Corporate Cybersecurity Governance:

The Role of Director IT Expertise in the Lifecycle of Cybersecurity Breaches

Abstract

Cybersecurity threats pose increasing risks to firms, yet the role of corporate governance—particularly board IT expertise—in enhancing cybersecurity resilience remains underexplored. Drawing on Socio-Technical Systems Theory, we examine how director IT expertise influences corporate vulnerability to a wide range of cyberattacks throughout the breach lifecycle, using data on U.S. public firms from 2010–2021. We find that firms led by more IT-savvy boards are significantly less prone to human behavior-driven attacks such as phishing, misconfiguration, and unauthorized access, and experience less severe outcomes when breaches occur, including fewer compromised records and lower financial costs. We further find that firms improve board IT expertise following cyberattacks—a remedial strategy that significantly reduces future breaches—thereby completing the feedback loop conceptualized by Liu and Babar (2024) in support of Organizational Learning Theory. Our findings are robust to various endogeneity tests, including an instrumental variable strategy exploiting state-level variations in the supply of IT-expert directors following staggered adoptions of data breach disclosure laws. This study provides timely insights for executives, investors, and policymakers seeking to strengthen corporate cybersecurity resilience.

Keywords: Cybersecurity; Cyber governance; Cyberattacks; IT directors; Board IT expertise; Board of Directors; Phishing; Malware; Misconfiguration; Data breach; IT governance.

JEL code: M14, K32

"[T]here are only two types of companies: those that have been hacked and those that will be."

--- Robert S. Mueller III,
Director, U.S. Federal Bureau of Investigation,
Keynote Speech at RSA Conference 2012.

1 INTRODUCTION

As cyberattacks grow in frequency and cost, firms face increasing pressure to defend cybersecurity, which often requires corporate leaders to tackle technical challenges beyond their expertise. High-profile breaches—such as the 2017 Equifax breach, which compromised the personal data of 147 million customers, and the 2022 Optus breach that prompted government intervention (Khan et al., 2022)—highlight the far-reaching consequences of corporate failures to safeguard cybersecurity. A recent IBM report estimates the global cost of data breaches to average $4.88 million, representing a 10% increase from the previous year (IBM, 2024). Given the growing urgency to enhance firms' cybersecurity resilience, researchers have explored risk factors that influence vulnerability to cyberattacks (see e.g., Liu & Babar, 2024), including firm size and industry (Aldasoro et al., 2022; Kamiya et al., 2021), intangible investments (Ettredge et al., 2018; Kamiya et al., 2021), and organizational complexity (Liang et al., 2025; Tanriverdi et al., 2025).

Boards of directors play a critical role in overseeing cybersecurity risk management (Lowry et al., 2023). Yet most directors, while business experts or specialists in their own fields, typically lack the technical IT expertise to identify, assess, and mitigate cybersecurity threats. This challenge is compounded by growing calls to impose personal liability on directors for cybersecurity failures (Dinger & Wade, 2022; Frank et al., 2021). An important question arises as to whether IT expertise in the boardroom can help mitigate firms' cybersecurity risks. Prior research shows that director expertise in other areas—such as finance (Güner et al., 2008), law (Krishnan et al., 2011), and medicine (Jin et al., 2024)—improves corporate policies and outcomes in those fields. However, the impact of director IT expertise on cybersecurity risk remains underexplored, giving rise to a

critical gap in the literature, which this study seeks to address.

We adopt a holistic approach by examining the role of director IT expertise across the lifecycle of cybersecurity breaches—spanning pre-attack prevention, during-attack discovery and response, and post-attack remediation and recovery—thereby completing the feedback loop of organizational learning, which was conceptualized in Liu and Babar's (2024) theoretical framework of corporate cybersecurity risk management. We further integrate Socio-Technical Systems Theory by Trist and Bamforth (1951) into cybersecurity governance by examining a broad spectrum of cyberattacks—including phishing, malware, misconfiguration, and unauthorized access—recognizing that different attack methods rely on varying compositions of human-oriented and technical exploits, which necessitate distinct defense strategies.

Drawing on Upper Echelons and Resource Dependency Theories, we hypothesize that directors with IT education (i.e., "IT-expert directors") possess knowledge and professional networks that enable them to enhance firms' *ex ante* risk management, thereby reducing corporate susceptibility to cyberattacks. When breaches do occur, firms with more IT-savvy boards are expected to detect and contain breaches more effectively, limiting their scale and financial impacts. Under Organizational Learning Theory (Argyris & Schön, 1978) and building upon empirical evidence of post-failure governance restructurings (Aharony et al., 2015; Farber, 2005; Ferris et al., 2007), we expect firms to increase board IT expertise post-cyberattack to strengthen cyber governance which, if effective, would lead to fewer subsequent breaches.

Using a sample of cybersecurity incidents disclosed by U.S. public companies from 2010 to 2021 from Audit Analytics, we observe breach frequency to measure corporate vulnerability to cyberattacks, following prior studies (Ettredge et al., 2018; Kamiya et al., 2021; Lending et al., 2018). Under Socio-Technical Systems Theory (Trist, 1981; Trist & Bamforth, 1951), we

recognize that different attack methods necessitate varied socio-technical and technical defenses. For instance, phishing—a social engineering attack that exploits human errors—is most effectively mitigated through socio-technical measures such as risk awareness training, whereas malware prevention requires robust technical defenses, such as firewalls and regular system updates. Accordingly, we disaggregate different cyberattack types—phishing, malware (including ransomware), misconfiguration, unauthorized access, and unknown types—and examine each separately to investigate the effectiveness of board IT expertise in mitigating cyber threats of different natures. To measure board IT expertise, we obtain BoardEx director data to compute the proportion of directors with at least one IT-related degree on the board.

Our findings show that firms led by boards with greater IT expertise experience fewer cyberattacks, particularly those driven by human-oriented or behavioral weaknesses, such as phishing, misconfiguration, and unauthorized access. When breaches do occur, firms with more IT-savvy boards experience less severe outcomes, including fewer compromised records and lower financial costs, suggesting a greater preparedness to limit the scope and impact of cyberattacks. Firms are more likely to increase board IT expertise following a cyberattack, which leads to significantly fewer subsequent breaches, evidencing the effectiveness of this remedial strategy.

Our channel analysis reveals that IT-expert directors improve cyber outcomes by enhancing corporate cybersecurity culture, characterized by greater attention to cybersecurity issues in annual reports. While IT-expert directors do not advocate for greater IT expenditure, sufficient funding amplifies the impact of board IT expertise, supporting the notion that IT investments are a necessary but not sufficient condition for improving cyber resilience (Angst et al., 2017). Our findings are robust to various endogeneity strategies and additional tests, including a Heckman Selection Model using an instrumental variable to capture the local supply of IT-expert directors

in firms' headquartered states following staggered adoptions of breach disclosure laws, testing for industry-level endogeneity, and alternative sample constructions and model specifications. Overall, our findings provide a comprehensive view of the role of IT-expert directors in cyber governance throughout the lifecycle of cyberattacks, highlighting a feedback loop for firms to learn from past failures to improve future resilience through strengthening board expertise.

This paper makes several novel contributions to academic research, while offering practical implications for cybersecurity risk management in corporations. First, we respond to the call by Schneier and Vance (2025) to explore human-oriented factors—specifically IT expertise in corporate boardrooms—as a critical determinant of cybersecurity risk. Prior literature has largely focused on organizational and institutional-level factors influencing cybersecurity vulnerability, such as firm size (Kwong & Pearlson, 2024; Wynn et al., 2024) and mergers and acquisitions (Liang et al., 2025), with little attention paid to board-level IT expertise. Our findings address this gap by demonstrating that IT-savvy boards are linked to lower susceptibility to cyberattacks, particularly those driven by human error—such as phishing, misconfiguration, and unauthorized access. This evidence contributes to the empirical investigation of how board governance can mitigate cybersecurity risks, while offering actionable insights for executives and directors seeking to enhance cyber resilience through strategic director recruitment.

Second, we make a significant theoretical contribution by extending Organizational Learning Theory (Argyris & Schön, 1978) in the context of cybersecurity governance. Despite the ubiquity of cybersecurity threats, there is scant evidence on how organizations learn from past cyber breaches to improve future resilience. We find empirical evidence of a feedback loop conceptualized in Liu and Babar's (2024) theoretical framework of corporate cybersecurity risk management—where cyberattacks spur improvements in board IT expertise, which in turn reduces

subsequent breaches—thereby completing the cycle of organizational learning. Our evidence extends prior research on firms' short-term responses to cyberattacks (Kim et al., 2024; Nikkhah & Grover, 2022) by examining long-term learning effects. Our investigation complements the findings by Bana et al. (2025), who show that breached firms advertise more cybersecurity-related jobs in the workforce, by documenting changes at the board level beyond rank-and-file employees. Our evidence extends the existing literature on board restructuring following negative events such as fraud and misconduct (Brochet & Srinivasan, 2014; Cheng et al., 2010; Crutchley et al., 2015), offering new insights into organizational learning in the context of cybersecurity governance.

Third, we make a critical methodological contribution to the cybersecurity literature by highlighting the heterogeneity of cyberattack types. While most prior research (e.g., Kamiya et al., 2021) treats cybersecurity breaches as homogeneous, by integrating Socio-Technical Systems Theory (Trist & Bamforth, 1951), we distinguish different cyberattack types based on their human-oriented and technical components. Our evidence demonstrates that different cyberattacks require distinct defense strategies, which are not one-size-fits-all. This approach enables future researchers to adopt more targeted and nuanced empirical designs. By drawing insights on diverse cybersecurity threats from the computer science literature, we also bridge the interdisciplinary gap and contribute to an integrated approach to cybersecurity research advocated by Falco et al. (2019).

Fourth, our evidence contributes to the corporate governance literature (Agrawal & Chadha, 2005; Güner et al., 2008; Levit & Malenko, 2016; Yermack, 2004) by shedding light on the evolving role of directors in the digital age. Prior studies have examined the impact of board characteristics, such as board gender diversity (Adams & Ferreira, 2009; Adams & Funk, 2012), director experience (Chen et al., 2022), and social networks (Fracassi & Tate, 2012; Ishii & Xuan, 2014), on firm outcomes. Director educational expertise in other fields—such as financial (Erkens

& Bonner, 2013; Güner et al., 2008; Krishnan & Lee, 2009), legal (Black et al., 2021; Krishnan et al., 2011), medical (Jin et al., 2024), and industry-specific expertise (Burns et al., 2020; Dass et al., 2014)—has been found to be value-adding; our evidence extends this literature by highlighting the critical role of IT expertise on the board in combating cybersecurity threats.

Finally, our findings provide timely practical insights for corporate managers, investors, and policymakers seeking to strengthen cybersecurity resilience. For corporate leaders, our evidence underscores the importance of IT expertise in director recruitment. Furthermore, rather than relying on director turnover or post-breach interventions, companies can proactively invest in board-level IT training to equip existing directors with the necessary IT knowledge. For investors, the presence of IT expertise on boards could serve as a signal of a firm's proactive approach to cyber risk management, offering relevant information for ESG assessments and investment decisions. From a regulatory perspective, policymakers can consider encouraging or mandating the disclosure of board-level IT expertise in corporate reporting, to enhance transparency and incentivize stronger cybersecurity oversight. These practical strategies can help firms strengthen cybersecurity resilience and mitigate the growing threats of cyberattacks.

2 LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

2.1 Lifecycle of Cybersecurity Breaches

Cyberattacks cause financial and reputational damage to breached firms (e.g., Liu & Babar, 2024). News of breaches typically triggers negative stock market reactions (Amir et al., 2018; Chatterjee et al., 2019; Gwebu et al., 2018; Kamiya et al., 2021; Peng et al., 2023; Tosun, 2021). Cybersecurity breaches cause mistrust among stakeholders, including investors (Iyer et al., 2020), customers (Hoehle et al., 2022), suppliers (He et al., 2020a), and employees (Hovav & Gray, 2014), while impairing corporate growth (Kamiya et al., 2021), hampering financial performance

(Lending et al., 2018), and reducing dividends (Tosun, 2021), credit ratings (Kamiya et al., 2021), access to capital (Huang & Wang, 2020), and innovation (He et al., 2020b; Tosun, 2021).

The lifecycle of cybersecurity breaches typically comprises three stages: pre-attack prevention, during-attack discovery, and post-attack feedback and learning, as illustrated in Figure 1. First, prevention is key during the pre-cyberattack stage, as undetected IT security vulnerabilities—such as misconfigured security protocols or inadequate phishing training—remain unidentified and unexploited. Second, a breach occurs when attackers successfully exploit a firm's cybersecurity weaknesses. IBM (2024) reports that it takes on average 292 days to detect and contain breaches, which often alert firms to underlying cybersecurity flaws. Third, the post-attack phase centers on remediation and learning: under Organizational Learning Theory (Argyris & Schön, 1978), Liu and Babar (2024) propose a theoretical framework that conceptualizes a feedback loop (illustrated in Figure 2), wherein firms learn from past breaches to inform remedial actions and implement improvements to enhance future cybersecurity resilience, thereby completing the breach lifecycle.

[Insert Figure 1 and Figure 2]

2.2 Heterogeneity of Cyberattacks under Socio-Technical Systems Theory

Corporations face a wide array of cybersecurity threats. Common types of cyberattacks include phishing, malware, misconfiguration, and unauthorized access. According to Socio-Technical Systems Theory (Trist & Bamforth, 1951), organizational endeavors—including cybersecurity defenses—require both human-oriented social factors and technical factors, such as systems and technology. We integrate Socio-Technical Systems Theory into cybersecurity governance by recognizing that different cyberattack methods—with varied technical and human-oriented components—require distinct combinations of socio-technical and technical defenses. As a result, board-level IT expertise may impact various types of cyberattacks differently.

Phishing is a social engineering attack that deceives individuals into revealing sensitive information (Desolda et al., 2021; Sarker et al., 2024). Since phishing exploits human error and vulnerabilities (Sarker et al., 2024; Wright et al., 2023), effective mitigation requires a "bottom-up" employee-focused approach by adopting socio-technical defenses, such as employee training and awareness programs, as well as fostering a culture of vigilance.

Malware refers to malicious software that disrupts systems and networks (Bilot et al., 2024), including ransomware which encrypts files for ransom (Beaman et al., 2021). In contrast to phishing, malware's technical sophistication means that its defense requires a comprehensive technical strategy (Bilot et al., 2024), including implementation of firewalls, intrusion detection systems, antivirus software (Cram et al., 2017), and regular updates (Qamar et al., 2019). This "top-down" approach systematically secures infrastructure to address technical vulnerabilities.

Misconfiguration attacks occur when incorrect security settings are exploited by hackers (Bringhenti et al., 2023), such as a misconfigured cloud storage service which led to the Capital One data breach (Khan et al., 2022). Preventing misconfigurations requires both technical safeguards, such as conducting regular cybersecurity audits (Dietrich et al., 2018), and socio-technical interventions, including personnel training to enhance understanding of security protocols and improving within-team communications to prevent and identify misconfigurations.

Unauthorized access attacks—such as credential stuffing and SQL injections—exploit weak security protocols to gain access to sensitive data (Jang-Jaccard & Nepal, 2014). Effective protection relies on both firm-level safeguards and individual user practices, demanding both technical measures, such as patching system vulnerabilities, and socio-technical measures, such as multi-factor authentication (MFA), strong password policies, and monitoring user login activities.

Overall, under Socio-Technical Systems Theory, we posit that the diverse nature of

cyberattack methods requires multi-faceted defense strategies. By recognizing the different human-oriented and technical components of each attack method, our empirical investigation seeks to provide evidence on how board-level IT expertise can influence different aspects of firms' cybersecurity risk management, with different across various types of breaches.

2.3 Director IT Expertise and Cybersecurity Breaches

We hypothesize that board IT expertise plays a critical role in improving firms' cybersecurity outcomes. Drawing on Upper Echelons Theory (Hambrick, 2007; Hambrick & Mason, 1984) and Resource Dependency Theory (Hillman & Dalziel, 2003; Pfeffer & Salancik, 1978), we propose two distinct but complementary mechanisms through which IT-expert directors are expected to enhance corporate cybersecurity resilience.

First, under Upper Echelons Theory, which posits that individual experiences and perspectives influence managerial decision-making (Hambrick, 2007; Hambrick & Mason, 1984), the educational background of directors is expected to shape how they perceive and prioritize risks, even if subconsciously or informally. IT educational backgrounds provide directors with greater competency in recognizing potential risks, understanding technical issues, and formulating defense strategies in boardroom discussions. Consistent with prior evidence that directors with financial expertise improve access to capital (Güner et al., 2008) and financial reporting (Badolato et al., 2014), while legal experts help firms improve governance and litigation risk management (Black et al., 2021; Krishnan et al., 2011), we posit that IT-educated directors help foster a stronger cybersecurity culture by enhancing threat awareness within their firms. Such heightened vigilance is particularly relevant in defending against human-centric threats such as phishing and misconfiguration. We empirically test this mechanism by examining the relationship between board IT expertise and cybersecurity culture, as proxied by cybersecurity-related disclosures in

firms' annual reports.

