Therefore, our study adheres to this framework and categorizes employee-related social performance into two dimensions—employee-related CSR and employee-related CSiR—and investigates their individual effects.

[3] https://www.microsoft.com/en-us/security/blog/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/

[4] http://www.theworkfoundation.com/downloadpublication/report/245_245_iip270410.pdf

[5] http://www.rightmanagement.com.au/thought-leadership/e-newsletter/wellness-andproductivity-management.pdf

For our empirical analysis, we adopt a multistudy design for comprehensive validation. Our main analysis is based on a longitudinal dataset of US-listed firms over an eight-year period. The outcomes of our analysis reveal a significant negative correlation between firms' engagement in employee-related CSR and their security risks. Conversely, a positive association is observed between firms' engagement in employee-related CSiR and such risks. Our results are robust to endogeneity concerns by incorporating system generalized method of moments (GMM) panel data estimation and Heckman's two-stage approach, as well as alternative model specifications.

During our exploratory analysis, we examined the influence of the uniqueness of employee-related social performance as a moderator of the primary effects. Social comparison theory suggests that the motivational impact of incentives depends on their expectancy, shaped by comparisons with others (Buunk & Gibbons, 2007; Suls et al., 2002). Rare and unique incentives are more likely to capture attention and prompt responses, potentially resulting in amplified effects. For example, employees often compare welfare packages offered by different firms. If they find that their firms' benefits exceed industry standards or those of competitors, they may value these benefits more highly, seeing the firms' care as more significant (Kryscynski et al., 2021). This perception increases the incentives' value, aligning employees' interests more closely with their firm's interests. Conversely, if firms engage in rare irresponsible behaviors, employees may react with heightened shock, anger, and discontent, paying closer attention to these behaviors and further diverging from the firm's goals. Consequently, we predict that the impact of unique employee-related CS(i)R on information security will be strengthened. We investigated this concept as an empirical expansion of our research and found evidence that supports it.

As the limitations of conducting analysis solely based on secondary data, which may frequently involve an insufficiently comprehensive dataset for rigorous mechanism testing (Thau et al., 2014; Webster & Sell, 2007), we subsequently employed a scenario-based experiment to uncover the mechanisms underlying the effect of employee-related CSR.[6] We conducted a controlled online experiment with 204 participants recruited from Amazon's Mechanical Turk. The outcomes of this experiment provide empirical evidence supporting that the interest-alignment lever of employee-related social performance is indeed at work to influence a firm's information security performance.

In this paper, we make significant contributions to the literature in the following ways: First, while previous studies have predominantly concentrated on exploring the information security implications of technology-centric or security-related factors (e.g., Angst et al., 2017; Haislip et al., 2021), our research departs from this perspective by unveiling the substantial impact of certain human-centric and non-security measures, specifically employee-related social performance, on firms' security risks. This novel approach broadens and enriches the current discourse on security risk. Second, our research offers empirical support for the importance of the strategies that are capable of motivating employees to exhibit optimal security behaviors, aligning with the insights provided by the behavioral information security literature (e.g., Bulgurcu et al., 2010; Zhou et al., 2022). Third, our research goes beyond the conventional CSR research focus, which has primarily explored the economic outcomes of such engagement (e.g., Liu & Lu, 2021; Mackey et al., 2007). Instead, we emphasize the significance of employee-related social performance for information security, significantly broadening the scope of the CSR research. Fourth, we offer insights into the effects of firms' employee-related CSiR, an area largely overlooked in previous research. Our findings indicate that such negative behaviors can increase security risks, thus contributing valuable insights to this area.

2 Literature Review

There are two main streams of literature that are directly relevant to our study: (1) literature on employee-related social performance and (2) literature on information security.

2.1 Employee-Related Social Performance Literature

An organization's social performance includes its engagement in social responsibilities and interactions with stakeholders (Benitez et al., 2020). The relationship between employers and employees is crucial for fostering positive social performance. Management literature suggests that this is due to the established obligations between the parties when individuals become firm employees.

In the employer-employee relationship, exchanges define how individuals perceive the firms' actions as either transactional or relational obligations. On the one hand, transactional obligations involve exchanges that employees view as standard elements of maintaining employment, such as performing job duties in exchange

[6] Measuring and tracking specific employee actions and behaviors using secondary data proves challenging due to frequent internal system restrictions. To overcome this, experiments offer a powerful way to identify mechanisms when rich secondary data is lacking (Thau et al., 2014; Webster & Sell, 2007).

for a salary (Greulich et al., 2024; Millward & Hopkins, 1998). These obligations typically result in low-salience outcomes for the organization or merely meeting minimum job expectations. Relational obligations, on the other hand, involve exchanges that employees see as going beyond the typical employment requirements (e.g., salary, insurance benefits, retirement plans), such as employee-related CSR, which is the focus of this study. Relational obligations usually lead to higher-salience outcomes for the firm, such as employee loyalty, commitment, and prosocial behaviors (e.g., peer monitoring). Beyond the internal boundaries of the firm, relational obligations can also attract new employees and enhance the firm's appeal to current employees when there are alternative career options (Rousseau, 1990).

Therefore, a crucial aspect of organizational social performance is the employer-employee relationship, referred to as employee-related social performance (Barber, 2004; Garel & Petit-Romec, 2020), which encompasses both the positive and negative dimensions: employee-related CSR and employee-related CSiR. Employee-related CSR includes initiatives that enhance employee well-being, promote professional growth, and create a positive work environment, such as offering flexible work arrangements, investing in training and development, providing comprehensive healthcare benefits, fostering transparent communication, offering competitive incentives, and establishing robust employee assistance programs. These efforts contribute to increased job satisfaction, well-being, happiness, loyalty, and organizational identification. In contrast, employee-related CSiR involves actions that neglect or undermine employee interests and rights, such as cutting benefits, ignoring health and safety measures, or engaging in unfair employment practices. These actions can lead to dissatisfaction, higher turnover rates, and reputational damage.

While employee-related CSR is usually viewed positively and CSiR negatively, they can coexist within a firm. The outcomes of employee-related CSR and CSiR are not always opposed. For example, some employees may prioritize the benefits they receive while overlooking actions that compromise their interests. Therefore, it is necessary to examine the respective effects of employee-related CSR and CSiR separately.

At present, there is a trend in research towards investigating the impact of employee-related CSR. Specifically, these studies tend to emphasize the positive dimensions of such performance (i.e., employee-related CSR). Flammer and Luo (2017) suggest that firms can utilize employee-related CSR as an internal governance tool to align employee incentives and enhance their attention, commitment, and compliance, thereby significantly mitigating employees' adverse behaviors. Flammer (2015) emphasizes that robust employee-related CSR initiatives can effectively motivate, attract, and retain the most skilled workforce. Gubler et al. (2018) examined corporate wellness programs and found that such an employee-related CSR can enhance productivity by boosting employee motivation and skills. Other studies have explored internal CSR, observing its ability to elevate employees' perceived respect (Farooq et al., 2017) and organizational commitment (Mory et al., 2016). Moreover, employee-related CSR has been noted for its role in talent attraction (Albinger & Freeman, 2000), creating an insurance-like effect (Shiu & Yang, 2017), and addressing knowledge leakage (Flammer & Kacperczyk, 2019).

However, previous research has largely neglected the examination of the influence of employee-related CSiR. In response to this research gap, our study takes a comprehensive approach by examining both the positive and negative aspects of employee-related social performance and individually assessing their security implications.

2.2 Information Security Literature

Information security involves protecting information from unauthorized access, use, theft, inspection, modification, or destruction.[7] Data breaches occur when confidential or private information is accessed by unauthorized parties (Cheng et al., 2017; Sen & Borle, 2015). Despite media reports of high-profile hacking and malware insertion incidents, the public often assumes that data breaches are primarily caused by external malicious attacks. This is a misconception, as the vast majority of data breaches are related to non-malicious insider behavior, such as negligence, human error, or insider data theft (Chen et al., 2012; Safa et al., 2015).[8]

Data breaches can carry significant adverse consequences for firms, encompassing financial penalties, customer attrition, damage to reputation, and plummeting stock prices (Gwebu et al., 2018; Janakiraman et al., 2018; Kamiya et al., 2021). Consequently, researchers have directed their attention toward identifying effective preventive measures and comprehending firm-level variables that contribute to security risks. Table 1 offers a comprehensive overview of the literature examining the influence of firm-level factors (e.g., IT applications, IT security investments, and IT governance) on such risks. However, it is noteworthy that the factors under scrutiny are predominantly related to IT, IS, or security, highlighting the potential for further research expansion into areas beyond these conventional factors.

[7] SANS Institute: Information Security Resources (https://www.sans.org/security-resources/).

[8] The IBM Cyber Security Intelligence Index Report (2014) shows that human error is the main cause of 95% of cybersecurity breaches.

Table 1. A Literature Review on Security Risk Research

Literature	Journal	Organizational determinants	Main findings
Liu et al. (2020)	*Journal of Management Information Systems*	IT governance	• Universities that have centralized IT governance experience a lower number of data breaches. • Such an effect is moderated by the heterogeneity of universities, university type, and research intensity.
Sen & Borle (2015)	*Journal of Management Information Systems*	IT security investment	• There is a positive correlation between investment in IT security and the likelihood of a data breach within the state and industry sectors.
Angst et al. (2017)	*MIS Quarterly*	IT security investment	• Institutional factors can create conditions in which investments in IT security play a role in reducing security risks.
Kwon & Johnson (2014)	*MIS Quarterly*	IT security investment	• Proactive security investments are negatively related to security risks. • In healthcare security, proactive investments are more cost-effective than reactive investments.
Wang et al. (2015)	*MIS Quarterly*	Features of IT applications	• The likelihood of an IT application being targeted is high when it has high values, little application controls, high visibility and accessibility, and few protective measures.
Mcleod & Dolezel (2018)	*Decision Support Systems*	Technical facilitates, and organizational factors	• There are several technical facilities, such as EMR systems, neonatal intensive care units, lab barcoding systems, and health information exchange initiatives, that are highly vulnerable to data breaches. • Organizational factors such as the number of births, staff beds, and surgical operations are positively correlated with the incidence of data breaches.
Li et al. (2021)	*Journal of Management Information Systems*	IT security investment and IT strategies	• Security investments are associated with a reduced likelihood of data breaches in medical organizations with lower levels of digitalization but may increase the likelihood of data breaches in highly digitalized medical organizations.
Haislip et al. (2021)	*Information Systems Research*	IT skills of executives	• Executives with IT expertise are associated with lower data breach risk.
D'Arcy et al. (2020)	*Information Systems Research*	Social performance	• Firms that engage in extensive social-facing activities are more likely to experience data breaches, especially if they have a poor social performance record.

A notable trend is that most data breaches involve internal personnel, particularly employees. Internal errors (e.g., inadvertent disclosure due to incorrect email usage), negligence (e.g., losing devices), and malicious acts (e.g., theft or fraud) are often traced back to employees (Cheng et al., 2017; Colwill, 2009). Additionally, external attacks frequently exploit employee negligence or noncompliance as entry points for breaches (Guo, 2013; Herath & Rao, 2009). Thus, another crucial stream of literature focuses on the impact of employee behavior on firm information security. Theoretical perspectives such as protection motivation (Boss et al., 2015; Johnston & Warkentin, 2010; Johnston et al., 2015), deterrence (D'Arcy et al., 2009), social capital (Zhou et al., 2022), neutralization (Siponen & Vance, 2010), and accountability (Vance et al., 2013) highlight how employees' ideologies and behaviors—vigilance (Vance et al., 2015), commitment (Posey et al., 2015), compliance (Bulgurcu et al., 2010; Cram et al., 2019), and motivation (Boss et al., 2015; Johnston & Warkentin, 2010)—significantly impact information security performance. By linking findings from behavioral information security studies with those on employee-related social performance, we can anticipate that employee-related social performance influences firms' information security. This suggests opportunities to broaden research on organizational determinants of security risks to include employee-related social performance.

3 Theoretical Development and Hypotheses

3.1 Principal-Agent Framework

To investigate the relationship between employee-related social performance and security risk, this study employs the principal-agent framework (Eisenhardt, 1989; Ross, 1973). Principal-agent theory, also known as agency

theory, addresses the issues that arise between parties (i.e., principal and agent) with conflicting interests and proposes mechanisms to resolve these conflicts. In particular, an agency relationship arises when one party (the principal) delegates authority to another party (the agent). However, if the interests of the agent and principal are misaligned, the agent may be incentivized to engage in moral hazards that serve his own interests rather than those of the principal. In the context of an employee-employer relationship, moral hazards occur when employees underperform or do not exert sufficient effort.

To mitigate employees' moral hazard, principal-agent research suggests that managers can effectively motivate employees through incentive contracts that align the interests of both parties (Eisenhardt, 1989). Such alignment creates a sense of ownership among employees, which increases their tendency to engage in behaviors desired by the firm, promotes job commitment, and fosters engagement (Eisenhardt, 1989). Both monetary and non-monetary incentives have been identified as effective motivators for encouraging employees to align their actions with their firms' interests (Murdock, 2002; Sung et al., 2017); non-monetary incentives have been found to be particularly effective because they increase the intrinsic motivation of recipients (Crifo & Diaye, 2004). In sum, rooted in the principal-agent theory, firms can counteract moral hazards and suboptimal behaviors among employees by aligning interests through incentives.

