




Asymmetric Learning Effects of Chief Information Officer Outside Board Appointments: Cybersecurity Implications for Sender and Receiver Firms

Justin Short,^a John D’Arcy,^b Yili Hong^{c,*}

^aHaslam College of Business, University of Tennessee, Knoxville, Tennessee 37916; ^bLerner College of Business & Economics, University of Delaware, Newark, Delaware 19716; ^cMiami Herbert Business School, University of Miami, Coral Gables, Florida 33146

*Corresponding author

Contact: jshort3@utk.edu,  <https://orcid.org/0000-0002-1794-2657> (JS); jdarcy@udel.edu,  <https://orcid.org/0000-0003-0286-5772> (JD’A); khong@miami.edu,  <https://orcid.org/0000-0002-0577-7877> (YH)

Received: March 8, 2024

Revised: November 12, 2024; July 31, 2025;
September 29, 2025

Accepted: October 30, 2025

Published Online in Articles in Advance:
December 17, 2025

<https://doi.org/10.1287/isre.2024.1003>

Copyright: © 2025 INFORMS

Abstract. As cybersecurity becomes a critical board-level concern, public companies increasingly appoint chief information officers (CIOs) from other firms to their boards to enhance organizational learning. Drawing on the board interlock literature, we examine two pathways through which such appointments influence a firm’s cybersecurity learning: (a) the receiver pathway, where a firm appoints a CIO from another company and gains external cybersecurity expertise; and (b) the sender pathway, where a firm’s own CIO serves on an outside board and potentially brings back valuable insights. We consider the conditions that enable or constrain learning in each pathway and how these affect a firm’s data breach risk. Leveraging a panel data set of 17,227 CIO-firm-year-level observations (2005–2022), we find that sender firms—those whose CIOs serve on external boards—experience a significant increase in breach probability. In contrast, receiver firms—those appointing outside CIOs—see a significant decrease in breach probability. Further mechanism analyses show that these outcomes are shaped by heterogeneity in the cybersecurity practices of both sender and receiver firms. Sender firms face increased breach risk when the receiver firm lacks strong cybersecurity emphasis or has a breach history. This risk is mitigated if the sender firm has a chief information security officer (CISO) on its top management team. Receiver firms benefit when the sender firm emphasizes cybersecurity, but also when it has had a past breach. This latter finding diverges from typical contagion effects in the interlock literature, suggesting that negative cybersecurity events may serve as valuable learning opportunities. We attribute these asymmetric effects to the CIO’s unique role in interlocks. Unlike other executives, CIOs often act as deeply engaged educators and hands-on problem solvers in cybersecurity on the boards they join. Their focus on knowledge dissemination over acquisition, alongside their ongoing operational responsibilities within their home firm, appears to negate potential sender-side learning benefits. Our findings inform firms on their decisions about recruiting outside CIOs to their boards, permitting internal CIOs to join external boards, and guide policymakers aiming to strengthen cybersecurity expertise on corporate boards.

History: Kenneth Hsing Cheng, Senior Editor; Ling Xue, Associate Editor.

Supplemental Material: The online appendix is available at <https://doi.org/10.1287/isre.2024.1003>.

Keywords: data breach • chief information officer (CIO) • chief information security officer (CISO) • board interlock • cybersecurity • board of directors

Introduction

Corporate boards of directors are giving increased attention to their firms’ cybersecurity (Benaroch and Chernobai 2017, Parenty and Domet 2020, Lowry et al. 2025), in large part because of the widespread digitization of nearly all facets of business operations. Expanding digital infrastructures, such as systems needed to support remote work capabilities and diverse online transactions, increase the exposure of these systems to cybersecurity risk, and so, firms are seeking board-

level guidance and oversight to improve their resilience in this area. This shift reflects the growing role of corporate boards in actively overseeing and sharing responsibility for their firms’ cybersecurity (Proudfoot et al. 2023). A prominent example is the 2013 Target data breach, where the board faced intense criticism for its failures in risk oversight and insufficient focus on the company’s cybersecurity readiness (Srinivasan et al. 2019a). As cybersecurity has become a critical board-level concern, firms are increasingly seeking

board members with cybersecurity expertise, prompting the recent trend of firms inviting a chief information officer (CIO) from another firm to join their board (Zukis 2019, Johnson 2020) (see Online Appendix A for evidence of this trend and specific examples). This trend is likely to accelerate as the U.S. Securities and Exchange Commission (SEC) pushes public companies to enhance cybersecurity expertise on their boards and clearly demonstrate these competencies to investors (SEC 2023, Lowry et al. 2025).

In addition to any personal benefits CIOs may derive from outside board appointments, such as increased prestige, financial compensation, and expanded professional networks (Bandodkar and Grover 2022, Ramsawak et al. 2024), firms view these appointments as opportunities to deepen organizational learning in cybersecurity, ultimately improving the firm's performance in this area (Stephenson and Olson 2017). As top information technology (IT) executives who often bear ultimate responsibility for a data breach or other cybersecurity failure (Banker and Feng 2019), most CIOs today are not just responsible for strategic leadership but are tasked with operational oversight, ensuring that effective cybersecurity controls are designed, implemented, and adhered to on an ongoing basis (Benaroch and Chernobai 2017, Parenty and Domet 2020, Haislip et al. 2021). Cybersecurity is one of the principal obligations of a CIO and serves as a key performance metric for the role (Kappelman et al. 2019, Johnson et al. 2023). As one CIO we interviewed explained, "not having a data breach was something I was obsessed about."¹ Given this focus, CIOs are well positioned to share their cybersecurity expertise with any board of directors that they join and should be highly motivated to capitalize on any learning opportunities a board appointment affords them in this domain. In this manner, past research on the outside board service ("sent" board interlocks) of a firm's chief executive officer (CEO) and "received" board interlocks from CEOs of outside firms (e.g., Geletkanycz and Hambrick 1997, Perry and Peyer 2005) provides a basis for proposing two key pathways through which CIO outside board appointments can promote such learning.

One pathway is when a firm appoints a CIO from another firm to its board, thereby gaining direct access to external cybersecurity expertise as a receiver firm. Another is when a firm's own CIO serves on the board of another firm, indirectly gaining access to valuable cybersecurity insights and experiences that can potentially be absorbed and then transferred back to the sending firm (i.e., where the CIO is employed). Research on board interlocks suggests that such sender and receiver pathways involving CEOs constitute two distinct types of relationships (Geletkanycz and Boyd 2011), and whether firms achieve meaningful learning

outcomes through either pathway depends on several factors (e.g., industry, growth stage, governance structure) specific to the sender and/or receiver firms (Perry and Peyer 2005, Ramsawak et al. 2024). Notably, these dual pathways remain unexplored in the context of CIO board service, leaving open questions about whether firms benefit from the direct cybersecurity learning from appointing an outside CIO to their board or the more indirect form of this learning when their own CIO serves on an outside board. As we will discuss, the unique nature of the CIO role and their responsibilities in our interlock context—serving on outside boards as deeply engaged educators and hands-on problem solvers in cybersecurity while simultaneously overseeing efforts to combat daily cybersecurity risks within their own firms—sets CIO-board interlocks apart from those involving other executives.

Given the emerging trend of CIOs joining outside boards and the regulatory push that is likely to further accelerate this trend, it is important to understand the implications of such moves. Moreso, because firms incur "costs" from such appointments from both the sending (e.g., the CIO's time spent on the outside board service) and receiving (e.g., the financial compensation awarded to an outside CIO who is appointed to the board) perspectives, it is important to consider the conditions that either enable or limit cybersecurity learning outcomes in both pathways. We explore these issues in this research and, in doing so, provide empirical based guidance for firms and policymakers on effectively allocating cybersecurity expertise to boards of directors. We focus on a key cybersecurity implication pertinent to CIOs' performance—occurrences of data breaches.² Our focus on data breaches follows extant literature that considers the occurrence (or nonoccurrence) of a data breach as a central indicator of a firm's cybersecurity performance (e.g., Kwon and Johnson 2018, Banker and Feng 2019, Kim and Kwon 2019, Li et al. 2023).

To conduct our research, we construct a panel data set from multiple public sources that has 17,227 CIO-firm-year-level observations and spans the years 2005–2022. We find that a CIO concurrently serving on an outside board significantly *increases* the sender firm's likelihood of a data breach. We also find that having an outside CIO serve on the firm's own board (i.e., receiver firms) *decreases* the receiver firm's likelihood of breach. To explain these asymmetric effects and explore the underlying mechanisms driving these results, we consider heterogeneity in the cybersecurity experiences and practices of both the sender and receiver firms. Sender firms experience stronger increases in breach likelihood when (a) the receiver firm does not have a chief information security officer (CISO) on its top management team (TMT), (b) the receiver firm has had a past breach, and (c) the receiver

firm has relatively low investment in IT security applications. This risk is mitigated when the sender firm has a CISO on its own TMT. For receiver firms, they experience stronger decreases in breach likelihood when (i) the sender firm has a CISO on its TMT, (ii) the sender firm has had a past breach, and (iii) the sender firm has relatively high investment in IT security applications.

Broadly, our findings suggest complex learning dynamics arising from CIOs serving on outside boards, some of which diverge from conventional theoretical expectations regarding learning benefits. Notably, we identify instances where sender firms fail to realize anticipated beneficial cybersecurity learning outcomes when their CIO joins the board of another company, as well as the conditions under which such failures occur. This is an important finding, given that CIOs have strong financial and reputational incentives to join outside boards and because the SEC is ostensibly encouraging such actions for all public companies in its cybersecurity policy updates (SEC 2023, Lowry et al. 2025). Our finding that sender firms experience cybersecurity drawbacks diverges from several past studies that support the learning benefits for sender firms when their C-level executives (particularly CEOs and chief financial officers (CFOs)) serve on outside boards (Perry and Peyer 2005, Geletkanycz and Boyd 2011, Khan and Mauldin 2021, Cunningham et al. 2024). This finding highlights the distinct nature of CIO-board interlocks in terms of the dual cybersecurity-related responsibilities CIOs hold toward the outside boards they serve on and their obligations to their own (home) firms. Unlike other executives, CIOs typically assume the role of deeply engaged educators and hands-on problem solvers in cybersecurity on the boards they join. In this capacity, they function more as disseminators of knowledge than as active learners. The CIO position is also unique in that, unlike the primarily strategic focus of CEOs and CFOs in their home firm responsibilities, CIOs also have significant operational responsibilities at their home firms that include the critical role of overseeing the daily management of cybersecurity risk. Effective cybersecurity management demands constant vigilance and oversight, which is challenged when the CIO's attention is divided by the demands of board-related cybersecurity responsibilities. Together, these forces appear to negate any beneficial cybersecurity learning outcomes for sender firms.

In contrast to sender firms, our evidence highlights the cybersecurity benefits for receiver firms when a CIO from another firm joins their board, especially when that CIO's firm has made significant investments in IT security and has experienced a prior breach. Notably, the finding that receiver firms see a decrease in breach likelihood when the sender firm has had a past breach is counter to the typical contagion effect

found in the interlock literature, suggesting that negative cybersecurity events can, in fact, serve as valuable learning opportunities. Taken together, our findings of asymmetric learning effects suggest that appointing a CIO from another firm to a firm's own board is a more effective channel for creating beneficial cybersecurity learning outcomes than sending a CIO to serve on another firm's board.

In what follows, we provide a brief review of the literature on board interlocks to ground our subsequent conceptual arguments about potential cybersecurity learning outcomes that can result from CIO outside board appointments. We consider both sender and receiver firms, including conditions that may facilitate or constrain beneficial learning outcomes in each pathway, in terms of a firm's cybersecurity performance, as proxied by data breaches. Next, we describe our data and methods, followed by a series of empirical analyses and robustness tests, and finally a discussion of the key findings and their implications. Before proceeding, we provide Table 1 to clarify certain key concepts in this paper.

Background Literature on Board Interlocks

A board interlock occurs when a board member or executive from one company serves on the board of directors of another company (Khan and Mauldin 2021, Ma et al. 2024). The trend of CIOs participating in board interlocks is a relatively recent phenomenon,³ and consequently, research on the impact of CIOs serving on outside boards remains limited. However, there is substantial literature examining board interlocks involving other C-level executives, mainly CEOs and CFOs, with most studies exploring how outside board service affects sender firms (Lamb and Roundy 2016, Ramsawak et al. 2024). Many of these studies suggest that outside directorships can benefit sender firms, leading to outcomes such as enhanced shareholder perceptions of firm value (Perry and Peyer 2005), improved strategic decision making (Geletkanycz and Hambrick 1997, Khan and Mauldin 2021), more effective financial statement management (Khan 2019, Cunningham et al. 2024), and both short- and long-term performance gains (Geletkanycz and Boyd 2011, Khan and Mauldin 2021). A prevailing rationale for these benefits is that board interlocks function as channels for learning, allowing executives to gain valuable experience and insights from serving on outside boards, which they can then apply to their home firms to drive positive outcomes (Geletkanycz and Boyd 2011, Lamb and Roundy 2016, Ramsawak et al. 2024).