Second, under Resource Dependency Theory, directors serve the crucial function of helping firms access critical external resources to ensure corporate success and survival (Hillman & Dalziel, 2003; Pfeffer & Salancik, 1978). IT-educated directors possess specialized industry knowledge and professional networks that can help their firms access key resources—such as acquiring technical infrastructure, facilitating vendor partnerships, and advising on technology investments—to enhance defense capabilities against cyberattacks. As such, IT-expert directors not only exert internal cultural influence but also help firms acquire external resources necessary for boosting technical defenses, which are most relevant to preventing technically sophisticated attacks such as those involving malware. We test this mechanism by analyzing whether firms with greater board-level IT expertise influences IT expenditure and whether IT expenditure moderates the relationship between board IT expertise and breach incidence.

Based on these theoretical mechanisms, we specify our first hypothesis as follows:

H1: Firms with a greater proportion of directors with IT expertise experience fewer cybersecurity breaches.

As IT-expert directors contribute domain-specific knowledge to cybersecurity governance—either by formally boosting IT investments in technical defenses or informally fostering a culture of cybersecurity awareness—their impact in preventing cybersecurity breaches is expected to vary depending on the nature of attacks. As discussed in Section 2.2, different cyberattacks require distinct combinations of socio-technical and technical defenses. While phishing attacks are most effectively mitigated by socio-technical defenses such as strengthening cybersecurity culture and awareness programs, malware attacks require investments in technical defenses, such as firewalls and anti-virus software; in contrast, misconfiguration and unauthorized access require both

technical and socio-technical defenses in the form of security protocols, cybersecurity audits, monitoring user activities, and multi-factor authentication systems. Given the diverse nature of cyber threats, the relationship between board IT expertise and breach incidence is expected to differ across attack types, with human-oriented attacks (e.g., phishing) benefiting more from the socio-technical defenses that IT-expert directors help promote, while technically complex attacks (e.g., malware) being mitigated through greater investments in cybersecurity infrastructure.

2.4 Director IT Expertise and Severity of Cyberattacks

Detection plays a crucial role in containing cyberattacks and minimizing their impact. Early breach discovery and deployment of defense mechanisms can significantly reduce the scale and cost of breaches. Prior research shows that boards with risk committees (Kamiya et al., 2021) and technology committees (Higgs et al., 2016) help mitigate negative stock price reactions to breaches, whereas cyberattacks against older firms tend to have worse impacts on firm value (Kamiya et al., 2021), reflecting investors' assessment of their lower preparedness to address cyber intrusions.

Drawing on Upper Echelons and Resource Dependency Theories, we expect that IT-educated directors, with their specialized knowledge and skills, not only contribute to breach prevention, but also enhance firms' response to cyberattacks to limit their scale and impact. From a technical perspective, IT experts on boards may advocate for investments in technical tools, such as intrusion detection systems, network traffic and flow monitoring, or endpoint detection and response systems, which can aid in and expedite breach detection. From a cultural perspective, enhanced cybersecurity awareness may prompt employees to be more vigilant in monitoring their log-in history and alerting the firm to unusual activities. Therefore, in addition to the *incidence* of cybersecurity breaches, we expect board IT expertise to have a significant bearing on the *severity* of cyberattacks. Our second hypothesis is stated as follows:

H2: A greater proportion of directors with IT expertise is associated with lower severity of cybersecurity breaches against the firms.

2.5 Organizational Learning through Post-Breach Changes in Board IT Expertise

Cybersecurity breaches, while costly and disruptive, can serve as learning opportunities for breached firms. According to Organizational Learning Theory (Argyris & Schön, 1978), firms improve by detecting and correcting errors through single-loop learning—which involves adjusting actions to correct errors without changing underlying values and policies—or double-loop learning, which entails modifying underlying values and structures that shape those actions.

In the context of cybersecurity, firms practicing single-loop learning would rectify the technical vulnerability following a cyberattack, while double-loop learning would involve a re-evaluating leadership capability, for example, by changing board composition to enhance cybersecurity oversight. Prior studies document a range of post-breach responses aimed at improving cyber governance, such as reducing board size (Lending et al., 2018), establishing risk management committees (Kamiya et al., 2021), formalizing IT oversight duties (Lankton et al., 2021), and replacing key executives such as CEOs and CTOs to signal accountability and instigate changes (Banker & Feng, 2019; Lending et al., 2018; Say & Vasudeva, 2020).

Unlike punitive measures such as replacing executive officers, restructuring the board to increase IT expertise represents a forward-looking, capacity-enhancing response, consistent with double-loop organizational learning (Argyris & Schön, 1978). Analogous to board responses following financial fraud or misconduct—where firms often restructure boards to strengthen governance functions (Arthaud-Day et al., 2006; Fich & Shivdasani, 2007; Marcel & Cowen, 2014; Srinivasan, 2005), such as by increasing board independence (Farber, 2005; Ferris et al., 2007)—we argue that breached firms seek to improve cybersecurity governance by increasing board-level

IT expertise in response to cyberattacks. This adaptive learning is aligned with the feedback loop conceptualized by Liu and Babar (2024) (illustrated in Figure 2), whose theoretical framework proposes corporate cybersecurity governance as a cyclical learning process. In their theoretical model, a cyberattack triggers organizational learning, leading to governance restructuring aimed at reducing future cyber risk. Our study empirically examines this feedback loop by investigating whether breached firms increase board IT expertise following a cyberattack.

H3: Firms are more likely to increase board IT expertise following cybersecurity breaches.

Whether this restructuring strategy improves subsequent cybersecurity outcomes is central to the effectiveness of the learning process. Importantly, prior evidence on firms' post-breach responses remains mixed and inconclusive. While some document increased post-breach CEO and CTO turnover (Banker & Feng, 2019; Lending et al., 2018; Say & Vasudeva, 2020), others find no evidence of increased turnover for CEOs (Tosun, 2021), CFOs (Banker & Feng, 2019), or CTOs (Li et al., 2021). Some studies show that executive departures—such as CTO turnover—can help address IT control weaknesses (Li et al., 2021), whereas others find no significant impact on future breach likelihood (Say & Vasudeva, 2020). Punitive actions such as firing executives may not necessarily lead to meaningful improvements in cybersecurity resilience, as attributing organizational failures to individual managers represents a symbolic rather than strategic response. In contrast, increasing board IT expertise is expected to strengthen board oversight capabilities in cyber governance and help firms learn from past cyberattacks, which we expect to reduce future breaches. By examining the effectiveness of board restructuring aimed at improving oversight capabilities, we expand the scope of this investigation to encompass proactive, future-oriented changes in corporate leadership. Under Organizational Learning Theory (Argyris & Schön, 1978), we posit that restructuring the board to add IT expertise represents a double-loop learning process,

whereby firms re-evaluate their governance structure and seek to enhance oversight capabilities by acquiring technical expertise. Consequently, we expect that increasing board IT expertise would significantly improve future cybersecurity outcomes by reducing breach incidence.

H4: Changes in board IT expertise are negatively associated with subsequent breaches.

These hypotheses examine cybersecurity governance, as firms learn from prior attacks to improve their board oversight of cybersecurity governance. This process of learning and adaptation—central to Organizational Learning Theory and conceptualized as a feedback loop in Liu and Babar's (2024) cyber governance framework—forms a critical component of long-term cybersecurity risk management.

3 DATA AND METHODOLOGY

3.1 Sample Construction

We collect accounting data from Compustat and data on boards of directors from BoardEx. We construct our sample by merging firm-year observations from Compustat and BoardEx for the period 2010–2021. We collect institutional ownership data from Thomson Reuters' 13F Database. After merging data from all sources, our final sample consists of 22,106 firm-year observations, representing 3,811 unique firms.

3.2 Cybersecurity Breaches

We collect data on cybersecurity breaches from the Audit Analytics Cybersecurity Database, which records all cyberattack incidents disclosed by publicly listed firms since 2010. Our initial pool of cybersecurity breaches includes 1,374 cyberattack incidents disclosed by public firms between 2010 and 2021. By merging these breach records with our sample firms, we identify 674 cyberattacks that occurred within our sample firms covered by both Compustat and BoardEx. After excluding firm-years with missing values in variables for the baseline regressions, 428 unique

cyberattack incidents across 378 firm-years are matched to our final sample.

The Audit Analytics Cybersecurity Database provides detailed information on each cyberattack, including attack methods, number of records breached (if available), and the duration of the incident. Cyberattacks are classified into different categories based on their attack methods: phishing, malware (including ransomware), misconfiguration, unauthorized access, and attacks of an undisclosed nature. These categories are not mutually exclusive, as a single cyberattack can involve multiple methods (e.g., phishing combined with malware). Among cyberattacks with known types in our sample, malware attacks are the most common, accounting for 25.4% of incidents, followed by unauthorized access (18.4%) and phishing attacks (16.3%).

We compute our dependent variable as the total number of cybersecurity breaches (*Breach*) experienced by a firm in year *t*. We also compute a series of dependent variables denoting the number of each type of cyberattack experienced by a firm in year *t*: phishing (*Phishing*), malware including ransomware (*Malware*), misconfiguration (*Misconfigure*), unauthorized access (*Unauthorized*), and breaches of undisclosed nature (*Unknown*), as represented in Equation (1):

$$Breach_{i,t} = \begin{pmatrix} Phishing_{i,t} \\ Malware_{i,t} \\ Misconfiguration_{i,t} \\ Unauthorized_{i,t} \\ Unknown_{i,t} \end{pmatrix} \quad (1)$$

To measure breach severity, we employ two empirical proxies that capture the number of records breached and the financial costs of the breach, as disclosed by the firm. *Records_Breach* is calculated as the natural logarithm of the aggregated number of records breached across all cybersecurity incidents during year *t*, serving as a measure of the magnitude of breaches. *Cost_Breach* represents the total financial cost of all breaches disclosed by the firm in year *t*.[1] We

[1] If multiple breaches occur in year *t*, we compute the aggregated number of records and financial costs. If no breaches occur in year *t*, these variables are assigned a value of zero.

also compute the scale and costs associated with each individual type of cybersecurity breach.

3.3 Director IT Expertise

We collect data on director education from BoardEx. To identify directors with IT-related degrees, we search for relevant keywords in the names of all degrees held by each director, using the keyword dictionary as detailed in Appendix B. A director is classified as IT-educated if any of the keywords match at least one degree held by the director. Our key explanatory variable, *BoardIT*, is calculated as the proportion of directors with at least one IT-related degree in a given firm-year, scaled by the total number of directors on the board. We also compute lagged values of *BoardIT* for years *t*–1, *t*–2, and *t*–3 to capture the predictive power of past director IT expertise.

3.4 Regression Models

In our baseline model, we estimate ordinary least squares (OLS) regressions to predict cyberattack frequency, using the proportion of directors with IT expertise, as specified in Eqn. (2):

$$Breach_{i,t} = \alpha + \beta BoardIT_{i,t\,|\,t-1\,|t-2|\,t-3} + \gamma X_{i,t-1} + \theta Y_{i,t} + \varepsilon_{it} \quad (2)$$

where i and t index each firm-year. The dependent variable $Breach_{i,t}$ represents the total number of cyberattacks against firm i in year t. We also employ a series of alternative dependent variables, $Phishing_{i,t}$, $Malware_{i,t}$, $Misconfiguration_{i,t}$, $Unauthorized_{i,t}$, $Unknown_{i,t}$, each denoting the number of the specific type of cyberattacks against firm i in year t.

$X_{i,t}$ represents the vector of control variables. Financial variables include firm size proxied by the natural logarithm of total assets (*LnTA*), profitability proxied by return on assets (*ROA*), sales growth (*Salesgrowth*), firm age (*LnAge*) measured as the natural logarithm of the number of years since the firm's IPO, supplemented by the number of years since its first appearance in Compustat, Tobin's Q (*TobinQ*), debt-to-equity ratio (*Leverage*), and financial distress proxied by Altman's Z score (*Altmanz*). To capture the nature of firms' operations, we control for capital expenditure

(*Capex*), research and development expenditure (*R&D*), and labor intensity (*Intensity*) as the number of employees scaled by total firm assets. We further control for corporate governance factors, specifically institutional monitoring proxied by institutional blockholding (*Blockhold*) and board monitoring strength, measured by board size (*Boardsize*) (Yermack, 1996), independence (*Independence*) (Rosenstein & Wyatt, 1990), and gender diversity (*Female*) (Adams & Ferreira, 2009). All variables are defined in Appendix A. Continuous variables are winsorized at the 1st and 99th percentiles. $Y_{i,t}$ represents year and industry fixed effects, measured by two-digit SIC codes, consistent with the methodology employed by Kamiya et al. (2021).

3.5 Endogeneity

Endogeneity is a potential issue given the nonrandom selection of directors onto boards. We employ several empirical methodologies aimed at alleviating specific sources of potential endogeneity. To address potential selection bias, which may arise because firms that choose to appoint IT experts may differ from those that do not, we utilize a two-stage Heckman Selection Model, employing an instrumental variable (IV) in the first stage. Our instrument exploits the staggered adoption of data breach disclosure laws across various U.S. states as an exogenous shock to the supply of IT-expert directors in different regions. Specifically, we interact a dummy variable *Post*—which equals one if a firm is headquartered in a state that has adopted data breach disclosure laws and zero otherwise—with the total number of unique IT-expert directors in that state (*IT_Availability*), which captures the local availability of IT-educated directors. This interaction term serves as our IV in the first stage of the Heckman Selection Model, generating the Inverse Mills Ratio for inclusion in the second-stage regressions, to address potential selection bias.

Endogeneity could also arise from industry differences, as some industries may be inherently more susceptible to cyberattacks due to the nature of their operations; if these firms are also more

or less likely to appoint IT-expert directors, this could give rise to a spurious relationship between our independent and dependent variables. To mitigate this concern, we not only include industry fixed effects in all regression models (Kamiya et al., 2021), but we also conduct a robustness test using industry-adjusted dependent and independent variables, which enables comparison of firms with their industry peers (Liu et al., 2020). Furthermore, reverse causality may arise if firms facing greater cybersecurity threats intentionally appoint more IT-educated directors to combat these risks. It is important to note that this source of endogeneity would likely bias the results against our hypothesis, which predicts a negative relationship between board IT expertise and cybersecurity breaches. Nevertheless, we follow prior research (Dittmann et al., 2010; Harford et al., 2008; Joecks et al., 2013) by using lagged regressions, where our independent variable *BoardIT* is measured at years *t*–1, *t*–2, and *t*–3. Using past board IT expertise to predict subsequent breaches in year *t* helps reduce the likelihood of the results being driven by reverse causality.

4 EMPIRICAL RESULTS

4.1 Descriptive Statistics

Table 1 presents descriptive statistics for the 22,106 firm-year observations used in our baseline analysis. On average, 1.9 percent of firm-years report at least one cybersecurity breach, a rate consistent with the findings of Kamiya et al. (2021). When disaggregated by types of attacks, 0.3 percent of firm-years experience phishing attacks, 0.5 percent experience malware attacks, 0.2 percent misconfiguration attacks, 0.4 percent unauthorized access, and 0.6 percent report breaches of undisclosed nature. The average proportion of directors on the board is 0.1 percent, indicating that the vast majority of firms do not have any IT experts on their boards.

[Insert Table 1]

Table 2 reports the industry breakdown based on Standard Industry Classification (SIC) codes.

As shown in Column (2), Agriculture, Forestry, and Fishing exhibit the highest breach incidence, with 4.3 percent of firm-years affected, followed by Services (3.5 percent) and Retail Trade (3.3 percent). Column (3) reveals that Service and Finance industries both have the highest average board IT representation at 0.9 percent, whereas Agriculture, Retail, and Nonclassifiable industries have no board IT representation. These industry-level statistics suggest that board IT expertise is not systematically correlated with cyberattack frequency at the industry level, contrary to the potential endogeneity concern that board IT expertise and cybersecurity risk are jointly driven by industry characteristics. Specifically, industries with both high and low board IT representation, such as Service and Agriculture, both experience high breach incidence, reinforcing the absence of industry-driven patterns between board IT expertise and cyberattack vulnerability.[2]

Table 3 reports the Pearson correlation matrix for all independent variables in our baseline regression in Eqn. (1). There is no pairwise correlation coefficient exceeding 0.65, indicating that multicollinearity is not a significant concern in our research design (Hair et al., 2010).

[Insert Table 2 and Table 3]

4.2 Board IT Expertise and Cybersecurity Breaches

4.2.1 Baseline Regression Analyses

Table 4 reports the results from OLS regressions using board IT expertise (*BoardIT*) to predict cybersecurity breach incidence, specifically total breaches in Columns (1)–(2) and individual attack types in Columns (3)–(12). We report results from both parsimonious models using only *BoardIT* with industry- and year-fixed effects, and full models including all control variables. The findings show that IT expertise is significantly associated with a lower incidence of certain types of cyberattacks, specifically phishing, misconfiguration, and unauthorized access attacks, though

[2] Nevertheless, to further alleviate concerns over potential industry-level endogeneity, in addition to including industry fixed effects across all regressions models, we conduct industry-adjusted analyses in Section 4.2.2 (Table 7).

not the total number of breaches in Columns (1)–(2).

BoardIT is negative and significant in predicting phishing attacks, with coefficients of –0.028 (p<0.01) and –0.018 (p<0.01) in Columns (3) and (4), respectively. *BoardIT* also significantly predicts fewer misconfiguration attacks, with estimated coefficients of –0.019 and –0.011 (p<0.01 and p<0.05 in Columns (7)–(8), respectively). In Columns (9)–(10), the coefficients of *BoardIT* are negative and significant in predicting unauthorized access attacks (–0.036 and –0.030, p<0.01). These results indicate that a higher proportion of directors with IT expertise is associated with significantly fewer phishing, misconfiguration, and unauthorized access incidents.