The principal-agency framework has been applied by researchers at various levels, including owner-manager, employer-employee, buyer-supplier, and lawyer-client (Eisenhardt, 1989; Harris & Raviv, 1978). In particular, scholars have extensively used this theory to conceptualize the relationship between employees (agents) and employers (principals) (e.g., Christen et al., 2006; Eisenhardt, 1989; Hölmstrom, 1979; Jensen & Meckling, 1976; Ross, 1973). Agency issues often arise from the high costs of monitoring employees, leading to information asymmetry and moral hazards (Alchian & Demsetz, 1972). For example, in team environments, it can be challenging to discern individual contributions, leading to "free riders" or the "1/N problem," where employees tend to avoid responsibility due to the collective nature of any consequences.

Furthermore, IS scholars have widely adopted the principal-agency perspective to analyze security risks (Herath & Rao, 2009a; Shim, 2015), uncover the limitations of security technologies (Bauer & van Eeten, 2009; Shim, 2015), and propose solutions for reducing security risks (Anderson et al., 2007; Herath & Rao, 2009a). Our study aligns with this literature, using principal-agent theory to analyze the impact of employee-related social performance on information security.

3.2 Corporate-Employee Misaligned Security Goals and Associated Security Risks

In this section, we delve into the security risks that arise from the misalignment of security goals between employees and their firms. This sets the stage for our subsequent discussion in Section 3.3, where we analyze the security effectiveness of employee-related social performance through shaping this misalignment.

Typically, there is a misalignment of objectives between employees and organizations regarding information security. On the one hand, information is a crucial asset for organizations, particularly in today's digital age, where information plays a pivotal role in business expansion and gaining competitive advantage. Moreover, the loss of information can lead to significant costs, encompassing hefty fines, damage to reputation, and loss of customers (Gwebu et al., 2018; Janakiraman et al., 2018; Kamiya et al., 2021). Consequently, organizations typically place great importance on information security. A 2020 survey by PricewaterhouseCoopers underscores this, revealing that more than half of US chief executive officers (CEOs) have expressed extreme concern about cybersecurity risks, ranking them as the most significant threat to their organizations.[9]

On the other hand, information security often takes a back seat in employees' priorities. This is because evaluating individual contributions to security within complex IT networks frequently proves challenging for firms. As a result, employees' security efforts are rarely directly tied to personal benefits, leading to their lack of motivation to demonstrate good performance in this area (Bulgurcu et al., 2010; Zhou et al., 2022). Moreover, employees often do not directly bear the costs of data breaches, dampening their motivation to fully engage in security practices (Shim, 2015). Compounding this, security measures often clash with employees' personal interests. Studies have highlighted that security protocols can frequently disrupt employees' daily tasks and introduce stress into their workflows (D'Arcy et al., 2014; D'Arcy & The, 2019). Consequently, employees, especially when under significant work pressure, tend to prioritize personal gains over security concerns.

This *misalignment* between employee and firm security goals generates employees' moral hazards and various security risks. For example, pursuing personal interests (e.g., convenience, efficiency), employees often disregard security best practices and lack motivation to adhere to security protocols (e.g., encryption, strong passwords), contributing to a myriad of inadvertent security breaches caused by employee actions.[10] On the other hand, employees with divergent interests—regarding job

[9] https://www.pwc.com/gx/en/ceo-survey/2020/reports/pwc-23rd-global-ceo-survey.pdf

[10] Appendix F presents several real-world data breach cases where breaches occurred due to employees' lack of sufficient

termination, for example—may leak sensitive information for personal gain, also leading to considerable data breaches (Straub & Nance, 1990; Willison et al., 2018).[11]

In summary, our evidence underscores that the *misalignment* between employee and firm security goals yields significant security risks.

3.3 Security Effectiveness of Employee-Related Social Performance: A Principal-Agent Perspective

In this section, we analyze how employee-focused social performance can potentially shape the *alignment* of interests between employees and firms, thereby influencing the information security landscape. We propose that this influence is likely to operate through three distinct channels: (1) shaping employees' commitment to security, (2) impacting peer monitoring intentions, and (3) molding employee loyalty and firm appeal. To further delve into this topic, we also break down employee-related social performance into two dimensions: employee-related CSR and employee-related CSiR. In the following sections, we explore the impact of employee-related social performance on security through each of these three channels, considering both employee-related CSR and employee-related CSiR.

3.3.1 Through Shaping Employees' Security Commitment

Employee-related social performance, whether through employee-related CSR or employee-related CSiR, can shape employee commitment to security, influencing security outcomes. Employee-related CSR represents a firm's care, respect, and support for its employees. When employees perceive this level of well-being and support from their employers, it can enhance their trust and strengthen the belief that their success is closely tied to that of the firm—a concept known as "one succeeds, both succeed" (Posey et al., 2015, p. 190). This alignment often results in their increased commitment and effort in various aspects, including information security (Bulgurcu et al., 2010; Posey et al., 2015).[12] Consequently, we propose that employee-related CSR nurtures employee commitment, ultimately reducing security risks for the firm.

Conversely, employee-related CSiR could undermine employee commitment to security and potentially lead to suboptimal security outcomes. Research indicates that when firms engage in negative actions towards employees, such as neglecting their needs, increasing work pressure, or displaying unfair treatment, employee satisfaction declines (Avgoustaki, 2021; Etehadi & Karatepe, 2019). This is likely to result in employees feeling that their goals are misaligned with those of the firm (Eisenhardt, 1989). Consequently, employees may reduce their commitment and engagement in security-related tasks. Such situations could contribute to an increase in security risks arising from suboptimal employee behaviors, such as errors and negligence.

3.3.2 Through Influencing Peer Monitoring Intentions

We also contend that employee-focused social performance can influence information security by affecting employees' willingness to engage in peer security monitoring. On the one hand, employee-focused CSR can promote shared norms and strong interpersonal relationships among employees, fostering a sense of belonging and commitment to common goals (Flammer & Luo, 2017). This sense of community can motivate employees to voluntarily oversee each other's behavior, including adherence to security policies and regulations (Chua et al., 2012; Kirsch et al., 2010), potentially enhancing the effectiveness of a firm's security controls.[13]

On the other hand, employee-centered negative actions (employee-focused CSiR) have the potential to reduce employees' willingness to engage in mutual supervision, thus negatively impacting information security. Such actions often compromise employees' interests, leading to doubts about their firms' objectives and diminishing

effort. In the context of the Regal Entertainment Group and Wendy's International data breaches, employee oversight in handling information security was a key contributor. Likewise, in the case of Sea Ray Boats, employee lack of caution led to the inadvertent transmission of sensitive information to an incorrect recipient via email, resulting in the exposure of confidential data.

[11] Appendix F also highlights several real-world data breach cases where employees engaged in malicious theft for personal gain, resulting in breaches. For instance, breaches at Wal-Mart Stores Inc., HSBC Auto Finances, Tenet Healthcare, and First Republic Bank were caused by departing employees pursuing personal interests. On the other hand, breaches at MasTec, Verizon Wireless, and Wells Fargo were carried out by current employees for their own benefit through data theft.

[12] This perspective can be supported by existing literature, which emphasizes that employees' engagement in security practices is highly influenced by their job satisfaction (D'Arcy & Greene, 2014; Sharma & Warkentin, 2019) and the foundation of trust (Zhou et al., 2022).

[13] Peer supervision has proven highly effective in safeguarding information security (Hsu et al., 2015). This is due to the fact that employees' suboptimal security behaviors often stem from negative work attitudes and occur in the "grey areas" of security management (Herath & Rao, 2009b; Vance et al., 2015). As a result, conventional security controls frequently struggle to fully address these complexities (D'Arcy et al., 2014; Post & Kagan, 2007). In this context, the informal peer monitoring facilitated by employee-related CSR serves as a valuable complement to formal security measures, effectively fostering a secure work environment.

their enthusiasm for the organization's success (Bavik et al., 2018). These emotional responses could cause employees to view firm security as unimportant, increasing the likelihood that they might overlook irresponsible security behavior exhibited by their peers. Furthermore, a firm's engagement in employee-centered negative actions may erode team cohesion, as it can harm employees' interests. In such scenarios, employees may become more self-centered and distant (Mitchell & Ambrose, 2007; Morrison & Robinson, 1997), no longer motivated to invest extra effort in curbing unsafe behavior among their peers. The effects resulting from employee-focused CSiR, as described above, suggest a potential increase in security risks.

3.3.3 Through Molding Employee Loyalty and Firm Appeal

We contend that employee-related social performance can impact a firm's information security by shaping employee loyalty and the firm's appeal. Specifically, when firms engage in employee-related CSR initiatives that enhance employee benefits and demonstrate their commitment to their workforce, it deepens employees' sense of belonging and increases their loyalty to their employers (Albinger & Freeman, 2000; Bode et al., 2015). This heightened loyalty is likely to reduce employee turnover and the risk of data theft during departures.[14] Additionally, employee-related CSR can send positive signals to job seekers about the firm's culture, values, and strong responsibility (Albinger & Freeman, 2000; Jones et al., 2014), making it easier for firms to attract security talent. The functions of employee-focused CSR described above suggest a possible decrease in security risks for firms that engage in such activities.

Conversely, a firm's engagement in employee-related CSiR can weaken employee loyalty and the firm's appeal, potentially raising security risks. This may occur if CSiR actions threaten employees' interests, leading to decreased loyalty and prompting them to seek other opportunities (Eisenberger et al., 1986). This, in turn, could exacerbate security risks linked to employee departures.[15] Furthermore, external candidates may hesitate to join firms with negative reputational signals, consequently reducing the pool of available security talent and compromising the firm's security control capabilities (Haislip et al., 2021). Additionally, notable data breaches have shown that unhappy employees may engage in revenge data attacks when dissatisfied with their workplace or business management.[16] Thus, harm to employees' interests through employee-related CSiR may trigger employees' strong negative emotions and cause revengeful attacks. The aforementioned scenarios involving employee-focused CSiR underscore the potential for heightened security risks in firms that engage in such activities.

3.4 Hypotheses

In summary, we suggest that employee-related CS(i)R can strengthen (weaken) the alignment between employees' and firms' interests, consequently impacting security risks. This mechanism of influence is likely to manifest through multiple channels, including shaping employees' commitment to security, influencing their inclination for peer monitoring, and molding employee loyalty. As a result, we present the following hypotheses:

H1: A firm's engagement in employee-related CSR is negatively associated with its security risks.

H2: A firm's engagement in employee-related CSiR is positively associated with its security risks.

4 Data and Variable Construction

4.1 Data and Sample Selection

We collected data from multiple sources to test our research model. The sources included the Privacy Rights Clearinghouse (PRC) and the Identity Theft Resource Center (ITRC) for data breach information, the Kinder, Lydenberg, and Domini (KLD) database for CSR data, and the COMPUSTAT database for accounting information.

To ensure a comprehensive and thorough collection of data breaches, we relied on two authoritative sources—PRC and ITRC. Our approach encompassed data breaches that affected firms listed in the US. If a data

[14] A substantial number of data breaches are associated with departing employees. For instance, in 2007, Wal-Mart experienced a data breach in its staff data system when a former employee left their position with confidential records. Similarly, in 2008, a former employee of Tenet Healthcare was convicted of identity theft after gaining access to the personal information of approximately 37,000 patients. (Source: https://www.idtheftcenter.org/).

[15] According to a survey by Biscom, a quarter of departing employees steal data and information when they leave (source: https://www.biscom.com/employee-departure-creates-gaping-security-hole-says-new-data/). As a result, the security risks linked to employee departures are significant.

[16] An example of employees' revenge attacks is the data breach caused by Juliana Barile, who, after being terminated, maliciously destroyed over 21 gigabytes of data belonging to her former employer. Regarding this breach, Acting US Attorney Jacquelyn M. Kasulis commented: "In an act of revenge for being terminated, Barile surreptitiously accessed the computer system of her former employer, a New York Credit Union, and deleted mortgage loan applications and other sensitive information maintained on its file server" (Source: https://www.bleepingcomputer.com/news/security/fired-ny-credit-union-employee-nukes-21gb-of-data-in-revenge/).

breach was documented in either PRC or ITRC and pertained to a US-listed firm, it was included in our dataset. To achieve this, we manually cross-referenced the firm names reported in PRC or ITRC with those in the COMPUSTAT database to gather ticker symbol information. In cases where the names were similar but not exact matches, we conducted further research, including exploring firms' websites and other sources, to ensure accurate alignment. Additionally, data breaches occurring at nonlisted subsidiaries of listed firms were attributed to their respective listed parent firms.[17]

We sourced employee-related social performance data from the KLD database, a reliable resource that has annually reported firms' social performance ratings since 1991. This database has been widely employed in prior research to construct social performance measures (e.g., Flammer & Kacperczyk, 2019; Flammer & Luo, 2017; Shiu & Yang, 2017). The KLD database provides social performance ratings across various dimensions, encompassing environment, employees, community, governance, and product. For our study's emphasis on employee-related CSR, we specifically focused on the employee dimension within the KLD data. This dimension centers on interactions between firms and their employees in aspects such as employee welfare, health and safety, and labor relations. This metric is in line with our defined concept of employee-related social performance.

Finally, we obtained all accounting information from COMPUSTAT and used it to measure a subset of our controls. We merged the collected data with ticker symbols and years and then excluded observations with missing accounting information and firms located outside the US. This resulted in a final sample of 9,620 firm-year observations, including 271 data breaches that occurred between 2007 and 2014. Our sample period ends in 2014 because the data structure for employee-related CSR in the KLD dataset underwent significant changes after 2013 (Laplume et al., 2021), and we employed a one-year lagged independent variable in our analysis.