However, there are studies that fail to find evidence of the benefits of outside board service on sender

Table 1. Key Concepts

Concept	Description
Sender firm	The firm that sends a CIO to an outside board.
Receiver firm	The firm that receives a CIO to its own board.
Home firm	The firm where the CIO is employed.
Outside firm	The firm where the CIO serves on the board but is not employed by the firm.
Outside board	The board of directors at an outside firm.

firms, indicating that the anticipated learning benefits can be difficult to internalize or may not materialize at all (Lamb and Roundy 2016, Ramsawak et al. 2024). A key insight from this work is that the success of board interlocks in delivering positive outcomes for sender firms depends on specific factors or conditions (e.g., Geletkanycz and Boyd 2011). These include the type of executive serving on the outside board (i.e., CEO versus CFO) and the characteristics of both the sender and receiver firms (Perry and Peyer 2005, Khan and Mauldin 2021, Ramsawak et al. 2024). Without favorable conditions, the potential for positive learning outcomes may be reduced, and interlocks can result in no observable performance improvement or even negative performance outcomes.

Beyond these contingent factors, another potential reason for the inconsistency in positive results is that serving on an outside board demands time and effort, which can limit the executive’s ability to absorb new knowledge and effectively transfer that knowledge back to their home firm (Ramsawak et al. 2024). This “busyness effect” can also impair the executive’s performance at their home firm, as they may become distracted by the demands of outside board service, which negatively impacts their home firm’s performance (Rosenstein and Wyatt 1994, Perry and Peyer 2005, Cunningham et al. 2024). This concern appears especially relevant for executives with greater involvement in day-to-day operations and decision making, as research suggests that CEOs with more hands-on managerial approaches may see their home firm’s performance suffer when they serve on outside boards (Booth and Deli 1996).

Board interlocks also carry the risk of facilitating the transfer of poor or unethical corporate practices among the interlocked firms. Such practices may conflict with the long-term interests of a firm (either as a sender or receiver) and its shareholders, ultimately harming the firm’s performance (Ma et al. 2024). Several studies support such negative contagion effects, showing that firms may emulate the detrimental behaviors of their interlocked partners, such as corporate misreporting, tax evasion, or suboptimal executive compensation practices, particularly when governance safeguards are weak, for example, shared auditors or socially connected influential board members across interlocks (Bizjak et al. 2009, Chiu et al. 2013, Lamb

and Roundy 2016, Ma et al. 2024, Ramsawak et al. 2024). These findings underscore the importance of considering the potential downsides of board interlocks.

Another key observation from the board interlock literature is that the potential learning effects and corresponding impacts on firm performance for receiver firms (those that recruit an executive from another company to join their board) have been largely overlooked. Whereas some studies have combined both the sender and receiver perspectives (e.g., Geletkanycz and Hambrick 1997), scholars also argue that these represent two distinct relationships, and both can facilitate the interorganizational transfer of numerous practices and information (Perry and Peyer 2005, Geletkanycz and Boyd 2011). The important distinction is that the receiver firm can acquire knowledge directly, whereas the sender firm relies on the executive successfully absorbing any new knowledge and then effectively transferring it back to their home firm. Geletkanycz and Boyd (2011, p. 345) emphasize the distinct importance of the receiver channel, noting that “the linkages created by inviting outside directors to serve on a source firm’s board appear systematically different from the ties created by executive outside board service.” Although empirical research on receiver firms is limited, available evidence suggests that much like for sender firms, the learning benefits to receiver firms are contingent on specific factors or conditions, such as the industry of the executive’s home (sending) firm and its governance structure (Perry and Peyer 2005).

The information systems (IS) literature has explored the impact of board interlocks to a limited extent. For example, Cheng et al. (2021) explain how the learning channels created by board interlocks can positively impact strategic IT investment decisions and overall firm performance. They identified a positive relationship between a focal firm’s strategic IT investments and those of its interlocked firms, leading to enhanced performance for the focal firm, particularly when the interlocked firms had stronger IT capabilities. Similarly, Liu et al. (2024) found that board interlocks among IT and non-IT firms increased IT innovation for the non-IT firms. Their theoretical reasoning was that the board interlocks provide a learning channel for non-IT firms to acquire the requisite IT knowledge to develop their IT innovations. In another study more

closely aligned with ours, Smith et al. (2021) found that firms with a CIO serving on an outside board experienced a decreased likelihood of data breach. They attributed this outcome to the cybersecurity learning the CIO gained through their outside board appointment. However, this study focuses only on large S&P 500 firms, uses a small sample constructed using fragmented data sources (e.g., hand-collected CIO information), and does not account for important heterogeneities in the effects. Our work builds on and extends this research in several important ways.

In all, a central tenet of board interlock research is that whereas learning can occur, it is not guaranteed; any learning benefits for firms may depend on the presence of specific enabling conditions. In their absence, interlocks may yield little to no benefit or even negative outcomes. Building on this work and extending the limited research on the impact of CIOs serving on outside boards from the sender firm perspective, we develop conceptual arguments regarding the learning outcomes associated with cybersecurity when CIOs join outside boards, considering both the sender and receiver firm perspectives. As we will describe, the distinctive nature of CIO-board interlocks introduces countervailing forces that complicate predictions about whether positive cybersecurity learning outcomes will occur in both pathways. We begin by presenting our arguments for receiver firms, where the learning outcomes related to cybersecurity may seem more directional and advantageous. We then turn to the cybersecurity learning outcomes that may arise for sender firms when their CIOs serve on outside boards.

Theoretical Overview: Perspectives for the Cybersecurity Implications of CIO Outside Board Service for Sender and Receiver Firms

Receiver Firms

Organizational learning has been described as the process by which an organization acquires knowledge through experience (Argote and Hwang 2018). Beyond their own experiences, organizations can enhance their learning by drawing on the experiences, strategies, and practices of other firms (Basten and Haamann 2018). One means for this knowledge acquisition is “learning by hiring,” where firms recruit experts from other organizations, gaining insights that may significantly differ from their existing knowledge base (Song et al. 2003, Tzabbar et al. 2015). Similarly, in the context of board interlocks, firms can add new outside directors to the board to increase the depth or diversity of knowledge and experience represented (Khan and Mauldin 2021). Concerning the focus of this paper, a firm can gain direct external cybersecurity expertise by

appointing a CIO from another firm to serve on its board.

There are several benefits to a firm’s cybersecurity when a CIO from another firm joins its board. For example, the outside CIO can use their experience and judgment to explain the (receiver) firm’s technology risks, including the impact of potential breach scenarios, to help guide the firm in its cybersecurity efforts (Parenty and Domet 2020). This view is echoed in a *Harvard Business Review* article that advocates for adding an outside CIO to the board of directors, in part because of their ability to independently address cybersecurity threats and risks and to contribute valuable external expertise in this area (Stephenson and Olson 2017). As noted, cybersecurity is one of the principal obligations of a CIO and serves as a key performance metric for the role. Data breaches in particular have been described as “visible signals of IT performance failure for CIOs who are directly responsible for IT functions” (Banker and Feng 2019, p. 312). Accordingly, the CIO is tasked with ensuring that effective cybersecurity controls are designed, implemented, and adhered to on an ongoing basis (Benaroch and Chernobai 2017, Parenty and Domet 2020, Haislip et al. 2021). The CIO is also a main source of cybersecurity messaging in the firm, such as communications about new threats and recommended protective actions and cyber risk updates to firm leadership (Smith et al. 2021). With this cybersecurity experience and knowledge base, the CIO is well positioned to transfer it to a receiver firm when they serve on that firm’s board.

More specifically, appointing an outside CIO to the board can create a unique private channel for learning that may not be accessible through public sources, such as industry reports and cybersecurity consortia. The outside CIO can share their unique experiences and expertise with the receiver firm in a manner that is often more candid than what the outside firm might disclose publicly. This is particularly relevant for cybersecurity-related information, as firms are typically reluctant to publicly divulge detailed elements of their cybersecurity strategies for fear of providing a roadmap for hackers and other adversaries who seek to penetrate their protections. Empirical research hints at such positive cybersecurity outcomes for firms with board-level expertise in this area. Higgs et al. (2016), for example, find that having an established board-level technology committee (albeit this is not the same as having an outside CIO on the board) reduces the likelihood of a data breach. These authors also find that such a committee mitigates the negative stock market reaction to a data breach, thus implying that it sends a positive signal to investors of the firm’s competence in cybersecurity.

Whereas the cybersecurity learning benefits of recruiting a CIO to a board (as a receiver firm) appear

theoretically clear, as noted, the limited literature on receiver firms suggests that any potential learning gained is contingent on other factors. Therefore, positive learning outcomes for receiver firms are not necessarily assured. Moreover, drawing on studies of learning by hiring in other contexts (Song et al. 2003, Tzabbar et al. 2015), it could be that the cybersecurity expertise acquired through the CIO's presence on the board may not be sufficient for achieving positive cybersecurity performance outcomes. To elaborate, when a CIO joins the board of another firm, their formal role is to provide advisory and oversight functions (Cheng et al. 2021, Proudfoot et al. 2023). Even if positive learning in cybersecurity is occurring based on the CIO's presence on the board, it is unclear whether the CIO's influence will extend deeply enough into the operational aspects of cybersecurity to meaningfully improve cybersecurity outcomes. Relatedly, it is possible that firms are motivated to recruit a CIO to their board for strictly symbolic reasons (Lowry et al. 2025), coinciding with the SEC's push for more cybersecurity expertise at the board level, rather than out of a genuine desire to gain cybersecurity learning. In this way, the outside CIO may have limited or no influence on the receiver firm, and/or little knowledge transfer may occur if the firm is not particularly receptive.

A counterargument to these points, however, is that cybersecurity has become a top board-level priority, which suggests that the board has significant influence over the firm's cybersecurity strategies and practices, making the firm more receptive to external expertise in this area. This perspective aligns with the attention-based view of the firm (Ocasio 1997), which posits that a firm's actions and outcomes are shaped by what its decision makers focus their attention on. From this standpoint, adding a CIO to the board alters the firm's attentional structure by embedding expertise in IT and cybersecurity at the highest level of firm governance. The CIO's presence elevates the salience of these issues in board deliberations and, through the board's oversight and advisory roles, signals their importance to the firm (Benaroch and Chernobai 2017). As such, the receiving firm is more likely to value, listen to, and act upon the CIO's guidance, having explicitly chosen to incorporate the CIO's expertise at the board level.

Building on this point, it is important to consider the CIO's cybersecurity-related responsibilities to the outside board, which suggest a significant level of influence and involvement. CIOs are often appointed to outside boards to serve as cybersecurity experts because others on the board are less familiar with the topic (Reilly 2022). Moreover, as we discovered in our interviews with CIOs, they tend to be appointed to an outside board to solve a cybersecurity problem or address ongoing cybersecurity concerns at the outside

firm, thereby demanding more hands-on attention than would be expected of other board members. As one CIO explained, "I was an active board member diving into cyber issues at a level that was quite deeper than most board members, because the company needed it. Most people in the room are a bunch of CEOs, CFOs, maybe CMOs [Chief Marketing Officers], that don't have the skill set to address cybersecurity. So, I probably take a more aggressive role than the average board member because I understand the [cyber] risks. My three public company board sample size would suggest that it's more than a coincidence that I've had that level of detail at all three companies." This CIO went on to explain their educator role on the outside board as "having to reshape the board's mindset about cybersecurity risk, and there's not many people who have the skill set to do that better than a CIO."

Another CIO we interviewed shared a similar perspective, describing their role as a cybersecurity educator and problem solver with substantial influence over the outside board and its firm's approach to cybersecurity: "I am the cyber and technology expert on the board. And so, in my primary role [on the board], everybody looks at me as, like, 'Does this make sense to you from a cyber perspective?' I'm also the person that if the firm replaces someone in technology or cybersecurity, I'm always asked to interview those people. And then, of course, I'm always asked to review the firm's roadmaps [for cybersecurity]." Expanding on this depth of engagement, this CIO explained, "It's a strange dynamic, because the responsibility of the board is governance. But there are times when I've been asked to delve deeper than what you would say governance should do. There was a problem and maybe the CEO wanted my opinion on some sort of a ransomware event or some other cybersecurity event."

