



Research Paper

The Impact of Corporate Governance and Board Characteristics on Information Technology and Cybersecurity Risks: Evidence from Manufacturing Firms Listed on the Tehran Stock Exchange¹

Maryam Ghasemiansaghi²  and Aghil Farhangian^{*3} 

Journal of Information System and Technology Auditing
Iranian Information Technology Audit Scientific
Association

Vol. 2, No. 1, Spring & Summer 2026
pp. 187-232

Received: 2026.08.11
Revised: 2026.09.30
Accepted: 2026.10.28

Abstract

The purpose of this study is to examine the impact of corporate governance and board characteristics on information technology (IT) and cybersecurity risk disclosure among manufacturing companies listed on the Tehran Stock Exchange. To measure the level of IT and cybersecurity risk disclosure, a researcher-developed index, CSRisk, was designed based on the components of the COBIT 2019 and NIST CSF 2.0 frameworks and evaluated using content analysis of corporate official reports. The research sample comprises 117 manufacturing companies over the period from 2021 to 2025(1400–1404 SH), totaling 585 firm-year observations. The research hypotheses were tested using panel data regression with cross-sectional fixed effects. Explanatory variables include board independence, board size, board financial expertise, board IT expertise, CEO duality, and the presence of a specialized IT/risk committee, while firm size, financial leverage, return on assets(ROA), and Tobin's Q serve as control variables. The empirical findings reveal that, among the examined variables, only the presence of a specialized IT/risk committee exhibits a statistically significant relationship with the level of IT and cybersecurity risk disclosure. The direction of this relationship is negative, indicating that the existence of such a committee is associated with a reduction in public cyber risk disclosure. This phenomenon can be attributed to the adoption of a “security confidentiality” approach and a preference for internal risk management over public disclosure.

Keywords: Corporate Governance; Board of Directors; Cybersecurity Risk Disclosure; Cybersecurity; Information Technology.

JEL classification: G34, M41, M15, G32.

¹ <https://doi.org/10.22034/JISTA.2026.578486.1085>

¹ Selected paper of the 2nd National Conference on Corporate Governance and Information Technology Risk Management

² Department of Management and Accounting, National University of Skills, Tehran, Iran. Email: mehrabghasemy6@gmail.com

³ Department of Accounting, ST.C., Islamic Azad University, Tehran, Iran. (Corresponding Author). Email: aghil.farhangian@iau.ac.ir

1. INTRODUCTION

In the contemporary digital economy, corporate information technology (IT) systems and cyber assets have become integral to strategic operations, value creation, and competitive positioning. Concurrently, the proliferation, sophistication, and severity of cyber threats have elevated cybersecurity and IT-related risks from operational hazards to primary strategic and systemic challenges. Effective corporate governance mechanisms are conventionally perceived as structural instruments that enforce financial transparency, mitigate information asymmetry, and promote voluntary disclosures to safeguard shareholder wealth. However, within the specific domain of cybersecurity, corporate boards encounter an acute informational and strategic paradox: while capital markets, institutional investors, and regulatory bodies demand granular disclosures to evaluate corporate risk exposures accurately, public disclosure of technical vulnerabilities, incident management architectures, or security configurations creates significant proprietary hazards. Malicious external actors may exploit detailed disclosures, inadvertently jeopardizing firm security and corporate value. Grounded in Agency Theory, Resource Dependency Theory, and Proprietary Cost Theory, this empirical research investigates the relationship between board structural characteristics, specialized governance committees, and the extent of IT and cybersecurity risk disclosure among non-financial manufacturing firms listed on the Tehran Stock Exchange (TSE). By examining an emerging market characterized by regulatory transitions, digital transformation, and geopolitical cyber pressures, this study provides novel empirical insights into the delicate balance between corporate governance oversight and selective confidentiality.

2. MATERIALS AND METHODS

The target statistical population encompasses non-financial manufacturing companies continuously listed on the Tehran Stock Exchange over a 5-year observation period from 2021 to 2025 (corresponding to the Iranian calendar years 1400–1404). Applying



a systematic multi-stage screening procedure—excluding financial intermediaries, investment companies, banks, firms with fiscal year-end changes, and entities with incomplete trading or financial datasets—yielded a balanced panel of 117 manufacturing firms, generating 585 firm-year observations.

The dependent variable, the Cybersecurity and Information Technology Risk Disclosure Index (*CSRisk*), was constructed using structured manual content analysis applied to comprehensive annual financial reports, board of directors' activity reports, and published market disclosures. Drawing upon international cybersecurity and governance frameworks—principally COBIT 2019 and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF 2.0)—the disclosure index spans seven core functional dimensions: Governance, Identify, Protect, Detect, Respond, Recover, and Continual Improvement. The finalized checklist encompasses 21 distinct items scored on a trichotomous scale: 0 for non-disclosure, 1 for qualitative or general narrative disclosure, and 2 for specific, quantitative, or technically verifiable disclosure, resulting in a maximum potential disclosure score of 42. Inter-coder reliability was confirmed through independent dual-coding, achieving a Cohen's Kappa coefficient of $\kappa = 0.697$, indicating substantial inter-rater consistency.

The independent variables operationalizing board governance attributes comprise: board independence (*BIND*, proportion of non-executive directors), board size (*BSIZE*, total number of board members), board financial expertise (*BFIN*, proportion of directors holding certified financial, accounting, or economic qualifications), board IT expertise (*BIT*, proportion of directors with formal technological, computer science, or IT backgrounds), CEO duality (*DUAL*, a binary indicator capturing simultaneous tenure as board chairman and chief executive officer), and the presence of a specialized Risk or IT Committee (*ITC*, an indicator variable denoting an active specialized committee). To control for extraneous confounding firm-level heterogeneity, the econometric specifications incorporate firm size (*SIZE*, natural logarithm of total assets), financial leverage (*LEV*, total liabilities over total assets), firm profitability (*ROA*, return on assets), and market valuation prospects (*Tobin's*).



3. RESULTS AND DISCUSSION

Descriptive statistics revealed that the dependent variable (*CSRisk*) exhibited a sample mean of 21.19 (standard deviation of 9.23), ranging from 8 to 40, representing an average disclosure level of approximately 45.7% relative to the theoretical maximum. Model specification diagnostics decisively rejected the pooled OLS estimator via the Chow test ($F = 5.563, p < 0.001$). Furthermore, the Hausman specification test yielded a significant test statistic ($\chi^2 = 23.234, p = 0.0099$), confirming that the Cross-Section Fixed Effects panel model was the statistically appropriate estimator. Diagnostic testing for cross-sectional heteroskedasticity indicated residual variance instability; consequently, the empirical model was estimated employing Cross-Section SUR (PCSE) robust standard errors. The fitted regression model exhibited substantial explanatory power ($R^2 = 0.6212$, Adjusted $R^2 = 0.5170$, and $F = 5.962, p < 0.001$).

Contrary to agency theory assumptions regarding internal monitoring efficacy, conventional board governance characteristics failed to demonstrate statistically significant associations with cybersecurity disclosure: board independence ($\beta = 1.495, t = 0.251, p = 0.8018$), board size ($\beta = -1.554, t = -0.206, p = 0.8368$), board financial expertise ($\beta = -4.194, t = -0.393, p = 0.6942$), board IT expertise ($\beta = 0.622, t = 0.059, p = 0.9530$), and CEO duality ($\beta = -2.189, t = -1.026, p = 0.3052$). Likewise, firm-level control variables (*SIZE*, *LEV*, *ROA*, and *Tobin's*) showed no statistically significant coefficients. Crucially, the presence of an active specialized Risk/IT Committee (*ITC*) was the sole explanatory mechanism displaying a statistically significant relationship, exerting a marked negative impact on cybersecurity risk disclosure ($\beta = -8.635, t = -2.239, p = 0.0257$). This empirical outcome directly corroborates Proprietary Cost Theory: specialized committees, possessing advanced technical sophistication and deep comprehension of digital vulnerability landscapes, deliberately curtail public disclosures of cyber risks and IT vulnerabilities to prevent asymmetric exploitation by hostile threat actors and to safeguard critical corporate assets.



4. CONCLUSION

The empirical evidence indicates that corporate governance in the context of digital vulnerability operates through selective withholding rather than broad transparency. Specialized IT and risk oversight committees perceive technical cybersecurity disclosures as asymmetric competitive liabilities rather than value-enhancing market signals. Consequently, these governance bodies strategically constrain external disclosure to minimize proprietary costs and avert targeted cyber-attacks. These findings generate vital policy implications for capital market authorities, notably the Securities and Exchange Organization (SEO). Regulatory entities must formulate standardized, mandatory cyber-incident and risk-reporting frameworks that distinguish defensive technical configurations—which warrant strict proprietary confidentiality—from high-level strategic posture and governance assessments required by market participants for sound capital allocation.

COPYRIGHT



This license allows others to download the works and share them with others as long as they credit them, but they can't change them in any way or use them commercially.