4.2 Operationalization of Variables

4.2.1 Dependent Variable: Security Risk

We operationalized security risk (*Security*) as a binary variable taking the value 1 if a firm reported at least one data breach in the fiscal year and 0 otherwise. To address concerns about reverse causality, we measured security risk in year t+1.

4.2.2 Independent Variable: Employee-Related Social Performance

The KLD dataset includes employee-related social performance data categorized into two dimensions: strength and concern. The strength dimension evaluates positive aspects, like exemplary employee health and safety records, good training opportunities, positive relationships with employees, and competitive compensation. Conversely, the concern category assesses negatives like labor disputes or violations of employee rights. Both dimensions consist of various rating items, and each rating item is a binary indicator of the firm's annual criteria fulfillment in the corresponding performance domain. Appendix A details these rating items. Consistent with preceding CSR literature (e.g., Fu et al., 2020; Tang et al., 2015), we aggregated all the rating items in the strength category of the employee dimension of the KLD dataset to measure *employee-related CSR*. Similarly, we aggregated all the rating items in the concern category of the employee dimension of the KLD dataset to measure *employee-related CSiR*.

4.2.3 Control Variables

To account for firm characteristics that may influence security risks, we included several control variables in our analysis. First, we controlled for firm size (*Size*) since larger firms are more likely to experience data breaches. Second, given that firms' economic performance and available capital can affect their ability to invest in information security, we included controls for firm leverage (*Leverage*), return on assets (*ROA*), and sales growth (*Sales growth*) in our analysis. Third, we considered the attractiveness of firms with many innovations or intensive advertising promotions to external hackers by including R&D expenses (*R&D*) and advertising intensity (*Advertising*) as additional controls. Fourth, we accounted for resource leanness, which could contribute to data breaches, by including measures of financial slack (*Financial slack*), operational slack (*Operational slack*), and human slack (*Human slack*). Detailed definitions and data sources for all variables used in the primary analysis are provided in Appendix B. Descriptive statistics for these variables are presented in Table 2. Collinearity between these variables is discussed in Appendix C.

[17] Authors of this study were independently involved in the coding process. The percentage of agreement between them was 98.51%.

Table 2. Descriptive Statistics of the Regression Variables

	Variable	Obs.	Mean	*SD*	Min.	Max.
1	Security$_{t+1}$	9,620	0.028	0.165	0.000	1.000
2	Employee-related CSR	9,620	0.344	0.834	0.000	7.000
3	Employee-related CsiR	9,620	0.408	0.691	0.000	5.000
4	Size	9,620	7.355	1.652	3.943	12.118
5	Leverage	9,620	2.414	5.103	0.029	36.745
6	ROA	9,620	0.030	0.134	-3.173	0.399
7	Sales growth	9,620	0.097	0.263	-0.523	1.779
8	R&D	9,620	0.012	0.026	0.000	0.151
9	Advertising	9,620	0.054	0.194	0.000	4.141
10	Financial slack	9,620	11.365	18.483	0.133	134.655
11	Operational slack	9,620	0.005	0.005	0.000	0.036
12	Human slack	9,620	0.316	0.903	0.016	31.353

Table 3. Main Analysis Results

Variable	**Fixed-effect LPM** **Dependent variable: *Security* (subsequent year)**		
	Model 1	**Model 2**	**Model 3**
Employee-related CSR	**-0.010**** **(-2.207)**		**-0.011**** **(-2.325)**
Employee-related CSiR		**0.014**** **(2.401)**	**0.014**** **(2.551)**
Controls	Included	Included	Included
Firm fixed effects	Included	Included	Included
Year fixed effects	Included	Included	Included
Number of observations	9,620	9,620	9,620

Note: Results for the main analysis. The dependent variable is *Security* and is measured in year $t + 1$. t statistics are in parentheses (* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$).

5 Empirical Results

5.1 Main Analysis

Table 3 presents the results of our main analysis, using a sample of 9,620 firm-year observations across 2,022 unique firms. We used a fixed-effects linear probability model (LPM) regression, consistent with prior research on security risk (D'Arcy et al., 2020; Haislip et al., 2021). We chose this model because a fixed-effect logit model would have excluded observations for firms that did not experience a data breach in any year of our sample (Angst et al., 2017; D'Arcy et al., 2020; Haislip et al., 2021). To account for potential correlation of regression residuals across years for a given firm, we clustered robust standard errors at the firm level. We controlled for firm fixed effects to account for unobserved heterogeneity and introduced year fixed effects to account for systematic differences across years that could affect firms' security risks.

In Model 1 (Table 3), we display the results concerning the influence of employee-related CSR on security risks. The employed panel regression model is as follows:

$$Security_{i,j+1} = \beta_0 + \beta_1 Employee\text{-}related\ CSR_{i,j} + \sum \alpha_r Control_{i,j} + \upsilon_i + \omega_j + \varepsilon_{ij}. \quad (1)$$

Here, i and j index the firm and year, respectively; *Control* denotes the control variables described in Section 4.2.3; υ_i and ω_j represent firm- and year-fixed effects, respectively; $\varepsilon_{i,j}$ is the error term. β_1 captures the relationship between employee-related CSR and security risks (H1). This model shows that a higher level of employee-related CSR is linked to reduced security risks for firms, as indicated by the negative and statistically significant coefficient of *Employee-related CSR* (β_1 = -0.010, $p < 0.05$). Specifically, a one-unit increase in a firm's employee-related CSR level is expected to reduce the probability of data breaches in the following year by 1.0%. Given the mean data breach likelihood is 2.8%, this represents a 35.7% reduction in firms' security risks. Hence, the results support H1.

In Model 2 (Table 3), we present the results of the impact of employee-related CSiR on security risks—as estimated by the following empirical model:

$$Security_{i,j+1} = \beta_0 + \beta_1 Employee\text{-}related\ CSiR_{i,j} + \sum \alpha_r Control_{i,j} + \upsilon_i + \omega_j + \varepsilon_{ij}. \quad (2)$$

Here, β_1 indicates the relationship between employee-related CSiR and security risks (H2). This model shows that the coefficient of *Employee-related CSiR* is positive and significant ($\beta_1 = 0.014$, $p < 0.05$), indicating a positive correlation between employee-related CSiR and security risks. More specifically, a one-unit decrease in a firm's employee-related CSiR level leads to a 1.4% decrease in the likelihood of data breaches in the subsequent year, roughly accounting for 50% of the average data breach probability of 2.8%. These findings support H2.

In Model 3 (Table 3), we introduce both *Employee-related CSR* and *Employee-related CSiR* into the same model to assess their individual impacts, given that a firm's engagement in employee-related CSR and employee-related CSiR can potentially mutually influence each other's effects. The utilized panel regression model is as follows:

$$Security_{i,j+1} = \beta_0 + \beta_1 Employee\text{-}related\ CSR_{i,j} + \beta_2 Employee\text{-}related\ CSiR_{i,j} + \sum \alpha_r Control_{i,j} + v_i + \omega_j + \varepsilon_{ij}. \quad (3)$$

Here, β_1 and β_2 capture the security impact of employee-related CSR and employee-related CSiR, respectively. Model 3 (Table 3) demonstrates that β_1 remains significantly negative and β_2 remains significantly positive, aligning with the results observed in Models (1) and (2). These results provide additional evidence to support H1 and H2.

Furthermore, we extended our analysis to assess whether the effects of reducing security risks through increasing employee-related CSR and through decreasing employee-related CSiR differ. Following the approach outlined by Wooldridge (2015), we conducted a *t*-test to assess the difference between the coefficients for *Employee-related CSR* and *Employee-related CSiR* in Model 3 (Table 3). The results show no statistical significance for this difference ($p > 0.1$). This suggests that the reductions in the likelihood of data breaches in the subsequent year resulting from a one-unit increase in employee-related CSR and a one-unit decrease in employee-related CSiR do not show significant differences.

5.2 Endogeneity

The main analysis estimates could be biased by three primary sources of endogeneity. The first is reverse causality, where past security failures may influence current investments in employee-related CSR. In the present study, this concern is mitigated because the dependent variable is security risks in the following year that occur after changes in the level of employee-related CSR.

The second potential source of endogeneity is unobservable firm heterogeneity, which is associated with both employee-related social performance and security risks. For example, well-managed firms are more likely to engage in employee-related socially responsible activities and have lower security risks, making it difficult to establish a causal relationship between employee-related social performance and security risks. Such concerns may hinder an accurate answer to the primary question that could be used to provide practical recommendations. To address the issue of endogeneity, we used the panel dataset we had and employed the system GMM estimation technique (Arellano & Bond, 1991), as described in Subsection 5.2.1.

The third potential source of endogeneity is related to the coverage of firms' employee-related CSR information in the KLD database, which is unlikely to be random. Some listed firms may have a low propensity to disclose or invest in their employee-related CSR information, which could potentially bias our results. To address this concern, we used Heckman's two-stage approach (Heckman, 1977), described in Subsection 5.2.2, to mitigate any relevant endogeneity issues.

5.2.1 System Generalized Method of Moments (GMM)

To address the issue of unobserved heterogeneity in our study, we used the system GMM estimator (Arellano & Bond, 1991), a method designed to improve causal inference and avoid dynamic panel bias. Although instrumental variables are also commonly used to account for unobserved heterogeneity, obtaining strictly exogenous instruments can be challenging, as noted in previous research (Roodman, 2009; Yiu et al., 2020). Therefore, we chose the more advanced system GMM estimator, which is considered one of the "most robust methods for unbalanced panels with endogenous variables" (Flannery & Hankins, 2013, p. 13). Unlike instrumental variables, the system GMM estimator creates instruments by transforming the existing variables in the model. One of the key assumptions of the GMM estimator is that the lagged differences of the idiosyncratic errors are serially uncorrelated, which helps ensure unbiased and consistent estimates.

To employ the GMM estimator, we modified Equations (1), (2), and (3) and developed the dynamic unobserved effects models with the following specifications:

$$Security_{i,j+1} = \beta_0 + \delta_1 Security_{i,j} + \delta_2 Security_{i,j-1} + \beta_1 Employee\text{-}related\ CSR_{i,j} + \sum \alpha_r Control_{i,j} + v_i + \omega_j + \varepsilon_{ij}. \quad (4)$$

$$Security_{i,j+1} = \beta_0 + \delta_1 Security_{i,j} + \delta_2 Security_{i,j-1} + \beta_1 Employee\text{-}related\ CSiR_{i,j} + \sum \alpha_r Control_{i,j} + v_i + \omega_j + \varepsilon_{ij}. \quad (5)$$

$$Security_{i,j+1} = \beta_0 + \delta_1 Security_{i,j} + \delta_2 Security_{i,j-1} + \beta_1 Employee\text{-}related\ CSR_{i,j} + \beta_2 Employee\text{-}related\ CSiR_{i,j} + \sum \alpha_r Control_{i,j} + v_i + \omega_j + \varepsilon_{ij}. \quad (6)$$

In each of these, we accounted for the possible influence of past security performance by further including lagged security risks ($Security_{i,j}$ and $Security_{i,j-1}$). Then, we estimated the modified dynamic panel models by using a system GMM estimator in Stata 14.2 with the *xtabond* command. For brevity, we provide detailed information on the GMM estimation procedure and discuss the results of the validity tests in Appendix D.

Table 4. System GMM Results

Variable	Fixed-effect LPM Dependent variable: *Security* (subsequent year)		
	Model 1	**Model 2**	**Model 3**
Security	0.056 (0.971)	0.056 (0.977)	0.057 (0.989)
Security (lagged)	0.089 (1.616)	0.090 (1.633)	0.090 (1.638)
Employee-related CSR	**-0.010*** **(-1.827)**		**-0.010*** **(-1.752)**
Employee-related CSiR		**0.024**** **(2.005)**	**0.024*** **(1.939)**
Controls	Included	Included	Included
Firm fixed effects	Included	Included	Included
Year fixed effects	Included	Included	Included
Number of observations	6,850	6,850	6,850
Arellano-Bond test for AR(1) in first differences	z = -8.53; Pr > z = 0.000;	z = -8.51; Pr > z = 0.000	z = -8.53; Pr > z = 0.000;
Arellano-Bond test for AR(2) in first differences	z = -0.38; Pr > z = 0.704	z = -0.39; Pr > z = 0.698	z = -0.40; Pr > z = 0.690
Hansen test of restrictions	chi2(14) = 16.57 Pr > z = 0.280	chi2(14) = 18.87 Pr > z = 0.170	chi2(13) = 14.67 Pr > z = 0.329

Note: Results for system-GMM analysis. The dependent variable is *Security* and is measured in year $t + 1$. t statistics are in parentheses (* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$).

The results of our GMM estimation are presented in Table 4 and are broadly consistent with those of the main analysis. The results give us confidence that the potential endogeneity of employee-related CSR and security risks did not significantly bias our results.

5.2.2 Heckman's Two-Stage Analysis

In order to address the potential endogeneity problem arising from the fact that the KLD database may not randomly cover all firms' employee-related CSR information, we used Heckman's two-stage analysis (Heckman, 1977) in our study. This method helps address selection bias due to non-random selection processes, such as self-selection or non-response.