These results are not only statistically but also economically significant. For phishing attacks, the coefficient of –0.018 in Column (4) indicates that an increase in *BoardIT* by one standard deviation is linked to a reduction in *Phishing* equivalent to 6% of its sample mean.[3] For misconfiguration attacks, the coefficient of *BoardIT* (–0.011) in Column (8) suggests that a one-standard-deviation increase in board IT expertise is linked to a 5.5% reduction in misconfiguration attacks.[4] For unauthorized access attacks, the coefficient of –0.030 in Column (10) indicates that a one-standard-deviation increase in board IT expertise is equivalent to a 7.5% reduction of unauthorized access incidents.[5] Nevertheless, *BoardIT* is not significant in predicting the total frequency of cyberattacks (in Columns (1)–(2)), malware attacks (in Columns (5)–(6)), or those of unknown types (in Columns (11)–(12)).

Consistent with H1, our findings show that board IT expertise is significantly associated with lower incidences of specific cyberattacks, namely phishing, misconfiguration, and unauthorized access. Importantly, these types of cyberattacks can be mitigated through socio-technical solutions,

[3] This is calculated as 0.018 (estimated coefficient of *BoardIT* in Column (4), Table 4) x 0.010 (standard deviation of *BoardIT*) / 0.003 (sample mean of *Phishing*) = 6%.
[4] 0.011 (estimated coefficient) x 0.010 (standard deviation of *BoardIT*) / 0.002 (mean of *Misconfiguration*) = 5.5%.
[5] 0.030 (estimated coefficient) x 0.010 (standard deviation of *BoardIT*) / 0.004 (mean of *Unauthorized Access*) = 7.5%.

such as employee phishing awareness training, improving internal communication on security protocols and configurations, and strengthening password policies. This evidence suggests that IT-expert directors are more effective in improving "soft" cyber defenses by adopting socio-technical measures rather than enhancing "hard" defenses through upgrading technical infrastructure, which would be needed to address more technically sophisticated cyberattacks such as malware attacks.

Among the control variables, firm size (*LnTA*) is consistently positive and significant in predicting breach frequency across all attack types, suggesting that larger firms are more likely to be targeted. R&D expenditure is positively associated with total breach frequency ($p<0.10$) in Column (2), as well as malware attacks ($p<0.05$) in Column (6), indicating that firms with valuable R&D are more likely to be targeted in malware attacks. Institutional blockholding (*Blockhold*) exhibits a negative relationship with total breaches, as well as malware, misconfiguration, and undisclosed type of attacks ($p<0.05$ or better), suggesting that firms with greater institutional ownership are better positioned to defend against these types of attacks through cyber governance.

[Insert Table 4]

Table 5 presents OLS regression results estimating breach frequency using *lagged* board IT expertise, measured at years *t*–1, *t*–2, and *t*–3.[6] The results confirm those reported in Table 4, showing that the proportion of IT-expert directors is significantly associated with lower incidences of phishing, misconfiguration, and unauthorized access attacks, but not the total number of breaches or malware attacks. In Column (4), the coefficient of $BoardIT_{t-3}$ (–0.018, $p<0.01$) indicates that board IT expertise in year *t*–3 is significantly associated with a lower frequency of

[6] We report the regressions predicting total breaches (*Breach*) in Columns (1)–(3), phishing attacks (*Phishing*) in Columns (4)–(6), malware attacks in Columns (7)–(9), misconfiguration attacks in Columns (10)–(12), and breaches involving unauthorized access in Columns (13)–(15). The regression models predicting the number of unknown types of cyberattacks are untabulated for succinctness, as the coefficients of *BoardIT* (lagged at years *t*–1, *t*–2, and *t*–3) are not statistically significant in predicting the incidence of cyberattacks of unknown types.

subsequent phishing attacks in year *t*; similarly, the coefficients of $BoardIT_{t-2}$ and $BoardIT_{t-1}$ are significant and negative (Columns (5)–(6), $p<0.05$), suggesting that board IT expertise in previous years is associated with fewer subsequent phishing attacks. Furthermore, lagged *BoardIT* during *t*–3, *t*–2, and *t*–1 is also significant in predicting fewer misconfiguration attacks (Columns (10)–(12), $p<0.05$) and breaches involving unauthorized access (Columns (13)–(15), $p<0.01$).[7]

These findings further support H1 by demonstrating the persistent role of board IT expertise, highlighting its long-term value in enhancing cybersecurity resilience, particularly against less technically sophisticated cyberattacks—such as phishing, misconfiguration, and unauthorized access—that require socio-technical solutions.

[Insert Table 5]

4.2.2 Heckman Selection Model

We employ a series of empirical approaches aimed at alleviating endogeneity concerns, given the nonrandom selection of IT experts onto corporate boards. One potential source of endogeneity is the self-selection of IT-educated directors into certain types of firms, which may be inherently exposed to higher or lower levels of cybersecurity risks. To combat this endogeneity concern, we employ a Heckman Selection Model with an instrumental variable (IV) in the first-stage regression.

The IV captures the state-level availability of local IT-expert directors following the adoption of data breach disclosure laws in a firm's headquarter state. By exploiting the staggered adoption

[7] As an additional robustness test, we match the timing of the presence of IT directors with the year in which the cybersecurity breach *started* (instead of the year in which the incident was *reported*, as used in the baseline regressions). Given potential lags between the onset of a breach and its disclosure, board compositions may have changed during this period. This approach provides more accurate timing for observing the presence of IT directors, allowing us to examine their preventative role prior to a breach. In untabulated results, the coefficients and statistical significance of key independent variables remain consistent with those reported in Tables 4–5. Specifically, board IT expertise is significantly and negatively associated with phishing, misconfiguration, and unauthorized access incidents, reinforcing our baseline findings in support of H1. A limitation of this approach is that some reported breach incidents do not have a recorded starting date (many are unknown due to the practical difficulty for firms to identify an accurate starting date of the breach)—these missing values result in a reduced sample size of matched breach incidents. Therefore, we conduct this analysis as a robustness test rather than as a replacement for our baseline analysis.

of data breach disclosure laws across different U.S. states, the IV captures both temporal and geographical variations across states and years. The IV is calculated as an interaction term between *Post*, a binary variable equal to one if a firm's headquarter state has adopted a breach disclosure law by year *t* and zero otherwise, and *IT_Availability*, computed as the number of unique IT-expert directors serving on the boards of firms headquartered in that state in a given year.

The interaction term, *Post*×*IT_Availability*, represents the post-law adoption availability of IT-expert directors in the state in which the firm is headquartered. This IV satisfies the relevance criterion, because a greater supply of local IT-educated directors is expected to increase the likelihood for firms to appoint such individuals to their boards, especially following regulatory changes that heighten awareness of cybersecurity governance. This IV also meets the exclusion restriction, given the exogenous and staggered nature of regulatory adoptions of data breach disclosure laws, whose timing is inherently unpredictable due to uncertainties in the legislative process. For these reasons, *Post*×*IT_Availability* constitutes a valid instrument. In the second-stage regression, we include the Inverse Mills Ratio calculated from the first-stage Heckman model to account for potential selection bias. The results are reported in Table 6.

In Table 6, results from the Heckman Selection Model support our baseline findings, reinforcing the role of board IT expertise in reducing corporate vulnerabilities to phishing, misconfiguration, and unauthorized access attacks. Consistent with the baseline results, the coefficients of *BoardIT* remain negative and significant in predicting the frequency of phishing attacks ($p<0.01$, Columns (5)–(8)). Similarly, board IT expertise is negatively and significantly associated with misconfiguration attacks ($p<0.05$ or better, Columns (13)–(16)) and unauthorized access incidents ($p<0.01$, Columns (17)–(20)). The inclusion of the Inverse Mills Ratio further accounts for potential selection bias. Its coefficient is not statistically significant in the second-

stage regressions, suggesting that our baseline results are not driven by selection bias. Overall, the Heckman Selection Model provides evidence that confirms our baseline results in support of H1, demonstrating that the presence of IT expertise on corporate boards has a meaningful impact in reducing firms' vulnerability to cybersecurity threats.

[Insert Table 6]

4.2.3 Industry-Adjusted Analysis

Another potential source of endogeneity concerns arises from the possibility that IT-expert directors are concentrated in certain industries that are inherently more or less susceptible to cyberattacks. This industry-driven endogeneity may result in a spurious relationship between board IT expertise and corporate cybersecurity risk. To combat this source of endogeneity, we compute industry-adjusted dependent and key independent variables, enabling comparisons of firms' board IT expertise and cyberattack frequency relative to their industry peers. Specifically, we calculate $BoardIT_{(\text{industry-adjusted})}$ as the proportion of IT-expert directors on the board minus the industry mean of *BoardIT*, using two-digit SIC codes. Similarly, we compute $Breach_{(\text{industry-adjusted})}$ as the number of breaches in year *t* adjusted by the industry average number of breaches within the two-digit SIC industry. Using the same methodology, we compute industry-adjusted measures of each type of cyberattack. We then re-estimate our baseline regressions using the industry-adjusted dependent and key independent variables. The results are reported in Table 7.

Consistent with our baseline findings, the coefficients of $BoardIT_{(\text{industry-adjusted})}$—including contemporaneous and lagged up to three years—remain negative and significant in predicting the industry-adjusted frequency of phishing attacks (Columns (5)–(8), $p<0.01$), misconfiguration attacks (Columns (13)–(16), $p<0.05$), and unauthorized access incidents (Columns (17)–(20), $p<0.01$). Overall, the industry-adjusted analysis corroborates our baseline findings by confirming

the significant predictive power of board IT expertise over the frequency of cyberattacks involving phishing, misconfiguration, and unauthorized access, after accounting for industry-level variations. These results further contribute to alleviating concerns about potential industry-level endogeneity.

[Insert Table 7]

4.2.4 Additional Analyses

We conduct additional analyses to verify the robustness of our findings by employing both alternative sampling and different model specifications. First, since the presence of IT-expert directors is relatively rare in our sample, we adopt a random sampling approach to address the imbalance between the number of treatment and control observations. We construct an augmented sample by including all treatment observations, with at least one IT-expert director, and randomly selecting 75 percent of the control observations with no IT-expert directors to re-estimate Eqn. (2). The regression results confirm the robustness of our findings. In untabulated results, the negative coefficients of *BoardIT* (lagged and contemporaneous) remain statistically significant in predicting phishing attacks ($p<0.05$ or better), misconfiguration attacks ($p<0.05$), and unauthorized access incidents ($p<0.01$). These results confirm that, consistent with H1, IT expertise on the board is an important predictor of reduced exposure to specific types of cybersecurity threats.

As an additional robustness test, we employ Tobit models in lieu of OLS regression models, given the left-censoring in the dependent variable containing a large number of zero values. In untabulated results, the estimated coefficients of *BoardIT* remain consistent in both economic magnitude and statistical significance with our baseline results in Tables 4 and 5. Specifically, *BoardIT* measured in years t, t–1, t–2, and t–3 is consistently negative and significant in predicting phishing, misconfiguration, and unauthorized access attacks ($p<0.05$ or better).

4.3 Channel Analyses

We explore the channels through which directors with IT expertise may enhance a firm's resilience to cyberattacks. Specifically, we investigate two potential mechanisms: corporate cybersecurity culture and IT expenditure. We posit that IT-expert directors are better equipped to identify and assess potential cybersecurity vulnerabilities. This technical expertise enables them to contribute to risk mitigation and improve a firm's cybersecurity practices in two alternative ways: advocating for increased IT spending to strengthen technical defenses or by promoting a corporate culture of heightened cybersecurity awareness, which enhances socio-technical defenses. In this section, we explore each mechanism in turn.

4.3.1 Corporate Cybersecurity Culture

Our first channel analysis focuses on corporate cybersecurity culture, measured by the presence of cybersecurity-related words in 10-K filings. Cybersecurity culture encompasses intangible cyber defenses within a firm, such as adopting cybersecurity policies (Afshari-Mofrad et al., 2024) and enhancing threat awareness (Li et al., 2023), both contributing to reducing cybersecurity risk. We expect that IT-expert directors can foster a robust cybersecurity culture by increasing corporate attention to cybersecurity threats and defenses, thereby enhancing the firm's ability to prevent breaches.

To measure cybersecurity culture, we utilize a novel empirical approach by analyzing the text of 10-K reports filed with the Securities and Exchange Commission (SEC). Following Calderon and Gao (2021), we conduct wildcard searches for cybersecurity-related language within each 10-K report, using a dictionary of keywords: cyber security, cyber-security, cybersecurity, security measure*, authentication, information security, network security, computer security, computer virus*, security incident*, cyber attack, cyber-attack, cyberattack, security breach*, network breach*, computer breach*, hacker, encryption, intrusion, denial of service, security monitoring,

access control, security management, infosec, computer intrusion*, security expenditure* (where * denotes regular expressions (Regex) used to accommodate ambiguous content). We compute *Cyber_Culture* as the number of cybersecurity-related words found in each 10-K filing, scaled by the total word count of the 10-K report (expressed as percentage points). A higher value of *Cyber_Culture* indicates a stronger culture marked by greater attention to cybersecurity issues.

In Panel A, Table 8, we estimate OLS regressions using lagged *BoardIT* (measured at *t*–3, *t*–2, and *t*–1, in turn) as the key explanatory variable to predict *Cyber_Culture* at year *t*–1. In Columns (1)–(3), the estimated coefficients of *BoardIT* are consistently positive and significant in predicting *Cyber_Culture* ($p<0.01$), indicating that board IT expertise is positively associated with corporate cybersecurity culture. These results support the notion that IT-expert directors contribute to enhancing a firm's cybersecurity culture by directing more attention to cybersecurity-related issues.

In Panel B, Table 8, we re-estimate the baseline regressions predicting cyberattack frequency using the interaction term between *BoardIT* and *Cyber_Culture*, which allows us to examine how cybersecurity culture mediates the relationship between board IT expertise and cyberattack frequency. The coefficient of *BoardIT*×*Cyber_Culture* is significant in predicting fewer phishing, misconfiguration, and unauthorized access attacks. Specifically, for phishing attacks, the interaction term is negative and significant ($p<0.10$ in Column (4), $p<0.05$ in Columns (5)–(6)). Similarly, for misconfiguration attacks, *BoardIT*×*Cyber_Culture* is negative and significant in Column (10) ($p<0.10$) and Columns (11)–(12) ($p<0.05$). For unauthorized access attacks, the interaction term remains significant across Columns (13)–(15) ($p<0.01$). These results suggest that a stronger cybersecurity culture enhances the ability of IT-expert directors to reduce cyberattack frequency, particularly for phishing, misconfiguration, and unauthorized access attacks.

Overall, our evidence shows that IT experts in the boardroom foster a stronger corporate

cybersecurity culture, which in turn strengthens the relationship between board IT expertise and lower breach frequency. These findings highlight cybersecurity culture as a key mechanism through which IT-expert directors can reduce firm vulnerability to phishing, misconfiguration, and unauthorized access attacks—threats that require socio-technical countermeasures rather than purely technical defenses. Unlike malware attacks, which demand technical and systematic defenses such as firewalls and intrusion detection systems, phishing and unauthorized access attacks can be mitigated through socio-technical solutions, such as employee training to increase awareness of phishing risks and promoting stronger password management practices to prevent credential stuffing. These socio-technical measures are more likely to be implemented in firms with a robust cybersecurity culture. In line with our baseline findings, the evidence in Table 8 further supports the notion that IT-expert directors help mitigate corporate cybersecurity risks by fostering a strong cybersecurity culture and focusing corporate attention on cybersecurity issues, particularly effective in thwarting cyberattacks that rely on socio-technical defenses.

[Insert Table 8]

4.3.2 Corporate IT Expenditure

We next examine an alternative mechanism for reducing cybersecurity risk by increasing corporate IT expenditure. Directors with IT expertise may advocate for greater IT spending to fund upgrades or expansions of technical cybersecurity infrastructure to protect the firm against cyber threats. Since firms do not typically report IT expenses separately (Jee-Hae et al., 2011), we use selling, general, and administrative (SG&A) expenses, scaled by total sales, as a proxy for IT expenditure, following prior research that documents a high correlation between IT expenditure and SG&A expenses (Mithas & Rust, 2016; Mitra & Chaya, 1996).

Our channel analysis consists of two steps: first, we examine whether board IT expertise

(*BoardIT* measured in years *t*–3, *t*–2, and *t*–1) is positively associated with SG&A expenses in year *t*–1; second, we use the interaction term between *BoardIT* and *SGA* to predict the frequency of cybersecurity breaches. As reported in Panel A, Table 9, the coefficients of board IT expertise are not statistically significant in predicting SG&A expenses, providing no evidence to suggest that IT-expert directors demand increased IT spending. In Panel B, Table 9, the interaction term between *BoardIT* and *SGA* is significant and negative in predicting phishing attacks ($p<0.10$), but only when *BoardIT* is measured in year *t*–1 in Column (6). For misconfiguration and unauthorized access attacks, the interaction term *BoardIT*×*SGA* is consistently negative and significant ($p<0.05$ and $p<0.01$ in Columns (10)–(12) and (13)–(15), respectively).