مقاله پژوهشی

رابطه حاکمیت شرکتی و ویژگی های هیئت مدیره با ریسک فناوری اطلاعات و امنیت سایبری: شواهدی از شرکت های تولیدی پذیرفته شده در بورس اوراق بهادار تهران^۱

مریم قاسمیان سقی^۲ و عقیل فرهنگیان^{۳*}

تاریخ دریافت: ۱۴۰۵/۰۵/۲۰

تاریخ بازنگری: ۱۴۰۵/۰۷/۰۸

تاریخ پذیرش: ۱۴۰۵/۰۸/۰۶

حسابرسی سیستم ها و فناوری اطلاعات

انجمن حسابرسی فناوری اطلاعات ایران

سال دوم، پیاپی ۱، بهار و تابستان ۱۴۰۵

صص ۱۸۷ - ۲۳۲

چکیده

هدف پژوهش حاضر بررسی تأثیر حاکمیت شرکتی و ویژگی های هیئت مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری در شرکت های تولیدی پذیرفته شده در بورس اوراق بهادار تهران است. در این پژوهش، به منظور سنجش سطح افشای ریسک فناوری اطلاعات و امنیت سایبری، شاخص پژوهشگر ساخته CSRisk بر اساس مؤلفه های چارچوب COBIT 2019 و NIST CSF 2.0 طراحی و با استفاده از تحلیل محتوای گزارش های رسمی شرکت ها اندازه گیری شد. نمونه پژوهش شامل ۱۱۷ شرکت تولیدی طی دوره ۱۴۰۰ تا ۱۴۰۴ و در مجموع ۵۸۵ مشاهده شرکت - سال است. برای آزمون فرضیه ها از رگرسیون داده های تابلویی با اثرات ثابت مقطعی استفاده شد. متغیرهای توضیحی پژوهش شامل استقلال، اندازه، تخصص مالی و تخصص فناوری اطلاعات هیئت مدیره، دوگانگی مدیرعامل و وجود کمیته تخصصی ریسک فناوری اطلاعات و متغیرهای کنترلی شامل اندازه شرکت، اهرم مالی، بازده دارایی ها و کیوتوین بودند. نتایج پژوهش نشان داد در میان متغیرهای مورد بررسی، تنها وجود کمیته تخصصی فناوری اطلاعات/ریسک رابطه آماری معناداری با سطح افشای ریسک فناوری اطلاعات و امنیت سایبری دارد. جهت این رابطه منفی است؛ بدین معنا که وجود کمیته مذکور با کاهش میزان افشای عمومی ریسک های سایبری همراه است؛ پدیده ای که می تواند ناشی از اتخاذ رویکرد «محرمانگی امنیتی» و تمرکز بر مدیریت درون سازمانی ریسک ها به جای افشای عمومی آن ها باشد.

واژه های کلیدی: حاکمیت شرکتی، هیئت مدیره، افشای ریسک امنیت سایبری، امنیت سایبری، فناوری اطلاعات.

طبقه بندی موضوعی: G34, M41, M15, G32.

^۱ <https://doi.org/10.22034/IJSTA.2026.578486.1085>

^۲ مقاله منتخب دومین همایش ملی حاکمیت شرکتی و مدیریت ریسک های فناوری اطلاعات

^۳ گروه مدیریت و حسابداری، دانشگاه شریعی، تهران، ایران. (mehrbraghasemy6@gmail.com)

^۳ گروه حسابداری، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران. (نویسنده مسئول). (aghil.farhangian@iau.ac.ir)

مقدمه

تحول دیجیتال و گسترش فناوری‌های نوین، شیوه انجام فعالیت‌های اقتصادی، پردازش اطلاعات و تصمیم‌گیری سازمان‌ها را به طور اساسی تغییر داده است. وابستگی فزاینده شرکت‌ها به سامانه‌های اطلاعاتی، رایانش ابری، هوش مصنوعی و زیرساخت‌های دیجیتال، در کنار ایجاد فرصت‌های جدید، سازمان‌ها را با ریسک‌های گسترده‌ای همچون اختلال سامانه‌ها، افشای اطلاعات، حملات سایبری و تهدیدهای مرتبط با امنیت داده مواجه کرده است. از این رو، افشای ریسک فناوری اطلاعات و امنیت سایبری دیگر صرفاً یک موضوع فنی و درون‌سازمانی نیست، بلکه به یکی از موضوعات مهم حاکمیت شرکتی و مسئولیت‌های نظارتی هیئت‌مدیره تبدیل شده است. شواهد پژوهش‌های اخیر نیز بر اهمیت نظارت هیئت‌مدیره و تخصص فناوری اطلاعات اعضای آن در تقویت حاکمیت و افشای ریسک‌های سایبری تأکید دارند (گائو و کالدرون^۱، ۲۰۲۵؛ لینگ و همکاران^۲، ۲۰۲۵: ۶).

در این میان، ساختار و ویژگی‌های هیئت‌مدیره می‌تواند بر توانایی شرکت در شناسایی، ارزیابی، کنترل و افشای ریسک‌های فناوری اطلاعات و امنیت سایبری اثرگذار باشد. استقلال و اندازه هیئت‌مدیره، تخصص مالی و فناوری اطلاعات اعضا، دوگانگی مدیرعامل و وجود ساختارهای تخصصی مانند کمیته ریسک فناوری اطلاعات، از جمله سازوکارهایی هستند که می‌توانند کیفیت نظارت بر ریسک‌های دیجیتال را تحت تأثیر قرار دهند (جنسن و مک‌لینگ^۳، ۱۹۷۶: ۳۱۰). اهمیت این موضوع برای شرکت‌های پذیرفته‌شده در بورس اوراق بهادار تهران، با توجه به حجم بالای اطلاعات، ارتباط مستمر با سرمایه‌گذاران و وابستگی روزافزون فعالیت آنها به فناوری‌های دیجیتال، دوچندان است. با وجود این، بخش عمده مطالعات داخلی حاکمیت شرکتی بر عملکرد، کیفیت گزارشگری مالی و ریسک‌های مالی متمرکز بوده و نقش ویژگی‌های هیئت‌مدیره در افشای ریسک فناوری اطلاعات و امنیت سایبری کمتر مورد بررسی قرار گرفته است؛ بنابراین، بررسی این رابطه در محیط نهادی و اطلاعاتی ایران می‌تواند شکاف موجود در ادبیات پژوهش را تا حدی پوشش دهد.

^۱ Gao & Calderon

^۲ Ling et al.

^۳ Jensen & Meckling



باتوجه به محدودیت دسترسی پژوهشگران و ذی‌نفعان بیرونی به اطلاعات داخلی مربوط به فرایندهای افشای ریسک فناوری اطلاعات و امنیت سایبری، سنجش مستقیم کیفیت مدیریت این ریسک‌ها در سطح شرکت دشوار است. ازاین‌رو، در پژوهش حاضر، «افشای اطلاعات مرتبط با ریسک فناوری اطلاعات و امنیت سایبری» به‌عنوان سنجه قابل مشاهده‌ای از میزان توجه سازمان به شفافیت، پاسخگویی و اطلاع‌رسانی درباره سازوکارهای مرتبط با این ریسک‌ها در نظر گرفته شده است. براین‌اساس، هدف پژوهش حاضر بررسی تأثیر ویژگی‌های حاکمیت شرکتی و هیئت‌مدیره بر میزان افشای ریسک فناوری اطلاعات و امنیت سایبری در شرکت‌های نمونه است.

مبانی نظری و توسعه فرضیه‌ها

افزایش وابستگی شرکت‌ها به فناوری اطلاعات و زیرساخت‌های دیجیتال، ریسک‌های ناشی از اختلال سامانه‌ها، حملات سایبری، افشای اطلاعات و نقض محرمانگی داده‌ها را به یکی از مهم‌ترین ریسک‌های نوظهور سازمانی تبدیل کرده است. در چنین شرایطی، افشای ریسک فناوری اطلاعات و امنیت سایبری را نمی‌توان صرفاً مسئولیتی فنی در سطح واحد فناوری اطلاعات دانست؛ بلکه این موضوع به بخشی از نظام حاکمیت شرکتی و نظارت هیئت‌مدیره تبدیل شده است. چارچوب امنیت سایبری مؤسسه ملی استانداردها و فناوری^۱ با افزودن و برجسته‌سازی کارکرد حاکمیت^۲ در کنار شناسایی^۳، حفاظت^۴، تشخیص^۵، پاسخگویی^۶ و بازیابی^۷، بر نقش حاکمیت و مدیریت ارشد در هدایت و نظارت بر ریسک سایبری تأکید می‌کند (پاسکو و همکاران^۸، ۲۰۲۴: ۱۴). از سوی دیگر، چارچوب کوبیت ۲۰۱۹ نیز فناوری اطلاعات را در چارچوب حاکمیت و مدیریت سازمانی قرار داده و بر بهینه‌سازی ریسک، پاسخگویی و ایجاد ارزش از فناوری اطلاعات تأکید دارد (ایساکا^۹، ۲۰۱۹: ۴۲).

^۱ NIST CSF 2.0

^۲ Govern

^۳ Identify

^۴ Protect

^۵ Detect

^۶ Respond

^۷ Recover

^۸ Pascoe et al.

^۹ ISACA



از منظر نظری، نظریه نمایندگی یکی از مبانی اصلی تبیین رابطه میان ویژگی‌های هیئت‌مدیره و مدیریت ریسک سایبری است بر اساس این نظریه، جدایی مالکیت از مدیریت می‌تواند موجب شکل‌گیری تضاد منافع و عدم تقارن اطلاعاتی میان مدیران و سهام‌داران شود. در این شرایط، هیئت‌مدیره به‌عنوان سازوکار اصلی نظارت بر مدیریت، باید بر ریسک‌های اساسی شرکت نیز نظارت کند. ریسک‌های فناوری اطلاعات و امنیت سایبری، به دلیل آثار بالقوه آنها بر عملکرد، ارزش شرکت و اعتبار سازمان، بخشی از همین مسئولیت نظارتی محسوب می‌شوند (امانی و همکاران^۱، ۲۰۲۵: ۶۱۰)؛ بنابراین، هرچه ظرفیت نظارتی هیئت‌مدیره بیشتر باشد، انتظار می‌رود شرکت سازوکارهای منسجم‌تری برای افشای ریسک‌های سایبری ایجاد کند (الودات و همکاران^۲، ۲۰۲۵: ۱۸؛ هروکس و فورتین^۳، ۲۰۲۴: ۵۴۰).