In the first stage of the Heckman analysis, we constructed a selection model to predict the overall likelihood (*Selection probability*) that an observation will appear in our sample. *Selection probability* equals 1 if a firm disclosed its employee-related social performance information in the focal year, and 0 otherwise. In particular, this stage involves using at least one instrument, which appears exclusively in the first stage, impacts the overall likelihood of an observation appearing in the sample, and does not influence the ultimate dependent variable of interest in the second-stage model. Accordingly, we introduced the instrument of peer disclosure rate (*Peer selection*), which was operationalized as the average employee-related social performance disclosure rate from peer firms within the three-digit Standard Industrial Classification (SIC) industry. This instrument was chosen because it is likely to influence the disclosure intentions of focal firms through mimetic isomorphism (DiMaggio & Powell, 1983; Maksimov et al., 2019); at the same time, this instrument is unlikely to directly impact a firm's security risks. We provide more details on our first-stage Heckman regression in Appendix E.

In the second stage, we included the inverse Mill's ratio (IMR) generated in the first-stage Heckman regression as an additional control and repeated our baseline analysis. Table 5 presents results that are consistent with those of the baseline analysis, thus addressing the endogeneity concern arising from potential sample selection bias.

5.3 Additional Robustness Checks

To ensure the validity of our findings, we conducted additional tests using alternative models, as shown in Table 6. We described our testing procedures below. First, we tested the sensitivity of our analysis by using a fixed-effect logit regression model as an alternative. This was done because our dependent variable (*Security*) is binary. The results in Columns 1-3 of Table 6 are highly consistent with those obtained from the baseline analysis. Second, the level of security risks within a firm during a specific period could be influenced by its historical patterns. For instance, a firm that recently experienced a breach might become more cautious, reducing the likelihood of another breach. Consequently, neglecting information about a firm's past security risk levels could introduce omitted variable bias. To address this concern, we adopted a first-differenced specification employed in previous research (e.g., Amior & Manning, 2018; Lam et al., 2016). The results are presented in Columns 4-6 of Table 6 and are consistent with those of the baseline analysis. Taken together, these robustness checks provide further support for the conclusions drawn from our research.

Table 5. Heckman Two-Stage Analysis

Variable	Fixed-effect LPM Dependent variable: *Security* (subsequent year)		
	Model 1	**Model 2**	**Model 3**
Employee-related CSR	**-0.010**** **(-2.153)**		**-0.010**** **(-2.229)**
Employee-related CSiR		**0.015**** **(2.571)**	**0.015***** **(2.664)**
IMR	0.003 (0.393)	0.012 (1.389)	0.010 (1.083)
Controls	Included	Included	Included
Firm fixed effects	Included	Included	Included
Year fixed effects	Included	Included	Included
Number of observations	9,612	9,612	9,612

Note: Results for Heckman's two-stage analysis. The dependent variable is *Security* and is measured in year $t + 1$. Details of the first-stage Heckman model and the regression results are provided in Appendix E. In the second-stage Heckman model, we repeat our baseline analysis by adding IMR as an additional control. *t* statistics are in parentheses (* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$).

Table 6. Additional Robustness Checks

Variable	Fixed-effect logit *Security* (subsequent year)			Fixed-effect LPM (First-Differenced Specification) *Security* (subsequent year)		
	Model 1	**Model 2**	**Model 3**	**Model 4**	**Model 5**	**Model 6**
Employee-related CSR	**-0.221**** **(-2.184)**		**-0.202**** **(-2.163)**	**-0.010***** **(-3.396)**		**-0.009***** **(-3.482)**
Employee-related CSiR		**0.367**** **(2.552)**	**0.343**** **(2.494)**		**0.014***** **(3.733)**	**0.013***** **(3.633)**
Security				-0.163*** (-14.241)	-0.164*** (-14.356)	-0.165*** (-14.420)
Controls	Included	Included	Included	Included	Included	Included
Firm fixed effects	Included	Included	Included	Included	Included	Included
Year fixed effects	Included	Included	Included	Included	Included	Included
Number of observations	925	925	925	9,620	9,620	9,620

Note: Results for robustness checks. First, we repeat our baseline analysis by alternatively using the fixed-effect logit model and show the results in Columns (1) to (3). The sample in the test consists of 925 firm-years given all the firm-year observations in which firms had not experienced any data breach during our sample period have been automatically excluded in the fixed-effect logit regressions. Second, we repeat our baseline analysis by alternatively using a first-differenced specification, in which we incorporate an additional control of *Security* (current year). The results are reported in Columns (4) to (6). *t* statistics are in parentheses (* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$).

5.4 Exploratory Analysis: Why Does the Uniqueness of Employee-Related Social Performance Matter?

Based on our previous analyses, we have identified that firms can mitigate security risks by embracing employee-related CSR or seeking to prevent employee-related CSiR. We attribute these effects to the notion that both forms of effort can enhance employee well-being and align their interests with the firm's goals. Nevertheless, the degree of well-being that employees perceive from these actions is also contingent upon contextual factors, such as the uniqueness of these initiatives relative to their peers (Hull & Rothenberg, 2008; Nardi et al., 2022). In this section, we explore the moderating impact of the uniqueness of employee-related social performance.

We begin by examining how the uniqueness of employee-related CSR moderates its impact on security. Psychological studies have indicated that unique incentives are highly valued and perceived as more significant (Lynn & Snyder, 2002; Kryscynski et al., 2021). In the CSR domain, unique strategies foster differentiation and amplified effects (Hull & Rothenberg, 2008; Nardi et al., 2022). Therefore, we expect that unique employee-related CSR will have a greater positive impact on security, as employees will place higher value on these actions.

We also explore how the uniqueness of employee-related CSiR affects its influence on security risks. Research suggests that negative behaviors that are common among peer firms are perceived as less severe (Cialdini & Goldstein, 2004; Sherif, 1935), whereas unique negative behaviors are viewed more severely and often attract more media attention, leading to stronger negative impacts (Smith et al., 2021). Thus, we predict that unique employee-related CSiR will significantly increase security risks.

Table 7. Moderating Effect of CSR Uniqueness

Variable	Fixed-effect LPM Dependent variable: *Security* (subsequent year)		
	Model 1	**Model 2**	**Model 3**
Employee-related CSR	0.004 (0.545)		0.004 (0.510)
Employee-related CSiR		-0.007 (-0.899)	-0.007 (-0.910)
Employee-Related CSR × Employee-related CSR uniqueness	**-0.024*** **(-1.887)**		**-0.024*** **(-1.886)**
Employee-related CSiR × Employee-related CSiR uniqueness		**0.068***** **(3.624)**	**0.069***** **(3.658)**
Employee-related CSR uniqueness	-0.002 (-0.144)	-0.033*** (-3.367)	-0.004 (-0.274)
Employee-related CSiR uniqueness	0.032*** (3.222)	-0.037* (-1.959)	-0.036* (-1.892)
Controls	Included	Included	Included
Firm fixed effects	Included	Included	Included
Year fixed effects	Included	Included	Included
Number of observations	9,620	9,620	9,620

Note: Results for the main analysis. The dependent variable is *Security* and is measured in year $t + 1$. t statistics are in parentheses (* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$).

Following prior studies (Litov & Zenger, 2010; Nardi et al., 2022), we operationalized *Employee-related CSR uniqueness* and *Employee-related CSiR uniqueness* in the following manner. We defined a firm's peers as those belonging to the same three-digit SIC industry as the firm. For each rating item considered in constructing *Employee-related CSR* or *Employee-related CSiR*, we measured the uniqueness of this item by squaring the difference between 1 and the average fulfillment rate of this item among the firm's peers. Subsequently, at the firm level, we measured a firm's *Employee-related CS(i)R uniqueness* as the average uniqueness of all employee-related CSR strength (concern) rating items for the firm in the focal year. Therefore, a higher value of *Employee-related CS(i)R uniqueness* indicates that all employee-related CS(i)Rs in which the firm engages are, on average, unique.

Table 7 elucidates the results of moderating effect tests concerning these uniqueness factors. In Column 1 of Table 7, the interaction term's coefficient is significantly negative, indicating that employee-related CSR uniqueness strengthens the negative impact of employee-related CSR on security risks. In Column 2 of Table 7, the interaction term's coefficient is significantly positive, suggesting that employee-related CSiR uniqueness strengthens the positive impact of employee-related CSiR on security risks. We also introduced both *Employee-related CSR uniqueness* and *Employee-related CSiR uniqueness* within the same model. The results, shown in Column 3 of Table 7, align entirely with the earlier results and provide additional support for the robustness of our findings. In summary, our investigation shows that the uniqueness of employee-related social performance, either in the dimension of employee-related CSR or employee-related CSiR, amplifies the security impacts of such engagement.

6 Identification of the Mechanism Underlying the Main Effect

In our follow-up study, our aim was to uncover the theoretical mechanism driving the security impact of employee-related social performance. Our theory suggests that such performance influences security by shaping employees' interest-aligned security behavior, which encompasses (1) determining their security commitment, (2) influencing peer monitoring intentions, and (3) molding employee loyalty and firm appeal. In this section, we present empirical evidence in support of our theory.

6.1 Design and Procedure (Scenario-Based Experiment)

We recruited 204 "Turkers" and conducted a controlled online scenario-based experiment on a Chinese Amazon's Mechanical Turk (Gai & Puntoni, 2021; Huang & Sengupta, 2020). Preceding the experiment, we carried out a prescreening process to ensure participants' decision-making qualifications, with further details provided in Appendix G.

The experiment comprised three distinct scenario-based groups: employee-related CSR (ECSR; T_{ECSR}; n = 69), employee-related CSiR (ECSiR; T_{ECSiR}; n = 68), and control conditions (C; n = 67). Random assignment placed participants into one of these groups, requiring them to read a scenario description (an employee-related CSR vignette, an employee-related CSiR vignette, or a control vignette) concerning a fictitious entity of "Company X." Appendix G provides a comprehensive scenario depiction, the questions posed, and the design to test the validity of the scenario manipulation.

Table 8. Perceived Employee Interest-Alignment Behavior Across Groups

Group	One-way ANOVA		
	"Security commitment"	**"Security peer-monitoring"**	**"Employee loyalty and firm appeal"**
	(1-7 scale)	(1-7 scale)	(1-7 scale)
ECSR	6.34 (0.43)	5.80 (0.78)	6.07 (0.48)
ECSiR	5.36 (1.55)	4.34 (1.70)	4.57 (1.84)
C	5.85 (0.82)	5.19 (1.22)	5.43 (1.20)
	F (2, 201) = 15.20, $p < 0.01$	F (2, 201) = 22.22, $p < 0.01$	F (2, 201) = 23.11, $p < 0.01$

Our metric for the level of employee-related social performance was drawn from established scales (Donia et al., 2017; Wong & Kim, 2020) employing a 7-point scale spanning from 1 (*strongly disagree*) to 7 (*strongly agree*) (Question module 1, Table G1, Appendix G). The measure's robustness was confirmed with a Cronbach's alpha of 0.86.

Employing a one-way ANOVA, we found significant differences in participants' perceptions of employee-related social performance among the groups (F (2, 201) = 131.71, $p < 0.01$). Subsequent Tukey post hoc analysis unveiled considerably higher perceived employee-related social performance within the ECSR group, relative to both the ECSiR and C groups. Conversely, the ECSiR group demonstrated significantly lower perceived employee-related social performance compared to the C group (ECSR – ECSiR, $p < 0.01$; ECSiR – C, $p < 0.01$; ECSiR – C, $p < 0.01$). These results provide additional evidence that our scenario manipulation was able to effectively shape participants' evaluations of employee-related social performance aligned with their respective scenarios.

6.2 Analysis and Results (Scenario-Based Experiment)

The experiment's results are summarized in Table 8. Utilizing a one-way ANOVA, we found that participants in the ECSR, ECSiR, and C groups perceived distinct employee interest-alignment behavior in the respective scenarios. This encompassed varying levels of (1) security commitment: F (2, 201) = 15.20, $p < 0.01$; (2) security peer-monitoring: F (2, 201) = 22.22, $p < 0.01$; and (3) loyalty and perception of firm appeal: F (2, 201) = 23.11, $p < 0.01$.

We employed Tukey's post hoc test to discern the group differences. Regarding "security commitment," participants in the ECSR group perceived higher employee security commitment compared to the ECSiR group ($T_{ECSR} - T_{ECSiR}$, $p < 0.01$) and the control group (T_{ECSR} – C, $p < 0.05$), and conversely, participants in the ECSiR group perceived lower employee security commitment than the control group (T_{ECSR} – C, $p < 0.01$). For "security peer-monitoring," participants reported significantly greater engagement in security-related peer monitoring in the ECSR group compared to the ECSiR group ($T_{ECSR} - T_{ECSiR}$, $p < 0.01$) and the control group (T_{ECSR} – C, $p < 0.05$); however, this tendency was lower in the ECSiR group than in the control group (T_{ECSiR} – C, $p < 0.01$). Concerning "employee loyalty and firm appeal," ECSR participants reported higher levels compared to both ECSiR ($T_{ECSR} - T_{ECSiR}$, $p < 0.01$) and the control group (T_{ECSR} – C, $p < 0.05$), and conversely, ECSiR participants reported lower levels compared to the control group (T_{ECSiR} – C, $p < 0.01$). In sum, these findings indicate that in an information security context, employees perceive higher (lower) commitment, peer monitoring, and loyalty and perception of firm appeal in the employee-related CSR (employee-related CSiR) scenario than in other scenarios.