These results suggest that, while IT expenditure does not mediate the relationship between board IT expertise and cyberattack frequency, it moderates this relationship by enhancing the ability of board IT expertise to reduce specific types of cyberattacks, particularly misconfiguration and unauthorized access attacks. Both misconfiguration and unauthorized access attacks require a combination of socio-technical solutions and technical defenses. Misconfiguration can be prevented through staff training (a form of socio-technical defense) and regular cybersecurity audits—a technical solution requiring systematic implementation. Similarly, unauthorized access can be mitigated by both socio-technical improvements, such as stronger password policies, and technical defenses such as multifactor authentication (MFA). Our results show that IT expenditure amplifies the role of IT-expert directors in reducing corporate vulnerability to misconfiguration and unauthorized access attacks, as technical defenses such as cybersecurity audits and MFA require financial investment and depend on the availability of IT budgets. Our findings are consistent with prior research evidence that IT security investment is a necessary but not sufficient condition to enhance organization cybersecurity, requiring substantive rather than symbolic

adoptions to achieve effective improvements (Angst et al., 2017).

Overall, our channel analyses reveal that improving corporate cybersecurity culture serves to mediate the relationship between board IT expertise and reduced cyberattacks. The presence of IT-expert directors fosters a culture of greater attention and awareness to cybersecurity issues, enabling the firm to reduce phishing, misconfiguration, and unauthorized access attacks. In contrast, IT expenditure only moderates but does not mediate this relationship: while directors with IT-expert directors do not advocate for greater IT spending, the availability of funds enhances the role of board IT expertise in reducing misconfiguration and unauthorized access attacks.

[Insert Table 9]

4.4 Board IT Expertise and Severity of Cyberattacks

We next examine the relationship between board IT expertise and the *severity* of cyberattacks, using two empirical proxies: [1] breach scale measured by the number of records breached and [2] financial costs of the breach. Accordingly, we compute two sets of dependent variables: First, *Records_Breach* is computed as the natural logarithm of the total number of records breached in a given firm-year. Additionally, we compute five variables—*Records_Phishing*, *Records_Malware*, *Records_Misconfiguration*, *Records_Unauthorized*, and *Records_Unknown*—representing the natural logarithm of the number of records breached in individual attack types: phishing, malware, misconfiguration, unauthorized access, and undisclosed types, respectively. Second, we compute *Cost_Breach* as the natural logarithm of the pecuniary cost of the breach, disclosed by the firm, for all cyberattacks in a given firm-year, along with five variables for the individual types of cyberattacks. If a firm experiences multiple breaches in a given year, we aggregate the number of records breached and costs incurred. If no cyberattack occurs in a given year, the value of *Records_Breach* and *Cost_Breach* is set to zero. We re-estimate Eqn. (2) using each severity

variable in turn as the dependent variable. The results are reported in Table 10.

In Panel A, the results show a statistically significant relationship between board IT expertise and *Records_Breach*. The coefficients of *BoardIT* measured at *t*, *t*–1, *t*–2, and *t*–3 are consistently negative and significant ($p<0.01$) in Columns (1)–(4), indicating that firms with greater IT expertise on their boards experience fewer records breached across all cyberattacks. Among individual types of attacks, misconfiguration and unauthorized access show the most significant relationship between board IT expertise and breach severity ($p<0.05$ and $p<0.01$, respectively). The negative coefficient of *BoardIT* indicates that board IT expertise is associated with fewer records compromised in misconfiguration and unauthorized access attacks. These results support H2 by demonstrating that board IT expertise helps mitigate the scale of cybersecurity breaches.

Panel B reports the regression results estimating the financial costs of cyberattacks.[8] While *BoardIT* is not statistically significant in predicting the total costs of all cyberattacks (*Cost_Breach*) in Columns (1)–(4), it is negative and significant in predicting the costs of phishing attacks (*Cost_Phishing*) in Columns (5)–(8) ($p<0.10$ or better), unauthorized access breaches (*Cost_Unauthorized*) in Columns (15)–(16) ($p<0.10$), and cyberattacks of undisclosed nature (*Cost_Unknown*) in Columns (17)–(20) ($p<0.05$). These results suggest that the relationship between board IT expertise and the financial costs of breaches is context-dependent and significant only in certain types of cyberattacks, such as phishing and misconfiguration.[9]

[8] In Panel B, the results from the regressions predicting the pecuniary costs of misconfiguration attacks (*Cost_Misconfiguration*) are omitted due to the lack of sufficient variation in the dependent variable.

[9] As an additional robustness test, we align the timing of observing IT director presence on the board with the year in which a cybersecurity breach was *discovered* (instead of the year in which it was *reported*, as shown in Table 10). This analysis allows us to pinpoint the precise timing for observing board IT expertise when it matters the most in the discovery and containment of cybersecurity breaches. We measure board IT expertise in year *t* (the year of breach discovery) and lagged years *t*–1 through *t*–3. In untabulated results, the regression coefficients and statistical significance of our key independent variable, *BoardIT*, remain consistent with those reported in Table 10, confirming our findings. A limitation of this analysis is that not all breaches have a recorded discovery date; these missing values reduce the number of matchable incidents in our sample. Therefore, while we conduct this timing-matched analysis as a robustness test, we do not replace our original baseline analysis.

Overall, our empirical evidence supports H2 by showing that greater IT expertise on boards is associated with lower severity of cyberattacks, both in terms of breach scale and financial costs. As firms navigate increasingly complex cyber threats and challenges, our findings highlight the nuanced role of IT-expert directors, not only in reducing the *incidence* of cybersecurity breaches but also in mitigating the scale of breaches when they occur.

[Insert Table 10]

4.5 Post-Cyberattack Changes in Board IT Expertise

This section explores the relationship between cyberattacks and subsequent changes in board IT expertise. In light of our previous findings linking board IT expertise to reduced cyberattacks, we investigate whether firms increase IT expertise on their boards post-breach in an attempt to improve future cyber resilience. We examine changes in the number of IT directors on the board (*ΔBoardIT*) over three periods from year *t* to years *t*+1, *t*+2, and *t*+3. Table 11 reports OLS regression results estimating *ΔBoardIT* during *t*(0,+1), *t*(0,+2), and *t*(0,+3), in turn, using the cyberattack frequency in year *t* as the independent variable while controlling for the severity of cyberattacks, in addition to all control variables in Eqn. (2).

Table 11 shows a significant positive relationship between cybersecurity breaches in year *t* and a subsequent increase in IT-expert directors. In Columns (1)–(3), the coefficient of total breaches in year *t* (*Breach*) is positive and significant in predicting changes in IT directors across all periods *t*(0,+1), *t*(0,+2), and *t*(0,+3) ($p<0.05$, $p<0.01$, and $p<0.01$, respectively). This indicates that firms are more likely to increase board IT experts following cyberattacks, consistent with the expectation that firms respond to attacks by enhancing cyber governance and oversight capabilities.

We also examine individual breach types in predicting the change in board IT expertise. The results in Columns (4)–(6) provide nuanced insights: the number of malware attacks in year *t*

(*Malware*) is positive and significant in predicting *ΔBoardIT*, but only across longer time periods *t*(0,+2) and *t*(0,+3) ($p<0.10$ and $p<0.05$ in Columns (5)–(6), respectively). Misconfiguration attacks (*Misconfiguration*) and unauthorized access incidents (*Unauthorized*) both significantly predict a positive change in board IT expertise over periods *t*(0,+1) and *t*(0,+2) ($p<0.10$). Finally, attacks of undisclosed types (*Unknown*) are significantly associated with an increase in board IT expertise over the longer-term periods of *t*(0,+2) and *t*(0,+3) ($p<0.05$ and $p<0.01$, respectively).

These results shed light on firms' governance responses to cybersecurity breaches, which vary across distinct types of attacks. While our evidence supports H3 by showing a general increase in board IT expertise during the one-, two-, and three-year periods following cyberattacks, we observe notable differences across breach types. Malware attacks prompt the most significant response to increase board IT expertise, followed by misconfiguration and undisclosed attacks. These varied responses may be attributable to malware attacks requiring more *technical* defenses (unlike phishing attacks, which can be mitigated by improving employee awareness as a socio-technical defense); while misconfiguration attacks also require systematic checks and audits, particularly in cloud environments. The perception that these attacks demand more technical-savvy solutions may motivate firms to increase board IT expertise to strengthen oversight capabilities.

[Insert Table 11]

4.6 Past Breaches, Changes in Board IT Expertise, and Cybersecurity Risk

We further investigate whether post-breach increases in board IT expertise can reduce subsequent cyberattacks. Specifically, we estimate OLS regressions to predict the number of cybersecurity breaches in year *t*, using changes in board IT expertise and firms' previous breach experience as independent variables: *ΔBoardIT* is measured over the preceding three-year *t*(–3,0), two-year *t*(–2,0), and one-year *t*(–1,0) periods in turn. Firms' previous breaches are captured by

the cumulative number of past breaches experienced by the firm in all years in the sampling period prior to year *t*. *Prev_Breach* represents the total number of all previous cyberattacks, while *Prev_Phishing*, *Prev_Malware*, *Prev_Misconfiguration*, *Prev_Unauthorized*, and *Prev_Unknown* capture the cumulative number of each type of previous cyberattacks experienced by the firm.

As reported in Table 12, the coefficient of $\Delta BoardIT_{t(-3,0)}$ is negative and significant ($p<0.01$) in Column (1), indicating that increased board IT expertise over the preceding three years is linked to fewer total breaches in year *t*. In Columns (2)–(3), changes in board IT expertise over *t*(–2,0) and *t*(–1,0) are also significant in predicting fewer breaches ($p<0.05$). These results support H4 by demonstrating that increases in board IT expertise are linked to reduced likelihood of subsequent cyberattacks. Previous breaches are generally associated with a higher incidence of total breaches ($p<0.01$), unauthorized access incidents (p<0.05), and breaches of undisclosed types ($p<0.01$), consistent with the view that attackers often repeatedly target firms that have been compromised.

When disaggregating individual types of breaches, we find that the impact of increased board IT expertise varies by cyberattack methods. For malware attacks, increased board IT expertise is significantly linked to fewer subsequent breaches, regardless of whether the increase occurs over the one-, two-, or three-year period ($p<0.05$ or better in Columns (7)–(9)). In contrast, for phishing attacks, increased board IT expertise over the three-year period is the only significant predictor of reduced attack frequency (–0.002, $p<0.01$), but not over the one- and two-year periods. This suggests that the effectiveness of board IT expertise in mitigating cybersecurity risks is not immediate but takes time to manifest over longer periods. Similarly, changes in board IT over the three-year and two-year periods are associated with fewer instances of unauthorized access and undisclosed types of breaches ($p<0.05$ or better in Columns (13)–(14) and $p<0.10$ in Columns (16)–(17), respectively). These results show that while increasing board IT expertise is linked to

reducing overall breaches, such improvements are not uniform across different types of attacks, with some more responsive than others to governance changes.

Our empirical evidence offers insights into the role of improving board IT expertise. First, we find that increased board IT expertise is linked to fewer subsequent cybersecurity breaches, supporting its effectiveness in enhancing firms' cybersecurity resilience. Second, while board IT expertise is important to reducing breaches, its impact varies across different cyberattack types, some of which are more responsive to governance changes than others. Third, increased board IT expertise exhibits stronger predictive power in reducing cybersecurity risk when observed over longer periods (e.g., three- or two-year periods, $t(-3, 0)$ or $t(-2, 0)$, compared to the shorter $t(-1, 0)$ period), highlighting the long-term nature of IT governance improvements, whose effects are non-instantaneous and manifest over time into improved outcomes.

Overall, we observe a learning effect from improvements in cybersecurity outcomes driven by enhanced board IT expertise. Building on our findings in Section 4.5, we show that firms are more likely to strengthen their board-level IT expertise in the wake of cybersecurity breaches, which improves subsequent cybersecurity outcomes. This supports the existence of a feedback loop that allows firms to learn from past cyberattack experiences to mitigate future risks. In this process, enhancing board IT expertise constitutes a key avenue to enable organizations to improve IT oversight and reduce vulnerability to future cyberattacks.

[Insert Table 12]

5 CONCLUSION

Firms face growing pressure to strengthen cybersecurity as an important aspect of corporate social responsibility (Opderbeck, 2017). This study investigates the role of director IT expertise in mitigating corporate cybersecurity risks across different stages of the breach lifecycle. Our

findings show that firms with a higher proportion of IT-expert directors experience fewer cyberattacks involving phishing, misconfiguration, and unauthorized access. These results support the view that directors with IT education contribute to a firm's cyber defense strategies, particularly during the prevention phase of cybersecurity breaches. Furthermore, we observe that board-level IT expertise is associated with lower breach severity, as evidenced by fewer compromised records and lower financial costs. This suggests that directors with IT expertise not only help prevent breaches but also mitigate the impacts when breaches do occur.

Additionally, our results reveal a post-cyberattack feedback loop, as conceptualized by Liu and Babar (2024), linking previous breach experiences to future improvements in cybersecurity resilience through organizational learning. We find that cyberattacks are linked to an increase in board IT expertise post-breach, and such changes are followed by significantly fewer subsequent breaches, indicating that firms adapt their governance structure in response to breaches by strengthening board cybersecurity oversight. Moreover, our disaggregation of different cyberattack methods provides nuanced insights: board IT expertise is most impactful in mitigating cyberattacks that require less technical sophistication, such as phishing, misconfiguration, and unauthorized access incidents, which can be reduced through raising awareness and improving communication and user practices. Our channel analyses confirm that IT expert directors contribute to cyber governance primarily by enhancing corporate cybersecurity culture, rather than by advocating for increased IT investments in technical defenses.

Our findings make multifaceted contributions to the growing literature on corporate cybersecurity risk, as well as the corporate governance literature on boards of directors—specifically director education—and research on remedial changes following governance failures. This study provides practical guidance to corporate executives, directors, investors, and

policymakers seeking to strengthen corporate resilience against cyberattacks. As cybersecurity is increasingly regarded as a form of corporate social responsibility, executives and directors must recognize that cybersecurity is no longer considered a mere technical issue, but a major business risk that requires informed oversight and management. Boards can proactively evaluate their composition and enhance their IT expertise, either through new appointments or training existing directors, to ensure that they possess sufficient IT literacy to guide the firms in navigating cybersecurity challenges. For investors, IT expertise on the board is a relevant factor to consider when evaluating a firm's cybersecurity risk in investment decisions.

Our findings also offer two important insights to policymakers: First, as the frequency and impact of cyberattacks continue to escalate, imposing increasing negative externalities, regulators may consider implementing policies or recommending best practices that encourage corporate transparency and disclosure regarding directors' competence in assessing and mitigating cybersecurity risks, particularly for firms that handle sensitive customer data. Second, even in the absence of regulatory intervention, firms engage in self-driven governance restructuring post-cyberattack to enhance board IT capabilities—such efforts can be further supported and encouraged by policy initiatives, such as providing incentives for boards to engage in IT and cybersecurity training programs, particularly those designed for directors. Training or certification programs focused on cybersecurity risk management, the role of IT in corporate strategy, and emerging cyber threats could help bridge interdisciplinary knowledge gaps, empowering directors to more effectively oversee cybersecurity governance. Overall, this study provides new insights on the important role of director IT expertise in the lifecycle of cybersecurity breaches, providing relevant and timely evidence to inform corporate and broader societal efforts to enhance the cybersecurity resilience of public companies.

REFERENCES

Adams, R. B., and Ferreira, D. (2009). Women in the Boardroom and Their Impact on Governance and Performance, *Journal of Financial Economics* 94(2), 291–309.

Adams, R. B., and Funk, P. (2012). Beyond the Glass Ceiling: Does Gender Matter?, *Management Science* 58(2), 219–235.

Afshari–Mofrad, M., Amrollahi, A., and Abedin, B. (2024). Adopt Agile Cybersecurity Policymaking to Counter Emerging Digital Risks, *MIS Quarterly Executive* 23(4), 371–388.

Agrawal, A., and Chadha, S. (2005). Corporate Governance and Accounting Scandals, *Journal of Law and Economics* 48(2), 371–406.

Aharony, J., Liu, C., and Yawson, A. (2015). Corporate Litigation and Executive Turnover, *Journal of Corporate Finance* 34, 268–292.

Aldasoro, I., Gambacorta, L., Giudici, P., and Leach, T. (2022). The Drivers of Cyber Risk, *Journal of Financial Stability* 60, 100989.

Amir, E., Levi, S., and Livne, T. (2018). Do Firms Underreport Information on Cyber-attacks? Evidence from Capital Markets, *Review of Accounting Studies* 23(3), 1177–1206.

Angst, C. M., Block, E. S., D'arcy, J., and Kelley, K. (2017). When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches, *MIS Quarterly* 4(3), 893–916.

Argyris, C., and Schön, D. (1978). *Organizational Learning: A Theory of Action Perspective*. Reading, MA Addison–Wesley.

Arthaud–Day, M. L., Certo, S. T., Dalton, C. M., and Dalton, D. R. (2006). A Changing of the Guard: Executive and Director Turnover Following Corporate Financial Restatements, *Academy of Management Journal* 49(6), 1119–1136.

Badolato, P. G., Donelson, D. C., and Ege, M. (2014). Audit Committee Financial Expertise and Earnings Management: The Role of Status, *Journal of Accounting and Economics* 58(2), 208–230.

Bana, S. H., Brynjolfsson, E., Wang, J., Steffen, S., and Xiupeng, W. (2025). Human Capital Acquisition in Response to Data Breaches, *MIS Quarterly* 49(1), 367–388.

Banker, R. D., and Feng, C. (2019). The Impact of Information Security Breach Incidents on CIO Turnover, *Journal of Information Systems* 33(3), 309–329.