در کنار نظریه نمایندگی، نظریه وابستگی به منابع نیز می‌تواند رابطه میان ویژگی‌های هیئت‌مدیره و حاکمیت ریسک فناوری اطلاعات را توضیح دهد (پفر و سالانسیک^۴، ۲۰۰۳: ۴۵). بر اساس این دیدگاه، هیئت‌مدیره علاوه بر نقش نظارتی، منبعی از دانش، تجربه، ارتباطات و تخصص برای شرکت محسوب می‌شود. از این منظر، تنوع تخصصی اعضای هیئت‌مدیره، به‌ویژه برخورداری از دانش مالی و فناوری اطلاعات، می‌تواند ظرفیت شرکت برای شناخت و پاسخگویی به ریسک‌های پیچیده دیجیتال را افزایش دهد. همچنین، دیدگاه مبتنی بر منابع بیان می‌کند که دانش و تخصص اعضای هیئت‌مدیره می‌تواند به‌عنوان یک منبع سازمانی ارزشمند، قابلیت شرکت را برای مواجهه با محیط‌های پیچیده و متغیر افزایش دهد (الودات و همکاران، ۲۰۲۵: ۶).

این مبانی نظری با شواهد تجربی جدید نیز سازگار است؛ لینگ و همکاران (۲۰۲۵) با بررسی شرکت‌های پذیرفته‌شده چینی طی سال‌های ۲۰۰۷ تا ۲۰۲۲ نشان دادند که حضور اعضای دارای سابقه فناوری اطلاعات در هیئت‌مدیره، حاکمیت ریسک سایبری شرکت را بهبود می‌دهد و این اثر از طریق افزایش سرمایه‌گذاری فناوری اطلاعات و نوآوری دیجیتال نیز تقویت می‌شود. همچنین گائو و کالدرون^۵ (۲۰۲۵) نشان دادند که نظارت هیئت‌مدیره و تخصص سایبری اعضای

¹ Amani et al.

² Alodat et al.

³ Héroux & Fortin

⁴ Pfeffer and Salancik

⁵ Gao & Calderon



آن با افشای طولانی‌تر، شفاف‌تر و مشخص‌تر ریسک‌های امنیت سایبری ارتباط دارد؛ با این حال، هنگامی که نظارت هیئت‌مدیره جنبه نمادین داشته باشد و از سوی کمیته تخصصی پشتیبانی نشود، این اثر کاهش می‌یابد.

شواهد جدید در سال ۲۰۲۵ نیز اهمیت ساختار هیئت‌مدیره را تأیید می‌کند. مطالعه‌ای بر شرکت‌های فوتسی ۱۰۰^۱ بریتانیا نشان داده است که اندازه هیئت‌مدیره با سطح افشای امنیت سایبری رابطه مثبت دارد و وجود کمیته اختصاصی امنیت سایبری نیز به ارائه اطلاعات آینده‌نگرتر درباره ریسک‌ها و اقدامات کاهنده منجر می‌شود (الودات و همکاران، ۲۰۲۵: ۱۰). در محیط ایران نیز افزایش توجه سیاست‌گذاران به امنیت سایبری نشان‌دهنده اهمیت فزاینده این موضوع است. برای نمونه، «سند ستاد توسعه علوم و فناوری افتا» در سال ۱۴۰۴ با هدف توسعه ظرفیت‌های علمی و فناورانه امنیت سایبری به تصویب رسید (هیئت وزیران، ۱۴۰۴: مصوبه شماره ۳۶۶۰۸).

با وجود این تحولات، شواهد تجربی درباره رابطه میان ساختار هیئت‌مدیره و افشای ریسک فناوری اطلاعات و امنیت سایبری در شرکت‌های ایرانی همچنان محدود است. همچنین، مطالعات موجود عمدتاً یکی از ابعاد ساختار هیئت‌مدیره، مانند استقلال یا تخصص فناوری را بررسی کرده‌اند و کمتر پژوهشی مجموعه‌ای از ویژگی‌های ساختاری، تخصصی و نظارتی هیئت‌مدیره را به صورت هم‌زمان با یک شاخص ترکیبی و ساختاریافته برای افشای ریسک فناوری اطلاعات و امنیت سایبری ارزیابی نموده‌اند. پژوهش حاضر با تمرکز بر شرکت‌های پذیرفته‌شده در بورس اوراق بهادار تهران و استفاده از شاخصی مبتنی بر چارچوب کویت ۲۰۱۹ و چارچوب امنیت سایبری مؤسسه ملی استانداردها و فناوری، درصدد پاسخگویی به این خلأ است.

استقلال هیئت‌مدیره و افشای ریسک فناوری اطلاعات و امنیت سایبری

استقلال هیئت‌مدیره یکی از مهم‌ترین سازوکارهای حاکمیت شرکتی برای کاهش مشکلات نمایندگی و تقویت نظارت بر مدیریت است. اعضای مستقل و غیرموظف به دلیل وابستگی کمتر به مدیریت اجرایی و تمایل به حفظ اعتبار و سرمایه حرفه‌ای خود، از انگیزه و

¹ FTSE100



ظرفیت بیشتری برای ارزیابی بی‌طرفانه تصمیمات مدیران و نظارت بر ریسک‌های اساسی شرکت برخوردارند (هروکس و فورتین، ۲۰۲۴: ۵۳۱). در حوزه امنیت سایبری نیز استقلال هیئت‌مدیره موجب می‌شود موضوعات مرتبط با امنیت اطلاعات، کنترل‌های فناوری و ریسک‌های دیجیتال با دیدگاه مستقل‌تر و نقادانه‌تری بررسی شوند و احتمال پنهان‌سازی یا کم‌اهمیت جلوه دادن آسیب‌پذیری‌های سایبری توسط مدیران اجرایی کاهش یابد (ماتمانه و همکاران^۱، ۲۰۲۴: ۳۸؛ الودات و همکاران^۲، ۲۰۲۵: ۷؛ گائو و کالدرون، ۲۰۲۵: ۴).

از منظر نظریه نمایندگی، هیئت‌مدیره مستقل می‌تواند عدم تقارن اطلاعاتی میان مدیران و سهام‌داران را کاهش داده و مدیران را نسبت به شناسایی و افشای ریسک‌های بااهمیت پاسخگوتر کند؛ بنابراین، انتظار می‌رود شرکت‌هایی که از هیئت‌مدیره مستقل‌تری برخوردارند، سازوکارهای نظارتی قوی‌تر و سطح افشای جامع‌تری در زمینه ریسک‌های فناوری اطلاعات و امنیت سایبری داشته باشند. شواهد پژوهش‌های جدید نیز نشان می‌دهد ویژگی‌های هیئت‌مدیره می‌توانند در شکل‌دهی به کیفیت افشای سایبری مؤثر باشند، هرچند شدت این رابطه به ساختارهای مکمل نظارتی نیز وابسته است (ماتمانه و همکاران، ۲۰۲۴: ۴۸).

اندازه هیئت‌مدیره و افشای ریسک فناوری اطلاعات و امنیت سایبری

اندازه هیئت‌مدیره از دو مسیر بر کیفیت نظارت اثرگذار است. از یک سو، افزایش تعداد اعضا موجب تنوع بیشتر در دانش، تجربه، تخصص و دیدگاه‌های اعضا شده و ظرفیت هیئت‌مدیره را برای مواجهه با ریسک‌های پیچیده‌ای؛ مانند ریسک سایبری افزایش می‌دهد. از سوی دیگر، بزرگ‌شدن بیش از اندازه هیئت‌مدیره ممکن است هماهنگی، ارتباطات و سرعت تصمیم‌گیری را کاهش دهد. بااین‌حال در زمینه ریسک سایبری، اهمیت تنوع دانش و تخصص برجسته‌تر است. شواهد تجربی شرکت‌های شاخص فوتسی ۱۰۰ نشان داد که اندازه هیئت‌مدیره با سطح افشای امنیت سایبری رابطه مثبت دارد که ناشی از تنوع مهارتی در هیئت‌مدیره‌های بزرگ‌تر است؛ بنابراین، در بازار سرمایه ایران نیز انتظار می‌رود اندازه بهینه هیئت‌مدیره، ظرفیت نظارت بر ریسک‌های دیجیتال را بهبود بخشد (الودات و همکاران، ۲۰۲۵: ۹).

¹ Matemane et al.

² Alodat et al.



تخصص مالی هیئت‌مدیره و افشای ریسک فناوری اطلاعات و امنیت سایبری

تخصص مالی اعضای هیئت‌مدیره یکی از ویژگی‌هایی است که می‌تواند کیفیت نظارت بر ریسک‌های سازمانی را افزایش دهد (فصیحی و برشد، ۱۴۰۲: ۴۵؛ اسماعیلی و همکاران، ۲۰۲۳: ۱۱۲). اعضای دارای دانش حسابداری، مالی و حسابرسی، توانایی بیشتری در تحلیل پیامدهای اقتصادی ریسک‌ها، ارزیابی کنترل‌های داخلی و تفسیر اطلاعات مالی دارند. اگرچه امنیت سایبری در ظاهر ماهیتی فناورانه دارد، پیامدهای آن می‌تواند مستقیماً به زیان مالی، کاهش ارزش شرکت، اختلال عملیاتی، هزینه‌های بازایی و کاهش اعتماد سرمایه‌گذاران منجر شود (امانی و همکاران، ۲۰۲۵: ۶۰۸).