Naturally, with this level of influence, an outside CIO joining a board may also facilitate "bad learning" by transferring ineffective cybersecurity practices or negative experiences in this area from their own firm. As with any positive learning effect, this bad learning would need to be impactful enough to extend beyond the CIO's advisory role on the receiver firm's board to meaningfully shape that firm's cybersecurity approach. Moreover, the evidence of negative contagion in the interlock literature is typically for the spread of unethical or controversial corporate practices (e.g., tax evasion, fraud, suboptimal executive compensation practices) that have short-term benefits, rather than strategic priorities such as cybersecurity. It seems unlikely, therefore, that a CIO would transfer, and a receiver firm would be receptive to, poor or ineffective cybersecurity practices, given that the receiver firm and its shareholders would not benefit from such actions. Again, the motive for receiver firms to appoint a CIO to their board is clearly linked to beneficial learning around

cybersecurity. Nevertheless, the potential for outside CIOs to introduce negative learning to receiver firms cannot be dismissed. It seems more intuitively plausible, however, that if the sender firm has excelled in cybersecurity, their strong practices and positive experiences in this area could enhance learning at the receiver firm, potentially improving its cybersecurity performance (i.e., positive contagion). Whereas acknowledging the opposing dynamics described in this section and noting that the impact of an outside CIO on a receiver firm's cybersecurity performance has not been studied, nor have the specific conditions that may facilitate or hinder learning outcomes in this context, we leave these areas open for empirical investigation.

Sender Firms

Whereas the organizational learning gained from an outside CIO serving on a receiver firm's board is akin to learning by hiring and represents a more direct means of knowledge acquisition from external sources, any learning gained from having a firm's own CIO serve on an outside board is more indirect in that it needs to be acquired from the outside board service and then transferred back to the sender firm. Access to learning opportunities is thought to be one of the chief reasons that firms allow their executives to serve on outside boards (Perry and Peyer 2005, Geletkanycz and Boyd 2011, Lamb and Roundy 2016). The rationale is that the executive gains new knowledge through learning and/or networking channels, which is brought back to the sender firm and used to improve its performance. Supporting such knowledge transfer effects, research shows that in certain circumstances, firms with CFOs who sit on outside boards have fewer financial misstatements and improved strategic investment performance (Khan and Mauldin 2021, Cunningham et al. 2024) and that firms with CEOs on outside boards can have an increase in shareholder perceptions of firm value (Rosenstein and Wyatt 1994, Perry and Peyer 2005).

In the IS context, Cheng et al. (2021) provide evidence that organizational learning occurs through board interlocks in a way that improves sender firms' strategic IT investment decisions and, in turn, their overall firm performance. In particular, these authors argue that a combination of observational and conversational learning takes place when an executive joins an outside board, and this can be transferred back to the sender firm and amplified under certain conditions.

As described for receiver firms in the prior section, board interlocks provide a unique private channel for learning that is particularly conducive to sharing cybersecurity information that may not be otherwise publicly available. Regarding the cybersecurity implications for sender firms when their CIOs join outside boards, based on learning and knowledge transfer

effects, positive cybersecurity outcomes could occur. This is because the CIO can learn about new cybersecurity management styles or strategies used in other firms and bring them back to the home firm. Indeed, not all firms approach cybersecurity the same way (Sen and Borle 2015, Li et al. 2023), as evidenced by the heterogeneity in their cybersecurity investments and how these investments are integrated into firm-level processes and procedures (Angst et al. 2017). From a learning perspective, CIOs may even witness the downsides of *not* employing effective cybersecurity strategies and processes if the outside firm is deficient in these areas. Both positive and negative cybersecurity experiences can help a CIO inform the cybersecurity practices in their home firm. Regarding such learning experiences, practitioner literature is replete with anecdotes of how CIOs' outside board service enhances their real-world cybersecurity expertise and provides opportunities for advice on this topic from fellow board members, which they can then bring back to their home firm (e.g., Zukis 2019, Johnson 2020). The combination of new knowledge gained and access to social networks as a source of counsel and insight on cybersecurity matters supports the notion of improved cybersecurity effectiveness for a sender firm when its CIO joins an outside board.

However, there are compelling counterarguments that challenge whether the cybersecurity learning benefits from CIO-board interlocks will materialize as theoretically expected. Here, it is important to consider an important distinction of the sender firm channel in that any new knowledge must be absorbed by the executive serving on the outside board rather than being directly applied as in the receiver firm channel. Thus, any potential learning benefits to the sender firm are contingent on the extent to which the CIO can absorb new cybersecurity insights from the outside board service.

Unlike the types of knowledge more readily absorbed by CEOs and CFOs through interlocks, such as financial reporting or accounting practices, which are grounded in standardized (e.g., Generally Accepted Accounting Principles (GAAP); International Financial Reporting Standards (IFRS)), mature, and relatively stable domains, cybersecurity presents a far more dynamic and complex environment. The field is marked by rapid, ongoing change, with new vulnerabilities, threat actors, and regulatory requirements emerging constantly. This high rate of change makes any new knowledge acquisition especially challenging. Mehrizi et al. (2022) make a similar point in reviewing the literature on organizational learning from IS incidents, describing such events as "moving targets" that continually evolve in both their technological and social dimensions, rendering them difficult to fully comprehend. Absorbing new cybersecurity knowledge from outside board service is further complicated by the fragmented nature of

cybersecurity responsibilities within firms, which can be spread across IT, compliance, risk management, and legal functions (Haislip et al. 2021, Johnson et al. 2023). This diffusion of ownership makes it challenging to gain a holistic understanding of the outside firm's cybersecurity knowledge base. In contrast, domains such as finance and accounting are generally more centralized and clearly structured, enabling easier isolation and absorption of knowledge. Knowledge absorption may also be hindered by the unique cybersecurity responsibilities that CIOs assume when serving on outside boards. Again, CIOs are deeply engaged educators and problem solvers in cybersecurity on outside boards. In this capacity, they function more as providers of knowledge, rather than active recipients acquiring new cybersecurity insights.

Even when CIOs do acquire new cybersecurity insights through outside board service, their responsibilities at their own (home) firms may hamper their ability to translate these insights into meaningful learning outcomes at these firms. Whereas the CIO position has a strategic dimension (Chen et al. 2021, Bandodkar and Grover 2022), it also has a significant operational component (Banker et al. 2011). Just as CIOs act as problem solvers on outside boards, they are likewise expected to “get in the weeds” to address everyday operational issues within their own firms (Benaroch and Chernobai 2017, Kettles et al. 2024). This operational aspect is supported by the fact that most CIOs report to the CFO rather than the CEO, placing them two levels below the top of the organizational hierarchy (Banker et al. 2011). This contrasts with CEOs and CFOs, who, while serving on outside boards, simultaneously maintain primarily strategic responsibilities within their own firms.⁴ CIOs must juggle their strategic and operational responsibilities, as one CIO explained in a practitioner article (Page 2023): “CIOs are expected to successfully split their time between duties that can greatly vary day to day. There are days when we have incidents and all of my time goes into just keeping the business running.” This CIO estimated that, on an average day, 60% of their time is dedicated to strategic issues, with the remainder focused on daily operations.

Given that cybersecurity is a core responsibility of the CIO, any reduction in attention to it caused by outside board service can pose serious risk. As former Equifax CEO Richard Smith emphasized, “confronting cybersecurity risks is a daily fight” (Srinivasan et al. 2019b, p. 16). When CIOs serve on outside boards, they may become delinquent in their home firm cybersecurity responsibilities. This idea aligns with the busyness perspective in the board interlock literature, which argues that by taking on the outside board position, the executive is distracted by the added responsibilities, resulting in declined performance in their primary

duties for the home firm (Rosenstein and Wyatt 1994, Perry and Peyer 2005, Cunningham et al. 2024). In the case of cybersecurity, the potential impact of such distraction is especially acute. Consider again that cybersecurity is one of the CIO's top responsibilities and that effective cybersecurity management requires ongoing attention because the cybersecurity threat landscape is constantly changing. Even short lapses in attention can significantly increase the risk of breaches. For example, a zero-day vulnerability can be exploited almost immediately if not addressed. Similarly, in the well-known 2013 Target data breach, management failed to act on repeated cybersecurity alerts, a failure partly attributed to the demands of the busy holiday season. This brief lapse in oversight was identified as a key factor enabling the breach (Srinivasan et al. 2019a). Although a CISO or other senior IT manager typically directs the day-to-day functional aspects of cybersecurity, the CIO oversees and manages these individuals and thus plays a central role in (and bears ultimate responsibility for) the firm's cybersecurity program (Banker and Feng 2019, Haislip et al. 2021, Sahin and Vance 2025). Thus, a distracted CIO may have difficulty fulfilling their ongoing cybersecurity management responsibilities at the home firm.

This busyness concern is supported by empirical evidence showing that when CIOs take on additional roles beyond their core IT-related responsibilities, the likelihood of breach at their home firm significantly increases (Smith et al. 2021). The busyness angle is also supported by insights from our CIO interviews, which highlight the significant hands-on educational and problem-solving responsibilities of CIOs toward cybersecurity on outside boards. Furthering these points, one CIO described the depth of their involvement: “I get my hands dirty on the board. I probably put an operational CIO hat on for a couple years, and I still do that on the boards I serve on. A lot of other board members don't want to get their hands dirty [in cybersecurity].” Another CIO we interviewed commented on the time commitment required for outside board service, which is nontrivial, given that it is layered onto their primary job responsibilities: “Typically boards have five meetings a year. And the board meetings are typically a day and a half, and then you have the prep time that's required. So, from a time perspective, it's usually a week, five times a year. But for that week, you really have to prepare in the prior week beforehand.” This CIO further stressed that their commitment extends beyond scheduled meetings, as they remain actively engaged in cybersecurity-related matters with the board and its firm throughout the year.

Overall, whereas executive busyness from outside board service is a general concern when assessing potential learning benefits for sender firms, it is

especially salient in the case of CIO-board interlocks and cybersecurity outcomes, given that CIOs carry significant operational responsibilities at their home firms, including the need to maintain sustained, focused attention on everyday cybersecurity management.

To complete our discussion of the sender firm pathway, we note that outside board service can also potentially serve as a channel for transferring bad learning to the sender firm. We earlier reasoned that CIOs could benefit from both the positive and negative cybersecurity experiences of the firms on whose boards they serve. But being witness to poor cybersecurity experiences and practices at the outside firm could conceivably lead to a negative contagion effect or bad learning that is transferred back to the sender firm, ultimately harming its cybersecurity performance. While acknowledging this possibility, as similarly described for receiver firms, we view this scenario as unlikely because such actions would offer no benefit to the sender firm or its shareholders. The more plausible explanation for why meaningful cybersecurity learning benefits may fail to materialize for sender firms lies in the challenges outlined in this section: CIOs may struggle to absorb new, cybersecurity-specific knowledge from their outside board service, and the divided attention required by such service can be especially detrimental to their home firm's cybersecurity, given the operational dimension of the CIO's home firm responsibilities. While acknowledging the largely unexplored potential for both positive and negative cybersecurity learning outcomes for sender firms based on the competing dynamics described in this section, as with receiver firms, we present these issues as areas for empirical investigation in this study.

Empirical Methodology

Data and Sample Construction

To conduct our study, we begin with a panel data set of 80,672 firm-years covered by BoardEx and Compustat that spans 2005–2022. We then identify firms that have a CIO disclosed in BoardEx and keep observations with CIO disclosed.⁵ For these firms, we then identify whether the CIO concurrently serves on the board of directors at an outside company (i.e., whether it is a sender firm) using data from BoardEx. We can also identify whether each firm has a CIO from an outside company on its own board of directors (i.e., whether it is a receiver firm). We then identify whether the CIO's home firm had a data breach during our sample period using data from Audit Analytics and the Privacy Rights Clearinghouse.⁶

We obtain firm financial data from Compustat and I/B/E/S and further use BoardEx for data on outside board activities and characteristics. We also collect data on firms' investment in IT security applications from

the Computer Intelligence (CI) database, a widely utilized source of firm-level IT data (e.g., Xue et al. 2017, Cheng et al. 2021, Wang et al. 2023). We focus specifically on the variables for IT security applications (see Online Appendix C).⁷ To measure investments in IT security applications, we aggregate these individual components for each firm-year and classify the total as either above or below the industry mean. The CI database has known inconsistencies in variable measurements before 2011 (Wang et al. 2023). Because of these inconsistencies and our data access limit beyond 2020, we restrict our use of the CI database's IT security data to the period 2011–2020. Consequently, all analyses in this study involving this data are limited to firm-year observations within this time frame.

The full list of our study variables, their operationalizations, and their sources are in Online Appendix C. After removing observations without a disclosed CIO, observations missing variables necessary to estimate our regressions, and observations for which the CIO is always on an outside board,⁸ our combined data set is an unbalanced panel that has 17,227 CIO-firm-year-level observations for 4,419 unique CIO-firm pairs and 2,507 unique firms, with 764 data breaches and 310 instances of a CIO serving on an outside board. See Online Appendix D for further details of our sample construction. Also, see Online Appendix E for summary statistics of the study variables, Online Appendix F for details of the data breaches in our sample, and Online Appendix G for correlations among the study variables.