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., and Khan, M. K. (2021). Ransomware: Recent Advances, Analysis, Challenges and Future Research Directions, *Computers & Security* 111, 102490.

Bilot, T., Madhoun, N. E., Agha, K. A., and Zouaoui, A. (2024). A Survey on Malware Detection with Graph Representation Learning, *ACM Computing Surveys* 56(11), Article 278.

Black, J., Ham, C. G., Kimbrough, M. D., and Yee, H. Y. (2021). Legal Expertise and the Role of Litigation Risk in Firms' Conservatism Choices, *The Accounting Review* 97(4), 105–129.

Bringhenti, D., Marchetto, G., Sisto, R., and Valenza, F. (2023). Automation for Network Security Configuration: State of the Art and Research Trends, *ACM Computing Surveys* 56(3), Article 57. pp. 51 – 37.

Brochet, F., and Srinivasan, S. (2014). Accountability of Independent Directors: Evidence from Firms Subject to Securities Litigation, *Journal of Financial Economics* 111(2), 430–449.

Burns, N., Minnick, K., and Raman, K. (2020). Director Industry Expertise and Voluntary Corporate Disclosure, *The Quarterly Journal of Finance* 10(03), 2050012.

Calderon, T. G., and Gao, L. (2021). Cybersecurity Risks Disclosure and Implied Audit Risks: Evidence from Audit Fees, *International Journal of Auditing* 25(1), 24–39.

Chatterjee, S., Gao, X., Sarkar, S., and Uzmanoglu, C. (2019). Reacting to the Scope of a Data Breach: The Differential Role of Fear and Anger, *Journal of Business Research* 101, 183–193.
Chen, C., Hartmann, C. C., and Gottfried, A. (2022). The Impact of Audit Committee IT Expertise on Data Breaches, *Journal of Information Systems* 36(3), 61–81.
Cheng, C. S. A., Huang, H. H., Li, Y., and Lobo, G. (2010). Institutional Monitoring through Shareholder Litigation, *Journal of Financial Economics* 95(3), 356–383.
Cram, W. A., Proudfoot, J. G., and D'Arcy, J. (2017). Organizational Information Security Policies: A Review and Research Framework, *European Journal of Information Systems* 26(6), 605–641.
Crutchley, C. E., Minnick, K., and Schorno, P. J. (2015). When Governance Fails: Naming Directors in Class Action Lawsuits, *Journal of Corporate Finance* 35, 81–96.
Dass, N., Kini, O., Nanda, V., Onal, B., and Wang, J. (2014). Board Expertise: Do Directors from Related Industries Help Bridge the Information Gap?, *The Review of Financial Studies* 27(5), 1533–1592.
Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., and Costabile, M. F. (2021). Human Factors in Phishing Attacks: A Systematic Literature Review, *ACM Computing Surveys* 54(8), Article 173.
Dietrich, C., Krombholz, K., Borgolte, K., and Fiebig, T. (2018). Investigating System Operators' Perspective on Security Misconfigurations, in: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. Toronto, Canada: Association for Computing Machinery, 1272–1289.
Dinger, M., and Wade, J. T. (2022). The Strategic Problem of Information Security and Data Breaches, *The Coastal Business Journal* 17(1), 1.
Dittmann, I., Maug, E., and Schneider, C. (2010). Bankers on the Boards of German Firms: What They Do, What They Are Worth, and Why They Are (Still) There, *Review of Finance* 14(1), 35–71.
Erkens, D. H., and Bonner, S. E. (2013). The Role of Firm Status in Appointments of Accounting Financial Experts to Audit Committees, *The Accounting Review* 88(1), 107–136.
Ettredge, M., Guo, F., and Li, Y. (2018). Trade Secrets and Cyber Security Breaches, *Journal of Accounting and Public Policy* 37(6), 564–585.
Falco, G., Eling, M., Jablanski, D., Weber, M., Miller, V., Gordon, L. A., Wang, S. S., Schmit, J., Thomas, R., Elvedi, M., Maillart, T., Donavan, E., Dejung, S., Durand, E., Nutter, F., Scheffer, U., Arazi, G., Ohana, G., and Lin, H. (2019). Cyber Risk Research Impeded by Disciplinary Barriers, *Science* 366(6469), 1066–1069.
Farber, D. B. (2005). Restoring Trust after Fraud: Does Corporate Governance Matter?, *The Accounting Review* 80(2), 539–561.
Ferris, S. P., Jandik, T., Lawless, R. M., and Makhija, A. (2007). Derivative Lawsuits as a Corporate Governance Mechanism: Empirical Evidence on Board Changes Surrounding Filings, *Journal of Financial and Quantitative Analysis* 42(2), 143–166.
Fich, E. M., and Shivdasani, A. (2007). Financial Fraud, Director Reputation, and Shareholder Wealth, *Journal of Financial Economics* 86(2), 306–336.
Fracassi, C., and Tate, G. (2012). External Networking and Internal Firm Governance, *The Journal of Finance* 67(1), 153–194.
Frank, M. L., Grenier, J. H., and Pyzoha, J. S. (2021). Board Liability for Cyberattacks: The Effects of a Prior Attack and Implementing the Aicpa's Cybersecurity Framework, *Journal of Accounting and Public Policy* 40(5), 106860.
Güner, A. B., Malmendier, U., and Tate, G. (2008). Financial Expertise of Directors, *Journal of Financial Economics* 88(2), 323–354.
Gwebu, K. L., Wang, J., and Wang, L. (2018). The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management, *Journal of Management Information Systems* 35(2), 683–714.

Hair, J. F., Black, W. C., Babin, B. J., and Anderson, R. E. (2010). *Multivariate Data Analysis*, (7th ed.). Upper Saddle River, NJ: Prentice Hall.
Hambrick, D. C. (2007). Upper Echelons Theory: An Update, *Academy of Management Review* 32(2), 334–343.
Hambrick, D. C., and Mason, P. A. (1984). Upper Echelons: The Organization as a Reflection of Its Top Managers, *Academy of Management Review* 9(2), 193–206.
Harford, J., Mansi, S. A., and Maxwell, W. F. (2008). Corporate Governance and Firm Cash Holdings in the US, *Journal of Financial Economics* 87(3), 535–555.
He, C., HuangFu, J., Kohlbeck, M. J., and Wang, L. (2020a). The Impact of Customer's Reported Cybersecurity Breaches on Key Supplier's Relationship–Specific Investments and Relationship Duration. Working Paper. Available at SSRN 3544245.
He, C. Z., Frost, T., and Pinsker, R. E. (2020b). The Impact of Reported Cybersecurity Breaches on Firm Innovation, *Journal of Information Systems* 34(2), 187–209.
Higgs, J. L., Pinsker, R. E., Smith, T. J., and Young, G. R. (2016). The Relationship between Board–Level Technology Committees and Reported Security Breaches, *Journal of Information Systems* 30(3), 79–98.
Hillman, A. J., and Dalziel, T. (2003). Boards of Directors and Firm Performance: Integrating Agency and Resource Dependence Perspectives, *Academy of Management Review* 28(3), 383–396.
Hoehle, H., Venkatesh, V., Brown, S. A., Tepper, B. J., and Kude, T. (2022). Impact of Customer Compensation Strategies on Outcomes and the Mediating Role of Justice Perceptions: A Longitudinal Study of Target's Data Breach, *MIS Quarterly* 46(1), 299–340.
Hovav, A., and Gray, P. (2014). The Ripple Effect of an Information Security Breach Event: A Stakeholder Analysis, *Communications of the Association for Information Systems* 34(1), 50.
Huang, H. H., and Wang, C. (2020). Do Banks Price Firms' Data Breaches?, *The Accounting Review* 96(3), 261–286.
IBM. (2024). Cost of a Data Breach Report 2024. https://www.ibm.com/reports/data-breach (Accessed 2 February 2024).
Ishii, J., and Xuan, Y. (2014). Acquirer–Target Social Ties and Merger Outcomes, *Journal of Financial Economics* 112(3), 344–363.
Iyer, S. R., Simkins, B. J., and Wang, H. (2020). Cyberattacks and Impact on Bond Valuation, *Finance Research Letters* 33, 101215.
Jang–Jaccard, J., and Nepal, S. (2014). A Survey of Emerging Threats in Cybersecurity, *Journal of Computer and System Sciences* 80(5), 973–993.
Jee–Hae, L., Dehning, B., Richardson, V. J., and Smith, R. E. (2011). A Meta–Analysis of the Effects of IT Investment on Firm Financial Performance, *Journal of Information Systems* 25(2), 145–169.
Jin, D., Lu, F., Li, S., and Yan, C. (2024). Medical Boards and CEOs, Working Paper. HKU Jockey Club Enterprise Sustainability Global Research Institute. Available at SSRN: https://ssrn.com/abstract=3912479.
Joecks, J., Pull, K., and Vetter, K. (2013). Gender Diversity in the Boardroom and Firm Performance: What Exactly Constitutes a "Critical Mass?", *Journal of Business Ethics* 118(1), 61–72.
Kamiya, S., Kang, J.–K., Kim, J., Milidonis, A., and Stulz, R. M. (2021). Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms, *Journal of Financial Economics* 139(3), 719–749.
Khan, S., Kabanov, I., Hua, Y., and Madnick, S. (2022). A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned, *ACM Transactions on Privacy and Security* 26(1), Article 3.
Kim, J.–B., Wang, C., and Wu, F. (2024). Privacy Breaches and the Effect of Customer Notification, *MIS Quarterly* 48(4), 1483–1502.

Krishnan, J., and Lee, J. E. (2009). Audit Committee Financial Expertise, Litigation Risk and Corporate Governance *Auditing: A Journal of Practice & Theory* 28(1), 241–261.
Krishnan, J., Yuan, W., and Wanli, Z. (2011). Legal Expertise on Corporate Audit Committees and Financial Reporting Quality, *The Accounting Review* 86(6), 2099–2130.
Kwong, J. K., and Pearlson, K. (2024). How Large Companies Can Help Small and Medium–Sized Enterprise (SME) Suppliers Strengthen Cybersecurity, *MIS Quarterly Executive* 23(4), 387–398.
Lankton, N., Price, J. B., and Karim, M. (2021). Cybersecurity Breaches and the Role of Information Technology Governance in Audit Committee Charters, *Journal of Information Systems* 35(1), 101–119.
Lending, C., Minnick, K., and Schorno, P. J. (2018). Corporate Governance, Social Responsibility, and Data Breaches, *Financial Review* 53(2), 413–455.
Levit, D., and Malenko, N. (2016). The Labor Market for Directors and Externalities in Corporate Governance, *The Journal of Finance* 71(2), 775–808.
Li, W., Phang, S.–Y., Choi, K. W., and Ho, S. Y. (2021). The Strategic Role of Cios in IT Controls: IT Control Weaknesses and CIO Turnover, *Information & Management* 58(6), 103429.
Li, W. W., Leung, A. C. M., and Yue, W. T. (2023). Where Is IT in Information Security? The Interrelationship among IT Investment, Security Awareness, and Data Breaches, *MIS Quarterly* 47(1), 317–342.
Liang, H., Srinivas, S., and Yajiong, X. (2025). How Mergers and Acquisitions Increase Data Breaches: A Complexity Perspective, *MIS Quarterly* 49(1), 211–242.
Liu, C., and Babar, M. A. (2024). Cybersecurity Risk and Data Breaches for Corporations: A Systematic Review of Empirical Research, *Australian Journal of Management*. Forthcoming.
Liu, C., Cheong, C. S., and Zurbruegg, R. (2020). Rhetoric, Reality, and Reputation: Do CSR and Political Lobbying Protect Shareholder Wealth against Environmental Lawsuits?, *Journal of Financial and Quantitative Analysis* 55(2), 679–706.
Lowry, M., Vance, A., and Vance, M. D. (2023). Inexpert Supervision: Field Evidence on Boards' Oversight of Cybersecurity. Working Paper. Available at SSRN 4002794.
Marcel, J. J., and Cowen, A. P. (2014). Cleaning House or Jumping Ship? Understanding Board Upheaval Following Financial Fraud, *Strategic Management Journal* 35(6), 926–937.
Mithas, S., and Rust, R. T. (2016). How Information Technology Strategy and Investments Influence Firm Performance, *MIS Quarterly* 40(1), 223–246.
Mitra, S., and Chaya, A. K. (1996). Analyzing Cost–Effectiveness of Organizations: The Impact of Information Technology Spending, *Journal of Management Information Systems* 13(2), 29–57.
Nikkhah, H. R., and Grover, V. (2022). An Empirical Investigation of Company Response to Data Breaches, *MIS Quarterly* 46(4), 2163–2196.
Opderbeck, D. W. (2017). Cybersecurity, Encryption, and Corporate Social Responsibility, *Georgetown Journal of International Affairs* 18(3), 105–111.
Peng, J., Zhang, H., Mao, J., and Xu, S. (2023). Repeated Data Breaches and Firm Value, *Economics Letters* 224, 111001.
Pfeffer, J. M., and Salancik, G. R. (1978). *The External Control of Organizations: A Resource Dependence Perspective*. New York, NY: Harper & Row.
Qamar, A., Karim, A., and Chang, V. (2019). Mobile Malware Attacks: Review, Taxonomy & Future Directions, *Future Generation Computer Systems* 97, 887–909.
Rosenstein, S., and Wyatt, J. G. (1990). Outside Directors, Board Independence, and Shareholders Wealth, *Journal of Financial Economics* 26(2), 175–191.
Sarker, O., Jayatilaka, A., Haggag, S., Liu, C., and Babar, M. A. (2024). A Multi–Vocal Literature Review on Challenges and Critical Success Factors of Phishing Education, Training and Awareness, *Journal of Systems and Software* 208, 111899.

Say, G., and Vasudeva, G. (2020). Learning from Digital Failures? The Effectiveness of Firms' Divestiture and Management Turnover Responses to Data Breaches, *Strategy Science* 5(2), 117–142.

Schneier, B., and Vance, A. (2025). "Complexity Is the Worst Enemy of Security": Studying Cybersecurity through the Lens of Organizational Complexity, *MIS Quarterly* 49(1), 205–210.

Srinivasan, S. (2005). Consequences of Financial Reporting Failure for Outside Directors: Evidence from Accounting Restatements and Audit Committee Members, *Journal of Accounting Research* 43(2), 291–334.

Tanriverdi, H., Juhee, K., and Ghiyoung, I. (2025). Taming Complexity in the Cybersecurity of Multihospital Systems: The Role of Enterprise-wide Data Analytics Platforms, *MIS Quarterly* 49(1), 243–273.

Tosun, O. K. (2021). Cyber–Attacks and Stock Market Activity, *International Review of Financial Analysis* 76, 101795.

Trist, E. L. (1981). *The Evolution of Socio–Technical Systems*. Ontario Quality of Working Life Centre Toronto.

Trist, E. L., and Bamforth, K. W. (1951). Some Social and Psychological Consequences of the Longwall Method of Coal–Getting, *Human Relations* 4(1), 3–38.

Wright, R. T., Johnson, S. L., and Kitchens, B. (2023). Phishing Susceptibility in Context: A Multi–Level Information Processing Perspective on Deception Detection, *MIS Quarterly* 47(2), 803–832.

Wynn Jr, D., Salisbury, W. D., and Winemiller, M. (2024). Experiences and Lessons Learned at an Small and Medium–Sized Enterprise (SME) Following Two Ransomware Attacks, *MIS Quarterly Executive* 23(4), 429–448.

Yermack, D. (1996). Higher Market Valuation of Companies with a Small Board of Directors, *Journal of Financial Economics* 40(2), 185–211.

Yermack, D. (2004). Remuneration, Retention, and Reputation Incentives for Outside Directors, *The Journal of Finance* 59(5), 2281–2308.

APPENDIX A: VARIABLE DEFINITIONS

Variable Name	Variable Definition
	Dependent Variables
Breach	Total number of cybersecurity breaches against a firm in year *t*.
Phishing	Number of phishing attacks against a firm in year *t*.
Malware	Number of malware (including ransomware) attacks against a firm in year *t*.
Misconfiguration	Number of misconfiguration attacks against a firm in year *t*.
Unauthorized	Number of unauthorized access incidents against a firm in year *t*.
Unknown	Number of cyberattacks of undisclosed types against a firm in year *t*.
Breach (Industry-Adjusted)	Total number of cybersecurity breaches against a firm in year *t*, adjusted by the industry average number of cybersecurity breaches within each two-digit SIC code industry.
Phishing (Industry-Adjusted)	Number of phishing attacks against a firm in year *t*, adjusted by the industry average number of phishing attacks within each two-digit SIC code industry.
Malware (Industry-Adjusted)	Number of malware (including ransomware) attacks against a firm in year *t*, adjusted by the industry average number of malware attacks within each two-digit SIC code industry.
Unauthorized (Industry-Adjusted)	Number of unauthorized access incidents against a firm in year *t*, adjusted by the industry average number of unauthorized access incidents within each two-digit SIC code industry.
Misconfiguration (Industry-Adjusted)	Number of misconfiguration attacks against a firm in year *t*, adjusted by the industry average number of misconfiguration attacks within each two-digit SIC code industry.
Unknown (Industry-Adjusted)	Number of cyberattacks of undisclosed types against a firm in year *t*, adjusted by the industry average number of cyberattacks of undisclosed types within each two-digit SIC code industry.
Records_Breach	Natural logarithm of the total number of records breached from all cyberattacks against a firm in year *t*.
Records_Phishing	Natural logarithm of the total number of records breached from phishing attacks against a firm in year *t*.
Records_Malware	Natural logarithm of the total number of records breached from malware (including ransomware) attacks against a firm in year *t*.
Records_Misconfiguration	Natural logarithm of the total number of records breached from misconfiguration attacks against a firm in year *t*.
Records_Unauthorized	Natural logarithm of the total number of records breached from unauthorized access incidents against a firm in year *t*.
Records_Unknown	Natural logarithm of the total number of records breached from cyberattacks of undisclosed types against a firm in year *t*.
Cost_Breach	Natural logarithm of the financial cost of all cybersecurity breaches against a firm in year *t*.
Cost_Phishing	Natural logarithm of the financial cost of phishing attacks against a firm in year *t*.
Cost_Malware	Natural logarithm of the financial cost of malware (including ransomware) attacks against a firm in year *t*.
Cost_Unauthorized	Natural logarithm of the financial cost of misconfiguration attacks against a firm in year *t*.
Cost_Unknown	Natural logarithm of the financial cost of unauthorized access incidents against a firm in year *t*.
ΔBoardIT	Natural logarithm of the financial cost of cyberattacks of undisclosed types against a firm in year *t*.