We employed ordinary least squares (OLS) regressions to link the outcome variables with the dummy indicators of our treatment groups (ECSR and ECSiR), as shown in Equation (7). For each respondent i, the main estimation equation is as follows:

$$Y=\alpha+\beta_1 Treatment\_ECSR+\beta_2 Treatment\_ECSiR+\varepsilon. \quad (7)$$

Here, Y represents the outcome variable: security commitment, security peer-monitoring, and employee loyalty and perception of firm appeal. The results, presented in Table 9, reveal that employee-related CSR significantly enhances security commitment ($p < 0.01$), security peer-monitoring ($p < 0.01$), and employee loyalty and perception of firm appeal ($p < 0.01$). In contrast, employee-related CSiR significantly diminishes security commitment ($p < 0.05$), security peer-monitoring ($p < 0.01$), and employee loyalty and perception of firm appeal ($p < 0.01$).

Taken together, our findings reinforce the link between employee-related CSR (employee-related CSiR) and heightened (lowered) levels of security commitment, security peer monitoring, and employee loyalty and perception of firm appeal—key factors that extensively contribute to information security improvement. Thus, we find empirical evidence to support our proposed mechanism.

Table 9. OLS Results of Identifying Underlying Mechanisms

Variable	"Security commitment"	"Security peer-monitoring"	"Employee loyalty and firm appeal"
	(1)	(2)	(3)
Treatment_ECSR	**0.526*** (4.16)**	**0.612*** (3.52)**	**0.693*** (4.19)**
Treatment_ECSiR	**-0.433** (-2.09)**	**-0.806*** (-3.24)**	**-0.766*** (-2.95)**
Controls	Yes	Yes	Yes
Number of observations	204	204	204
adj. R^2	0.127	0.226	0.211

Note: Results for the scenario-based experiment. We used OLS regression. The *Treatment_ECSR* and *Treatment_ECSiR* variables are dummy variables taking a value of 1 for observations in the ECSR and ECSiR groups, respectively. To account for participant characteristics, we controlled for *Religious*—to what extent religiousness is important to them (1-7 scale), *Ethics*—whether they are ethical (1-7 scale), *Age*—age range (21-30, 31-40, 41-50, or above 50), *Work experience*—work experience range (3-5, 5-10, 10-20, or 20-30 years), and *Gender*—gender (Female or Male). *t*-statistics are in parentheses (* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$).

7 Discussion and Implications

In the rapidly evolving landscape of digital transformation, businesses are being confronted with unprecedented information security challenges. Effectively addressing these risks has become paramount. While recent research has focused on understanding the influence of IT, IS, and security-related factors on security risks, we introduce a fresh perspective—centered around a human-oriented strategy that prioritizes well-being: employee-related social performance.

Our study examines two distinct facets of employee-related social performance: the positive aspect (employee-related CSR) and the negative aspect (employee-related CSiR). Using the principal-agent theory as our analytical framework, we posit that each dimension can actively shape the alignment between employees and organizational interests, thus impacting security risks.

Our longitudinal analyses validate our hypotheses, demonstrating that both increased engagement in employee-related CSR and reduced involvement in employee-related CSiR have the potential to mitigate security risks. Moreover, the security risk reduction effects stemming from these strategies are notably similar. Expanding our investigation, our exploratory analysis of contextual factors reveals intriguing insights, highlighting the enhanced security benefits associated with unique forms of employee-related social performance. Lastly, we employ a scenario-based experiment to provide further empirical support for our theory grounded in the principal-agent perspective.

7.1 Theoretical Implications

The present study makes several contributions to the literature. First, it addresses a notable gap in security risk research. In response to data breaches that are escalating in frequency and impact, scholars have extensively explored organizational factors influencing security risks. However, the predominant focus has been on technology-related elements such as IT investments, governance, and resources (e.g., Angst et al., 2017; Haislip et al., 2021). Departing from this trend, our study introduces a fresh perspective by investigating the impact of employee-related social performance on security risks. This novel approach broadens and enriches the current discourse on security risk.

Second, our firm-level study finds that a firm's employee-related social performance can influence its information security. This analysis draws on behavioral information security research (e.g., Bulgurcu et al., 2010; Zhou et al., 2022), which typically focuses on the individual level. We extend the findings of behavioral information security from the individual level to the firm level, exploring how these dynamics work within an organizational context. In doing so, we validate and enrich behavioral information security theories at the firm level, deepening the understanding of these theories and their applicability.

Third, our study goes beyond the traditional scope of research on corporate social performance, which has mainly concentrated on economic outcomes such as financial performance and risk mitigation (e.g., Liu & Lu, 2021; Mackey et al., 2007). Instead, our study breaks new ground by revealing the significant influence of employee-related social performance on firms' information security. This broadening of focus contributes to a more comprehensive understanding of the multifaceted effects of firms' socially responsible practices. Additionally, D'Arcy et al. (2020) highlight the possibility that external-facing CSR initiatives could "greenwash" inadequate social performance, leading to increased security risks due to negative stakeholder perceptions. In contrast, our study focuses on inward-looking employee well-being and demonstrates that employee-related CSR can enhance information security by aligning employees' interests with their organizations. This fresh perspective

enriches our understanding of the CSR-information security relationship. In particular, our study relates to Flammer and Luo's (2017) study, which uses principal-agent theory to explore the impact of employee-related CSR on employee errors, finding a negative relationship. However, Flammer and Luo (2017) did not measure performance outcomes linked to employee-related CSR. We extend their findings by directly assessing the impact of employee-related CSR on information security. This deepens our understanding of how employee-related CSR affects firm performance, especially in the domain of information security.

Fourth, a prevalent trend in research has treated employee-related social performance as a one-dimensional construct, predominantly focusing on the positive dimension of employee-related CSR while overlooking its negative dimension—employee-related CSiR. Our study represents a pioneering effort to examine the security implications of employee-related CSiR. By finding that avoiding such detrimental employee-related actions can yield security benefits for the firm, we broaden the understanding of the consequences of negative organizational engagement.

7.2 Practical Implications

Our study offers practical implications in addition to theoretical contributions. First, our findings suggest that employee welfare and social performance investments can enhance information security. By fostering a positive organizational culture and improving employee welfare, firms can encourage employees to comply with security policies, thereby reducing the risk of data breaches. This highlights that advancing employee welfare is not just an ethical consideration but a strategic necessity for information security. For instance, according to our findings, employees who feel valued and well-treated are more likely to be vigilant and committed to protecting sensitive organizational information. This heightened sense of responsibility and loyalty can lead to a reduction in suboptimal security behaviors by employees and an enhancement of the firm's overall security posture.

Second, our study highlights the concurrent and collaborative impact of responsible and irresponsible employee-related behaviors on security outcomes. This indicates that firms should not solely focus on promoting positive engagement with employees but also take measures to prevent negative behaviors. Only through the implementation of a comprehensive strategy that integrates positive employee interactions with preventive measures against negative interactions can information security be adequately strengthened.

Third, another pivotal insight for managers is the uniqueness of employee-related social performance. When a firm's employee-related CSR efforts are unique, their potential to mitigate security risks is greatly magnified. Incorporating unique employee-related CSR programs and approaches in employee-related CSR decisions can yield heightened security benefits. On the other hand, our study also underscores that managers should exercise great caution when considering distinctive practices that might adversely affect employees (i.e., employee-related CSiR), as such actions could markedly exacerbate security risks.

7.3 Limitations and Future Research

Although this study has made significant contributions, its limitations provide several opportunities for future research. First, although our research emphasizes the role of employee-related CSR in promoting peer monitoring for information security, it's worth exploring the interplay between peer monitoring and formal technical systems like zero-trust models and access controls. Finding the optimal balance and potential trade-offs between these mechanisms could offer valuable insights. Second, our study primarily focuses on organizations' data breach prevention strategies, leaving out considerations of post-breach recovery efforts. Future research could examine whether CSR initiatives aid in alleviating the negative aftermath of data breaches. Third, our reliance on secondary data restricts our ability to directly measure the strengths of the mechanisms underlying the security impact of employee-related social performance. Future studies could benefit from individual-level research to provide a more nuanced understanding. Third, another limitation of this study is our secondary data focuses on publicly traded firms. However, the incentives for publicly listed firms may differ from those of private firms. Specifically, publicly listed firms often place a higher emphasis on shareholder value and their market image, potentially leading to aligned CSR strategies. In contrast, private firms are frequently not subject to the same market pressures. Therefore, to enhance the generalizability of our findings, future research could further expand our analysis by incorporating data from private firms or organizations in specific industries. Lastly, our study's sample period ends in 2014 due to significant changes in the data structure for employee-related CSR in the KLD dataset after 2013 (Laplume et al., 2021), and we employ a one-year lagged independent variable. Consequently, future research could explore alternative data sources or collection methods to extend the sample period and validate the findings in more recent years.

8 Conclusion

The rapid evolution of the business landscape brought about by digital transformation has introduced new risks, including security risks. Effective management of these risks is essential for digital environments to achieve their desired goals. To this end, we examine how enhancing employee well-being can help mitigate security risks. Our research shows that firms can effectively reduce security risks by promoting a "do good" or "do no harm" culture, especially when their peers cannot replicate it. Notably, existing research has focused primarily on technical countermeasures to mitigate security risks. Our study differs from traditional approaches in that we emphasize the security benefits of human-centered and well-being policies, such as employee-related social performance. This is a new area that should be further explored by future researchers.

Acknowledgments

The authors sincerely thank the senior editor, Yulin Fang, the associate editor, and the two anonymous reviewers for their exceptionally constructive and insightful feedback throughout the review process. Their guidance has been invaluable in shaping and refining this work.

References

Albinger, H. S., & Freeman, S. J. (2000). Corporate social performance and attractiveness as an employer to different job seeking populations. *Journal of Business Ethics*, *28*(3), 243-253.

Alchian, A. A., & Demsetz, H. (1972). Production, information costs, and economic organization. *The American Economic Review*, *62*(5), 777-795.

Amior, M., & Manning, A. (2018). The persistence of local joblessness. *American Economic Review*, *108*(7), 1942-1970.

Anderson, R., Moore, T., Nagaraja, S., & Ozment, A. (2007). Incentives and information security. In N. Nisan, T. Roughgarden, E. Tardos, & V. V. Vazirani (Eds.), *Algorithmic game theory* (pp. 633-649). Cambridge University Press.

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly*, *41*(3), 893-916.

Arellano, M., & Bond, S. (1991). Some tests of specification for panel data: Monte Carlo evidence and an application to employment equations. *Review of Economic Studies*, *58*(2), 277-297.

Avgoustaki, A. (2021). *Work intensity and unsustainable work: Evidence from the European Working Conditions Survey* (Working paper).

Azadegan, A., Patel, P. C., & Parida, V. (2013). Operational slack and venture survival. *Production and Operations Management*, *22*(1), 1-18.

Barber, L. (2004). *CSR for employees: Proof of "employer engagement." Institute for Employment Studies.*

Bauer, J. M., & Van Eeten, M. J. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, *33*(10-11), 706-719.

Bavik, Y. L., Tang, P. M., Shao, R., & Lam, L. W. (2018). Ethical leadership and employee knowledge sharing: Exploring dual-mediation paths. *The Leadership Quarterly*, *29*(2), 322-332.

Benitez, J., Ruiz, L., Castillo, A., & Llorens, J. (2020). How corporate social responsibility activities influence employer reputation: The role of social media capability. *Decision Support Systems*, *129*, 113223.

Bode, C., Singh, J., & Rogan, M. (2015). Corporate social initiatives and employee retention. *Organization Science*, *26*(6), 1702-1720.

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837-864.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548.

Bushway, S., Johnson, B. D., & Slocum, L. A. (2007). Is the magic still there? The use of the Heckman two-step correction for selection bias in criminology. *Journal of Quantitative Criminology*, *23*(2), 151-178.

Buunk, A. P., & Gibbons, F. X. (2007). Social. comparison: The end of a theory and the emergence of a field. *Organizational Behavior and Human Decision Processes*, *102*(1), 3-21.

Certo, S. T., Busenbark, J. R., Woo, H. s., & Semadeni, M. (2016). Sample selection bias and Heckman models in strategic management research. *Strategic Management Journal*, *37*(13), 2639-2657.

Chen, J., Zhao, X., Lewis, M., & Squire, B. (2016). A multi-method investigation of buyer power and supplier motivation to share knowledge. *Production and Operations Management*, *25*(3), 417-431.

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, *29*(3), 157-188.

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5), Article e1211.

Christen, M., Iyer, G., & Soberman, D. (2006). Job satisfaction, job performance, and effort: A reexamination using agency theory. *Journal of Marketing*, *70*(1), 137-150.

Chua, C. E. H., Lim, W.-K., Soh, C., & Sia, S. K. (2012). Enacting clan control in complex IT projects: A social capital perspective. *MIS Quarterly*, *36*(2), 577-600.

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annual Review of Psychology*, *55*(1), 591-621.

Colvin A. J. S., & Boswell, W. R. (2007). The problem of action and interest alignment: Beyond job requirements and incentive compensation. *Human Resource Management Review*, *17*(1), 38-

51.

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, *43*(2), 525-554.

Crifo, P., & Diaye, M.-A. (2004). *Incentives in agency relationships: To be monetary or non-monetary* (Working paper). Centre de'etude des Politiques Economiques de l'Universite d'Evry.

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

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, *22*(5), 474-489.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, *31*(2), 285-318.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79-98.

D'Arcy, J., & Teh, P.-L. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management*, *56*(7), Article 103151.

DeSimone, J. A., Harms, P. D., & DeSimone, A. J. (2015). Best practice recommendations for data screening. *Journal of Organizational Behavior*, *36*(2), 171-181.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, *48*(2), 147-160.