Model and Estimation

In our first model, we create an indicator variable for each observation, $Send_CIO_{it}$, coded as one if the CIO c at firm i serves on the board of directors at another firm in year t (sender firms). We also create an indicator variable for each observation, $Receive_CIO_{it}$, coded as one if an outside CIO serves on firm i 's own board in year t (receiver firms). We then create an indicator variable, $Breach_{it}$, equal to one if firm i discloses a data breach in year t .⁹ Consistent with past board interlock studies in IS, accounting, and finance, we measure our outcome variable ($Breach$) and our variables of interest ($Send_CIO$ and $Receive_CIO$) contemporaneously (i.e., all at year t) (e.g., Perry and Peyer 2005, Cheng et al. 2021, Khan and Mauldin 2021, Smith et al. 2021, Cunningham et al. 2024). This contemporaneous effect aligns with the conceptual reasoning that the cybersecurity performance outcomes resulting from CIO outside board appointments—both for sender and receiver firms—emerge relatively quickly (although we demonstrate that these effects persist over multiple years; see Online Appendix H). This is plausible considering the rapidly changing cybersecurity threat landscape, which necessitates swift responses from firms; consequently,

their actions (or inactions) regarding cybersecurity can have short-term consequences. Still, we later evaluate potential reverse causality in this estimation approach with a series of robustness tests.

We include an extensive set of control variables, each of which may affect a firm's risk of data breach. Specifically, we control for CIO tenure (*CIO_Tenure*), natural logarithm of total assets (*Ln_Assets*), return on assets (*ROA*), and whether the company is profitable (*Loss*). We include these because larger and more profitable firms are more frequent data breach targets and CIO tenure at the home firm has been linked to its breach likelihood (Haislip et al. 2021, Smith et al. 2021, Li et al. 2023, Zhu et al. 2024). We also control for R&D expenditures (*RD*) because firms with substantial R&D expenditures are likely to possess intellectual property, which makes them more attractive breach targets (Wang et al. 2023, Zhu et al. 2024). Similarly, we control for both advertising expenditures (*Ad*) and the number of analysts following the firm (*Num_analyst*) to capture its outward visibility and thus potential breach attractiveness (Li et al. 2023, Zhu et al. 2024). We control for firm age (*Firm_Age*) because younger firms may have less expertise in addressing cybersecurity threats (Wang et al. 2023, Li and Yoo 2024).

Concerning executive and board characteristics, we control for factors previously linked to breach likelihood, including whether the firm has a risk committee (*Risk_Comm*), a compliance committee (*Compliance_Comm*), and/or a technology committee (*Tech_Comm*) on its board (Higgs et al. 2016, Smith et al. 2021), and the IT expertise of the CEO and CFO (*CEO_Itexp*; *CFO_Itexp*) (Haislip et al. 2021). We also control for whether the CEO and CFO (*CEO_outside_bd* and *CFO_outside_bd*) have outside board memberships, which may influence the firm's governance effectiveness (Perry and Peyer 2005, Khan and Mauldin 2021, Cunningham et al. 2024). Finally, we control for whether the firm had a past breach (*Past_breach*) (Wang et al. 2023, Zhu et al. 2024). Equation (1) is defined as:

$$\begin{aligned} \text{Breach}_{ict} = & \alpha_0 + \alpha_1 \text{Send_CIO}_{it} + \alpha_2 \text{Receive_CIO}_{it} \\ & + \alpha_3 \text{CIO_Tenure}_{it} + \alpha_4 \text{CEO_Outside_bd}_{it} \\ & + \alpha_5 \text{CEO_It_Exp}_{it} + \alpha_6 \text{CFO_Outside_bd}_{it} \\ & + \alpha_7 \text{CFO_It_Exp}_{it} + \alpha_8 \text{Ln_Assets}_{it} + \alpha_9 \text{ROA}_{it} \\ & + \alpha_{10} \text{Loss}_{it} + \alpha_{11} \text{Lev}_{it} + \alpha_{12} \text{RiskComm}_{it} \\ & + \alpha_{13} \text{ComplianceComm}_{it} + \alpha_{14} \text{TechComm}_{it} \\ & + \alpha_{15} \text{RD}_{it} + \alpha_{16} \text{Past_breach}_{it} + \alpha_{17} \text{FirmAge}_{it} \\ & + \alpha_{18} \text{Ad}_{it} + \alpha_{19} \text{Num_analyst}_{it} + \text{Year}_t \\ & + \text{CIO} - \text{HomeFirm}_{ic} + \varepsilon_{ict}. \end{aligned} \quad (1)$$

One key feature of our data is that individual CIOs can leave one home firm and accept a CIO position at a different home firm during our sample period.¹⁰

Therefore, we are able to include both CIO–firm pair fixed effects (i.e., a fixed effect per unique CIO–home firm pair) and year fixed effects in Equation (1). The inclusion of unit (CIO–firm pair) and time (year) fixed effects allows us to effectively employ a difference-in-differences (DID) model such that the *Send_CIO* variable will compare changes in the likelihood of breach between outside board serving and nonoutside board serving years for CIO *c* at firm *i*, relative to changes in the likelihood of breach for our control group of CIO–firm pair observations (firms with CIOs who never serve on an outside board).¹¹ The same interpretation can be applied for the receiver firm perspective (*Receive_CIO*). This strengthens the causal inference in our estimation. Including CIO–firm pair fixed effects also allows us to control for time-invariant factors that could simultaneously drive the appointment of the firm's CIO to an outside board and its risk of breach. For instance, firms of a certain profile (i.e., highly visible and well-known firms) may be more likely to have their CIO recruited to an outside board but are simultaneously more natural targets for data breaches. As it relates to CIOs, it could be that the individual management/supervisory style of the CIO is related to both the likelihood they are recruited to an outside board and the likelihood of a breach at their home firm. Finally, including year fixed effects allows us to control for common time trends in breaches during our sample period and any shocks that impact all firms in a given year (e.g., D'Arcy et al. 2020).

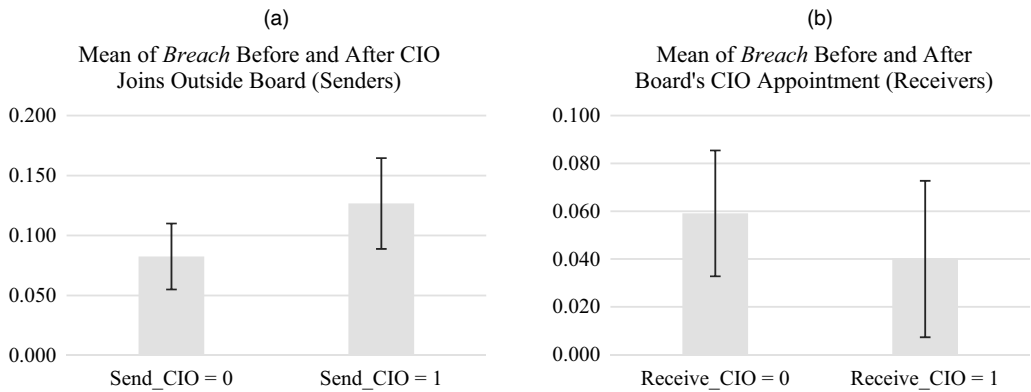
We estimate Equation (1) using a conventional panel data approach. Following prior research on data breaches, we estimate a linear probability model (LPM) with standard errors clustered by CIO–firm (Haislip et al. 2021, Wang et al. 2023). We use an LPM because it eases the interpretation of coefficients and it avoids incidental parameter issues, relative to a logistic or probit model, when including numerous fixed effects (Beck 2020, D'Arcy et al. 2020, Ganju et al. 2020, Haislip et al. 2021, Wang et al. 2023).¹²

Main Results

CIO Outside Board Service and Data Breaches at Sender and Receiver Firms. Figure A.1 in Online Appendix A shows that CIO outside board service rates have increased over the years and substantially after 2013, the year of one of the largest data breaches in history (Target data breach). This speaks to the increasing demand for IT and cybersecurity expertise on corporate boards.

In Figure 1(a), we illustrate a prepost difference for a sample that only contains CIO–home firm pairs at which the CIO joins an outside board during our sample period (i.e., sender firms). That is, in this figure, we focus only on CIO–firm pairs that change from being

Figure 1. Means (with 95% Confidence Intervals (CIs)) of Home Firm Breaches



Notes. (a) Before and after sending CIO to outside board. (b) Before and after receiving an outside CIO on board.

zero in earlier years to one in later years (i.e., the CIO joins an outside board while working at a particular home firm). Illustrating these differences allows us to hold the CIO and the home firm constant, whereas examining whether the likelihood of a breach changes after a firm's CIO is appointed to an outside board. It is clear that home firms are more likely report a data breach in years after the CIO joins an outside board (0.124) relative to years before the CIO joins an outside board (0.084).

In Figure 1(b), we illustrate a prepost difference for a sample that only contains CIO-home firm pairs at which an outside CIO is appointed to the firm's own board during our sample period (i.e., receiver firms). Here again, we only focus on CIO-firm pairs that change from being zero in earlier years to one in later years. It is clear that firms are less likely to report a breach in years after an outside CIO joins the firm's board (0.040) relative to years before an outside CIO joins the firm's board (0.059).

In Table 2, we estimate Equation (1). In column (1), we first report our regression results with *Send_CIO* and *Receive_CIO* included as the only time-varying predictors of *Breach*. The coefficient on *Send_CIO* is positive and significant, whereas the coefficient on *Receive_CIO* is negative and significant. Because we include CIO-firm and year fixed effects as time-invariant predictors in the regression, these results suggest that holding the CIO and the firm constant, firms that have a CIO join on an outside board (i.e., sender firms) have a significant increase in likelihood of a breach after the CIO joins the outside board relative to before the CIO joins the outside board. Moreover, this increase in breach likelihood is larger than any increase in breach likelihood experienced by control firms (i.e., those firms where the CIO is never on an outside board) over the same period. Also, firms that have an outside CIO join their own board (i.e., receiver firms) have a significant decrease in likelihood

of a breach after the outside CIO joins their board relative to before the outside CIO joins their board, and this decrease in breach likelihood is larger than any decrease in breach likelihood experienced by control firms (i.e., those firms where there is never an outside CIO on their board) over the same period. In the column (2) results, we include a set of time-varying control variables that are not captured by CIO-firm fixed effects and continue to find a positive and significant coefficient on *Send_CIO*. In terms of economic significance, firms with a CIO who joins an outside board have an increase in breach likelihood that is 6.2 percentage points higher than the change in breach likelihood experienced by control firms over the same period. This translates to an overall likelihood of a breach that is over twice as large (141% proportionally higher).¹³ Also in the column (2) results, we find a negative and significant coefficient on *Receive_CIO*. In terms of economic significance, firms with an outside CIO joining their board have a decrease in breach likelihood that is 3.6 percentage points lower than the change in breach likelihood experienced by control firms over the same period. This translates to an overall likelihood of a breach that is 82% proportionally lower. In column (3), we control for the home firm's investment in IT security applications and thus have the restricted sample period (2011–2020). The sample size drops because the CI database does not cover our entire sample period; however, we wanted to examine whether controlling for IT security investment affected our inferences. The results are aligned with column (2) in terms of the *Send_CIO* and *Receive_CIO* coefficients.

Robustness Tests

Pretreatment Trends. When performing a DID analysis, a primary assumption is that trends in the dependent variable for treatment and control groups are parallel prior to treatment (Bertrand et al. 2004). To evaluate whether this assumption is valid, we conduct

Table 2. Effect of CIO Outside Board Service on Data Breaches at the Home Firm

Variables	(1)		(2)		(3)	
	Breach		Breach		Breach	
<i>Send_CIO</i>	0.050**	(0.031)	0.062**	(0.030)	0.079**	(0.039)
<i>Receive_CIO</i>	−0.040**	(0.016)	−0.036**	(0.016)	−0.048*	(0.025)
<i>CIO_tenure</i>			−0.000	(0.001)	0.000	(0.002)
<i>CEO_Outside_bd</i>			−0.026**	(0.010)	−0.037***	(0.014)
<i>CEO_Itexp</i>			−0.023	(0.056)	−0.026	(0.048)
<i>CFO_Outside_bd</i>			0.015	(0.012)	0.019	(0.019)
<i>CFO_Itexp</i>			0.053	(0.057)	0.098	(0.072)
<i>Ln_assets</i>			0.020***	(0.008)	0.013	(0.011)
<i>ROA</i>			−0.015	(0.013)	−0.026	(0.024)
<i>Loss</i>			0.005	(0.005)	0.008	(0.008)
<i>Lev</i>			0.027	(0.023)	0.007	(0.032)
<i>RiskComm</i>			−0.010	(0.015)	0.001	(0.017)
<i>ComplianceComm</i>			0.058**	(0.023)	0.075**	(0.035)
<i>TechComm</i>			0.022	(0.019)	0.027	(0.026)
<i>Rd</i>			0.005*	(0.003)	0.004	(0.003)
<i>Past_breach</i>			−0.278***	(0.031)	−0.330***	(0.039)
<i>FirmAge</i>			−0.003	(0.002)	−0.003	(0.002)
<i>Ad</i>			−0.063	(0.228)	−0.514	(0.516)
<i>NumAnalyst</i>			0.001	(0.001)	0.001	(0.001)
<i>IT_security_app</i>					−0.026**	(0.013)
Constant	0.017	(0.008)	−0.108	(0.069)	0.018	(0.093)
CIO–firm pair fixed effects	Yes		Yes		Yes	
Year fixed effects	Yes		Yes		Yes	
Observations	17,227		17,227		10,977	
Adjusted R^2	0.1794		0.2081		0.2539	

Notes. Standard errors are in parentheses and based on two-tailed tests. Standard errors are clustered by CIO–firm pair. Independent variables of interest are bolded for ease of interpretation.