از این منظر، تخصص مالی می‌تواند به هیئت‌مدیره کمک کند تا ریسک فناوری اطلاعات را صرفاً به عنوان یک مسئله فنی تلقی نکند، بلکه پیامدهای مالی و راهبردی آن را نیز ارزیابی کند؛ بنابراین، انتظار می‌رود هیئت‌مدیره‌هایی که از اعضای دارای تخصص مالی بیشتری برخوردارند، انگیزه و توان بیشتری برای نظارت بر افشای ریسک‌های فناوری اطلاعات و امنیت سایبری داشته باشند (اسماعیلی و همکاران، ۲۰۲۳: ۱۱۵).

این استدلال با منطق نظریه نمایندگی نیز سازگار است؛ زیرا اعضای دارای تخصص مالی می‌توانند کیفیت نظارت بر گزارشگری و کنترل‌های مرتبط با ریسک را تقویت کنند و از کاهش شفافیت ناشی از عدم تقارن اطلاعاتی جلوگیری نمایند (امانی و همکاران، ۲۰۲۵: ۶۱۲).

تخصص فناوری اطلاعات هیئت‌مدیره و افشای ریسک فناوری اطلاعات و امنیت سایبری

تخصص فناوری اطلاعات را می‌توان یکی از مهم‌ترین قابلیت‌های هیئت‌مدیره در عصر تحول دیجیتال دانست. پیچیدگی تهدیدهای سایبری، وابستگی شرکت‌ها به سامانه‌های اطلاعاتی و سرعت تغییر فناوری موجب شده است که نظارت مؤثر بر این حوزه بدون درک حداقلی از فناوری‌های نوین، معماری اطلاعات، امنیت داده‌ها و تهدیدهای سایبری دشوار باشد.

لینگ و همکاران (۲۰۲۵) در مطالعه شرکت‌های بورسی چین نشان دادند که وجود مدیران دارای سابقه فناوری اطلاعات، به طور معناداری حاکمیت ریسک سایبری را بهبود می‌دهد و این اثر از طریق افزایش سرمایه‌گذاری فناوری اطلاعات و نوآوری دیجیتال نیز شکل می‌گیرد.

¹ Smaili et al.



همچنین، پژوهش گائو و کالدرون (۲۰۲۵) درباره حاکمیت ریسک سایبری نشان داد که تخصص سایبری هیئت‌مدیره با افشای دقیق‌تر و باکیفیت‌تر ریسک‌های امنیت سایبری ارتباط دارد؛ بنابراین، انتظار می‌رود حضور اعضای دارای دانش و تجربه فناوری اطلاعات در هیئت‌مدیره شرکت‌های ایرانی نیز ظرفیت شناسایی، ارزیابی و نظارت بر ریسک‌های فناوری و امنیت سایبری را افزایش دهد. در کنار ویژگی‌های مدیرعامل، ویژگی‌های فردی مدیران ارشد نیز مستقیماً بر میزان افشای سایبری اثرگذار است (ترین و همکاران^۱، ۲۰۲۵: ۳).

دوگانگی مدیرعامل و افشای ریسک فناوری اطلاعات و امنیت سایبری

دوگانگی مدیرعامل به ساختاری اشاره دارد که در آن یک فرد به طور هم‌زمان سمت مدیرعامل و ریاست هیئت‌مدیره را بر عهده دارد. این ساختار از یک سو با ایجاد وحدت فرماندهی، تسریع تصمیم‌گیری و بهبود هماهنگی میان مدیریت اجرایی و هیئت‌مدیره همراه است؛ اما از سوی دیگر استقلال نظارتی هیئت‌مدیره را کاهش می‌دهد و قدرت نظارت مدیران غیرموظف بر مدیرعامل را محدود می‌کند (نمازی و ابراهیمی میمند، ۱۳۹۵: ۱؛ الشیراح^۲، ۲۰۲۴: ۵۴).

از منظر نظریه نمایندگی، تجمع هم‌زمان قدرت اجرایی و نظارتی در دست یک فرد می‌تواند تعارض منافع را تشدید و اثربخشی سازوکارهای کنترل مدیریت را تضعیف کند (الشاعر و همکاران^۳، ۲۰۲۵). این مسئله در زمینه ریسک‌های فناوری اطلاعات و امنیت سایبری از اهمیت بیشتری برخوردار است؛ زیرا تصمیمات مرتبط با سرمایه‌گذاری فناوری، طراحی کنترل‌های امنیتی و افشای ریسک، ذاتاً به نظارت مستقل هیئت‌مدیره نیازمندند (ترین و همکاران، ۲۰۲۵: ۳).

بنابراین، از منظر تئوری نمایندگی انتظار می‌رود در صورت وجود هم‌زمانی احتمالی سمت مدیرعامل و رئیس هیئت‌مدیره، استقلال نظارت بر ریسک‌های فناوری اطلاعات و امنیت سایبری کاهش‌یافته و در نتیجه سطح افشای این ریسک‌ها پایین‌تر باشد؛ هرچند مقررات

¹ Trinh et al.

² Alshira'h

³ Al-Shaer et al.



حاکمیت شرکتی سازمان بورس اوراق بهادار تفکیک این دو سمت را الزامی کرده است، اما بررسی نمونه‌های پژوهش نشان‌دهنده لزوم کنترل این متغیر است.

کمیته ریسک فناوری اطلاعات و افشای ریسک فناوری اطلاعات و امنیت سایبری

تشکیل کمیته تخصصی ریسک یا فناوری اطلاعات، سازوکاری ساختاریافته برای نظارت مستمر بر تهدیدها، ارزیابی کنترل‌های امنیتی و گزارش‌دهی مستقیم به هیئت‌مدیره به شمار می‌رود. گائو و کالدرون (۲۰۲۵) تأکید می‌کنند که نظارت هیئت‌مدیره در صورتی که با پشتیبانی کمیته‌های تخصصی همراه نباشد، از اثربخشی پایینی برخوردار خواهد بود. افزون بر این، الودات و همکاران (۲۰۲۵) نشان دادند شرکت‌های دارای کمیته تخصصی، اطلاعات جامع‌تر و آینده‌نگرانه‌تری پیرامون ریسک‌ها و اقدامات کاهنده ارائه می‌دهند. با این وجود، درخصوص جهت‌گیری اثرگذاری این کمیته‌ها بر سطح افشای عمومی، دو رویکرد نظری متمایز در ادبیات حاکمیت شرکتی قابل ردیابی است:

از یک طرف، بر مبنای نظریه نمایندگی، استقرار این کمیته‌ها از مجرای ارتقای کارآمدی نظارت و کاهش عدم‌تقارن اطلاعاتی، مدیریت را به سمت شفاف‌سازی بیش‌تر مخاطرات و سازوکارهای کنترلی در گزارش‌های برون‌سازمانی سوق می‌دهد (گائو و کالدرون، ۲۰۲۵: ۴؛ الودات و همکاران، ۲۰۲۵: ۹).

در مقابل، نظریه هزینه‌های مالکانه استدلال می‌کند که افشای اطلاعات همواره سودمند نیست؛ زیرا انتشار عمومی اطلاعات حساس، ممکن است به جایگاه رقابتی یا امنیت شرکت آسیب برساند. در حوزه امنیت سایبری، اطلاعات مربوط به زیرساخت‌های فناوری، آسیب‌پذیری‌های سیستم و نقاط ضعف امنیتی، ماهیتی کاملاً استراتژیک و محرمانه دارند. از این دیدگاه، افشای تفصیلی این اطلاعات می‌تواند همانند ارائه یک «نقشه راه» به مهاجمان سایبری و رقبا عمل کرده و احتمال نفوذ و تحمیل هزینه‌های سنگین را به بنگاه افزایش دهد (لینگ و همکاران، ۲۰۲۵: ۶؛ فیروزی و محسنی^۱، ۲۰۲۳: ۴۶۰). از این‌رو، اعضای کمیته‌های تخصصی فناوری اطلاعات و ریسک با درک عمق این مخاطرات و اتخاذ رویکرد «صیانت امنیتی»، ترجیح می‌دهند تمرکز خود را بر تقویت کنترل‌های داخلی سازمان معطوف سازند و از

^۱ Firoozi & Mohsni



افشای علنی جزئیات این ریسک‌ها پرهیز کنند. بنابراین، سطح افشای ریسک سایبری حاصل یک موازنه بین دو نیروی متضاد است: ایجاد شفافیت اطلاعاتی برای بازار از یک‌سو، و حفاظت از اطلاعات حساس و حریم امنیتی شرکت از سوی دیگر (هروکس و فورتین، ۲۰۲۴: ۳۸۵).

لینگ و همکاران (۲۰۲۵)، با تحلیل داده‌های شرکت‌های بورسی چین طی سال‌های ۲۰۰۷ تا ۲۰۲۲ دریافتند که حضور اعضای دارای سابقه فناوری اطلاعات در هیئت‌مدیره، حاکمیت ریسک سایبری و نوآوری دیجیتال شرکت را بهبود می‌بخشد.

گائو و کالدرون (۲۰۲۵)، نیز نشان دادند که نظارت هیئت‌مدیره و تخصص سایبری اعضا با افشای طولانی‌تر، شفاف‌تر و مشخص‌تر ریسک‌های امنیت سایبری ارتباط دارد؛ هرچند در صورت نمادین بودن نظارت و نبود کمیته اختصاصی، این اثر تضعیف می‌شود.

الودات و همکاران (۲۰۲۵)، با مطالعه شرکت‌های شاخص فوتسی ۱۰۰ بریتانیا دریافتند که اندازه و استقلال هیئت‌مدیره با سطح افشای امنیت سایبری رابطه مثبت دارد و سازوکارهای نظارتی اختصاصی، ارائه اطلاعات آینده‌نگرتر درباره ریسک‌ها و اقدامات کاهنده را تسهیل می‌کند.