Donia, M. B., Ronen, S., Tetrault Sirsly, C.-A., & Bonaccio, S. (2019). CSR by any other name? The differential impact of substantive and symbolic CSR attributions on employee outcomes. *Journal of Business Ethics*, *157*(2), 503-523.

Donia, M. B., Tetrault Sirsly, C. A., & Ronen, S. (2017). Employee attributions of corporate social responsibility as substantive or symbolic: Validation of a measure. *Applied Psychology*, *66*(1), 103-142.

Eisenberger, R., Huntington, R., Hutchison, S., Sowa, D. & Guion R. (1986). Perceived organizational support. *Journal of Applied Psychology*, *71*(3), 500-507.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review*, *14*(1), 57-74.

Etehadi, B., & Karatepe, O. M. (2019). The impact of job insecurity on critical hotel employee outcomes: The mediating role of self-efficacy. *Journal of Hospitality Marketing & Management*, *28*(6), 665-689.

Fama, E. F. (1980). Agency problems and the theory of the firm. *Journal of Political Economy*, *88*(2), 288-307.

Flammer, C. (2015). Does corporate social responsibility lead to superior financial performance? A regression discontinuity approach. *Management Science*, *61*(11), 2549-2568.

Flammer, C., & Kacperczyk, A. (2019). Corporate social responsibility as a defense against knowledge spillovers: Evidence from the inevitable disclosure doctrine. *Strategic Management Journal*, *40*(8), 1243-1267.

Flammer, C., & Luo, J. (2017). Corporate social responsibility as an employee governance tool: Evidence from a quasi-experiment. *Strategic Management Journal*, *38*(2), 163-183.

Flannery, M. J., & Hankins, K. W. (2013). Estimating dynamic panel models in corporate finance. *Journal of Corporate Finance*, *19*, 1-19.

Fu, R., Tang, Y., & Chen, G. (2020). Chief sustainability officers and corporate social (Ir) responsibility. *Strategic Management Journal*, *41*(4), 656-680.

Gai, P. J., & Puntoni, S. (2021). Language and consumer dishonesty: A self-diagnosticity theory. *Journal of Consumer Research*, *48*(2), 333-351.

Garel, A., & Petit-Romec, A. (2021). Engaging employees for the long run: Long-term investors and employee-related CSR. *Journal of Business Ethics*, *174*(1), 35-63.

Greulich, M., Lins, S., Pienta, D., Thatcher, J. B., & Sunyaev, A. (2024). Exploring contrasting effects of trust in organizational security practices and protective structures on employees' security-related precaution taking. *Information Systems Research, 35*(4), 1586-1608.

Gubler, T., Larkin, I., & Pierce, L. (2018). Doing well by making well: The impact of corporate wellness programs on employee productivity. *Management Science*, *64*(11), 4967-4987.

Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, *35*(2), 683-714.

Haislip, J., Lim, J.-H., & Pinsker, R. (2021). The impact

of executives' IT expertise on reported data security breaches. *Information Systems Research*, *32*(2), 318-334.

Harris, M., & Raviv, A. (1978). Some results on incentive contracts with applications to education and employment, health insurance, and law enforcement. *The American Economic Review*, *68*(1), 20-30.

Heckman, J. J. (1977). *Sample selection bias as a specification error (with an application to the estimation of labor supply functions)* (NBER Working Paper Series no. 172). National Bureau of Economic Research.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.

Hölmstrom, B. (1979). Moral hazard and observability. *Bell Journal of Economics*, *10*(1), 74-91.

Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research*, *26*(2), 282-300.

Huang, Y., & Sengupta, J. (2020). The influence of disease cues on preference for typical versus atypical products. *Journal of Consumer Research*, *47*(3), 393-411.

Hull, C. E., & Rothenberg, S. (2008). Firm performance: The interactions of corporate social performance with innovation and industry differentiation. *Strategic Management Journal*, *29*(7), 781-789.

IBM. (2014). *IBM Security Services 2014 Cyber Security Intelligence Index*. IBM Corporation. https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF

IBM. (2022). *X-Force Threat Intelligence Index 2022*. IBM Corporation. https://www.ibm.com/downloads/cas/ADLMYLAZ

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, *82*(2), 85-105.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, *3*(4), 305-360.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549-566.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, *39*(1), 113-134.

Jones, D. A., Willness, C. R., & Madey, S. (2014). Why are job seekers attracted by corporate social performance? Experimental and field tests of three signal-based mechanisms. *Academy of Management Journal*, *57*(2), 383-404.

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. *Journal of Financial Economics*, *139*(3), 719-749.

Kang, C., Germann, F., & Grewal, R. (2016). Washing away your sins? Corporate social responsibility, corporate social irresponsibility, and firm performance. *Journal of Marketing*, *80*(2), 59-79.

Kim, H., Kim, H., & Lee, P. M. (2008). Ownership structure and the relationship between financial slack and R&D investments: Evidence from Korean firms. *Organization Science*, *19*(3), 404-418.

Kirsch, L. J., Ko, D.-G., & Haney, M. H. (2010). Investigating the antecedents of team-based clan control: Adding social capital as a predictor. *Organization Science*, *21*(2), 469-489.

Kryscynski, D., Coff, R., & Campbell, B. (2021). Charting a path between firm-specific incentives and human capital-based competitive advantage. *Strategic Management Journal*, *42*(2), 386-412.

Kutner, M. H., Nachtsheim, C. J., Neter, J., & Wasserman, W. (2004). *Applied linear regression models* (4th ed.). McGraw-Hill/Irwin.

Kwon, J., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly*, *38*(2), 451-A453.

Lam, H. K., Yeung, A. C., & Cheng, T. E. (2016).The impact of firms' social media initiatives on operational efficiency and innovativeness. *Journal of Operations Management*, *47-48*(1), 28-43.

Laplume, A., Walker, K., Zhang, Z., & Yu, X. (2021). Incumbent stakeholder management performance and new entry. *Journal of Business Ethics*, *174*(3), 629-644.

Lee, S. H., Lee, T. W., & Lum, C. F. (2008). The. effects of employee services on organizational

commitment and intentions to quit. *Personnel Review*, *37*(2), 222-237.

Li, H., Yoo, S., & Kettinger, W. J. (2021). The roles of IT strategies and security investments in reducing organizational security breaches. *Journal of Management Information Systems*, *38*(1), 222-245.

Litov, L., & Zenger, T. (2010). *Do investors value uniqueness in corporate strategy? Evidence from mergers and acquisitions* (Working paper). Washington University.

Liu, C.-W., Huang, P., & Lucas, H. C. (2020). Centralized IT decision making and cybersecurity breaches: Evidence from US higher education institutions. *Journal of Management Information Systems*, *37*(3), 758-787.

Liu, M., & Lu, W. (2021). Corporate social responsibility, firm performance, and firm risk: the role of firm reputation. *Asia-Pacific Journal of Accounting & Economics*, *28*(5), 525-545.

Lynn, M., & Snyder, C. R. (2002). Uniqueness Seeking. *Handbook of Positive Psychology* (pp. 395-410).

Mackey, A., Mackey, T. B., & Barney, J. B. (2007). Corporate social responsibility and firm performance: Investor preferences and corporate strategies. *Academy of Management Review*, *32*(3), 817-835.

Madhavan, V., Venugopalan, M., Gupta, B., & Sisodia, G. S. (2023). Addressing agency problem in employee training: The role of goal congruence. *Sustainability*, *15*(4), Article 3745.

Maksimov, V., Wang, S. L., & Yan, S. (2022). Global connectedness and dynamic green capabilities in MNEs. *Journal of International Business Studies*, *53*(4), 723-740.

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*, 57-68.

Millward, L. J., & Hopkins, L. J. (1998). Psychological contracts, organizational and job commitment. *Journal of Applied Social Psychology*, *28*(16), 1530-1556.

Mitchell, M. S., & Ambrose, M. L. (2007). Abusive supervision and workplace deviance and the moderating effects of negative reciprocity beliefs. *Journal of Applied Psychology*, *92*(4), 1159-1168.

Morrison, E. W., & Robinson, S. L. (1997). When employees feel betrayed: A model of how psychological contract violation develops. *Academy of Management Review*, *22*(1), 226-256.

Mory, L., Wirtz, B. W., & Göttel, V. (2016). Factors of internal corporate social responsibility and the effect on organizational commitment. *The International Journal of Human Resource Management*, *27*(13), 1393-1425.

Murdock, K. (2002). Intrinsic motivation and optimal incentive contracts. *RAND Journal of Economics*, *33*(4), 650-671.

Nardi, L., Zenger, T., Lazzarini, S. G., & Cabral, S. (2022). Doing well by doing good, uniquely: Materiality and the market value of unique CSR strategies. *Strategy Science*, *7*(1), 10-26.

Parkes, L. P., & Langford, P. H. (2008). Work-life bal ance or work-life alignment? A test of the importance of work-life balance for employee engagement and intention to stay in organisations. *Journal of Management & Organization*, *14*(3), 267-284.

Pendleton, A. (2006). Incentives, monitoring, and employee stock ownership plans: New evidence and interpretations. *Industrial Relations: A Journal of Economy and Society*, *45*(4), 753-777.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179-214.

Post, G. V., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security*, *26*(3), 229-237.

Roodman, D. (2009). How to do xtabond2: An introduction to difference and system GMM in Stata. *The Stata Journal*, *9*(1), 86-136.

Ross, S. A. (1973). The economic theory of agency: The principal's problem. *The American Economic Review*, *63*(2), 134-139.

Rousseau, D. M. (1990). New hire perceptions of. their own and their employer's obligations: A study of psychological contracts. *Journal of Organizational Behavior*, *11*(5), 389-400.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78.

Sartal, A., Rodríguez, M., & Vázquez, X. H. (2020). From efficiency-driven to low-carbon operations management: Implications for labor productivity. *Journal of Operations Management*, *66*(3), 310-325.

Schilke, O. (2018). A micro-institutional inquiry into resistance to environmental pressures. *Academy of Management Journal*, *61*(4), 1431-1466.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*(2), 314-341.

Sharma, S., & Warkentin, M. (2019). Do I really belong?: Impact of employment status on information security policy compliance. *Computers & Security*, *87*, Article 101397.

Sherif, M. (1935). *A study of some social factors in perception. Archives of psychology*. Columbia University.

Shim, W. (2015). Agency problems in information security: theory and application to korean business. *The Journal of Internet Electronic Commerce Research, 15*(5), 1-15.

Shiu, Y. M., & Yang, S. L. (2017). Does engagement in corporate social responsibility provide strategic insurance-like effects? *Strategic Management Journal*, *38*(2), 455-470.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487-502.

Smith, E., Chown, J., & Gaughan, K. (2021). Better in the shadows? Public attention, media coverage, and market reactions to female CEO announcements. *Sociological Science*, *8*(7), 119-149.

Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, *14*(1),45-60.

Suls, J., Martin, R., & Wheeler, L. (2002). Social comparison: Why, with whom, and with what effect? *Current Directions in Psychological Science*, *11*(5), 159-163.

Sung, S. Y., Choi, J. N., & Kang, S. C. (2017). Incentive pay and firm performance: Moderating roles of procedural justice climate and environmental turbulence. *Human Resource Management*, *56*(2), 287-305.

Tang, Y., Qian, C., Chen, G., & Shen, R. (2015). How CEO hubris affects corporate social (ir) responsibility. *Strategic Management Journal*, *36*(9), 1338-1357.

Thau, S., Pitesa, M., & Pillutla, M. (2014). Experiments in organizational behavior. In M. Webster, Jr. & J. Sell (Eds.), *Laboratory experiments in the social sciences* (2nd ed., pp. 433-447). Adademic Press

Thomas, S. P., Thomas, R. W., Manrodt, K. B., & Rutner, S. M. (2013). An experimental test of negotiation strategy effects on knowledge sharing intentions in buyer-supplier relationships. *Journal of Supply Chain Management*, *49*(2), 96-113.

Ungureanu, P., Bertolotti, F., & Pilati, M. (2019). What drives alignment between offered and perceived well-being initiatives in organizations? A cross-case analysis of employer-employee shared strategic intentionality. *European Management Journal*, *37*(6), 742-759.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, *29*(4), 263-290.

Vance, A., Lowry, P. B., & Eggett, D. L. (2015). Increasing accountability through the user interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Quarterly*, *39*(2), 345-366.

Verizon. (2022). *Data breach investigations report*. https://www.verizon.com/business/resources/T1c3/reports/dbir/2022-data-breach-investigations-report-dbir.pdf.

Wang, J., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly*, *39*(1), 91-112.

Webster Jr, M., & Sell, J. (2007). Theory and experimentation. *The SAGE Handbook of Social Science Methodology* (pp. 192-211). SAGE.

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*, *28*(2), 266-293.

Wong, A. K. F., & Kim, S. S. (2020). Development and validation of standard hotel corporate social responsibility (CSR) scale from the employee perspective. *International Journal of Hospitality Management*, *87*, Article 102507.

Wooldridge, J. M. (2015). *Introductory econometrics: A modern approach*. Cengage Learning.

Wu, Y., Zhang, K., & Xie, J. (2020). Bad greenwashing, good greenwashing: Corporate social responsibility and information transparency. *Management Science*, *66*(7), 3095-3112.

Yiu, L. D., Lam, H. K., Yeung, A. C., & Cheng, T. (2020). Enhancing the financial returns of R&D investments through operations management. *Production and Operations Management*, *29*(7), 1658-1678.