*** $p < 0.01$; ** $p < 0.05$; * $p < 0.10$.

a leads-and-lags analysis similar to Autor (2003). This analysis allows us to observe differences in breach likelihood between the treatment and control groups in both the pre- and posttreatment periods. In our relative time model in column (1) of Table H.1 in Online Appendix H, we define the treatment event as occurring in the year a CIO goes from not serving on an outside board to serving on an outside board while working at a particular home firm. We create pretreatment variables to capture three, two, and one year(s) before treatment, respectively (*Send_cio_t-3*, *Send_cio_t-2*, *Send_cio_t-1*). We then create posttreatment variables to capture the initial year of treatment (*Send_cio_t0*), one year after (*Send_cio_t+1*), and two years or more after (*Send_cio_t+2orlater*). We drop observations for the first year of our sample period (2005) because we cannot be certain whether the first year of our sample is also the first year the CIO joins an outside board. We follow Ozer et al. (2023) and use one year before treatment (*Send_cio_t-1*) as the base year for our treated group. Further, our control group includes CIO–firm pairs for which the CIO never serves on an outside board. As column (1) of Table H.1 indicates, there are no pretrends because the pretreatment years are statistically nonsignificant. This suggests that the parallel trends assumption is valid. Moreover, each of our posttreatment variables is positive and statistically significant,

suggesting the treatment effect persists past the initial year of treatment. We also perform a relative time model for our receiver firm tests in column (2) of Table H.1 of Online Appendix H, defining the treatment events and the pre- and posttreatment variables as we did for the sender firm analysis. We find that there are no pretrends because the pretreatment years are statistically nonsignificant. Each of our posttreatment variables is negative and statistically significant, suggesting that it is the treatment rather than preexisting trends that are driving the reduction in breach likelihood. These results support the parallel trends assumption and show that the treatment effect persists past the initial year of treatment.

Entropy Balancing. Another identification concern is that home firms with a CIO serving on an outside board may be considerably different from home firms whose CIOs do not hold such roles. Likewise, firms that appoint outside CIOs to their own board may be fundamentally different from those that do not. To provide additional evidence that our results are not driven by fundamental differences between sender (receiver) firms and nonsender (nonreceiver) firms, we reestimate our main analysis using entropy balancing (Hainmueller 2012, Haislip et al. 2021, Lee et al. 2022). Entropy balancing weights control sample units to achieve covariate balancing between treatment and

control groups. For our sender firm test, entropy balancing effectively allows us to reweight the sample such that firms with a CIO who does not serve on an outside board exhibit covariate values that are statistically indistinguishable from those of the firms with a CIO that does serve on an outside board. The same interpretation applies for our receiver firm test. A significant advantage of this approach is that it provides superior matching compared with propensity score matching (Hainmueller 2012, McMullin and Schonberger 2020). Also, unlike propensity score matching, it does not require us to discard any of our observations because of no good matches being available (Hainmueller 2012). Column (1) of Table H.2 in Online Appendix H presents our results after balancing covariates between sender firms and nonsender firms. The results indicate that, even after employing entropy balancing, firms that have a CIO join on an outside board have a significant increase in likelihood of a breach after the CIO joins the outside board, and this increase in breach likelihood is larger than any increase in breach likelihood experienced by control firms over the same period. For receiver firms, in column (2) of Table H.2 in Online Appendix H, the entropy balancing results indicate that firms that have an outside CIO join their own board have a significant decrease in likelihood of a breach after the outside CIO joins their board, and this decrease in breach likelihood is larger than any decrease in breach likelihood experienced by control firms over the same period. Together, these results help alleviate concerns that our results are driven by inherent differences between the treatment and control firms.

Poisson Pseudo-Maximum Likelihood Estimator.

Because breaches are relatively rare events in large firm samples (Kim et al. 2024), our *Breach* variable contains many zero values. Because we use an LPM, which is essentially ordinary least squares (OLS) with a binary dependent variable, we follow past studies that apply OLS to rare events. Specifically, we adopt a fixed-effects Poisson pseudo-maximum likelihood (PPML) estimator (e.g., Li et al. 2024, Tang et al. 2024). PPML effectively handles zero inflation (i.e., when a variable is rare and there are many zeroes in the data), and it does not suffer from the incidental parameters problem when multiple fixed effects are included (Aziz et al. 2023). It also provides consistent and robust standard errors when data are rare and exhibits overdispersion (Tang et al. 2024). As shown in Table H.3 in Online Appendix H, our inferences remain unchanged when using PPML, suggesting that our results are not driven by the sparsity/rarity of our outcome variable.

Further Addressing Endogeneity. A common issue with analysis of firm-level decisions and outcomes is

that firms self-select into certain treatments (i.e., most firm treatments are not randomly assigned). This raises concerns about endogeneity and the possibility that other factors correlated with both CIO outside board service and data breaches bias our results. In particular, simultaneity or reverse causality is a potential concern. From the sender firm perspective, CIOs at home firms with inherently higher ex ante breach risk may be more motivated to pursue outside board opportunities (i.e., to develop their personal reputation and skills). At the same time, outside firms may be more inclined to recruit CIOs from sender firms facing more complex cybersecurity concerns to benefit from the CIO's experience. From the receiver firm perspective, firms that are already taking initiatives to improve their cybersecurity may be more likely to appoint an outside CIO to their board. In effect, it might be true that ex ante data breach risk at sender (receiver) firms is driving the sending (recruitment) of CIOs to outside boards and not the other way around.

To further address the issue of endogeneity, we follow Saldanha et al. (2024) and use the Arellano–Bond dynamic panel model, which, under several assumptions,¹⁴ provides a robust alternative identification for dynamic relationships with endogeneity (Arellano and Bond 1991, Kitchens et al. 2018, Saldanha et al. 2020). The benefit of the Arellano–Bond dynamic panel model is that instruments are constructed from lagged values of endogenous regressors by making use of the panel's time series, eliminating the need to identify a valid external instrument. Similar to Saldanha et al. (2024), we take a conservative approach and perform the one-step version of the Arellano–Bond estimator, treating all firm-level variables as endogenous and using lags of the variables as instruments. This allows us to provide instruments for both *Send_CIO* and *Receive_CIO* in the same regression. We present our results in Table H.4 in Online Appendix H. Similar to our main analysis, we observe a positive and significant coefficient on *Send_CIO* and a negative and significant coefficient on *Receive_CIO*. Further, we perform Sargan's *J*, overidentifying restriction tests to assess instrument validity. The null of Sargan's *J* test is not rejected ($p > 0.10$), suggesting that the instruments are appropriate (Arellano and Bond 1991). We further test for second-order autocorrelation in the error terms because the Arellano–Bond model assumes there is no autocorrelation of error terms beyond first order. Here, we conduct a typical diagnostic test, the Arellano and Bond (1991) test for second-order autocorrelation of the error terms, AR(2). The AR(2) test does not reject the null that there is no autocorrelation ($p > 0.10$), suggesting second-order autocorrelation is not a concern in our analysis. In all, these analyses further alleviate concerns that endogeneity is driving our results.

Empirical Extensions and Mechanism Exploration

Having established the robustness of our main results, we next probe further into the relationship between sender/receiver firms and breaches to explore additional effects. We provide analyses based on different severities and types of breaches in Online Appendix I. We also consider heterogeneity in the cybersecurity experiences and practices of sender and receiver firms to uncover the potential underlying mechanisms for our main results, as discussed in the following sections.

Heterogenous Effects for the Sender Firm's Cybersecurity. To explore mechanisms for our sender firm effect, we seek to identify the circumstances in which a firm's own CIO serving on an outside board increases the likelihood of a breach and when it does not. Because any learning outcomes that accrue to the CIO's home firm likely depend on the firm on whose board the CIO serves (i.e., receiver firm), we first consider the heterogeneity of the receiver firms, particularly in terms of their cybersecurity profiles. Drawing on our portrayal of the CIO as a deeply engaged educator and problem solver in cybersecurity on the outside board, thus limiting the CIO's ability to transfer back beneficial practices to their home firm and even distracting them from effectively fulfilling their cybersecurity responsibilities at their home firm, our logic is that if the CIO of a sender firm joins the board of a receiver firm with a poor cybersecurity profile (i.e., poor cybersecurity experiences and practices), then an increase in the likelihood of breach at the CIO's home firm (i.e., sending firm) should be more likely than if the sender firm CIO joins the board of a receiving firm with a strong cybersecurity profile. The rationale is that CIOs become increasingly burdened when serving on the board of a receiver firm with a poor cybersecurity profile, as such firms require substantial guidance and oversight in cybersecurity.

We consider three measures of the receiver firm's cybersecurity profile. First, we consider whether the receiver firm has a CISO on its TMT.¹⁵ CISOs are senior executives with dedicated and direct responsibility for their firms' cybersecurity. The presence of a CISO on the TMT suggests a firm's dedication to strong cybersecurity. As such, we would expect an increase in breaches at sender firms to be more likely when their CIO joins the board of a receiver firm that does not have a CISO on the TMT. Second, we consider whether the receiver firm has experienced a past breach. Past breaches are clear signals of vulnerability and suggest poor cybersecurity practices. Therefore, we would expect an increase in breaches at sender firms to be more likely when their CIO joins the board of a receiver firm that has had a past breach. Finally, we consider investment in IT security. If a receiver firm has more reported IT security applications than

the median of its industry peers, then we consider that an indication that the receiver firm is relatively strong in its cybersecurity practices. Thus, we would expect an increase in breaches at sender firms to be more likely when their CIO joins the board of a receiver firm that has relatively low IT security investment when compared with industry peers.

We also perform an analysis based on whether the sender firm has a CISO on its own TMT to monitor cybersecurity while its CIO is serving on the outside board. When considering the potential busyness effect of CIO outside board service, the presence of a CISO on the TMT within the home firm can serve as a counterbalance to any cybersecurity-related distractions that the CIO may encounter when serving on an outside board. This measure may help mitigate cybersecurity vulnerabilities that the home firm might otherwise face in the absence of a dedicated cybersecurity leader. The presence of a CISO on the TMT can also signal to potential adversaries that even if the CIO's focus is occasionally divided, the home firm's security posture remains intact and consistently prioritized.

We present our analysis in Table 3. In columns (1)–(4), we split *Send_CIO* into two mutually exclusive variables, and firms with no change in whether the CIO serves on an outside board remain in the intercept as the base group. The interpretation of the coefficients are therefore effects compared with the control firms. In column (1), we split *Send_CIO* based on whether the receiver firm has a CISO on the TMT (*Send_Rec_CISO*) or not (*Send_Rec_NoCISO*). In column (2), we split *Send_CIO* based on whether the receiver firm had a past breach (*Send_Rec_pastbreach*) or not (*Send_Rec_nopastbreach*). In column (3), we split *Send_CIO* based on whether the receiver firm has a higher than industry median investment in IT security applications (*Send_Rec_security*) or not (*Send_Rec_lowsecurity*). In column (4), we split *Send_CIO* based on whether the sender firm has a CISO on the TMT (*Send_hf_CISO*) or not (*Send_hf_noCISO*). We find positive and significant coefficients on *Send_Rec_NoCISO*, *Send_Rec_pastbreach*, and *Send_Rec_lowsecurity* in columns (1), (2), and (3), respectively. We also find nonsignificant coefficients on *Send_Rec_CISO*, *Send_Rec_nopastbreach*, and *Send_Rec_security* in columns (1), (2), and (3), respectively. These results suggest that, relative to the change in the likelihood of breach experienced by control firms, sender firms experience a larger increase in breach likelihood after their CIO joins an outside receiver firm, with this effect driven by the receiver firm's poor cybersecurity experiences and practices. In column (4), we observe a positive and significant coefficient on *Send_hf_noCISO* and a nonsignificant coefficient on *Send_hf_CISO*. This suggests that whereas CIO outside board service results in increased breach likelihood, having a CISO on the TMT at the home firm can

Table 3. The Effect of the Characteristics of the Receiving Firm on the Sender Firm’s Cybersecurity