Variable Name	Variable Definition
Cyber_Culture	Number of cybersecurity-related words included in the firm's 10-K filing with SEC scaled by the total word count of the 10-K filing in year *t*–1. Cybersecurity-related wordcount is computed by conducting textual searches of the following wildcard keywords: "cyber security, cyber-security, cybersecurity, security measure*, authentication, information security, network security, computer security, computer virus*, security incident*, cyber attack, cyber-attack, cyberattack, security breach*, network breach*, computer breach*, hacker, encryption, intrusion, denial of service, security monitoring, access control, security management, infosec, computer intrusion*, security expenditure*" (where * denotes regular expressions used to accommodate ambiguous content).
SGA	Selling, general, and administrative (SG&A) expenses in year *t*–1 scaled by total sales revenue in year *t*–1 as a proxy for IT expenditure.
	Independent Variables
BoardIT	Proportion of directors with IT expertise on the board calculated as the number of directors with at least one IT-related degree scaled by the total number of directors on the board, measured alternatively in years *t*, *t*–1, *t*–2, and *t*–3.
BoardIT (Industry-Adjusted)	Proportion of directors with IT expertise on the board adjusted by the industry average proportion of directors with IT expertise on the board within each two-digit SIC code industry.
ΔBoardIT	Changes in the number of directors with IT expertise on the board, measured over alternative periods *t*(–1,0), *t*(–2,0), and *t*(–3,0).
Prev_Breach	Cumulative number of previous cybersecurity breaches across all types experienced by a firm in all years in the sampling period preceding year *t* (up to and including year *t*–1).
Prev_Phishing	Cumulative number of previous phishing attacks experienced by a firm in all years in the sampling period preceding year *t* (up to and including year *t*–1).
Prev_Malware	Cumulative number of previous malware (including ransomware) attacks experienced by a firm in all years in the sampling period preceding year *t*.
Prev_Misconfiguration	Cumulative number of previous misconfiguration attacks experienced by a firm in all years in the sampling period preceding year *t*.
Prev_Unauthorized	Cumulative number of previous unauthorized access incidents experienced by a firm in all years in the sampling period preceding year *t*.
Prev_Unknown	Cumulative number of previous cyberattacks of undisclosed types experienced by a firm in all years in the sampling period preceding year *t*.
Post×IT_Availability	Interaction term between *Post* and *IT_Availability* as the instrumental variable, which represents the local supply of IT-expert directors in firms' headquarter states following staggered adoptions of data breach disclosure laws. *Post* is a binary variable that equals one if the state in which the firm is headquartered has adopted data breach disclosure laws in a prior year or current year *t* and zero otherwise. *IT_Availability* is computed as the total number of unique IT-expert directors in that state in year *t*.
	Control Variables
LnTA	Firm size proxied by the natural logarithm of total assets of the firm in year *t*.
ROA	Firm performance proxied by return on assets, calculated as the net income (loss) divided by total assets in year *t*.
Salesgrowth	Sales growth calculated as the change in total sales from year *t*–1 to year *t* scaled by total sales in year *t*–1.
LnAge	Natural logarithm of firm age as at year *t*.
TobinQ	Market value of total assets divided by the book value of total assets in year *t*. The market value of assets is calculated as the book value of total liabilities plus market value of common shares outstanding.

Variable Name	Variable Definition
Leverage	Financial leverage proxied by debt-to-asset ratio in year *t*, calculated as the book value of total liabilities divided by the book value of total assets.
AltmanZ	Probability of financial distress in year *t*, calculated as 1.2*(working capital/total assets) + 1.4*(retained earnings/total assets) + 3.3*(EBIT/total assets) + 0.6*(total market capitalization/book value of total liabilities) + 1*(sales/total assets).
Capex	Capital expenditure (capex) scaled by total assets in year *t*.
R&D	Research and development (R&D) expenditure scaled by total assets in year *t*.
Intensity	Total number of employees scaled by total assets in year *t*.
Blockhold	Proportion of shares outstanding held by institutional blockholders measured at year *t*.
Boardsize	Number of directors on the board in year *t*.
Indep	Percentage of independent directors on the board calculated as the number of outside directors scaled by the total number of directors on the board in year *t*.
Female	Percentage of female directors on the board calculated as the number of female directors scaled by the total number of directors on the board in year *t*.

APPENDIX B: DIRECTOR IT EDUCATION KEYWORD DICTIONARY

This Appendix lists the keyword dictionary used to identify IT-related degrees in each director's education history. A degree is classified as IT-related if the name of the degree contains any keyword from the dictionary. Data source: BoardEx Director Education Database.

'Computing',	'Bachelor of Information Technology (BIT)',
'Computer',	'Certified Software Quality Analyst',
'Information Technology',	'Cisco Certified Network Professional (CCNP)',
'Certified Cyber Forensics Professional',	'Information Systems Security Architecture Professional (ISSAP)',
'Certified in the Governance of Enterprise IT (CGEIT)',	
'ITIL V3 Expert Certification',	'Certified Cloud Security Professional (CCSP)',
'Certified Ethical Hacker (CEH)',	'Certified Developer',
'Certified Information Systems Security Professional (CISSP)',	'Cisco Certified Design Professional (CCDP)',
	'Global Information Assurance Certification (GIAC)',
'Certified ScrumMaster (CSM)',	'Certified Data Processor (CDP)',
'Microsoft Certified Systems Engineer (MCSE)',	'Certified Forensic Computer Examiner (CFCE)',
'Certified Information Privacy Professional',	'Certified Computer Examiner (CCE)',
'Certified in Risk and Information Systems Control (CRISC)',	'Master of Computer Applications (MCA)',
	'Certified Chief Information Security Officer (CCISO)',
'Certified Information Technology Professional (CITP)',	'Certified Data Privacy Solutions Engineer (CDPSE)',
'CISA (Certified Information Security Auditor)',	'Certified Information Privacy Manager (CIMP)',
'Certificate of Cloud Security Knowledge (CCSK)',	'Certification in Control Self Assessment (CCSA)',
'Master of Management Information System (MMIS)',	'Chartered IT Professional',
'Certified Clinical Data Manager (CCDM)',	'Bachelor of Computer Science',
'Certified Information Systems Auditor (CISA)',	'Certified Economic Developer (CED)',
'Cisco Certified Internetwork Engineer (CCIE)',	'Certified Secure Software Lifecycle Professional (CSSLP)',
'Certified Information Security Manager (CISM)',	
'Information Technology Infrastructure Library (ITIL) Foundation Course',	'Microsoft Certified Solutions Expert (MCSE)',
	'Certified Network Security Specialist (CNSS)',
'Cisco Certified Network Associate (CCNA)',	'Microsoft Certified Database Administrator (MCDBA)',
'Microsoft Certified Professional',	'Microsoft Certified Solution Developer',
'Certified Risk and Information System Controls (CRISC)',	'Certified eMatrix Collaboration Developer',
	'Certified Information Privacy Technologist (CIPT)',
'Cisco Certified Internetwork Expert (CCIE)',	'Computer Science Telecommunication Program',

'Master of Library and Information Sciences (MLIS)',
'Certified Information Systems Manager (CISM)',
'Certified Healthcare Chief Information Officer (CHCIO)',
'Certified Professional in Health Information & Management Systems (CPHIMS)',
'Check Point Certified Security Administrator (CCSA)',
'Check Point Certified Security Expert NGX (CCSE)',
'Check Point Certified Security Expert Plus (CCSE Plus)',
'Red Hat Certified Technician (RHCT)',
'Certified Cloud Practitioner',
'Certified Information Systems Risk and Compliance Professional (CISRCP)',
'Information Systems Security Management Professional (ISSMP)',
'AccessData Certified Examiner (ACE)',
'Bachelor of Computing (BComp)',
'Certified Data Management Professional (CDMP)',
'Masters of Information Systems (MSIS)',
'Certified Internet Professional (CIP)',
'Human Computer Interaction (HCI) Graduate Program',
'Microsoft Certified Architect (MCA)',
'Certified Information Systems Security Officer (CISSO)',
'GIAC Cyber Threat Intelligence (GCTI)',
'Certified Government Chief Information Officers (CGCIO)',
'Certificate in Unix Programming',
'Certified Computing Professional (CCP)',
'Certification Programme for Information Systems Security Professionals (CISSP)',
'Certified Data Centre Professional (CDCP)',
'Java 2 Platform certification',
'Datametrics',
'Microsoft Certified Solutions Associate (MCSA)',
'Certified Information Systems Security Manager (CISSM)',
'Master Certified Network Engineer (MCNE)',
'Cisco Certified Voice Professional (CCVP)',
'Certification for Internet Professionalism (ePro)',
'Management Information System',
'Management Information Resource Program',
'Certified Software Asset Manager (CSAM)',
'Computer Information Systems Management',
'Certificate in Information Security (INFOSEC)',
'Microsoft Certified Systems Administrator (MCSA)',
'Citrix Certified Associate - Networking (CCA - N)',
'Certified Checkpoint Systems Administrator (CCSA)',
'Microsoft Certified Professional Developer (MCPD)',
'Certified Information Executive (CIE)',
'Cisco Certified Internetwork Professional (CCIP)',
'GIAC Certified Network Forensic Analyst (GNFA)',
'Registered Health Information Technician (RHIT)',
'Microsoft Office User Specialist (MOUS)',
'Certified Developer - Associate',
'Post Graduate Diploma in Computer Applications (PGDCA)',
'Certified Data Centre Design Professional (CDCDP)',
'Certified Data Centre Energy Professional (CDCEP)',
'Certified Data Centre Management Professional (CDCMP)',
'Microsoft Certified Desktop Support Technician (MCDST)',
'Microsoft Certified IT Professionals (MCITPs)',
'Microsoft Certified Technology Specialist (MCTS)',
'Microsoft Certified Trainers (MCTs)',
'Microsoft Technology Associate (MTA)',
'Information Systems Security Engineering Professional (ISSEP)',
'Professional Scrum Developer (PSD)',
'FISD Financial Information Associate',
'Information System Professional',
'Information Technology Certified Professional (ITCP)',
'Certified Application Developer (CAD)',
'Certified Software Tester (CSTE)',
'Certified Professional in Health Information Technology (CPHIT)',
'Certified SalesForce.Com Developer and Administrator',
'Certified Checkpoint Firewall Security Administrator (CCSA)',
'Cisco Campus ATM Solutions (CATM)',
'Cisco Certified Architect (CCA)',
'Cisco Certified Design Expert (CCDE)',
'Certified in the Governance of Information Technology (CGEIT)',
'Certified Data Scientist',
'MCITP (Microsoft Certified IT Professional)',
'Master of Science in Management Information Systems (MSMIS)',
'Master of Information Technology',
'Associate Insurance Data Manager (AIDM)',
'CCD Certified Community Developer',
'Certificate in Computer Hardware Maintenance (CCHM)',
'Medical Information Processing Specialist Program',
'Internet Safety Certified Trainer (ISCT)',
'Cognex Computer Vision Certified Engineer',
'Computer Hacking Forensic Investigator (CHFI)',
'Certified Java Architect',
'Post Graduate Diploma in Advanced Computing (PG-DAC)',
'Post Graduate Diploma in Computer Aided Management (PGDCM)',
'Cisco Certified Entry Networking Technician (CCENT)'

FIGURE

Figure 1 Lifecycle of Cybersecurity Breaches

This figure represents the lifecycle stages of a corporate cybersecurity breach.

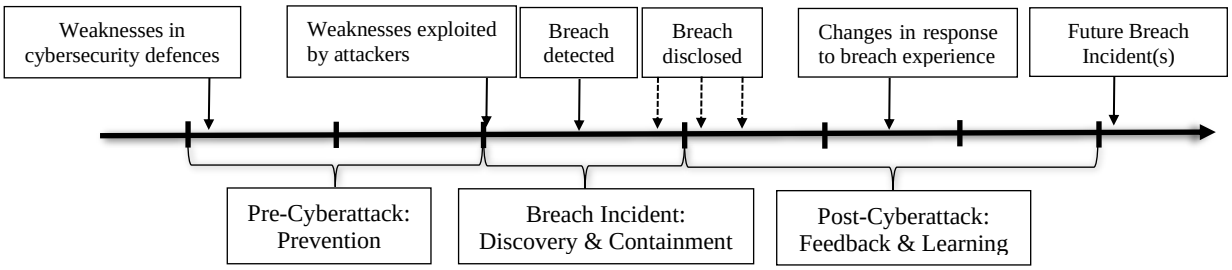
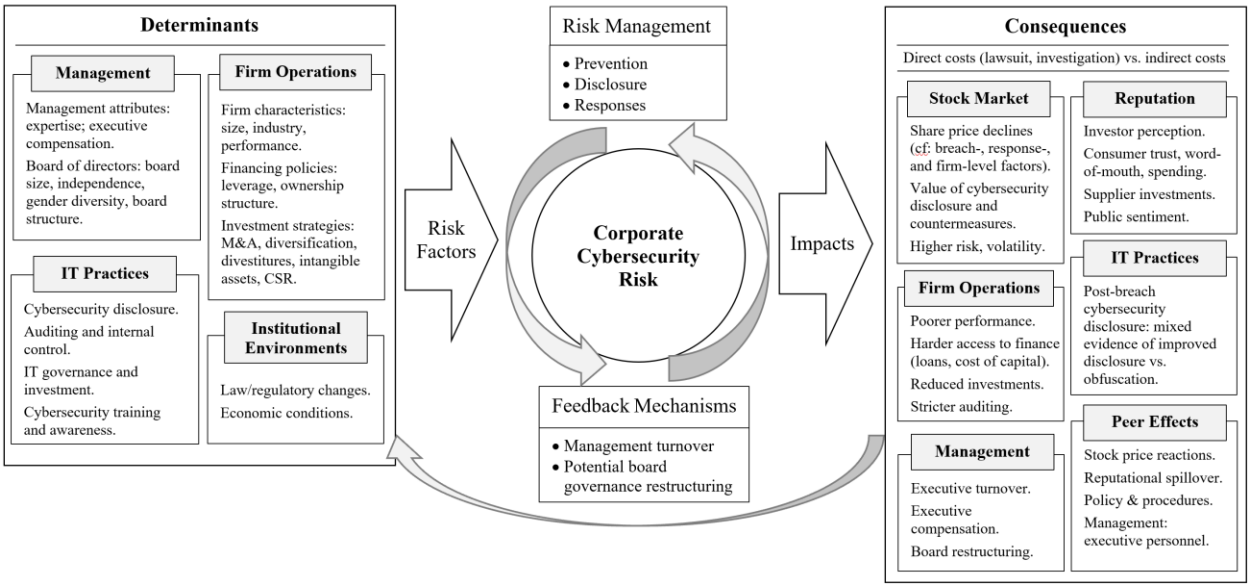


Figure 2 Conceptual Framework of Corporate Cybersecurity Risk Management

This figure illustrates the conceptual framework of corporate cybersecurity risk management developed by Liu and Babar (2024) (p. 7). This framework conceptualizes a feedback loop of organizational learning, whereby firms learn from past cybersecurity failures and make improvements in future cybersecurity defenses.



TABLES

Table 1 Descriptive Statistics

This table reports the descriptive statistics of the variables included in the baseline regressions. All variables are defined in Appendix A.

Variable	N	Mean	Median	Std. Dev.	Maximum	Minimum
Breach	22106	0.019	0.000	0.157	4.000	0.000
Phishing	22106	0.003	0.000	0.061	3.000	0.000
Malware	22106	0.005	0.000	0.073	2.000	0.000
Misconfiguration	22106	0.002	0.000	0.051	3.000	0.000
Unauthorized	22106	0.004	0.000	0.065	3.000	0.000
Unknown	22106	0.006	0.000	0.079	3.000	0.000
BoardIT	22106	0.001	0.000	0.010	0.500	0.000
LnTA	22106	6.864	6.857	1.868	11.164	2.689
ROA	22106	-0.016	0.032	0.196	0.300	-1.019
Salesgrowth	22106	0.132	0.061	0.467	3.326	-0.774
LnAge	22106	2.703	2.890	0.980	4.159	0.000
TobinQ	22106	2.271	1.651	1.773	10.767	0.642
Leverage	22106	1.377	0.946	3.819	22.637	-17.069
AltmanZ	22106	4.174	3.110	6.076	34.738	-12.867
Capex	22106	0.048	0.031	0.055	0.322	0.000
R&D	22106	0.063	0.003	0.123	0.688	0.000
Intensity	22106	0.004	0.002	0.006	0.040	0.000
Blockhold	22106	0.271	0.259	0.143	0.684	0.050
Boardsize	22106	8.466	8.000	2.153	15.000	4.000
Independence	22106	0.841	0.857	0.080	1.000	0.571
Female	22106	0.144	0.143	0.120	0.500	0.000

Table 2 Industry Breakdown

This table reports the industry breakdown of the sample by the one-digit Standard Industry Classification (SIC) code. All variables are defined in Appendix A.