Yoon, Y., & Sengupta, S. (2019). Employee share ownership, training, and early promotion policy as a bundle in enhancing labor productivity: A test of the three-way interaction effect. *Human Resource Management*, *58*(6), 603-620.

Zerbini, F. (2017). CSR initiatives as market signals: A review and research agenda. *Journal of Business Ethics*, *146*(1), 1-23.

Zhou, J., Fang, Y., & Grover, V. (2022). Managing collective enterprise information systems compliance: A social and performance management context perspective. *MIS Quarterly*, *46*(1), 71-100.

Appendix A: Information on Employee-Related Rating Items

Table A1 lists detailed information on the rating items used in this study.

Table A1. Rating Items in the Employee Dimension of KLD

Panel A: Strength dimension (*EMP_str*)		
Notation	**Rating Item**	**Description**
EMP_str_A	Union relations	Whether the firm has taken exceptional steps to treat its unionized workforce fairly
EMP_str_B	No-layoff policy	Whether the firm maintains a consistent no-layoff policy
EMP_str_C	Cash profit sharing	Whether the firm has a cash profit-sharing program through which it has recently made distributions to a majority of its workforce
EMP_str_D	Employee involvement	Whether the firm strongly encourages worker involvement and/or ownership through stock options available to a majority of its employees, gain sharing, stock ownership, sharing of financial information, or participation in management decision-making
EMP_str_F	Retirement benefits strength	Whether the firm has a notably strong retirement benefit
EMP_str_G	Employee health and safety	Whether the firm has strong health and safety programs
EMP_str_H	Supply chain labor standards	Whether the firm has a strong ability to manage labor standards within the supply chain to reduce risks of production disruption and brand value impairment
EMP_str_I	Compensation & benefits	Whether the firm offers competitive compensation and benefits plans
EMP_str_J	Employee relations	Whether the firm has a good management of employee relations
EMP_str_K	Professional development	Whether the firm has a professional development plan
EMP_str_L	Human capital management	Whether the firm has capability in human capital management, including attracting, retaining, and developing talent
EMP_str_M	Labor management	Whether the firm can effectively manage labor to reduce instability in workflow
EMP_str_N	Controversial sourcing	Whether the firm takes measures to mitigate risks related to using materials from regions with severe human rights and labor rights abuses
EMP_str_X	Employee relations other strength	Other exceptional performance aspects in employee relations management that are not covered by other KLD rating items
Panel B: Concern dimension (*EMP_con*)		
Notation	**Rating Item**	**Description**
EMP_con_A	Union relations	Whether the firm has a history of notably poor union relations
EMP_con_B	Employee health & safety	Whether the firm recently has either paid substantial fines or civil penalties for willful violations of employee health and safety standards or has been otherwise involved in major health and safety controversies
EMP_con_C	Workforce reductions	Whether the firm has recently made significant reductions in its workforce
EMP_con_D	Retirement benefits concern	Whether the firm has either a substantially under-funded defined benefit pension plan or an inadequate retirement benefits program
EMP_con_F	Supply chain	Whether the firm is experiencing controversies related to the treatment of workers within its supply chain
EMP_con_G	Child labor	Whether the firm recently has labor-management relationship disputes, including employee legal cases, layoffs, reduction of benefits, mistreatment of employees or contractors
EMP_con_H	Labor-management relations	Whether the firm is facing disputes related to labor-management relations, including issues like employee legal cases, layoffs, reduction in benefits, and improper treatment of employees or contractors
EMP_con_X	Employee relations other concerns	Other employee relations controversy that is not covered by other KLD rating items

Appendix B: Variable Descriptions

Table B1 shows the detailed definitions and data sources of all variables used in the main analysis.

Table B1. Variable Descriptions

Variables	Description	Source
Security	A dummy variable that equals 1 if a firm has a reported data breach in the fiscal year, and 0 if otherwise	PRC, ITRC
Employee-related CSR	Sum of all rating items within the employee-related social performance strength component, as in Tang et al. (2015)	KLD database
Employee-related CsiR	Sum of all rating items within the employee-related social performance concern component, as in Tang et al. (2015)	KLD database
Size	Natural logarithm of a firm's value of total assets (in $millions).	COMPUSTAT
Leverage	The ratio of the beginning total liabilities divided by the beginning total assets.	COMPUSTAT
ROA	The ratio of net income before extraordinary items divided by the total assets	COMPUSTAT
Sale change	The difference in firm sales between this and the last fiscal year	
R&D	R&D expenditures scaled by the total assets	COMPUSTAT
Advertising	Advertising expenses scaled by the total assets	COMPUSTAT
Financial slack	The ratio of quick assets to liabilities, as in Kim et al. (2008)	COMPUSTAT
Operational slack	Natural logarithm of the industry-adjusted ratio of annual sales to tangible assets, as in Azadegan et al. (2013)	COMPUSTAT
Human slack	Natural logarithm of the industry-adjusted ratio of annual sales to labor, as in Azadegan et al. (2013)	COMPUSTAT

Appendix C: Collinearity

Table C1 shows the correlation between the variables in the main analysis. Variance inflation factors (VIFs) are calculated for the full model to check for potential multicollinearity in the analysis. The average VIF value of the full model is 2.05. Given that the common VIF threshold is 10.0 (Kutner et al., 2004), multicollinearity is not a significant concern for our models.

Table C1. Correlation Matrix

	Variables	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**	**(9)**	**(10)**	**(11)**
(1)	Security	1.000										
(2)	Employee-related CSR	0.083	1.000									
(3)	Employee-related CSiR	0.112	0.175	1.000								
(4)	Size	0.223	0.364	0.283	1.000							
(5)	Leverage	0.065	-0.045	-0.140	0.309	1.000						
(6)	ROA	0.026	0.068	0.010	0.131	-0.105	1.000					
(7)	Sales growth	-0.025	-0.062	-0.091	-0.112	-0.096	0.065	1.000				
(8)	R&D	0.050	0.035	0.029	-0.003	-0.009	0.019	-0.003	1.000			
(9)	Advertising	-0.023	0.020	-0.055	-0.182	-0.020	-0.359	0.075	-0.027	1.000		
(10)	Financial slack	-0.003	-0.091	-0.075	-0.128	-0.104	0.023	0.030	0.031	-0.019	1.000	
(11)	Operational slack	0.036	-0.058	0.077	-0.120	-0.032	-0.024	-0.024	0.042	0.092	-0.085	1.000
(12)	Human slack	-0.014	-0.026	-0.052	-0.133	0.182	-0.224	0.026	0.046	0.613	-0.024	0.186

Appendix D: System Generalized Method of Moments (GMM)

In employing the system GMM estimator, we first modified Equations (1) and (2), which are used in the main analysis, to estimate a dynamic unobserved effects model with the following specifications:

$$Security_{i,j+1}=\beta_0+\delta_1 Security_{i,j}+\delta_2 Security_{i,j-1}+\beta_1 Employee\text{-}related\ CSR_{i,j}+\sum \alpha_r Control_{i,j}+v_i+\omega_j+\varepsilon_{ij}, \quad (A1)$$

$$Security_{i,j+1}=\beta_0+\delta_1 Security_{i,j}+\delta_2 Security_{i,j-1}+\beta_1 Employee\text{-}related\ CSiR_{i,j}+\sum \alpha_r Control_{i,j}+v_i+\omega_j+\varepsilon_{ij}, \quad (A2)$$

$$Security_{i,j+1}=\beta_0+\delta_1 Security_{i,j}+\delta_2 Security_{i,j-1}+\beta_1 Employee\text{-}related\ CSR_{i,j}+\beta_2 Employee\text{-}related\ CSiR_{i,j}+\sum \alpha_r Control_{i,j}+v_i+\omega_j+\varepsilon_{ij}, \quad (A3)$$

To account for past security performance's impact on the current one, we included lagged security risks ($Security_{i,j}$ and $Security_{i,j-1}$). Unobserved heterogeneity and systematic variations across years were addressed by introducing firm- (v_i) and year-fixed (ω_j) effects. We transformed Equations (A1), (A2), and (A3) into first-difference formats to mitigate dynamic panel bias, which could arise from endogeneity of the lagged dependent variable. Yet, concerns about weak instruments led us to use the system GMM estimator for first-differenced equations, augmented with extra lags of the dependent variable as instruments, as established by prior research (Sartal et al., 2020; Yiu et al., 2020).

We performed two classical tests to validate the instruments used in our system GMM estimation. The first test, the Arellano-Bond test, checks for autocorrelation in idiosyncratic disturbance terms. The results in Table D show no significant serial correlation for AR (2) ($p > 0.1$) across the three models, confirming the validity of the second lags of levels as instruments for the difference equation. The second diagnostic, the Hansen test, assesses instrument exogeneity. Across the three models, the Hansen test results in Table D are not significant ($p > 0.1$), indicating that the instruments are not correlated with the error term. This supports the instruments' exogeneity and provides evidence for a valid system GMM estimation. Both specification tests collectively confirm the validity of our system GMM estimates.

Table D. Specification Tests of the Instruments

Variable	**Fixed-effect LPM** **Dependent variable: *Security* (subsequent year)**		
	(1)	**(2)**	**(3)**
Security	0.056 (0.971)	0.056 (0.977)	0.057 (0.989)
Security (lagged)	0.089 (1.616)	0.090 (1.633)	0.090 (1.638)
Employee-related CSR	**-0.010*** **(-1.827)**		**-0.010*** **(-1.752)**
Employee-related CSiR		**0.024**** **(2.005)**	**0.024*** **(1.939)**
Controls	Included	Included	Included
Firm fixed effects	Included	Included	Included
Year fixed effects	Included	Included	Included
Number of observations	6,850	6,850	6,850
Arellano-Bond test for AR(1) in first differences	z = -8.53; Pr > z = 0.000;	z = -8.51; Pr > z = 0.000	z = -8.53; Pr > z = 0.000;
Arellano-Bond test for AR(2) in first differences	z = -0.38; Pr > z = 0.704	z = -0.39; Pr > z = 0.698	z = -0.40; Pr > z = 0.690
Hansen test of restrictions	chi2(14) = 16.57 Pr > z = 0.280	chi2(14) = 18.87 Pr > z = 0.170	chi2(13) = 14.67 Pr > z = 0.329

Note: Results for system-GMM analysis. The dependent variable is *Security* and is measured in year $t + 1$. t statistics are in parentheses ($^{*}p < 0.1$, $^{**}p < 0.05$, $^{***}p < 0.01$).

Appendix E. Information on the First-stage Heckman Regression

In the first stage of the Heckman's two-stage analysis, we modeled the probability (*Selection probability*) of an observation appearing in our sample. This selection model requires, in particular, the utilization of at least one instrument that meets the exclusion-restriction principles—i.e., (1) the variable(s) should not appear in the second stage; (2) the variable(s) should impact the overall likelihood of an observation's appearing in the sample (in our context, the probability of firms to disclose their employee-related CSR information); (3) the variable(s) should not influence the ultimate dependent variable of interest in the second-stage model (in our context, security risk) (Bushway et al., 2007; Certo et al., 2016). On the basis of the principles, the instrument that we adopted is the peer disclosure rate (*Peer selection*), which was operationalized as the average employee-related social performance disclosure rate from peer firms within the three-digit SIC industry. We adopted the instrument of *Peer selection* because the variable is likely to influence the disclosure intentions of focal firms through mimetic isomorphism (DiMaggio & Powell, 1983; Maksimov et al., 2019) and unlikely to influence the firms' security risks. Therefore, *Peer selection* is a good instrument in our context. Moreover, to increase the explanatory power of the selection model, we also included all the controls in the main analysis in the first-stage Heckman analysis. These predictors enabled us to generate inverse Mill's ratios by using a probit model.

Table E provides the results of the first-stage Heckman regression model. As expected, the coefficient of *Peer selection* is significantly positive, indicating that the instrument can significantly increase firms' likelihood of disclosing their employee-related CSR information. Beyond this situation, the expectations that the instrument satisfies the exclusion-restriction principles are further supported by the fact that neither shows a significant coefficient if included in the second-stage regression.

Table E. First-Stage Heckman Selection Regression

Variable	**Probit (*Selection probability*)**
Peer selection	4.586***
	(26.642)
Controls	Included
Industry fixed effects	Included
Year fixed effects	Included
Number of observations	13,605

Note: t-statistics are in parentheses (* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$).