Variables	(1)		(2)		(3)		(4)	
	Breach		Breach		Breach		Breach	
<i>Send_Rec_CISO</i>	0.028	(0.042)						
<i>Send_Rec_NoCISO</i>	0.088**	(0.036)						
<i>Send_Rec_pastbreach</i>			0.046	(0.030)				
<i>Send_Rec_pastbreach</i>			0.237**	(0.102)				
<i>Send_Rec_security</i>					−0.036	(0.075)		
<i>Send_Rec_lowsecurity</i>					0.106***	(0.040)		
<i>Send_hf_CISO</i>							0.036	(0.054)
<i>Send_hf_noCISO</i>							0.071**	(0.032)
<i>Receive_CIO</i>	−0.037**	(0.016)	−0.036**	(0.016)	−0.047*	(0.024)	−0.036**	(0.016)
<i>CIO_tenure</i>	−0.000	(0.001)	−0.000	(0.001)	0.001	(0.002)	−0.000	(0.001)
<i>CEO_Outside_bd</i>	−0.026**	(0.010)	−0.025**	(0.010)	−0.036***	(0.014)	−0.025**	(0.010)
<i>CEO_Itexp</i>	−0.024	(0.056)	−0.023	(0.055)	−0.027	(0.048)	−0.022	(0.056)
<i>CFO_Outside_bd</i>	0.014	(0.012)	0.015	(0.012)	0.018	(0.019)	0.014	(0.012)
<i>CFO_Itexp</i>	0.053	(0.057)	0.053	(0.057)	0.095	(0.071)	0.053	(0.057)
<i>Ln_assets</i>	0.020***	(0.008)	0.021***	(0.008)	0.012	(0.011)	0.019**	(0.008)
<i>ROA</i>	−0.014	(0.013)	−0.016	(0.013)	−0.026	(0.024)	−0.013	(0.013)
<i>Loss</i>	0.005	(0.005)	0.005	(0.005)	0.008	(0.008)	0.004	(0.005)
<i>Lev</i>	0.027	(0.023)	0.024	(0.023)	0.007	(0.032)	0.032	(0.022)
<i>RiskComm</i>	−0.010	(0.015)	−0.010	(0.015)	0.002	(0.017)	−0.011	(0.014)
<i>ComplianceComm</i>	0.060**	(0.023)	0.058**	(0.023)	0.080**	(0.034)	0.058**	(0.023)
<i>TechComm</i>	0.022	(0.019)	0.023	(0.019)	0.028	(0.025)	0.022	(0.019)
<i>Rd</i>	0.005*	(0.003)	0.005*	(0.003)	0.004	(0.003)	0.005*	(0.003)
<i>Past_breach</i>	−0.278***	(0.031)	−0.281***	(0.032)	−0.330***	(0.040)	−0.282***	(0.031)
<i>FirmAge</i>	−0.003	(0.002)	−0.003*	(0.002)	−0.002	(0.002)	−0.003	(0.002)
<i>Ad</i>	−0.066	(0.228)	−0.061	(0.228)	−0.511	(0.511)	−0.068	(0.228)
<i>NumAnalyst</i>	0.001	(0.001)	0.000	(0.001)	0.001	(0.001)	0.001	(0.001)
Constant	−0.107	(0.069)	−0.106	(0.069)	−0.000	(0.089)	−0.097	(0.069)
CIO–firm pair fixed effects	Yes		Yes		Yes		Yes	
Year fixed effects	Yes		Yes		Yes		Yes	
Observations	17,227		17,227		10,977		17,227	
Adjusted R ²	0.2084		0.2090		0.2545		0.2105	

Notes. Standard errors clustered by CIO–firm pair in parentheses. *p*-values based on two-tailed tests.
****p* < 0.01; ***p* < 0.05; **p* < 0.10.

counter this effect. The fact that we only observe an increase in breach likelihood when there is no home firm CISO suggests that the CIO may get distracted by outside board service, which is consistent with the conceptual arguments about executive busyness for sender firm CIOs serving on outside boards and how such busyness contributes to negating any potential learning benefits to sender firms.

Heterogeneous Effects for the Receiver Firm’s Cybersecurity. To explore mechanisms for our receiver firm effect, we seek to identify the circumstances in which an outside CIO serving on the firm’s own board decreases the likelihood of a breach and when it does not. Because any learning outcomes that accrue to the receiver firm likely depend on the home firm the CIO comes from (i.e., sender firm), we perform analyses based on the heterogeneity of the sender firms, considering their cybersecurity profiles. Drawing on similar arguments as in the previous section, conventional logic is that if a receiver firm appoints to its own board a CIO from a sender firm with a strong cybersecurity

profile, then a decrease in the likelihood of breach at the receiver firm should be more likely than if the receiver firm appoints a CIO from a sender firm with a poor cybersecurity profile.

We consider the same three measures of cybersecurity profile as in the previous section, but we focus on the sender firm instead. First, we consider whether the sender firm has a CISO on its TMT. Given that the presence of a CISO on the TMT suggests a firm’s dedication to strong cybersecurity, we would expect a decrease in breaches at receiver firms to be most likely when the CIO who joins their board comes from a sender firm that has a CISO on its TMT. Second, we consider whether the sender firm has experienced a past breach. Past breaches can be clear signals of vulnerability and poor cybersecurity, so we might expect a decrease in breaches at receiver firms to be more likely when the CIO who joins their board comes from a sender firm that has *not* had a past breach. On the other hand, past experience serving as a CIO at a breached company can provide valuable insights and lessons (Mehrizi et al. 2022), and because CIOs are

appointed to the board at receiver firms for their experience and knowledge, this could be a conduit for positive learning outcomes. As such, we might expect a decrease in breaches at receiver firms to be more likely when the CIO who joins their board comes from a sender firm that *has* had a past breach. Finally, we consider investment in IT security. If a sender firm has more reported IT security applications than the median of their industry peers, then we consider this as an indication that the sender firm is relatively strong in its cybersecurity practices. Thus, we would expect a decrease in breaches at receiver firms to be more likely when the CIO who joins their board comes from a sender firm that has relatively high IT security investment when compared with industry peers.

We present our analysis in Table 4. In column (1)–(3), we split *Receive_CIO* into two mutually exclusive variables and firms with no change in whether there is an outside CIO on their own board remain as the base group. In column (1), we split *Receive_CIO* based on whether the sender firm has a CISO on the TMT (*RecCIO_senderCISO*) or not (*RecCIO_sendernoCISO*). In column (2), we split *Receive_CIO* based on whether the

sender firm had a past breach (*RecCIO_sender_pastbreach*) or not (*RecCIO_sender_nopastbreach*). In column (3), we split *Receive_CIO* based on whether the sender firm has a higher than industry median investment in IT security applications (*RecCIO_sender_security*) or not (*RecCIO_sender_lowsecurity*). We find negative and significant coefficients on *RecCIO_senderCISO*, *RecCIO_sender_pastbreach*, and *RecCIO_sender_security* in columns (1), (2), and (3), respectively. We also find nonsignificant coefficients on (*RecCIO_sendernoCISO*, *RecCIO_sender_nopastbreach*, and *RecCIO_sender_lowsecurity* in columns (1), (2), and (3), respectively. These results suggest that, relative to the change in the likelihood of breach experienced by control firms, receiver firms experience a larger decrease in breach likelihood after an outside CIO from a sender firm joins their board, with this effect driven by the sender firm's cybersecurity experiences and practices. Of particular interest is the finding that receiver firms experience a *decrease* in breach likelihood after appointing to their board a CIO from a sender firm that has been breached in the past. This suggests that CIOs experienced in dealing with a breach likely have relevant and valuable insights to share with the

Table 4. The Effect of the Characteristics of the Sender Firm on the Receiver Firm's Cybersecurity

Variables	(1)		(2)		(3)	
	<i>Breach</i>		<i>Breach</i>		<i>Breach</i>	
<i>Send_CIO</i>	0.062**	(0.030)	0.063**	(0.030)	0.078**	(0.039)
<i>RecCIO_senderCISO</i>	−0.069**	(0.031)				
<i>RecCIO_sendernoCISO</i>	−0.016	(0.011)				
<i>RecCIO_sender_pastbreach</i>			−0.065**	(0.027)		
<i>RecCIO_sender_nopastbreach</i>			−0.010	(0.011)		
<i>RecCIO_sender_security</i>					−0.049*	(0.027)
<i>RecCIO_sender_lowsecurity</i>					−0.046	(0.029)
<i>CIO_tenure</i>	−0.000	(0.001)	−0.000	(0.001)	0.001	(0.002)
<i>CEO_Outside_bd</i>	−0.025**	(0.010)	−0.025**	(0.010)	−0.033**	(0.014)
<i>CEO_Itexp</i>	−0.023	(0.056)	−0.023	(0.056)	−0.028	(0.048)
<i>CFO_Outside_bd</i>	0.014	(0.012)	0.014	(0.012)	0.016	(0.019)
<i>CFO_Itexp</i>	0.054	(0.057)	0.054	(0.057)	0.095	(0.071)
<i>Ln_assets</i>	0.019**	(0.008)	0.019**	(0.008)	0.013	(0.011)
<i>ROA</i>	−0.013	(0.013)	−0.013	(0.013)	−0.026	(0.024)
<i>Loss</i>	0.004	(0.005)	0.004	(0.005)	0.007	(0.008)
<i>Lev</i>	0.032	(0.022)	0.032	(0.022)	0.006	(0.032)
<i>RiskComm</i>	−0.011	(0.014)	−0.011	(0.014)	0.000	(0.017)
<i>ComplianceComm</i>	0.058**	(0.023)	0.058**	(0.023)	0.075**	(0.035)
<i>TechComm</i>	0.023	(0.019)	0.022	(0.019)	0.027	(0.026)
<i>Rd</i>	0.005*	(0.003)	0.005*	(0.003)	0.004	(0.003)
<i>Past_breach</i>	−0.281***	(0.030)	−0.282***	(0.031)	−0.331***	(0.039)
<i>FirmAge</i>	−0.003	(0.002)	−0.003	(0.002)	−0.002	(0.002)
<i>Ad</i>	−0.068	(0.228)	−0.066	(0.228)	−0.490	(0.507)
<i>NumAnalyst</i>	0.001	(0.001)	0.001	(0.001)	0.001	(0.001)
Constant	−0.096	(0.069)	−0.096	(0.069)	−0.006	(0.089)
CIO–firm pair fixed effects	Yes		Yes		Yes	
Year fixed effects	Yes		Yes		Yes	
Observations	17,227		17,227		10,977	
Adjusted R ²	0.2105		0.2105		0.2544	

Notes. Standard errors clustered by CIO–firm pair in parentheses. *p*-values based on two-tailed tests.

****p* < 0.01; ***p* < 0.05; **p* < 0.10.

receiver firm about cybersecurity threats and strategies. More broadly, this suggests that in the cybersecurity context, negative events at interlocked firms can serve as opportunities for positive organizational learning for the receiving firms.

Discussion and Implications

The SEC's recent regulatory actions are expected to intensify competition among public firms for board-level cybersecurity expertise, an area where qualified candidates are already in high demand and the executive talent pool is limited (Parenty and Domet 2020, Reilly 2022, Lowry et al. 2025). Firms will likely continue to recruit CIOs from other firms to join their boards. In this study, we investigate two potential pathways of organizational learning in cybersecurity from CIO outside board service—sending and receiving—that influence a firm's cybersecurity performance in terms of occurrence of data breaches. On average, we find that a CIO concurrently serving on an outside board significantly *increases* the sender firm's likelihood of a data breach, whereas having an outside CIO serve on the firm's own board *decreases* the receiver firm's likelihood of breach. Through further analysis (reported in Online Appendix I), the sender firm effect appears to be driven more by malicious breaches. In contrast, the receiver firm effect reflects a broader reduction in breach likelihood across both malicious and accidental breach types.

Our finding of cybersecurity drawbacks for sender firms is particularly noteworthy, as it challenges a common narrative in the board interlock literature that emphasizes the learning benefits of outside board service. These benefits are often cited as a primary reason firms support their executives' participation on outside boards, and practitioner literature has specifically touted the cybersecurity value of CIOs gaining such appointments. Such optimistic views were echoed in our interviews with CIOs, who consistently described their outside board service as professionally enriching. Whereas they spoke of their deep engagement as cybersecurity educators and problem solvers on these boards, they also stressed that both they and their firms viewed such service favorably. One CIO recalled that their firm actively encouraged their outside board participation, framing it as a valuable opportunity for learning and leadership development. That CIO agreed, describing outside board service as "helping you adapt and grow and learn, which is a very important part of being any C-level executive ... You're trying to learn something new." However, our findings point to a key disconnect: despite the perceived leadership and development gains, firms may be overlooking the cybersecurity risks that CIO outside board service can introduce for sender firms. This

is an important and previously unrecognized cost of CIO-board interlocks.

Whereas our main results support the asymmetric learning effect of CIO outside board service, our mechanism explorations identify several important enabling or constraining conditions driving these outcomes. Regarding the cybersecurity drawbacks for sender firms, their failure to achieve positive cybersecurity learning outcomes appears tied to the poor cybersecurity profile of the receiver firm (i.e., lacking a CISO on its TMT, had a prior breach, underinvestment in IT security relative to industry peers). This finding aligns with our portrayal of CIOs in board interlock contexts as serving more as knowledge providers than recipients. When CIOs join boards of firms with a poor cybersecurity profile, they face greater demands on their time and attention, leaving limited capability for absorbing new cybersecurity insights and transferring any beneficial learning to their home firms. This constraint is amplified by the rapidly evolving and decentralized nature of cybersecurity within organizations. As our CIOs interviewees noted, their outside board roles often become year-round commitments, especially for receiver firms with subpar cybersecurity capabilities or facing major challenges in this area (e.g., ransomware incidents). These dynamics can explain why sender firms experience increased breach risk when their CIOs serve on the boards of firms with poor cybersecurity profiles and especially when the sender firm lacks a CISO on its own TMT to help shoulder daily cybersecurity management responsibilities.