Industry	SIC code	Observations	Breach (mean)	IT Directors (mean)
		(1)	(2)	(3)
Agriculture, Forestry and Fishing	01–09	69	0.043	0.000
Mining	10–14	1,240	0.003	0.003
Construction	15–17	214	0.009	0.005
Manufacturing	20–39	10,510	0.010	0.005
Transportation & Public Utilities	40–49	2,225	0.031	0.003
Wholesale Trade	50–51	809	0.014	0.002
Retail Trade	52–59	1,639	0.033	0.000
Finance	60–67	768	0.030	0.009
Services	70–89	4,606	0.035	0.009
Nonclassifiable	99	26	0.000	0.000
Full Sample		22,106	0.019	0.005

Table 3 Pearson Correlation Results

This table reports the Pearson correlation coefficients for each pairwise combination of the dependent, key independent, and control variables in the baseline regressions. All variables are defined in Appendix A. * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

	Correlation	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)
(1)	Breach	1.000															
(2)	BoardIT	0.001	1.000														
(3)	LnTA	0.126***	-0.037***	1.000													
(4)	ROA	0.033***	-0.007	0.376***	1.000												
(5)	Salesgrowth	-0.007	-0.007	-0.074***	-0.070***	1.000											
(6)	LnAge	0.016**	0.008	0.236***	0.266***	-0.181***	1.000										
(7)	TobinQ	0.020***	0.007	-0.144***	-0.101***	0.165***	-0.191***	1.000									
(8)	Leverage	0.010	-0.000	0.138***	0.023***	-0.012*	0.015**	-0.071***	1.000								
(9)	AltmanZ	-0.002	0.005	-0.053***	0.327***	0.065***	-0.037***	0.490***	-0.095***	1.000							
(10)	Capex	-0.007	-0.029***	0.097***	0.114***	0.092***	-0.046***	-0.016**	0.006	0.015**	1.000						
(11)	R&D	-0.023***	0.005	-0.351***	-0.554***	0.224***	-0.274***	0.411***	-0.059***	0.019***	-0.158***	1.000					
(12)	Intensity	-0.004	-0.010	-0.160***	0.084***	-0.072***	0.051***	-0.036***	0.009	0.007	0.073***	-0.159***	1.000				
(13)	Blockhold	-0.013*	-0.024***	0.064***	0.006	-0.001	-0.074***	-0.015**	0.018***	0.009	-0.041***	0.016**	0.001	1.000			
(14)	Boardsize	0.087***	-0.023***	0.615***	0.184***	-0.058***	0.202***	-0.044***	0.091***	-0.063***	0.012*	-0.175***	-0.051***	0.020***	1.000		
(15)	Independence	0.034***	-0.013*	0.304***	0.025***	-0.038***	0.067***	-0.035***	0.067***	-0.105***	-0.032***	-0.025***	-0.066***	0.158***	0.354***	1.000	
(16)	Female	0.074***	0.019***	0.323***	0.073***	-0.062***	0.114***	0.079***	0.055***	-0.005	-0.061***	-0.052***	0.003	0.064***	0.311***	0.242***	1.000

Table 4 Board IT Expertise and Cybersecurity Breaches

This table reports the results from OLS regressions estimating the number of cybersecurity breaches in year *t* using the key explanatory variable, *BoardIT*, which represents the proportion of directors on the board with IT expertise. The dependent variables capture the total number of cybersecurity breaches (*Breach*) in Columns (1)–(2) and individual types of cyberattacks in Columns (3)–(12), specifically the number of phishing cyberattacks (*Phishing*) in Columns (3)–(4), malware attacks in Columns (5)–(6), misconfiguration cyberattacks in Columns (7)–(8), unauthorized access in Columns (9)–(10), and cybersecurity breaches of unknown types in Columns (11)–(12). Columns (1), (3), (5), (7), (9), and (11) report the results from parsimonious models including only the key explanatory variable and fixed effects, and Columns (2), (4), (6), (8), (10), and (12) report the results from the full regression models including control variables. All variables are defined in Appendix A. *P*-values in parentheses. * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

	Total Breaches		Phishing		Malware		Misconfiguration		Unauthorized		Unknown Type	
	Breach	Breach	Phishing	Phishing	Malware	Malware	Miscon-figuration	Miscon-figuration	Unautho-rized	Unautho-rized	Unknown	Unknown
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
BoardIT	-0.001	0.050	-0.028***	-0.018**	0.015	0.026	-0.019***	-0.011**	-0.036***	-0.030***	0.067	0.083
	(0.986)	(0.560)	(0.000)	(0.011)	(0.712)	(0.512)	(0.000)	(0.015)	(0.000)	(0.000)	(0.364)	(0.266)
LnTA		0.011***		0.001***		0.003***		0.002***		0.001***		0.004***
		(0.000)		(0.002)		(0.000)		(0.002)		(0.001)		(0.000)
ROA		-0.011**		-0.001		-0.001		-0.003*		-0.004		-0.002
		(0.039)		(0.595)		(0.695)		(0.098)		(0.101)		(0.419)
Salesgrowth		0.001		-0.000		0.000		-0.000		0.001		0.001
		(0.682)		(0.242)		(0.773)		(0.269)		(0.383)		(0.577)
LnAge		0.002		-0.000		0.001**		0.001*		0.001*		-0.000
		(0.102)		(0.463)		(0.034)		(0.062)		(0.076)		(0.958)
TobinQ		0.001		-0.000		0.000		0.001		0.000		0.001
		(0.114)		(0.759)		(1.000)		(0.159)		(0.640)		(0.114)
Leverage		-0.000		-0.000		-0.000***		-0.000		0.000		-0.000
		(0.210)		(0.945)		(0.004)		(0.475)		(0.319)		(0.252)
AltmanZ		0.000		-0.000		0.000		0.000		0.000		-0.000**
		(0.936)		(0.303)		(0.886)		(0.284)		(0.289)		(0.028)
Capex		0.007		-0.004		-0.003		0.023**		0.006		-0.015**
		(0.776)		(0.572)		(0.742)		(0.042)		(0.524)		(0.043)
R&D		0.020**		-0.002		0.010**		0.003		0.003		0.005
		(0.025)		(0.550)		(0.022)		(0.375)		(0.438)		(0.223)
Intensity		-0.145		0.114		0.099		0.017		-0.051		-0.332***
		(0.529)		(0.297)		(0.426)		(0.786)		(0.590)		(0.003)
Blockhold		-0.034***		0.005		-0.012***		-0.006**		-0.004		-0.017***
		(0.000)		(0.109)		(0.002)		(0.013)		(0.196)		(0.000)
Boardsize		0.001		0.000*		0.000		0.000		0.000		-0.000
		(0.152)		(0.084)		(0.704)		(0.500)		(0.131)		(0.550)

Independence		-0.006		0.001		0.004		-0.010		-0.008		0.006
		(0.666)		(0.820)		(0.589)		(0.143)		(0.227)		(0.325)
Female		0.004		-0.007*		-0.003		0.002		0.009*		0.004
		(0.655)		(0.086)		(0.406)		(0.421)		(0.052)		(0.398)
Constant	0.041	-0.031	-0.003***	-0.014***	-0.006***	-0.028***	-0.002***	-0.009**	-0.005***	-0.013**	0.058*	0.034
	(0.240)	(0.373)	(0.000)	(0.003)	(0.000)	(0.000)	(0.000)	(0.041)	(0.000)	(0.030)	(0.091)	(0.307)
Industry FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	22106	22106	22106	22106	22106	22106	22106	22106	22106	22106	22106	22106
Adjusted R^2	0.018	0.034	0.004	0.005	0.006	0.010	0.003	0.008	0.008	0.010	0.007	0.016

Table 5 Lagged Board IT Expertise and Cybersecurity Breaches

This table reports the results from OLS regressions estimating the number of cybersecurity breaches in year *t* using lagged explanatory variable, *BoardIT*, measured at years *t*–1, *t*–2, and *t*–3. The dependent variables capture the total number of cybersecurity breaches (*Breach*) in Columns (1)–(3) and the number of individual types of cyberattacks in Columns (4)–(15), specifically phishing cyberattacks (*Phishing*) in Columns (4)–(6), malware attacks (*Malware*) in Columns (7)–(9), misconfiguration cyberattacks (*Misconfiguration*) in Columns (10)–(12), and unauthorized access (*Unauthorized*) in Columns (13)–(15). The regressions predicting the number of cybersecurity breaches of unknown types are untabulated for succinctness. All variables are defined in Appendix A. *P*-values in parentheses. * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

	Total Breaches			Phishing			Malware			Misconfiguration			Unauthorized		
	Breach	Breach	Breach	Phishing	Phishing	Phishing	Malware	Malware	Malware	Miscon-figuration	Miscon-figuration	Miscon-figuration	Unautho-rized	Unautho-rized	Unautho-rized
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)
$BoardIT_{t-3}$	0.160			-0.018***			0.059			-0.016**			-0.031***		
	(0.302)			(0.001)			(0.433)			(0.010)			(0.000)		
$BoardIT_{t-2}$		0.113			-0.022**			0.042			-0.013**			-0.033***	
		(0.373)			(0.012)			(0.455)			(0.014)			(0.001)	
$BoardIT_{t-1}$			0.072			-0.019**			0.029			-0.012**			-0.030***
			(0.466)			(0.013)			(0.489)			(0.011)			(0.001)
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Constant	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	20259	21065	21859	20259	21065	21859	20259	21065	21859	20259	21065	21859	20259	21065	21859
Adjusted R^2	0.036	0.035	0.034	0.006	0.005	0.005	0.011	0.011	0.011	0.008	0.008	0.008	0.011	0.011	0.011

Table 6 Heckman Selection Model with Instrumental Variable

This table reports the results from the second-stage regressions of the Heckman Selection Model by including the Inverse Mills Ratio calculated from the first-stage regressions utilizing an instrumental variable (IV), which exploits the staggered adoption of cybersecurity breach disclosure laws across various U.S. states. The IV represents the post-law-adoption availability of local IT-expert directors in the state in which the firm is headquartered. In the second-stage regression, the dependent variables capture the total number of cybersecurity breaches in Columns (1)–(3) and the number of individual types of cyberattacks in Columns (4)–(24). All variables are defined in Appendix A. *P*-values in parentheses. * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

	Total Breaches				Phishing				Malware			
	Breach	Breach	Breach	Breach	Phishing	Phishing	Phishing	Phishing	Malware	Malware	Malware	Malware
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
BoardIT$_{t-3}$	0.061				-0.021***				0.029			
	(0.545)				(0.005)				(0.538)			
BoardIT$_{t-2}$		0.085				-0.021***				0.031		
		(0.445)				(0.008)				(0.517)		
BoardIT$_{t-1}$			0.132				-0.023***				0.045	
			(0.347)				(0.010)				(0.469)	
BoardIT$_{t}$				0.193				-0.019***				0.066
				(0.260)				(0.002)				(0.426)
Inverse Mills Ratio	-0.001	0.002	0.013	-0.026	-0.005	-0.006	-0.003	0.008	0.008	0.009	0.013	-0.024
	(0.975)	(0.946)	(0.750)	(0.687)	(0.588)	(0.620)	(0.835)	(0.724)	(0.451)	(0.477)	(0.424)	(0.367)
Controls & Constant	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry & Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	19009	18815	18128	17442	19009	18815	18128	17442	19009	18815	18128	17442
Adjusted R^2	0.034	0.034	0.035	0.036	0.006	0.006	0.006	0.006	0.010	0.011	0.011	0.011

	Misconfiguration				Unauthorized				Unknown Type			
	Miscon-figuration	Miscon-figuration	Miscon-figuration	Miscon-figuration	Unautho-rized	Unautho-rized	Unautho-rized	Unautho-rized	Unknown	Unknown	Unknown	Unknown
	(13)	(14)	(15)	(16)	(17)	(18)	(19)	(20)	(21)	(22)	(23)	(24)
BoardIT$_{t-3}$	-0.014***				-0.034***				0.102			
	(0.008)				(0.000)				(0.243)			
BoardIT$_{t-2}$		-0.014***				-0.033***				0.123		
		(0.007)				(0.000)				(0.222)		
BoardIT$_{t-1}$			-0.014**				-0.034***				0.159	
			(0.014)				(0.001)				(0.206)	
BoardIT$_{t}$				-0.016**				-0.031***				0.192
				(0.020)				(0.000)				(0.205)
Inverse Mills Ratio	-0.003	-0.003	-0.002	-0.003	-0.003	-0.003	-0.002	-0.007	0.003	0.007	0.008	-0.001
	(0.795)	(0.788)	(0.913)	(0.898)	(0.793)	(0.780)	(0.892)	(0.762)	(0.818)	(0.620)	(0.653)	(0.977)
Controls & Constant	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry & Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	19009	18815	18128	17442	19009	18815	18128	17442	19009	18815	18128	17442
Adjusted R^2	0.008	0.008	0.008	0.008	0.011	0.012	0.012	0.012	0.016	0.016	0.017	0.015

Table 7 Industry-Adjusted Analysis: Board IT Expertise and Cybersecurity Breaches

This table reports the results from OLS regressions estimating the industry-adjusted number of cybersecurity breaches in year *t* using *BoardIT* (industry-adjusted), which represents the proportion of directors with IT expertise adjusted by the industry mean within each two-digit SIC industry as measured at years *t*, *t*–1, *t*–2, and *t*–3. The dependent variables capture the number of cybersecurity breaches adjusted by the industry mean in Columns (1)–(4) and the industry-adjusted number of individual types of cyberattacks in Columns (5)–(24). All variables are defined in Appendix A. *P*-values in parentheses. * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

	Total Breaches (Industry-Adjusted)				Phishing (Industry-Adjusted)				Malware (Industry-Adjusted)			
	Breach (ind-adj)	Breach (ind-adj)	Breach (ind-adj)	Breach (ind-adj)	Phishing (ind-adj)	Phishing (ind-adj)	Phishing (ind-adj)	Phishing (ind-adj)	Malware (ind-adj)	Malware (ind-adj)	Malware (ind-adj)	Malware (ind-adj)
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
BoardIT$_{t-3}$ (industry-adjusted)	0.174 (0.260)				-0.018*** (0.001)				0.064 (0.398)			
BoardIT$_{t-2}$ (industry-adjusted)		0.126 (0.322)				-0.023*** (0.009)				0.046 (0.408)		
BoardIT$_{t-1}$ (industry-adjusted)			0.082 (0.403)				-0.020*** (0.008)				0.033 (0.431)	
BoardIT$_{t}$ (industry-adjusted)				0.061 (0.477)				-0.020*** (0.007)				0.030 (0.451)
Controls & Constant	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry & Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	20259	21065	21859	22106	20259	21065	21859	22106	20259	21065	21859	22106
Adjusted R^2	0.024	0.024	0.023	0.023	0.002	0.002	0.002	0.002	0.006	0.006	0.005	0.005

	Misconfiguration (Industry-Adjusted)				Unauthorized (Industry-Adjusted)				Unknown Type (Industry-Adjusted)			
	Miscon-figuration (ind-adj)	Miscon-figuration (ind-adj)	Miscon-figuration (ind-adj)	Miscon-figuration (ind-adj)	Unautho-rized (ind-adj)	Unautho-rized (ind-adj)	Unautho-rized (ind-adj)	Unautho-rized (ind-adj)	Unknown (ind-adj)	Unknown (ind-adj)	Unknown (ind-adj)	Unknown (ind-adj)
	(13)	(14)	(15)	(16)	(17)	(18)	(19)	(20)	(21)	(22)	(23)	(24)
BoardIT$_{t-3}$ (industry-adjusted)	-0.015** (0.019)				-0.029*** (0.000)				0.173 (0.208)			
BoardIT$_{t-2}$ (industry-adjusted)		-0.012** (0.022)				-0.032*** (0.002)				0.146 (0.198)		
BoardIT$_{t-1}$ (industry-adjusted)			-0.011** (0.016)				-0.029*** (0.001)				0.110 (0.213)	
BoardIT$_{t}$ (industry-adjusted)				-0.010** (0.025)				-0.029*** (0.001)				0.090 (0.227)
Controls & Constant	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry & Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	20259	21065	21859	22106	20259	21065	21859	22106	20259	21065	21859	22106
Adjusted R^2	0.005	0.005	0.004	0.004	0.007	0.007	0.006	0.006	0.008	0.008	0.008	0.008