ماتمانه و همکاران (۲۰۲۴)، با اتکا به نظریه نمایندگی در بازارهای نوظهور نشان دادند که سازوکارهای نظارتی هیئت‌مدیره، انگیزه مدیران برای پنهان‌سازی ضعف‌های امنیتی را کاهش داده و کیفیت افشای ریسک سایبری را ارتقا می‌دهد.

کریمی و صیفی (۱۴۰۳)، نشان دادند متغیرهای ساختاری هیئت‌مدیره از جمله درصد اعضای غیرموظف و وجود کمیته حسابرسی/ریسک، شرکت‌ها را به ارائه اطلاعات تحلیلی‌تر درباره خطرات نوظهور عملیاتی و دیجیتال ترغیب می‌کند.

فصیحی و برشد (۱۴۰۲)، دریافتند حضور اعضای دارای سواد مالی و تسلط بر فناوری‌های نوین، تمایل به مخفی‌کاری درباره ریسک‌های زیرساختی را کاهش داده و شفافیت شرکتی را به‌صورت معنادار تقویت می‌کند.

بر اساس تئوری نمایندگی، در شرکت‌هایی که با وجود ضوابط سازمان بورس، به‌صورت موردی یا انتقالی مدیرعامل هم‌زمان رئیس یا نایب‌رئیس هیئت‌مدیره است، به دلیل تمرکز قدرت و تضعیف نقش نظارتی هیئت‌مدیره، تمایل کمتری به شفاف‌سازی تهدیدات و آسیب‌پذیری‌های فناوری وجود دارد؛ این موضوع در پژوهش‌های (نمازی و ابراهیمی میمند،



(۱۳۹۵) در بازار ایران و (الگمال و همکاران^۱، ۲۰۱۸) در سطح بین‌المللی مورد تأیید قرار گرفته است.

مرور اجمالی پژوهش‌های داخلی از جمله نمازی و ابراهیمی میمند (۱۳۹۵)؛ فصیحی و برشد (۱۴۰۲) و کرمی و صیفی (۱۴۰۳) حاکی از آن است که ادبیات موجود عمدتاً بر افشای ریسک‌های سنتی (مالی، اعتباری و بازار) یا شفافیت گزارشگری مالی متمرکز بوده‌اند و باوجود رشد تهدیدات دیجیتال، ریسک فناوری اطلاعات و امنیت سایبری در شرکت‌های تولیدی ایرانی کمتر به‌صورت تجربی و با یک شاخص ترکیبی و ساختاریافته ارزیابی شده است. افزون بر این، در ادبیات داخلی متغیرهای نوینی مانند تخصص فناوری اطلاعات اعضای هیئت‌مدیره و وجود کمیته تخصصی ریسک/فناوری اطلاعات، به‌ندرت در کنار متغیرهای کلاسیک حاکمیت شرکتی و متغیرهای کنترلی مالی در قالب یک مدل یکپارچه آزمون شده‌اند. پژوهش حاضر باهدف پوشش این شکاف، به تبیین نقش هم‌زمان این ویژگی‌ها با استفاده از شاخص ترکیبی در شرکت‌های تولیدی بورس اوراق بهادار تهران طی سال‌های ۱۴۰۰ تا ۱۴۰۴ می‌پردازد.

فرضیه‌های پژوهش

- استقلال هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.
- اندازه هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.
- تخصص مالی هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.
- تخصص فناوری اطلاعات هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.
- دوگانگی مدیرعامل بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.
- بین وجود کمیته تخصصی فناوری اطلاعات/ریسک در هیئت‌مدیره و سطح افشای ریسک فناوری اطلاعات و امنیت سایبری رابطه معناداری وجود دارد.

¹ Elgammal et al.



جامعه آماری و نمونه پژوهش

جامعه آماری پژوهش حاضر شامل کلیه شرکت‌های پذیرفته‌شده در بورس اوراق بهادار تهران در بازه زمانی پنج‌ساله ۱۴۰۰ الی ۱۴۰۴ است. در این پژوهش، تمرکز بر شرکت‌های تولیدی (غیرمالی) قرار گرفته است؛ چرا که نهادهای مالی و واسطه‌گری نظیر بانک‌ها، بیمه‌ها و شرکت‌های سرمایه‌گذاری به دلیل ماهیت عملیاتی متمایز، ساختار ترازنامه و سرمایه متفاوت و همچنین تبعیت از الزامات نظارتی و استانداردهای گزارشگری خاص نهادهای بالادستی (نظیر بانک مرکزی و بیمه مرکزی)، از سازوکارهای حاکمیتی و رفتارهای افشای متفاوتی نسبت به بخش تولیدی پیروی می‌کنند. بنابراین، ادغام آن‌ها با شرکت‌های تولیدی موجب ناهمگنی شدید و سوگیری در نتایج مدل‌های رگرسیونی می‌گردد.

جدول ۱

جامعه آماری پژوهش

مرحله	معیار	تعداد شرکت‌های باقیمانده
۱	کل شرکت‌های جامعه آماری	۳۹۵
۲	حذف شرکت دارای توقف معاملاتی بیش از ۳ ماه و عدم دسترسی به اطلاعات	(۸۰)
۳	حذف شرکت‌هایی که سال مالی آنها منتهی به اسفندماه نیست	(۷۵)
۴	حذف شرکت‌های سرمایه‌گذاری، بانک و بیمه	(۱۲۳)
نهایی	شرکت‌های واجد شرایط	۱۱۷

پس از اعمال محدودیت‌های فوق، تعداد ۱۱۷ شرکت به‌عنوان نمونه نهایی پژوهش انتخاب شد که با در نظر گرفتن دوره زمانی پنج‌ساله، مجموعاً ۵۸۵ مشاهده شرکت سال را تشکیل می‌دهند.

روش گردآوری اطلاعات

اطلاعات پژوهش به روش کتابخانه‌ای و اسنادی گردآوری شد. برای استخراج اطلاعات مربوط به متغیرهای حاکمیت شرکتی و ویژگی‌های هیئت‌مدیره، گزارش‌های هیئت‌مدیره،



صورت‌های مالی، گزارش‌های سالانه و سایر اطلاعات منتشر شده توسط شرکت‌ها بررسی شد. همچنین اطلاعات مالی مورد نیاز برای محاسبه متغیرهای کنترلی از صورت‌های مالی و اطلاعات تاریخی شرکت‌ها استخراج گردید. برای سنجش افشای ریسک فناوری اطلاعات و امنیت سایبری، گزارش‌های هیئت‌مدیره و سایر گزارش‌های رسمی شرکت‌ها با استفاده از تحلیل محتوای ساختاریافته بررسی شد. شاخص مورد استفاده با اتکا به مؤلفه‌های مرتبط با حاکمیت مدیریت ریسک و امنیت سایبری در چارچوب COBIT 2019 و NIST CSF 2.0 طراحی شد و اطلاعات کیفی موجود در گزارش‌های شرکت‌ها به شاخص کمی و قابل مقایسه تبدیل گردید.

سنجش متغیر وابسته و نحوه گردآوری اطلاعات

متغیر وابسته پژوهش، شاخص افشای ریسک فناوری اطلاعات و امنیت سایبری (*CSRisk*) است که میزان جزئیات افشای شرکت را در ۷ حوزه (حاکمیت، شناسایی، حفاظت، کشف، پاسخ، بازیابی و بهبود مستمر) اندازه‌گیری می‌کند. با توجه به عدم دسترسی مستقیم به فرآیندهای درون‌سازمانی، اسناد رسمی شرکت‌ها در دوره ۱۴۰۰ تا ۱۴۰۴ شامل «گزارش‌های هیئت‌مدیره»، «یادداشت‌های توضیحی صورت‌های مالی» و «گزارش‌های کنترل داخلی و حسابرس» از طریق سامانه کدال (*Codal.ir*) و پایگاه مدیریت فناوری بورس استخراج شد (داده‌های مالی کنترلی نیز با استفاده از پایگاه ره‌آورد نوین صحنه‌گذاری شدند). سپس با استفاده از روش تحلیل محتوای ساختاریافته، متون اسناد بر مبنای ۲۱ قلم افشا (برگرفته از استانداردهای COBIT 2019 و NIST CSF 2.0) ارزیابی شدند. امتیاز هر قلم در مقیاس سه‌سطحی (عدم افشا: ۰، افشای کلی: ۱، و افشای تفصیلی: ۲) تعیین شد؛ به گونه‌ای که مجموع امتیازات شاخص *CSRisk* را در دامنه ۰ تا ۴۲ تشکیل می‌دهد.

تعریف عملیاتی متغیرهای پژوهش

تعریف عملیاتی متغیرهای پژوهش در جدول ۲ نشان داده شده است.