For receiver firms where the CIO joins the board in an advisory role, achieving learning that is impactful enough to influence cybersecurity outcomes may initially seem challenging. Moreover, CIOs may not always be immersed in cutting-edge cybersecurity practices within their own firms, potentially limiting effective knowledge transfer to receiver firms. Yet our results suggest otherwise. Indeed, our findings suggest that receiver firms gain positive cybersecurity learning, ultimately reducing breach likelihood, driven by key elements of a strong cybersecurity profile in the sender firm—specifically, having a CISO on its TMT and strong IT security investment relative to industry peers. These findings align with the idea of positive contagion, where strong practices at the sender firm translate into beneficial learning outcomes at the receiver firm through the CIO's board role. Notably, we also find that past breaches in sender firms are tied to reduced breach likelihood at receiver firms, suggesting that these negative events can be valuable learning experiences. This finding diverges from typical negative contagion effects in board interlock studies, underscoring the unique and complex learning dynamics in CIO-board interlocks.

This study informs two main streams of research. First, whereas a stream of past board interlock research has examined the effects of CEO and CFO outside board service on firm-level outcomes, little attention is paid to the rigorous examination of the effects of CIO outside directorships. Past findings have documented a beneficial effect of CFO outside directorships on firm outcomes (Khan and Mauldin 2021, Cunningham et al. 2024) and mixed effects with respect to CEO outside directorships (Rosenstein and Wyatt 1994, Perry and Peyer 2005, Geletkanycz and Boyd 2011). Research has also demonstrated that whether the home firm experiences positive or negative outcomes from their executives' outside board service is dependent on contextual factors (Perry and Peyer 2005, Khan and Mauldin 2021, Ramsawak et al. 2024). Extending this line of inquiry to the IS and cybersecurity contexts, our findings align with this more nuanced perspective in that certain conditions facilitate either positive or negative learning outcomes from CIO-board interlocks. We take a more expansive view than past interlock studies and consider both the sender and receiver pathways for CIO outside board service, which allows us to uncover the unique, asymmetric learning effect specific to this interlock type. The increased breach likelihood for sender firms suggests that the anticipated learning benefits of outside board service may be difficult to realize for CIOs and in the context of cybersecurity, especially because of the constraints posed by the receiver firm's cybersecurity profile. In diverging from many past studies that support positive learning effects for sender firms, we surmise that our observation of a lack of positive learning outcomes in this channel is likely attributable to the unique role and responsibilities of CIOs in board interlock contexts and the complexities of the cybersecurity landscape. Because of the complex and rapidly evolving nature of cybersecurity, CIOs may face obstacles in fully leveraging the learning opportunities in this domain that outside board service might otherwise afford. Furthermore, in acting mostly as knowledge providers in this context, CIOs may struggle to absorb new, cybersecurity-specific insights from their outside board service, and the divided attention required by such service can be especially detrimental to their home firm's cybersecurity, given the operational dimension of the CIO's home firm responsibilities. Effective home firm cybersecurity requires the CIO's focused attention on IT operational stability and constant vigilance to evolving cybersecurity threats. Thus, a distracted CIO may have difficulty fulfilling their ongoing cybersecurity management responsibilities at the home firm.

An additional contribution to the board interlock literature is that, to our knowledge, this study is the first to explore the receiver firm pathway within CIO-

board interlocks. Our evidence of positive cybersecurity learning through this channel, driven by aspects of a strong cybersecurity profile, is a novel addition. Furthermore, we extend interlock research in IS with evidence that positive learning outcomes for receiver firms can emerge from negative IS events (i.e., past breaches) in sender firms. This finding contrasts with interlock research in non-IS contexts (Perry and Peyer 2005), where receiver firms are penalized for appointing outside directors from firms with poor governance structures. Contrary to the concept of negative contagion, we show that "good learning can come from bad events" in CIO-board interlocks, extending the idea that past IS incidents provide valuable organizational learning opportunities (Mehrizi et al. 2022), now demonstrated to apply across firms.

Second, research on data breaches is growing, particularly as it relates to the influence of top management and board-level oversight. Prior studies have explored the impact of manager compensation (Kwon et al. 2013), the presence of board-level technology committees (Higgs et al. 2016), and management IT expertise (Haislip et al. 2021) on breach outcomes. However, little attention has been paid to the outside commitments of top IT executives directly charged with overseeing the management of cybersecurity (e.g., the CIO). We extend this literature with a nuanced and rigorous set of analyses, estimating the effects and uncovering the conditions and potential mechanisms for the effects of CIO outside board service on both the sender and receiver firms' cybersecurity outcomes. In doing so, we address calls from IS scholars to investigate the cybersecurity implications of board interlocks (Cheng et al. 2021).

Our study offers important practical insights, especially for how sender firms allocate their limited cybersecurity resources amid the continued trend of CIOs joining outside boards—a practice that many firms appear to support. Given the elevated risk of malicious breaches in this context, sender firms should ensure they have adequate investments in preventative and detective cybersecurity controls specifically designed to counter intentional, targeted attacks. This includes threat detection and response capabilities through tools such as real-time security information and event management (SIEM) systems and user behavior analytics that can identify anomalies linked to external hackers or insider threats. These investments can help mitigate the impact of the CIO's reduced focus on home firm cybersecurity because of external board commitments. Additionally, sender firms should prioritize strong, visible cybersecurity leadership by appointing a CISO to the TMT, ensuring dedicated oversight of cybersecurity operations and reinforcing cybersecurity resilience in the wake of the CIO's outside board service. This recommendation is consistent with recent regulatory efforts to enhance the visibility,

authority, and strategic importance of the CISO role within firms (Lowry et al. 2025).

Our study also has important implications for firms considering whether to recruit outside CIOs to their boards and permit their own CIOs to serve on outside boards and for policymakers seeking to strengthen cybersecurity expertise at the board level. The clearest takeaway for firms is that if the goal is to gain cybersecurity learning benefits, recruiting an outside CIO to serve on the board is a more effective approach than allowing a CIO to join an outside board. This is not to suggest that firms should avoid supporting CIO outside board service entirely, but from a cybersecurity perspective, there are important constraints. Thus, for cybersecurity outcomes, firms should be cautious about allowing their CIOs to serve on outside boards while being receptive to outside CIOs joining their own boards. When considering permitting their CIOs to serve on outside boards, it is important that home firm executive leadership assess the cybersecurity profile of the receiver firms. Firms that lack a prominent CISO, have had past breaches, and do not demonstrate robust IT security investments should be approached cautiously as potential board placements for the CIO. Understandably, this limitation may create tension, as such firms are often those actively recruiting CIOs to outside board service with attractive incentives. Nevertheless, our study suggests that sender firms would benefit from discouraging these particular outside board appointments. For firms considering the recruitment of a CIO to their board, our results suggest a strategic focus on candidates from firms with a strong cybersecurity profile—specifically, those with a prominent CISO and robust IT security investment. Interestingly, firms should also seek CIOs from firms that have encountered past breaches, as their experience managing such incidents seems to offer a valuable opportunity for the recruiting firm to benefit from real-world cybersecurity insights.

Finally, for policymakers like the SEC, who seek to enhance cybersecurity expertise on corporate boards, our findings suggest that a blanket approach advocating for increased board-level expertise may be too simplistic and potentially detrimental to certain firms. Instead, more nuanced guidelines could be recommended, encouraging firms to consider the cybersecurity experiences and practices of the external firms to which they send their CIOs, as well as those from which they recruit CIOs to their own boards.

Endnotes

¹ To gain deeper insight into the phenomenon of CIOs serving on outside boards, we interviewed three CIOs from public companies (see Online Appendix B), each of whom has served on multiple outside boards. These individuals are part of the dataset used in our empirical analyses, and we incorporate their perspectives at various points throughout the paper.

² A data breach incident “involves unauthorized access to sensitive, protected, or confidential data resulting in the compromise or potential compromise of confidentiality, integrity, and availability of affected data” (Sen and Borle 2015, p. 315). Data breaches are becoming more frequent and costly, impacting businesses of all sizes and sectors (IBM 2024).

³ Cheng et al. (2021) noted that CIOs were seldom on corporate boards in their sample that covered 2001–2008 (only three instances in 1,952 of their firm-year observations). In contrast, in our longer, more comprehensive, and more recent sample period covering 2005–2022, we found 310 instances of CIOs serving on outside corporate boards.

⁴ The CFO has become a key strategic leader in recent decades, typically reporting to the CEO and ranking just behind them in TMT importance because of the central role of finance in firm strategy (Zhang et al. 2025).

⁵ Our independent variables of interest (e.g., whether the firm’s CIO serves on an outside board) require a disclosed CIO in BoardEx. Therefore, we removed 58,199 firm-year observations without a CIO listed/disclosed (see Online Appendix C).

⁶ Privacy Rights Clearinghouse collects data breach announcements from the media, law enforcement, state government reporting agencies, and other public sources. Audit Analytics uses these same sources and SEC filings.

⁷ We follow previous studies (e.g., Kwon and Johnson 2014, Angst et al. 2017) that use the number of IT security applications as a proxy for IT security investment.

⁸ For our analyses, we define the CIO “control” group as those who never serve on an outside board during the study period. As such, we exclude 103 CIO-firm-year observations in which the CIO is always on an outside board. For robustness, we reran all analyses, including these observations, and the results and inferences remain unchanged.

⁹ For breaches with a disclosed occurrence date, we use that year as the *Breach* year. Otherwise, we assume that the breach occurrence and disclosure happened in the same year, following past breach studies. In our sample, only 53 observations have an earlier occurrence year than the disclosure year. Coding these as $t - 1$ did not affect our results.

¹⁰ There are 1,912 CIO turnover events at home firms in our sample, suggesting that firm fixed effects alone will not fully capture time-invariant effects of specific CIOs. Including CIO-firm pair fixed effects in Equation (1) means that *Send_CIO* captures changes in whether a preexisting CIO serves on an outside board (i.e., going from not serving on an outside board to serving on an outside board and going from serving on an outside board to not serving on an outside board) rather than capturing the hiring of a new CIO who already serves on an outside board. In the latter case, it is not possible to determine whether any effect on breaches is driven by the new appointment in and of itself or the fact that the newly appointed CIO serves on an outside board. Studies on manager effects include both firm and manager fixed effects for this reason (e.g., Bertrand and Schoar 2003, Bamber et al. 2010, Ge et al. 2011, Cunningham et al. 2024).

¹¹ A two-way fixed effects DID design does not use the traditional *treatment* and *post* variables as in a matched-sample DID. Instead, the coefficient on the variable of interest simulates a *treatment* \times *post* interaction effect using the unit and time fixed effects. For an expanded explanation, see Bertrand and Mullainathan (2003).

¹² Haslip et al. (2021) and Wang et al. (2023) explain that an LPM is preferred when using firm and year fixed effects, as logistic regression would drop observations for all firms that do not disclose a breach during the sample period.

¹³ For sender firms, we calculate the marginal effect as: 0.062 (coefficient)/0.044 (mean of breach for all firms) = 1.41, or 141%; for

receiver firms: 0.036 (coefficient)/0.044 (mean of breach for all firms) = 0.82, or 82%.

¹⁴ The key assumptions are (a) no serial correlation in errors beyond first order, and (b) instruments are uncorrelated with the differenced error term. We respectively test these assumptions with the AR(2) test and Sargan's J.

¹⁵ Following prior literature that treats certain C-level executives as part of the TMT (e.g., CIOs in Ashraf et al. 2020, Haislip et al. 2021, CISOs in Ashraf 2022), we view a CISO as part of the TMT if they appear in the BoardEx database. Inclusion in BoardEx indicates that the executive is publicly disclosed via communication mechanisms such as SEC filings, press releases, or the company website. We infer that such disclosure signifies the importance and influence of the CISO in the firm (as opposed to firms that have a CISO but do not publicly disclose it).