Appendix F: Example Breach Descriptions and Types

Table F. Data Breach Examples

Source	Company name	Breach year	Description of example breaches (from PRC or ITRC)
ITRC	HSBC Auto Finances	2008	HSBC Auto Finances files may have been taken in an unauthorized manner by a former employee prior to separation from the company. The information included names, account numbers for loans, and, in some cases, Social Security numbers (SSNs)
ITRC	MasTec	2008	MasTec North America discovered that an employee disclosed an HR report to third parties. Both the employee and the third parties were arrested. The information included names, dates of birth, SSNs, and employee identification numbers. MasTec found out about it on Oct 29. Ninety-five people in MD were affected.
ITRC	Regal Entertainment Group	2008	On September 17, ID Experts notified the New Hampshire Attorney General's Office that a backup tape belonging to Regal Entertainment Group that contained personal data was lost on August 29, 2008. In its notification to those affected, the company wrote: "We recently learned that individual employees violated established procedures during a routine exercise and lost some supplier's and other individual's data which was contained on a system backup tape."
PRC & ITRC	Tenet Healthcare	2008	A former employee of a locally connected national hospital chain who was convicted of identity theft had access to the personal information of about 37,000 patients, according to a company spokesman. In 2008, Tenet Healthcare Corp. owned 54 hospitals in a dozen states, including Hilton Head Regional Medical Center and Coastal Carolina Medical Center. The Texas employee worked in the billing center for about two years and is confirmed to have stolen names, SSNs, and other information of about 90 patients. He had access to 37,000 other accounts.
ITRC	Verizon Wireless	2008	According to information contained in a notice to the NH AG's office, a Verizon telesales employee allegedly printed out screens containing customers' names, addresses, SSNs, and/or and/or Verizon Wireless account numbers.
PRC & ITRC	Wendy's International	2008	An administrative error at Life Choices Service Center caused 2008 benefit confirmation statements to be sent to some incorrect addresses. The information of some Wendy's employees included dependent information for other Wendy's employees. Names, SSNs, and dates of birth may have gone to the wrong people. The error occurred on November 29.
ITRC	First Republic Bank	2009	A former San Francisco bank mailroom supervisor accused in an identity theft scam faces up to seven years in prison if convicted, prosecutors said today. San Francisco prosecutors say that over a six-month period beginning in April 2007, he allegedly opened customer mail at a First Republic Bank branch containing both commercial and personal identifying information. He then allegedly made copies of checks and sold those copies as part of a larger identity theft scheme. The checks were later used by someone else to replicate the bank account and issue checks from that account. The Secret Service revealed that as many as 560 pieces of mail may have been opened.
ITRC	Sea Ray Boats	2009	On October 21, an employee of Sea Ray Boats unintentionally sent an email to 698 dealership personnel that contained the names, contact information, and SSNs of 341 of the 698 employees.
ITRC	Wal-Mart Stores Inc.	2009	Wal-Mart suffered a breach in its staff data system due to a former employee leaving their job with confidential records. The information allegedly involved 48,000 staff members in Illinois.
ITRC	Wells Fargo	2009	A Wells Fargo Bank employee working inside a bank call center was arrested Friday using customer account access to pay her own debts, open credit card accounts, and obtain ATM cards, according to the US Attorney's office.

Note: Privacy Rights Clearinghouse (PRC); Identity Theft Resource Center (ITRC).

Appendix G: Additional Information on Scenario-Based Experiment

Design and Procedure

Participant Eligibility Verification

Prior to conducting the experiment, stringent participant screening procedures were implemented to ensure decision-making eligibility. This was achieved through the implementation of two distinct screening conditions, following standardized experimental protocols (Schilke, 2018). The initial screening process involved identifying participants with inadequate information security knowledge. To achieve this, participants were presented with a series of quizzes pertaining to real-life information security scenarios. These quizzes assessed participants' familiarity with concepts such as: "Cybersecurity is solely IT staff's responsibility," requiring a "True" or "False" response. The second screening step aimed to exclude participants displaying insufficient engagement. This was done by introducing a concealed screener question (e.g., "Please choose 'strongly agree'") within the post-task questionnaire. The purpose was to gauge the level of participant focus. Furthermore, respondents falling below a minimum time threshold (less than 2 minutes) or exceeding a maximum time limit (more than 6 minutes) in completing the questionnaire were also excluded from the analysis (DeSimone et al., 2015).

Assessment of Scenario Realism

Furthermore, to ensure the fidelity of our scenario-based setting in mirroring real-life business contexts, an additional realism evaluation was integrated into the survey process. This assessment gauged the authenticity of the scenarios by asking participants to rate their realism using a 7-item scale (ranging from 1 to 7), as established by Dabholkar (1996). This approach has been widely adopted to validate the authenticity of scenario-based experiments (e.g., Chen et al., 2016; Thomas et al., 2013). Specifically, upon reviewing the scenarios, participants were requested to express the extent to which they perceived (1) "The situation described was realistic" and (2) "I had no difficulty in imagining myself in the situation." The average score for these two realism items stood at 5.45 (out of 7), aligning closely with findings from earlier studies (e.g., Hora and Klassen (2013) reported a mean of 5.25, while Chen et al. (2016) reported a mean of 5.35).

Vignettes, Questions, and Manipulation Check

In our scenario-based experiment, participants were randomly assigned to one of three distinct groups: (1) employee-related CSR (ECSR; T_{ECSR}; n = 69), (2) employee-related CSiR (ECSiR; T_{ECSiR}; n = 68), or (3) control experimental conditions (C; n = 67). Each group was exposed to a scenario description centered around a fictitious company referred to as "Company X." For comprehensive scenario descriptions, please refer to Table G1; the specific questions posed can be found in Table G2.

To identify the validity of the scenario manipulation, we utilized three specific criteria:

- "Company X < actively, did not, sometimes > spoke out against sweatshops"
- "Company X has < always, sometimes, never > been a frequent believer and supporter of Business for Social Responsibility guidelines for manufacturing practices"
- "Company X offers compensation packages < ahead of, in line with, below > its competitors"

Our analysis, utilizing one-way ANOVA, revealed significant score differences across the experimental groups for each of the criteria. This suggests that our scenario manipulation effectively influenced participants' perceptions, supporting the validity of the scenario manipulation.

Table G1. Vignettes for Testing Underlying Mechanisms

Employee-related CSR (ECSR) vignette Most people associate Company X with Internet and computers. However, little is known that Company X is a pioneer in its active role as a corporate champion of the fair working environment. Unlike most of its major competitors, Company X has taken an active stand against the "sweatshop" conditions. Company X is one of the few major electronics companies to adopt the Business for Social Responsibility guidelines for manufacturing practices in their operations of major companies and has allocated significant human or financial resources to monitor and enforce these guidelines in its calculator-manufacturing operations. Company X is also far ahead of its competitors in providing its factory workers with compensation packages (including health, retirement, and educational benefits) that are well above the "basic needs" based recommendations of the International Labor Organization. Thus, it is not surprising that, unlike some of its major competitors, Company X is prominently present on the 2012 Trendsetters List (compiled by the human rights group Witness)—an exclusive list of manufacturers who have been exemplary in instituting humane working conditions in their overseas facilities. In sum, Company X has constantly been a believer and supporter of a fair working environment, and its values come through amply in its grassroots support as well as its corporate championship of this issue.
Employee-related CSiR (ECSiR) vignette Most people associate Company X with Internet and computers. However, little is known that Company X is a laggard in ensuring a fair business environment. Unlike most of its major competitors, Company X has never taken a stand against the "sweatshop" conditions. Company X is one of the few major electronics companies that have yet to adopt the Business for Social Responsibility guidelines for manufacturing practices in their operations of major companies and has allocated no human or financial resources to monitor and enforce these guidelines in its own calculator-manufacturing operations. Company X is also behind its competitors in providing its factory workers with compensation packages (including health, retirement, and educational benefits) that are in line with the "basic needs" based recommendations of the International Labor Organization. Thus, it is not surprising that, unlike some of its major competitors, Company X is prominently absent from the 2012 Trendsetters List (compiled by the human rights group Witness)—an exclusive list of manufacturers who have been truly exemplary in instituting humane working conditions. In sum, Company X has never been a believer and supporter of fair overseas manufacturing practices, and its values come through amply in its lack of both grassroots support and corporate championship of this issue.
Control vignette Company X produces Internet and computers. It is an established electronics company in the world. It does manufacture at various locations in the world and hires employees from multiple countries.

Table G2. Questionnaires in the Scenario-Based Experiment

Variables	**Factor loading** (Factor analysis)
Question Module 1: Employee-related social performance (average variance extracted [AVE] = 0.898, composite reliability [CR] = 0.992)	
This company treats employees fairly and respectfully.	0.946
This company provides a safe and healthy working environment to all employees.	0.949
The company is concerned with employees' needs and wants.	0.956
The company's policies encourage employees to have a good work and life balance (interest class, recreational gathering or open day for family members on a regular basis, etc.).	0.942
The company encourages employees to acquire further education for career advancement.	0.942
The company always cares about its employees and provides decent working conditions such as welfare facilities to them (staff restaurant, lockers room, leisure room or accommodation and transportation arrangements during adverse weather, etc.).	0.955
The company provides activities to enhance employees' emotional well-being (stress management workshops or counseling services, etc.).	0.945
Question Module 2: Related to "security commitment" (AVE = 0.756, CR = 0.945)	
I place high value on reaching the security goals of our organization.	0.911
I have a high willingness to invest a large amount of effort (e.g., to be highly compliant with firm security policy) in my security-related operations.	0.860
I expect that our organization could reach its security goal.	0.836

Question Module 3: Related to "peer-monitoring" (AVE = 0.694, CR = 0.942)	
I would appreciate when other employees provide insight to improve my information security behaviors.	0.822
Individuals in my workgroup would be receptive when I remind them about proper information security behaviors.	0.898
My managers would value when employees inform them of best information security behaviors.	0.830
It would never bother me when someone in my workgroup reminds me about best information security practices.	0.778
Question Module 4: Related to "employee loyalty and firm appeal" (AVE = 0.795, CR = 0.957)	
Our organization has a "unique personality" to retain security expertise.	0.905
Our organization has a "distinct identity" to retain talented employees.	0.904
Compared to other firms, our organization could attract talent.	0.866
Question Module 5: Share your thoughts in reference to the scenario.	
The situation described was realistic.	-
I had no difficulty in imagining myself in the situation.	-

Appendix H. Additional Analysis on the Overall Level of Employee-Related Social Performance

To further enrich our analysis, this appendix provides insights into the relationship between a firm's overall employee-related social performance and its information security performance. Firms can enhance their employee-related social performance by increasing responsible activities related to employees and/or decreasing irresponsible activities associated with them (Fu et al., 2020). Then, by integrating our key findings that employee-related CSR diminishes firms' security risks while employee-related CSiR heightens such risks, we predict that overall employee-related social performance within firms is likely to mitigate their security risks.

As a firm's overall employee-related social performance tends to increase with engaging employee-related CSR but decreases with involving employee-related CSiR, we operationalize a firm's overall employee-related social performance (*Employee-related social performance*) as the difference between its *Employee-related CSR* and *Employee-related CSiR*. This operationalization also aligns with previous CSR studies (e.g., Fu et al., 2020; Tang et al., 2015). Next, we examine the impact of overall employee-related CSR performance on security risks using the following panel regression model, which is similar to our baseline analysis:

$$Security_{i,j+1}=\beta_0+\beta_1 Employee\text{-}related\ social\ performance_{i,j}+\sum\alpha_r Control_{i,j}+v_i+\omega_j+\varepsilon_{ij}. \quad \text{(A4)}$$

In Table H1, we present the findings regarding the impact of overall employee-related social performance on security risks. The model indicates that a high level of total overall employee-related social performance is associated with a decrease in firms' security risks, as evidenced by the negative and significant coefficient of *Employee-related social performance* (β_1 = -0.012, $p < 0.01$). Specifically, a one standard deviation (0.985) increase in firms' overall employee-related social performance is expected to reduce the likelihood of data breaches in the subsequent year by 1.2% (0.012×0.985). Given the mean data breach likelihood is 2.8%, this represents a 42.9% reduction in firms' security risks in the subsequent year. Hence, the result supports our prediction.

Table H1. Main Analysis Results

Variable	**Fixed-effect LPM** **Dependent variable: *Security* (subsequent year)**
Employee-related social performance	**-0.012***** **(-3.315)**
Controls	Included
Firm fixed effects	Included
Year fixed effects	Included
Number of observations	9,620

Note: The dependent variable is *security* and is measured in year $t + 1$. t statistics are in parentheses (* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$).

About the Authors

Qian Wang is an assistant professor in the Faculty of Business Administration, University of Macau. Her research interests include data breaches, corporate governance, and information security. Her work has appeared in several international journals, such as *Journal of the Association for Information Systems, Journal of Operations Management, Production and Operations Management,* and *Journal of Management Information Systems.*

Daniel Pienta is an assistant professor in the Department of Accounting and Information Management and a Research Fellow of the Neel Corporate Governance Center at the University of Tennessee, Knoxville. His research interests include information security and privacy. He serves as an associate editor for the *Journal of the Association for Information Systems.* His work has appeared in numerous international journals, such as *Journal of the Association for Information Systems, MIS Quarterly, Information Systems Research,* and *Journal of Management Information Systems.*

Shenyang Jiang is an assistant professor at the Advanced Institute of Business, Tongji University. His research interests include supply chain management, people-centric operations, digital operations, and generative AI. His research has appeared in numerous international journals including *Journal of the Association for Information Systems, Management Science, Journal of Operations Management,* and *Production and Operations Management.*

Eric W. T. Ngai is a professor in the Department of Management & Marketing at The Hong Kong Polytechnic University. His research spans e-commerce, decision support systems, supply chain management, knowledge management & innovation, IoT, and AI methods and applications. He has published in numerous leading journals, including *Journal of the Association for Information Systems, MIS Quarterly, Production and Operations Management, Journal of Operations Management, Journal of Management Information Systems,* and *INFORMS Journal of Computing.*

Jason Bennett Thatcher is a professor at the Leeds School of Business, University of Colorado Boulder. His research explores individual decision-making, strategic alignment, and workforce issues related to information technology in organizations, with a focus on cybersecurity, social media, and digital upper echelons. His work has been published in numerous leading journals such as *Journal of the Association for Information Systems, MIS Quarterly, Information Systems Research, Journal of Applied Psychology,* and *Harvard Business Review.*