جدول ۲

تعریف عملیاتی متغیرهای پژوهش

نوع متغیر	متغیر	نماد	تعریف عملیاتی
وابسته	افشای ریسک فناوری اطلاعات و امنیت سایبری	CSRisk	شاخص افشای مبتنی بر مؤلفه‌های COBIT 2019 و NIST CSF
مستقل	استقلال هیئت‌مدیره	BIND	نسبت اعضای غیرموظف/مستقل به کل اعضای هیئت‌مدیره
مستقل	اندازه هیئت‌مدیره	BSIZE	لگاریتم طبیعی تعداد اعضای هیئت‌مدیره
مستقل	تخصص مالی هیئت‌مدیره	BFIN	نسبت اعضای دارای تحصیلات یا تجربه حرفه‌ای مرتبط با مالی، حسابداری یا حسابرسی به کل اعضا
مستقل	تخصص فناوری اطلاعات	BIT	نسبت اعضای دارای تحصیلات یا تجربه حرفه‌ای مرتبط با فناوری اطلاعات، سیستم‌های اطلاعاتی یا امنیت سایبری به کل اعضا
مستقل	دوگانگی مدیرعامل	DUAL	در صورت هم‌زمانی سمت مدیرعامل و رئیس هیئت‌مدیره برابر ۱ و در غیر این صورت صفر
مستقل	کمیت ریسک فناوری اطلاعات	ITC	متغیر مجازی؛ در صورت وجود کمیت تخصصی مرتبط با ریسک فناوری اطلاعات/امنیت سایبری برابر ۱ و در غیر این صورت صفر
کنترلی	اندازه شرکت	Size	لگاریتم طبیعی مجموع دارایی‌های شرکت
کنترلی	اهرم مالی	Lev	نسبت کل بدهی‌ها به کل دارایی‌ها
کنترلی	بازده دارایی‌ها	ROA	نسبت سود خالص به کل دارایی‌ها
کنترلی	Q توبین	TQ	ارزش بازار حقوق صاحبان سهام + ارزش دفتری بدهی‌ها / ارزش دفتری دارایی‌ها

مدل آزمون فرضیه‌ها

برای آزمون فرضیه‌های پژوهش، از مدل رگرسیون چندمتغیره استفاده می‌شود. مدل پایه پژوهش به صورت زیر تعریف می‌شود:

$$CSRisk_{i,t} = \beta_0 + \beta_1 BIND_{i,t} + \beta_2 BSIZE_{i,t} + \beta_3 BFIN_{i,t} + \beta_4 BIT_{i,t} + \beta_5 DUAL_{i,t} + \beta_6 ITC_{i,t} + \beta_7 Size_{i,t} + \beta_8 Lev_{i,t} + \beta_9 ROA_{i,t} + \beta_{10} TQ_{i,t} + \varepsilon_{i,t}$$



که در آن، CSRisk افشای ریسک فناوری اطلاعات و امنیت سایبری، BIND استقلال هیئت‌مدیره، BSIZE اندازه هیئت‌مدیره، BFIN تخصص مالی، BIT تخصص فناوری اطلاعات، DUAL دوگانگی مدیرعامل و ITC وجود کمیته ریسک فناوری اطلاعات است. همچنین Size، Lev، ROA و TQ متغیرهای کنترلی مدل هستند. در آزمون فرضیه‌ها، علامت و معناداری ضرایب β_1 تا β_6 مبنای ارزیابی فرضیه‌های پژوهش قرار می‌گیرد. به طور مشخص، انتظار می‌رود ضرایب استقلال هیئت‌مدیره، اندازه هیئت‌مدیره، تخصص مالی، تخصص فناوری اطلاعات و کمیته ریسک فناوری اطلاعات مثبت و ضریب دوگانگی مدیرعامل منفی باشد.

فنون تجزیه و تحلیل داده‌ها

در مرحله نخست، از آمار توصیفی شامل میانگین، میانه، انحراف معیار، حداقل و حداکثر برای توصیف متغیرهای پژوهش استفاده و سپس پیش‌فرض‌های لازم برای برآورد مدل بررسی شد. از جمله این آزمون‌ها می‌توان به بررسی هم‌خطی بین متغیرهای توضیحی، ناهمسانی واریانس، خودهمبستگی و وابستگی مقطعی اشاره کرد. باتوجه به ساختار داده‌ها که شامل اطلاعات چند شرکت در چند سال است، داده‌ها به صورت تابلویی تحلیل شدند. پس از تعیین مدل مناسب از طریق آزمون‌های چاو و هاسمن، مدل رگرسیونی با اثرات ثابت مقطعی برآورد و معناداری ضرایب با استفاده از آماره t بررسی شد. همچنین، برای بررسی هم‌خطی میان متغیرهای توضیحی، شاخص‌های VIF و Tolerance محاسبه شدند. در صورت مشاهده ناهمسانی واریانس یا خودهمبستگی بر اساس آزمون‌های تشخیصی مربوط، برآورد مدل با استفاده از خطاهای استاندارد مقاوم یا روش برآورد متناسب با ویژگی داده‌ها انجام شد.

روایی و پایایی شاخص پژوهش

از آنجاکه متغیر وابسته با استفاده از یک شاخص پژوهشگر ساخته و مبتنی بر تحلیل محتوای گزارش‌های شرکت‌ها اندازه‌گیری می‌شود، اعتبار آن از دو جنبه بررسی شد. نخست، روایی محتوایی شاخص از طریق انطباق مؤلفه‌ها با چارچوب‌های کوبیت ۲۰۱۹ و چارچوب امنیت سایبری نیست (NIST CSF 2.0)^۱ تأمین می‌شود. استفاده از چارچوب‌های

^۱ NIST Cybersecurity Framework (NIST CSF)



استاندارد و شناخته‌شده بین‌المللی موجب می‌شود شاخص طراحی شده ابعاد اصلی حاکمیت، مدیریت و پاسخگویی به ریسک‌های فناوری اطلاعات و امنیت سایبری را پوشش دهد. دوم، برای افزایش پایداری کدگذاری، دستورالعمل مشخصی برای تحلیل محتوای گزارش‌ها شد و کدگذاری اقلام شاخص بر اساس معیارهای از پیش تعیین شده انجام شد. در صورت امکان، بخشی از گزارش‌ها توسط کدگذار دوم نیز بررسی و میزان توافق میان کدگذاران با استفاده از ضریب مناسب توافق ارزیابی می‌شود.

مراحل انجام پژوهش

فرایند اجرای پژوهش در چند مرحله انجام شد:

- مرحله اول: شناسایی مبانی نظری و مطالعات مرتبط با حاکمیت شرکتی، ساختار هیئت‌مدیره، افشای ریسک فناوری اطلاعات و امنیت سایبری.
- مرحله دوم: طراحی شاخص افشای ریسک فناوری اطلاعات و امنیت سایبری بر اساس مؤلفه‌های مرتبط در چارچوب‌ها.
- مرحله سوم: شناسایی شرکت‌های جامعه آماری و اعمال معیارهای انتخاب نمونه.
- مرحله چهارم: جمع‌آوری گزارش‌های سالانه، گزارش‌های هیئت‌مدیره، صورت‌های مالی و سایر اطلاعات موردنیاز شرکت‌ها برای دوره ۱۴۰۰ تا ۱۴۰۴.
- مرحله پنجم: کدگذاری اطلاعات مرتبط با ریسک فناوری اطلاعات و امنیت سایبری و محاسبه شاخص CSRisk.
- مرحله ششم: محاسبه متغیرهای مستقل و کنترل بر اساس اطلاعات منتشرشده شرکت‌ها.
- مرحله هفتم: انجام آمار توصیفی و آزمون‌های تشخیصی و بررسی ویژگی‌های داده‌های ترکیبی.
- مرحله هشتم: برآورد مدل رگرسیونی و آزمون فرضیه‌های پژوهش.
- مرحله نهم: تفسیر ضرایب، بررسی معناداری روابط و ارائه نتایج و پیامدهای کاربردی پژوهش.

در مجموع، پژوهش حاضر با استفاده از داده‌های شرکت‌های پذیرفته‌شده در بورس اوراق بهادار تهران طی سال‌های ۱۴۰۰ تا ۱۴۰۴، رابطه میان ویژگی‌های حاکمیت شرکتی و هیئت‌مدیره



و سطح افشای ریسک فناوری اطلاعات و امنیت سایبری را بررسی کرد. نوآوری روش شناختی پژوهش در این است که به جای اتکا به سنجه‌های کلی ریسک، شاخص مشخصی برای افشای ریسک فناوری اطلاعات و امنیت سایبری بر اساس چارچوب‌های کوبیت (COBIT ۲۰۱۹) (2019) و چارچوب امنیت سایبری ان‌آی‌اس‌تی (NIST CSF) ایجاد شده و سپس ارتباط آن با ویژگی‌های ساختاری و تخصصی هیئت‌مدیره در قالب داده‌های ترکیبی آزمون می‌شود.

طراحی و محاسبه شاخص افشای ریسک فناوری اطلاعات و امنیت سایبری (CSRisk)
در پژوهش حاضر، به منظور اندازه‌گیری سطح افشای ریسک فناوری اطلاعات و امنیت سایبری، شاخصی ترکیبی با عنوان CSRisk طراحی شده است. مبنای طراحی این شاخص، مؤلفه‌های مرتبط با حاکمیت، مدیریت ریسک و امنیت سایبری بر اساس چارچوب‌های کوبیت ۲۰۱۹ و چارچوب امنیت سایبری (NIST CSF 2.0) است.

انتخاب این دو چارچوب به این دلیل است که کوبیت ۲۰۱۹ بر حاکمیت و مدیریت فناوری اطلاعات در سطح سازمان تأکید دارد، در حالی که چارچوب امنیت سایبری نیست (NIST CSF 2.0) چارچوبی ساختاریافته برای مدیریت ریسک امنیت سایبری ارائه می‌کند. ترکیب این دو رویکرد امکان می‌دهد شاخص پژوهش علاوه بر جنبه‌های فنی امنیت سایبری، ابعاد حاکمیتی، مدیریتی، کنترلی و پاسخگویی ریسک‌های فناوری اطلاعات را نیز پوشش دهد.