References

- Angst CM, Block ES, 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 Quart.* 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. *Rev. Econom. Stud.* 58(2):277–297.
- Argote L, Hwang E (2018) Organizational learning. Augier M, Teece D, eds. *The Palgrave Encyclopedia of Strategic Management* (Palgrave Macmillan, London).
- Ashraf M (2022) The role of peer events in corporate governance: Evidence from data breaches. *Accounting Rev.* 97(2):1–24.
- Ashraf M, Michas PN, Russomanno D (2020) The impact of audit committee information technology expertise on the reliability and timeliness of financial reporting. *Accounting Rev.* 95(5):23–56.
- Autor DH (2003) Outsourcing at will: The contribution of unjust dismissal doctrine to the growth of employment outsourcing. *J. Labor Econom.* 21(1):1–42.
- Aziz A, Li H, Telang R (2023) The consequences of rating inflation on platforms: Evidence from a quasi-experiment. *Inform. Systems Res.* 34(2):590–608.
- Bamber LS, Jiang J, Wang IY (2010) What's my style? The influence of top managers on voluntary corporate financial disclosure. *Accounting Rev.* 85(4):1131–1162.
- Bandodkar N, Grover V (2022) Does it pay to have CIOs on the board? Creating value by appointing C-level IT executives to the board of directors. *J. Assoc. Inform. Systems* 23(4):838–888.
- Banker RD, Feng C (2019) The impact of information security breach incidents on CIO turnover. *J. Inform. Systems* 33(3):309–329.
- Banker RD, Hu N, Pavlou PA, Luftman J (2011) CIO reporting structure, strategic positioning, and firm performance. *MIS Quart.* 35(2):487–504.
- Basten D, Haamann T (2018) Approaches to organizational learning: A literature review. *Sage Open* 8(3):1–20.
- Beck N (2020) Estimating grouped data models with a binary dependent variable and fixed effects via a logit versus a linear probability model: The impact of dropped units. *Political Anal.* 28(1):139–145.
- Bertrand M, Mullainathan S (2003) Enjoying the quiet life? Corporate governance and managerial preferences. *J. Political Econom.* 111(5):1043–1075.
- Bertrand M, Schoar A (2003) Managing with style: The effects of managers on firm policies. *Quart. J. Econom.* 118(4):1169–1208.
- Bertrand M, Duflo E, Mullainathan S (2004) How much should we trust differences-in-differences estimates? *Quart. J. Econom.* 119(1):249–275.
- Benaroch M, Chernobai A (2017) Operational IT failures, IT value destruction, and board-level IT governance changes. *MIS Quart.* 41(3):729–762.
- Bizjak J, Lemmon M, Whitby R (2009) Option backdating and board interlocks. *Rev. Financial Stud.* 22(11):4821–4847.
- Booth JR, Deli DN (1996) Factors affecting the number of outside directorships held by CEOs. *J. Financial Econom.* 40:81–104.
- Chen DQ, Zhang Y, Xiao J, Xie K (2021) Making digital innovation happen: A chief information officer issue selling perspective. *Inform. Systems Res.* 32(3):987–1008.
- Cheng Z, Rai A, Tian F, Xue SX (2021) Social learning in information technology investment: The role of board interlocks. *Management Sci.* 67(1):547–576.
- Chiu PC, Teoh SH, Tian F (2013) Board interlocks and earnings management contagion. *Accounting Rev.* 88(3):915–944.
- Cunningham LM, Myers LA, Short JC (2024) Do CFO outside directorships benefit or harm home firm financial reporting quality? *Accounting Horizons* 38(2):101–119.
- D'Arcy J, Adjerid I, Angst CM, Glavas A (2020) Too good to be true: Firm social performance and the risk of data breach. *Inform. Systems Res.* 31(4):1200–1223.
- Ganju KK, Atasoy H, McCullough J, Greenwood B (2020) The role of decision support systems in attenuating racial biases in healthcare delivery. *Management Sci.* 66(11):5171–5181.
- Ge W, Matsumoto D, Zhang JL (2011) Do CFOs have style? An empirical investigation of the effect of individual CFOs on accounting practices. *Contemporary Accounting Res.* 28(4):1141–1179.
- Geletkanycz MA, Boyd BK (2011) CEO outside directorships and firm performance: A reconciliation of agency and embeddedness views. *Acad. Management J.* 54(2):335–352.
- Geletkanycz MA, Hambrick DC (1997) The external ties of top executives: Implications for strategic choice and performance. *Admin. Sci. Quart.* 42(4):654–681.
- Hainmueller J (2012) Entropy balancing for causal effects: A multivariate reweighting method to produce balanced samples in observational studies. *Political Anal.* 20(1):25–46.
- Haislip J, Lim J, Pinsker R (2021) The impact of executives' IT expertise on reported data security breaches. *Inform. Systems Res.* 32(2):318–334.
- Higgs JL, Pinsker RE, Smith TJ, Young GR (2016) The relationship between board-level technology committees and reported security breaches. *J. Inform. Systems* 30(3):79–98.
- IBM (2024) Cost of data breach report 2024. Accessed July 21, 2025, <https://www.ibm.com/reports/data-breach>.
- Johnson M (2020) Five compelling reasons why CIOs should pursue board seats now. *CIO* (October 1), <https://www.cio.com/article/194057/5-compelling-reasons-why-cios-should-pursue-board-seats-now.html>.
- Johnson V, Torres R, Maurer C, Guerra K, Srivastava S (2023) The 2022 SIM IT issues and trends study. *MIS Quart. Executive* 22(1):6.
- Kappelman L, Johnson V, Torres R, Maurer C, McLean E (2019) A study of information systems issues, practices, and leadership in Europe. *Eur. J. Inform. Systems* 28(1):26–42.
- Kettles D, Mazzola D, Richardson B (2024) The path to becoming a fortune 500 CIO. *MIS Quart. Executive* 23(2):213–234.
- Khan S (2019) CFO outside directorship and financial misstatements. *Accounting Horizons* 33(4):59–75.
- Khan S, Mauldin E (2021) Benefit or burden? A comparison of CFO and CEO outside directorships. *J. Bus. Finance Accounting* 48(7–8):1175–1214.
- Kim SH, Kwon J (2019) How do EHRs and a meaningful use initiative affect breaches of patient information? *Inform. Systems Res.* 30(4):1184–1202.
- Kim J-B, Wang C, Wu F (2024) Privacy breaches and the effect of customer notification. *MIS Quart.* 48(4):1483–1502.
- Kitchens B, Kumar A, Pathak P (2018) Electronic markets and geographic competition among small, local firms. *Inform. Systems Res.* 29(4):928–946.
- Kwon J, Johnson ME (2014) Proactive versus reactive security investments in the healthcare sector. *MIS Quart.* 38(2):451–471.

- Kwon J, Johnson ME (2018) Meaningful healthcare security: Does meaningful-use attestation improve information security performance? *MIS Quart.* 42(4):1043–1068.
- Kwon J, Ulmer JR, Wang T (2013) The association between top management involvement and compensation and information security breaches. *J. Inform. Systems* 27(1):219–236.
- Lamb NH, Roundy P (2016) The “ties that bind” board interlocks research: A systematic review. *Management Res. Rev.* 39(11):1516–1542.
- Lee K, Jin Q, Animesh A, Ramaprasad J (2022) Impact of ride-hailing services on transportation mode choices: Evidence from traffic and transit ridership. *MIS Quart.* 46(4):1875–1900.
- Li H, Yoo S (2024) Information systems sourcing strategies and organizational cybersecurity breaches. *IEEE Trans. Engrg. Management* 71:481–490.
- Li WW, Leung ACM, Yue WT (2023) Where is IT in information security? The interrelationship among IT investment, security awareness, and data breaches. *MIS Quart.* 47(1):317–342.
- Li Z, Lee G, Raghu TS, Shi ZM (2024) Impact of the GDPR on the global mobile app market: Digital trade implications of data protection and privacy regulations. *Inform. Systems Res.* 36(2):669–689.
- Liu X, Pinsonneault A, Qu WG, Dong JQ (2024) Board interlocks with information technology firms and innovation outcomes: A resource dependence perspective. *J. Management Inform. Systems* 41(3):812–838.
- Lowry MR, Vance A, Vance MD (2025) Inexpert supervision: Field evidence on boards’ oversight of cybersecurity. *Management Sci.*, ePub ahead of print May 23, <https://doi.org/10.1287/mnsc.2023.04147>.
- Ma Z, Shi L, Yu K, Zhou N (2024) Director interlocks: Information transfer in board networks. *Encyclopedia* 4(1):117–124.
- McMullin JL, Schonberger B (2020) Entropy-balanced accruals. *Rev. Accounting Stud.* 25(1):84–119.
- Mehrzi MHR, Nicolini D, Model JR (2022) How do organizations learn from information systems incidents? A synthesis of the past, present, and future. *MIS Quart.* 46(1):531–590.
- Ocasio W (1997) Towards an attention-based view of the firm. *Strategic Management J.* 18(S1):187–206.
- Ozer GT, Greenwood BN, Gopal A (2023) Digital multisided platforms and women’s health: An empirical analysis of peer-to-peer lending and abortion rates. *Inform. Systems Res.* 34(1):223–252.
- Page R (2023) Examining the CIO time management dilemma. *CIO* (January 25), <https://www.cio.com/article/419707/examining-the-cio-time-management-dilemma.html>.
- Parenty TJ, Domet JJ (2020) *A Leader’s Guide to Cybersecurity: Why Boards Need to Lead—And How to Do It* (Harvard Business Review Press, Boston).
- Perry T, Peyer U (2005) Board seat accumulation by executives: A shareholder’s perspective. *J. Finance* 60(4):2083–2123.
- Proudfoot JG, Cram WA, Madnick S, Coden M (2023) The importance of board member actions for cybersecurity governance and risk management. *MIS Quart. Executive* 22(4):235–250.
- Ramsawak R, Buertey S, Maheshwari G, Dang D, Phan CT (2024) Interlocking boards and firm outcomes: A review. *Management Decision* 62(4):1291–1322.
- Reilly D (2022) How the board can help in the fight against cybersecurity threats. *Fortune* (June 22), <https://fortune.com/2022/06/22/modern-board-cybersecurity-threats-attacks/>.
- Rosenstein S, Wyatt JG (1994) Shareholder wealth effects when an officer of one corporation joins the board of directors of another. *Managerial Decision Econom.* 15(4):317–327.
- Sahin Z, Vance A (2025) What do we need to know about the chief information security officer? A literature review and research agenda. *Comput. Security* 148:104063.
- Saldanha TJ, Andrade-Rojas MG, Kathuria A, Khuntia J, Krishnan MS (2024) How the locus of uncertainty shapes the influence of CEO long-term compensation on information technology capital investments. *MIS Quart.* 48(2):459–490.
- Saldanha TJ, Sahaym A, Mithas S, Andrade-Rojas MG, Kathuria A, Lee HH (2020) Turning liabilities of global operations into assets: IT-enabled social integration capacity and exploratory innovation. *Inform. Systems Res.* 31(2):361–382.
- SEC (2023) Final rule: Cybersecurity risk management, strategy, governance, and incident disclosure. Accessed August 5, 2023, <https://www.sec.gov/files/rules/final/2023/33-11216.pdf>.
- Sen R, Borle S (2015) Examining the contextual risk of data breach: An empirical study. *J. Management Inform. Systems* 32(2):314–341.
- Smith T, Tadesse AF, Vincent NE (2021) The impact of CIO characteristics on data breaches. *Internat. J. Accounting Inform. Systems* 43:100532.
- Song J, Almedia P, Wu G (2003) Learning-by-hiring: When is mobility more likely to facilitate interfirm knowledge transfer? *Management Sci.* 49(4):351–365.
- Srinivasan S, Payne LS, Goyal N (2019a) Cyber breach at Target. HBR Case 117-027, Harvard Business School, Boston.
- Srinivasan S, Pitcher Q, Goldberg JS (2019b) Data breach at Equifax. HBR Case 9-118-031, Harvard Business School, Boston.
- Stephenson C, Olson N (2017) Why CIOs make great board directors. *Harvard Bus. Rev.* (March 15), <https://hbr.org/2017/03/why-cios-make-great-board-directors>.
- Tang C, Li S, Ding Y, Gopal RD, Zhang G (2024) Racial discrimination and anti-discrimination: The COVID-19 pandemic’s impact on Chinese restaurants in North America. *Inform. Systems Res.* 35(3):1274–1295.
- Tzabbar D, Silverman BS, Aharonson BS (2015) Learning by hiring or hiring to avoid learning? *J. Management Psych.* 30(5):550–564.
- Wang Q, Ngai EWT, Pienta D, Thatcher JB (2023) Information technology innovativeness and data breach risk: A longitudinal study. *J. Management Inform. Systems* 43(4):1139–1170.
- Xue L, Ray G, Zhao X (2017) Managerial incentives and IT strategic posture. *Inform. Systems Res.* 28(1):180–198.
- Zhang Z, Mount MP, Zhang SX (2025) A database of chief financial officer turnover and dismissal in S&P 500 firms, 2000–2022. *Strategic Management J.* 46(5):1293–1321.
- Zhu JJ, Tuo L, Thomson M (2024) A preemptive and curative solution to mitigate data breaches: The double-layer of protection from corporate social responsibility. *J. Marketing Res.* 61(4):778–801.
- Zukis B (2019) Why CIOs make the perfect corporate board members. *Forbes* (April 22), <https://www.forbes.com/sites/bobzukis/2019/04/22/why-cios-make-the-perfect-corporate-board-members/>.