Table 8 Channel Analysis: Corporate Cybersecurity Culture

This table explores corporate cybersecurity culture as a mechanism in the relationship between board IT expertise and cybersecurity breaches. Panel A reports the results from OLS regressions estimating the number of cybersecurity-related words included in the firm's 10-K filing with the Securities and Exchange Commission scaled by the total word count of the 10-K filing in year *t*-1 (*Cyber_Culture*), using the key explanatory variable, *BoardIT*, measured at years *t*–1, *t*–2, and *t*–3. Panel B reports the results from OLS regressions estimating the number of cybersecurity breaches in year *t* using the interaction term between *Cyber_Culture* and *BoardIT* at years *t*–1, *t*–2, and *t*–3. All variables are defined in Appendix A. *P*-values in parentheses. * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

Panel A: Board IT Expertise and Corporate Cybersecurity Culture

	Cybersecurity-Related Wordcount in SEC 10-K Filings		
	Cyber_Culture	Cyber_Culture	Cyber_Culture
	(1)	(2)	(3)
$BoardIT_{t-3}$	0.007***		
	(0.001)		
$BoardIT_{t-2}$		0.007***	
		(0.000)	
$BoardIT_{t-1}$			0.007***
			(0.000)
Controls & Constant	Yes	Yes	Yes
Industry & Year FE	Yes	Yes	Yes
Observations	14779	15305	15469
Adjusted R^2	0.247	0.250	0.248

Panel B: Board IT Expertise, Corporate Cybersecurity Culture, and Cybersecurity Breaches

	Total Breaches			Phishing			Malware			Misconfiguration			Unauthorized			Unknown		
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)	(18)
$BoardIT_{t-3}$*Cyber_Culture	37.947			-2.894*			-2.274			-3.898*			-6.146***			53.108		
	(0.503)			(0.056)			(0.369)			(0.052)			(0.004)			(0.374)		
$BoardIT_{t-2}$*Cyber_Culture		19.368			-2.266**			-1.658			-2.424**			-4.726***			30.401	
		(0.561)			(0.047)			(0.302)			(0.043)			(0.001)			(0.388)	
$BoardIT_{t-1}$*Cyber_Culture			16.367			-2.565**			-1.835			-2.683**			-5.299***			28.709
			(0.607)			(0.042)			(0.287)			(0.038)			(0.001)			(0.398)
Controls & Constant	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry & Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Obs.	14779	15305	15469	14779	15305	15469	14779	15305	15469	14779	15305	15469	14779	15305	15469	14779	15305	15469
Adj. R^2	0.034	0.033	0.033	0.003	0.003	0.003	0.012	0.011	0.011	0.009	0.009	0.009	0.011	0.011	0.011	0.013	0.014	0.014

Table 9 Channel Analysis: Board IT Expertise and Selling, General, and Administrative Expenses

This table explores corporate IT expenditure, as proxied by selling, general, and administrative (SG&A) expenses, as a mechanism facilitating the relationship between board IT expertise and cybersecurity breaches. Panel A reports the results from OLS regressions estimating the SG&A expenses of a firm in year *t*–1 scaled by total sales revenue (*SGA*) using the key explanatory variable, *BoardIT*, measured at years *t*–1, *t*–2, and *t*–3. Panel B reports the results from OLS regressions estimating the number of cybersecurity breaches in year *t* using the interaction term between *SGA* and *BoardIT* at years *t*–1, *t*–2, and *t*–3. All variables are defined in Appendix A. *P*-values in parentheses. * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

Panel A: Board IT Expertise and SG&A Expenses

	Selling, General, and Administrative Expenses		
	SGA	SGA	SGA
	(1)	(2)	(3)
$BoardIT_{t-3}$	0.290		
	(0.330)		
$BoardIT_{t-2}$		0.263	
		(0.286)	
$BoardIT_{t-1}$			0.288
			(0.166)
Controls & Constant	Yes	Yes	Yes
Industry & Year FE	Yes	Yes	Yes
Observations	15087	15631	15827
Adjusted R^2	0.611	0.620	0.618

Panel B: Board IT Expertise, SG&A Expenses, and Cybersecurity Breaches

	Total Breaches			Phishing			Malware			Misconfiguration			Unauthorized			Unknown		
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)	(18)
$BoardIT_{t-3}$*SGA	0.077			-0.014			0.001			-0.034***			-0.036***			0.160		
	(0.663)			(0.122)			(0.965)			(0.009)			(0.006)			(0.389)		
$BoardIT_{t-2}$*SGA		0.064			-0.017			-0.000			-0.030**			-0.038***			0.149	
		(0.688)			(0.106)			(0.981)			(0.011)			(0.005)			(0.374)	
$BoardIT_{t-1}$*SGA			0.039			-0.018*			-0.003			-0.030**			-0.038***			0.128
			(0.784)			(0.097)			(0.868)			(0.012)			(0.005)			(0.396)
Controls & Constant	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry & Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Obs.	15087	15631	15827	15087	15631	15827	15087	15631	15827	15087	15631	15827	15087	15631	15827	15087	15631	15827
Adj. R^2	0.033	0.032	0.031	0.003	0.002	0.002	0.014	0.013	0.013	0.009	0.009	0.009	0.010	0.010	0.010	0.013	0.014	0.014

Table 10 Board IT Expertise and Severity of Cybersecurity Breaches

This table reports the results from the OLS regressions estimating the scale of cybersecurity breaches in year *t* using the key explanatory variable, *BoardIT*, as measured at years *t*, *t*–1, *t*–2, and *t*–3. In Panel A, the dependent variables capture the natural logarithm of the number of records breached from all cyberattacks in Columns (1)–(4) and individual types of cyberattacks in Columns (5)–(24), specifically the number of records breached in phishing attacks (*Phishing*) in Columns (5)–(8), malware attacks in Columns (9)–(12), misconfiguration attacks in Columns (13)–(16), unauthorized access in Columns (17)–(20), and cybersecurity breaches of undisclosed types in Columns (21)–(24). In Panel B, the dependent variables capture the natural logarithm of the pecuniary cost of all cyberattacks in Columns (1)–(4) and individual types of cyberattacks in Columns (5)–(20), specifically the costs of phishing attacks (*Phishing*) in Columns (5)–(8), malware attacks in Columns (9)–(12), unauthorized access in Columns (13)–(16), and cybersecurity breaches of undisclosed types in Columns (17)–(20) (the regressions estimating the financial costs of misconfiguration attacks, *Cost_Misconfiguration*, are omitted as the regressions did not return any results due to the lack of variations in that variable). All variables are defined in Appendix A. *P*-values in parentheses. * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

Panel A: Number of Records Breached

	Total Breaches				Phishing				Malware			
	Records_ Breach	Records_ Breach	Records_ Breach	Records_ Breach	Records_ Phishing	Records_ Phishing	Records_ Phishing	Records_ Phishing	Records_ Malware	Records_ Malware	Records_ Malware	Records_ Malware
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
$BoardIT_{t-3}$	-0.412***				-0.036				-0.037			
	(0.002)				(0.100)				(0.338)			
$BoardIT_{t-2}$		-0.384***				-0.076				-0.026		
		(0.002)				(0.156)				(0.432)		
$BoardIT_{t-1}$			-0.366***				-0.063				-0.036	
			(0.001)				(0.167)				(0.243)	
$BoardIT_{t}$				-0.344***				-0.057				-0.033
				(0.002)				(0.179)				(0.279)
Controls & Constant	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry & Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	20259	21065	21859	22106	20259	21065	21859	22106	20259	21065	21859	22106
Adjusted R^2	0.019	0.020	0.019	0.019	0.006	0.006	0.006	0.006	0.004	0.004	0.004	0.004

	Misconfiguration				Unauthorized				Unknown Type			
	Records_ Miscon-figuration	Records_ Miscon-figuration	Records_ Miscon-figuration	Records_ Miscon-figuration	Records_ Unautho-rized	Records_ Unautho-rized	Records_ Unautho-rized	Records_ Unautho-rized	Records_ Unknown	Records_ Unknown	Records_ Unknown	Records_ Unknown
	(13)	(14)	(15)	(16)	(17)	(18)	(19)	(20)	(21)	(22)	(23)	(24)
$BoardIT_{t-3}$	-0.083*				-0.215***				-0.023			
	(0.062)				(0.001)				(0.164)			
$BoardIT_{t-2}$		-0.064*				-0.210***				-0.022		
		(0.086)				(0.000)				(0.141)		
$BoardIT_{t-1}$			-0.056*				-0.199***				-0.022	
			(0.088)				(0.000)				(0.124)	
$BoardIT_{t}$				-0.050				-0.196***				-0.021
				(0.112)				(0.000)				(0.125)

Controls & Constant	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry & Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	20259	21065	21859	22106	20259	21065	21859	22106	20259	21065	21859	22106
Adjusted R^2	0.005	0.005	0.004	0.004	0.011	0.011	0.010	0.010	0.000	0.000	0.000	0.000

Panel B: Financial Cost of Breaches

	Total Breaches				Phishing				Malware			
	Cost_ Breach	Cost_ Breach	Cost_ Breach	Cost_ Breach	Cost_ Phishing	Cost_ Phishing	Cost_ Phishing	Cost_ Phishing	Cost_ Malware	Cost_ Malware	Cost_ Malware	Cost_ Malware
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
$BoardIT_{t-3}$	1.871				-0.066*				1.076			
	(0.215)				(0.059)				(0.348)			
$BoardIT_{t-2}$		1.569				-0.057*				0.778		
		(0.218)				(0.053)				(0.362)		
$BoardIT_{t-1}$			1.225				-0.052**				0.568	
			(0.228)				(0.045)				(0.373)	
$BoardIT_t$				1.182				-0.050**				0.549
				(0.226)				(0.042)				(0.368)
Controls & Constant	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry & Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	20259	21065	21859	22106	20259	21065	21859	22106	20259	21065	21859	22106
Adjusted R^2	0.007	0.006	0.006	0.006	0.002	0.002	0.002	0.002	0.004	0.004	0.004	0.004

	Unauthorized				Unknown Type			
	Cost_ Unautho-rized	Cost_ Unautho-rized	Cost_ Unautho-rized	Cost_ Unautho-rized	Cost_ Unknown	Cost_ Unknown	Cost_ Unknown	Cost_ Unknown
	(13)	(14)	(15)	(16)	(17)	(18)	(19)	(20)
$BoardIT_{t-3}$	-0.051				-0.081**			
	(0.135)				(0.020)			
$BoardIT_{t-2}$		-0.042				-0.071**		
		(0.141)				(0.018)		
$BoardIT_{t-1}$			-0.043*				-0.064**	
			(0.089)				(0.019)	
$BoardIT_t$				-0.047*				-0.068**
				(0.054)				(0.013)
Controls & Constant	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry & Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	20259	21065	21859	22106	20259	21065	21859	22106
Adjusted R^2	0.003	0.003	0.003	0.003	0.001	0.001	0.001	0.001

Table 11 Post-Cyberattack Changes in Board IT Expertise

This table reports the results from OLS regressions estimating changes in the number of directors with IT expertise during the periods $t(0,+1)$, $t(0,+2)$, and $t(0,+3)$ using cybersecurity breaches in year t. In Columns (1)–(3), the key explanatory variable *Breach* captures the total number of cybersecurity breaches in year t. In Columns (4)–(6), the five key explanatory variables capture the number of individual types of cyberattacks in year t, namely phishing, malware, misconfiguration, unauthorized access, and undisclosed types. All variables are defined in Appendix A. *P*-values in parentheses. * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

Variable	Total Breaches			Individual Breach Types		
	ΔBoardIT $t(0,+1)$	ΔBoardIT $t(0,+2)$	ΔBoardIT $t(0,+3)$	ΔBoardIT $t(0,+1)$	ΔBoardIT $t(0,+2)$	ΔBoardIT $t(0,+3)$
	(1)	(2)	(3)	(4)	(5)	(6)
Breach	0.0003*	0.001***	0.001***			
	(0.062)	(0.008)	(0.007)			
Phishing				0.0001	0.0001	-0.000
				(0.658)	(0.825)	(0.942)
Malware				0.000	0.001*	0.001**
				(0.219)	(0.097)	(0.041)
Misconfiguration				0.0004*	0.001*	0.001
				(0.084)	(0.053)	(0.544)
Unauthorized				0.001*	0.001*	0.000
				(0.084)	(0.070)	(0.608)
Unknown				0.000	0.001**	0.002***
				(0.500)	(0.048)	(0.007)
LnTA	0.0002	0.0005**	0.0004*	0.0002	0.0005**	0.0004*
	(0.122)	(0.017)	(0.078)	(0.122)	(0.017)	(0.079)
ROA	0.001	-0.004*	-0.005	0.001	-0.004*	-0.005
	(0.758)	(0.062)	(0.185)	(0.758)	(0.062)	(0.185)
Salesgrowth	0.001	0.000	0.000	0.001	0.000	0.000
	(0.181)	(0.697)	(0.908)	(0.182)	(0.697)	(0.908)
LnAge	-0.000	-0.000	0.000	-0.000	-0.000	0.000
	(0.909)	(0.329)	(0.891)	(0.908)	(0.329)	(0.890)
TobinQ	0.000*	0.000*	0.000	0.000*	0.000*	0.000
	(0.078)	(0.052)	(0.646)	(0.079)	(0.053)	(0.647)
Leverage	0.000	0.000	0.000	0.000	0.000	0.000
	(0.325)	(0.936)	(0.508)	(0.326)	(0.937)	(0.508)
AltmanZ	-0.000	-0.000	0.000	-0.000	-0.000	0.000
	(0.390)	(0.862)	(0.774)	(0.389)	(0.861)	(0.773)
Capex	0.001	0.002	0.002	0.001	0.002	0.002
	(0.559)	(0.526)	(0.653)	(0.561)	(0.527)	(0.651)
R&D	-0.001	-0.009	-0.012	-0.001	-0.009	-0.012
	(0.824)	(0.175)	(0.175)	(0.824)	(0.175)	(0.174)
Intensity	0.032	0.054*	0.060	0.032	0.054*	0.060
	(0.109)	(0.095)	(0.142)	(0.109)	(0.094)	(0.141)
Blockhold	0.003**	0.006***	0.008***	0.003**	0.006***	0.008***
	(0.010)	(0.001)	(0.001)	(0.010)	(0.001)	(0.001)
Boardsize	0.000	-0.000	-0.000	0.000	-0.000	-0.000
	(0.567)	(0.850)	(0.723)	(0.567)	(0.852)	(0.721)
Independence	-0.001	-0.002	-0.002	-0.001	-0.002	-0.002
	(0.405)	(0.424)	(0.419)	(0.407)	(0.424)	(0.418)
Female	-0.002	-0.007*	-0.009*	-0.002	-0.007*	-0.009*
	(0.357)	(0.081)	(0.060)	(0.357)	(0.081)	(0.060)
Constant	-0.001	-0.002	-0.002	-0.001	-0.002	-0.002
	(0.435)	(0.371)	(0.501)	(0.434)	(0.367)	(0.492)
Controls & Constant	Yes	Yes	Yes	Yes	Yes	Yes
Industry & Year FE	Yes	Yes	Yes	Yes	Yes	Yes
Observations	18786	15662	12843	18786	15662	12843
Adjusted R^2	-0.001	0.003	0.006	-0.001	0.002	0.006

Table 12 Changes in Board IT Expertise, Previous Cyberattacks, and Subsequent Cybersecurity Breaches

This table reports the results from OLS regressions estimating cybersecurity breaches in year *t* using both the changes in board IT expertise in the preceding periods, *t*(–3,0), *t*(–2,0), and *t*(–1,0), and the firm's previous experience with cybersecurity breaches, as independent variables. The dependent variables capture the total number of cybersecurity breaches in Columns (1)–(3) and the number of individual types of cyberattacks in Columns (4)–(24), namely phishing, malware, misconfiguration, unauthorized access, and undisclosed types. All variables are defined in Appendix A. *P*-values in parentheses. * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

	Total Breaches			Phishing			Malware			Misconfiguration			Unauthorized			Unknown		
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)	(18)
ΔBoardIT$_{t(-3,0)}$	-0.012***			-0.002**			-0.004**			-0.001			-0.003***			-0.002*		
	(0.004)			(0.023)			(0.019)			(0.193)			(0.009)			(0.085)		
ΔBoardIT$_{t(-2,0)}$		-0.010**			-0.001			-0.005**			-0.001			-0.003**			-0.002*	
		(0.014)			(0.217)			(0.015)			(0.328)			(0.050)			(0.068)	
ΔBoardIT$_{t(-1,0)}$			-0.011**			-0.001			-0.006***			-0.000			-0.003			-0.001
			(0.044)			(0.385)			(0.005)			(0.748)			(0.106)			(0.276)
Prev_Breach	0.079***	0.079***	0.080***															
	(0.000)	(0.000)	(0.000)															
Prev_Phishing				0.020	0.019	0.020												
				(0.312)	(0.318)	(0.312)												
Prev_Malware							0.018	0.018	0.018*									
							(0.109)	(0.102)	(0.096)									
Prev_Misconfig.										0.112	0.112	0.113						
										(0.167)	(0.166)	(0.165)						
Prev_Unauthorized													0.150**	0.150**	0.150**			
													(0.016)	(0.016)	(0.016)			
Prev_Unknown																0.033***	0.033***	0.033***
																(0.000)	(0.000)	(0.000)
Controls & Const.	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ind. + Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Obs.	20259	21065	21859	20259	21065	21859	20259	21065	21859	20259	21065	21859	20259	21065	21859	20259	21065	21859
Adj. R^2	0.066	0.065	0.064	0.006	0.006	0.006	0.012	0.012	0.012	0.034	0.033	0.033	0.037	0.036	0.036	0.025	0.025	0.025