جدول ۳

چارچوب شاخص افشای ریسک فناوری اطلاعات و امنیت سایبری CSRisk

منبع چارچوبی	نمونه موارد قابل شناسایی در گزارش شرکت	مؤلفه مورد بررسی	بُعد اصلی
COBIT 2019 / NIST CSF 2.0	اشاره به مسئولیت هیئت‌مدیره، مدیریت ارشد یا کمیته تخصصی در قبال امنیت اطلاعات و ریسک سایبری	مسئولیت هیئت‌مدیره و مدیریت ارشد	حاکمیت و راهبری
COBIT 2019 / NIST CSF 2.0	وجود سیاست، برنامه یا راهبرد رسمی امنیت اطلاعات و سایبری	سیاست‌ها و راهبرد امنیت سایبری	
COBIT 2019 / NIST CSF 2.0	اشاره به نظارت، گزارش‌دهی یا پایش ریسک‌های فناوری اطلاعات	نظارت بر ریسک فناوری اطلاعات	
NIST CSF 2.0	شناسایی سامانه‌ها، داده‌ها، زیرساخت‌ها و دارایی‌های دیجیتال	شناسایی دارایی‌ها و زیرساخت‌های اطلاعاتی	



منبع چارچوبی	نمونه موارد قابل‌شناسایی در گزارش شرکت	مؤلفه مورد بررسی	بعد اصلی
NIST CSF 2.0	اشاره به تهدیدهای سایبری، آسیب‌پذیری‌ها یا مخاطرات فناوری	شناسایی تهدیدها و آسیب‌پذیری‌ها	شناسایی و ارزیابی ریسک
COBIT 2019 / NIST CSF 2.0	شناسایی، ارزیابی یا اولویت‌بندی ریسک‌های فناوری اطلاعات و سایبری	ارزیابی ریسک	
NIST CSF 2.0	کنترل دسترسی کاربران، احراز هویت و مدیریت مجوزها	کنترل دسترسی	حفاظت و کنترل
NIST CSF 2.0	پشتیبان‌گیری، رمزنگاری، حفاظت از اطلاعات محرمانه و داده‌های حساس	حفاظت از داده‌ها	
COBIT 2019 / NIST CSF 2.0	استفاده از کنترل‌ها و راهکارهای امنیتی برای حفاظت از سامانه‌ها	کنترل‌های امنیتی و فناوری	
NIST CSF 2.0	نظارت مستمر بر سامانه‌ها و رویدادهای امنیتی	پایش مستمر	کشف و پایش
NIST CSF 2.0	سازوکارهای شناسایی حملات، نفوذ و رخدادهای امنیتی	شناسایی رخدادهای سایبری	
COBIT 2019	ممیزی، ارزیابی یا آزمون اثربخشی کنترل‌های فناوری اطلاعات	ارزیابی کنترل‌ها	
NIST CSF 2.0	وجود برنامه یا رویه مشخص برای مقابله با رخدادهای سایبری	برنامه پاسخ به رخداد	پاسخ و مدیریت رخداد
NIST CSF 2.0	تعیین مسئولیت افراد یا واحدهای سازمانی در زمان وقوع رخداد	مسئولیت‌ها و فرایند پاسخگویی	
NIST CSF 2.0	گزارش‌دهی رخدادهای مهم به مدیریت یا مراجع ذی‌ربط	اطلاع‌رسانی و گزارش رخداد	
COBIT 2019 / NIST CSF 2.0	برنامه‌های تداوم فعالیت در صورت اختلال فناوری یا حمله سایبری	تداوم کسب‌وکار	
NIST CSF 2.0	پشتیبان‌گیری و بازیابی اطلاعات و سامانه‌ها پس از رخداد	بازیابی سامانه‌ها و داده‌ها	بازیابی و تاب‌آوری
NIST CSF 2.0	اصلاح فرایندها و کنترل‌ها پس از رخدادهای امنیتی	درس‌آموخته‌ها و بهبود مستمر	
COBIT 2019 / NIST CSF 2.0	آموزش کارکنان و افزایش آگاهی امنیت سایبری	آموزش و آگاهی امنیتی	مدیریت و بهبود مستمر
NIST CSF 2.0	توجه به ریسک‌های امنیتی ناشی از طرف‌های ثالث و تأمین‌کنندگان	مدیریت ریسک تأمین‌کنندگان	
COBIT 2019 / NIST CSF 2.0	بازنگری سیاست‌ها، کنترل‌ها و فرایندهای مدیریت ریسک	بهبود مستمر حاکمیت سایبری	

منبع: یافته‌های پژوهشگر



این ساختار، ۲۱ قلم قابل مشاهده برای سنجش افشای ریسک فناوری اطلاعات و امنیت سایبری را در هفت حوزه محتوایی پوشش می‌دهد. هر قلم بر اساس محتوای واقعی گزارش‌های رسمی شرکت‌ها کدگذاری و امتیازدهی شد و مجموع امتیازات به‌عنوان شاخص CSRisk مورد استفاده قرار گرفت.

نحوه امتیازدهی: برای هر قلم، در صورت نبود اطلاعات مربوط، امتیاز صفر؛ در صورت ارائه اطلاعات کلی، امتیاز یک؛ و در صورت ارائه اطلاعات مشخص، تفصیلی و قابل شناسایی، امتیاز دو در نظر گرفته شد؛ بنابراین، امتیاز بالاتر بیانگر سطح بالاتر افشای اطلاعات مرتبط با ریسک فناوری اطلاعات و امنیت سایبری است.

روش امتیازدهی شاخص: برای جلوگیری از قضاوت ذهنی و افزایش قابلیت تکرارپذیری پژوهش، برای هر قلم شاخص از مقیاس امتیازدهی سه سطحی استفاده می‌شود.

جدول ۴

روش امتیازدهی شاخص‌ها

وضعیت افشا	امتیاز	معیار
عدم افشا	۰	هیچ اطلاعات قابل شناسایی درباره مؤلفه موردنظر ارائه نشده است
افشای کلی	۱	به موضوع اشاره شده، اما اطلاعات محدود و غیر تفصیلی است
افشای مشخص و تفصیلی	۲	اطلاعات مشخص، قابل مشاهده و نسبتاً تفصیلی درباره سازوکار، فرایند یا اقدام شرکت است

استفاده از مقیاس سه سطحی امکان تمایز میان نبود افشا، افشای کلی و افشای مشخص و تفصیلی را فراهم می‌کند و در مقایسه با کدگذاری دودویی، اطلاعات بیشتری درباره عمق و سطح جزئیات افشا در اختیار پژوهش قرار می‌دهد. امتیاز خام هر شرکت - سال از رابطه زیر محاسبه می‌شود:

$$CSRisk_{it} = \sum_{j=1}^{21} Score_{ijt}$$

حداکثر امتیاز قابل کسب برابر است با:

$$0 \leq CSRisk_{it} \leq 42$$



$$\text{Maximum Score} = 21 \times 2 = 42$$

حداکثر امتیاز نظری شاخص برابر با ۴۲ است؛ بنابراین، $\text{CSRisk} = 0$ نشان‌دهنده نبود افشای قابل‌شناسایی در اقلام شاخص و $\text{CSRisk} = 42$ نشان‌دهنده دریافت بالاترین امتیاز ممکن در تمام اقلام شاخص است. در نتیجه، مقدار بالاتر CSRisk بیانگر سطح بالاتر افشای اطلاعات مرتبط با ریسک فناوری اطلاعات و امنیت سایبری است.

کنترل روایی شاخص CSRisk

به منظور کنترل روایی محتوایی شاخص افشای ریسک فناوری اطلاعات و امنیت سایبری، ابتدا فهرست اولیه‌ای مشتمل بر ۲۴ مؤلفه بر پایه چارچوب‌های بین‌المللی COBIT 2019 و NIST CSF 2.0 تدوین گردید. سپس این فهرست به همراه تعاریف عملیاتی در اختیار پنلی متشکل از ۷ نفر از خبرگان دانشگاهی و حرفه‌ای (شامل ۳ عضو هیئت‌علمی حسابداری و حاکمیت شرکتی، ۲ حسابرس ارشد معتمد بورس و ۲ متخصص مدیریت فناوری اطلاعات و امنیت سایبری) قرار گرفت. خبرگان هر مؤلفه را از حیث «میزان اهمیت»، «ارتباط مفهومی با افشای ریسک» و «قابلیت سنجش در گزارش‌های هیئت‌مدیره بورس تهران» ارزیابی نمودند. بر اساس جمع‌بندی نظرات خبرگان:

- سه مؤلفه به دلیل همپوشانی بالا و عدم امکان افشای عمومی به دلایل محرمانگی (نظیر افشای مستقیم آسیب‌پذیری‌های فنی و تفکیک جزئی درس آموخته‌ها) حذف یا در سایر مؤلفه‌ها ادغام گردیدند.
- سه مؤلفه جدید و بااهمیت متناسب با بستر گزارشگری ایران (از جمله الزام به افشای گواهینامه‌های انطباق و استانداردهای امنیتی، ممیزی‌های دوره‌ای فناوری اطلاعات و نظارت کمیته‌های تخصصی هیئت‌مدیره) به چارچوب افزوده شد.
- نگارش و تعریف عملیاتی ۴ مؤلفه نیز به منظور رفع ابهام و سهولت در کدگذاری اصلاح شد.

در نهایت، ۲۱ مؤلفه نهایی در قالب ۷ بُعد اصلی (شامل: ۱. حاکمیت و راهبری، ۲. شناسایی و ارزیابی ریسک، ۳. حفاظت و کنترل، ۴. کشف و پایش، ۵. پاسخ و مدیریت رخداد، ۶. بازیابی



و تاب‌آوری، ۷. مدیریت و بهبود مستمر) به تأیید نهایی پنل خبرگان رسید و مبنای کدگذاری و سنجش شاخص SCRISK در پژوهش حاضر قرار گرفت.

پایایی کدگذاری شاخص

به منظور بررسی پایایی فرایند کدگذاری شاخص افشای ریسک فناوری اطلاعات و امنیت سایبری، ۴۰ شرکت به صورت تصادفی انتخاب شد و گزارش‌های آنها در کل دوره ۱۴۰۰ تا ۱۴۰۴ به صورت مستقل توسط کدگذار دوم کدگذاری شد و سپس میزان توافق میان دو کدگذار با استفاده از ضریب کاپای کوهن در نرم‌افزار SPSS محاسبه گردید. مقدار ضریب کاپا برابر با ۰/۶۹۷ به دست آمد که بیانگر توافق قابل قبول میان دو کدگذار در فرایند کدگذاری اقلام شاخص است. موارد اختلاف نیز از طریق بازبینی تعاریف عملیاتی اقلام و بررسی مجدد متن گزارش‌ها تعیین تکلیف و همسان‌سازی شد.

یافته‌های پژوهش

آمار توصیفی پژوهش

خلاصه آماره‌های توصیفی متغیرهای مورد بررسی شامل شاخص‌های مرکزی (میانگین و میانه) و شاخص‌های پراکندگی (انحراف معیار، حداقل و حداکثر) در جدول ۵ قابل مشاهده است.

نتایج مندرج در جدول ۵ نشان می‌دهد متغیر وابسته افشای ریسک فناوری اطلاعات و امنیت سایبری دارای میانگین ۲۱/۱۹ و انحراف معیار ۹/۲۳ است. دامنه تغییرات این شاخص بین حداقل ۸ و حداکثر ۴۰ قرار دارد. با توجه به حداکثر امتیاز نظری ۴۲، میانگین مشاهده شده معادل حدود ۴۵/۷ درصد از حداکثر امتیاز قابل کسب است که بیانگر سطح متوسط افشای اطلاعات مرتبط با ریسک فناوری اطلاعات و امنیت سایبری در شرکت‌های مورد بررسی است. همچنین، انحراف معیار شاخص نشان‌دهنده تفاوت قابل توجه در سطح افشای این اطلاعات میان شرکت‌های نمونه است. علاوه بر این، آماره‌های مربوط به دوگانگی مدیرعامل نشان می‌دهد میانگین این متغیر ۰/۰۷ است؛ این مقدار بیانگر آن است که تنها در حدود ۷ درصد از مشاهدات سال-شرکت، هم‌زمانی این دو سمت یا عدم تفکیک کامل مشاهده شده و در اکثریت قریب به اتفاق شرکت‌ها تفکیک وظایف رعایت شده است.



جدول ۵

آماره‌های توصیفی متغیرهای پژوهش

نماد متغیر	نام متغیر	میانگین	میان	حداکثر	حداقل	انحراف معیار
CSRISKe	افشای ریسک فناوری اطلاعات و سایبری	۱۹/۲۱	۱۵/۰۰	۴۰/۰۰	۸/۰۰	۹/۲۳
BIND	استقلال هیئت‌مدیره	۰/۷۱	۰/۷۰	۱/۰۰	۰/۲۰	۰/۱۲
BSIZE	اندازه هیئت‌مدیره	۱/۶۲	۱/۶۱	۱/۹۵	۱/۶۱	۰/۰۶
BFIN	تخصص مالی هیئت‌مدیره	۰/۲۹	۰/۳۰	۰/۴۰	۰/۰۰	۰/۱۱
BIT	تخصص فناوری اطلاعات هیئت‌مدیره	۰/۰۱	۰/۰۰	۰/۲۰	۰/۰۰	۰/۰۴
DUAL	دوگانگی وظیفه مدیرعامل	۰/۰۷	۰/۰۰	۱/۰۰	۰/۰۰	۰/۲۶
ITC	کمیت ریسک / فناوری اطلاعات	۰/۰۳	۰/۰۰	۱/۰۰	۰/۰۰	۰/۱۶
SIZE	اندازه شرکت	۱۷/۴۳	۱۷/۱۰	۲۲/۴۶	۱۳/۰۳	۱/۷۸
LEV	اهرم مالی	۰/۵۲	۰/۴۹	۲/۶۴	۰/۰۸	۰/۲۷
ROA	بازده دارایی‌ها	۲۰/۹۵	۲۰/۷۵	۷۱/۱۴	-۶۲/۳۴	۱۸/۱۴
TQ	کیوتوبین	۰/۹۸	۰/۹۰	۳/۲۰	۰/۲۵	۰/۳۹

منبع: یافته‌های پژوهشگر

ماتریس همبستگی پیرسون

نتایج ماتریس همبستگی پیرسون در جدول ۶، نشان می‌دهد که ضرایب همبستگی دوتایی میان متغیرهای توضیحی عمدتاً در سطح پایینی قرار دارند. بالاترین همبستگی مثبت میان متغیرهای توضیحی مربوط به تخصص مالی هیئت‌مدیره و استقلال هیئت‌مدیره با ضریب ۰/۳۶ است. با توجه به پایین بودن ضرایب همبستگی دوتایی، نشانه‌ای از همبستگی شدید میان متغیرهای توضیحی مشاهده نمی‌شود. با این حال، از آنجاکه بررسی همبستگی دوتایی به تنهایی برای تشخیص هم‌خطی چندگانه کافی نیست، شاخص‌های VIF و Tolerance نیز محاسبه و در جدول ۷ گزارش شده‌اند.



جدول ۶

ماتریس همبستگی پیرسون

متغیر	BFIN	BIND	BIT	BSIZE	CSRISK	DUAL	ITC	LEV	ROA	SIZE	TQ
TQ	۱/۰۰	—	۱/۰۰	—	۱/۰۰	۱/۰۰	۱/۰۰	۱/۰۰	۱/۰۰	۱/۰۰	۱/۰۰
SIZE	۰/۳۶ (۰/۰۰)	۱/۰۰	۰/۰۱ (۰/۷۴)	—	۱/۰۰	۱/۰۰	۱/۰۰	۱/۰۰	۱/۰۰	۱/۰۰	۱/۰۰
ROA	۰/۰۱ (۰/۷۴)	۰/۰۱ (۰/۷۴)	۰/۰۱ (۰/۷۴)	۰/۰۱ (۰/۷۴)	۰/۰۱ (۰/۷۴)	۰/۰۱ (۰/۷۴)	۰/۰۱ (۰/۷۴)	۰/۰۱ (۰/۷۴)	۰/۰۱ (۰/۷۴)	۰/۰۱ (۰/۷۴)	۰/۰۱ (۰/۷۴)
LEV	۰/۰۸ (۰/۰۴)	۰/۰۸ (۰/۰۴)	۰/۰۸ (۰/۰۴)	۰/۰۸ (۰/۰۴)	۰/۰۸ (۰/۰۴)	۰/۰۸ (۰/۰۴)	۰/۰۸ (۰/۰۴)	۰/۰۸ (۰/۰۴)	۰/۰۸ (۰/۰۴)	۰/۰۸ (۰/۰۴)	۰/۰۸ (۰/۰۴)
CSRISK	۰/۰۶ (۰/۱۶)	۰/۰۶ (۰/۱۶)	۰/۰۶ (۰/۱۶)	۰/۰۶ (۰/۱۶)	۰/۰۶ (۰/۱۶)	۰/۰۶ (۰/۱۶)	۰/۰۶ (۰/۱۶)	۰/۰۶ (۰/۱۶)	۰/۰۶ (۰/۱۶)	۰/۰۶ (۰/۱۶)	۰/۰۶ (۰/۱۶)
DUAL	۰/۲۳ (۰/۰۰)	۰/۲۳ (۰/۰۰)	۰/۲۳ (۰/۰۰)	۰/۲۳ (۰/۰۰)	۰/۲۳ (۰/۰۰)	۰/۲۳ (۰/۰۰)	۰/۲۳ (۰/۰۰)	۰/۲۳ (۰/۰۰)	۰/۲۳ (۰/۰۰)	۰/۲۳ (۰/۰۰)	۰/۲۳ (۰/۰۰)
ITC	۰/۱۷ (۰/۰۰)	۰/۱۷ (۰/۰۰)	۰/۱۷ (۰/۰۰)	۰/۱۷ (۰/۰۰)	۰/۱۷ (۰/۰۰)	۰/۱۷ (۰/۰۰)	۰/۱۷ (۰/۰۰)	۰/۱۷ (۰/۰۰)	۰/۱۷ (۰/۰۰)	۰/۱۷ (۰/۰۰)	۰/۱۷ (۰/۰۰)
LEV	۰/۰۳ (۰/۴۷)	۰/۰۳ (۰/۴۷)	۰/۰۳ (۰/۴۷)	۰/۰۳ (۰/۴۷)	۰/۰۳ (۰/۴۷)	۰/۰۳ (۰/۴۷)	۰/۰۳ (۰/۴۷)	۰/۰۳ (۰/۴۷)	۰/۰۳ (۰/۴۷)	۰/۰۳ (۰/۴۷)	۰/۰۳ (۰/۴۷)
ROA	۰/۱۰ (۰/۰۱)	۰/۱۰ (۰/۰۱)	۰/۱۰ (۰/۰۱)	۰/۱۰ (۰/۰۱)	۰/۱۰ (۰/۰۱)	۰/۱۰ (۰/۰۱)	۰/۱۰ (۰/۰۱)	۰/۱۰ (۰/۰۱)	۰/۱۰ (۰/۰۱)	۰/۱۰ (۰/۰۱)	۰/۱۰ (۰/۰۱)
SIZE	۰/۲۷ (۰/۰۰)	۰/۲۷ (۰/۰۰)	۰/۲۷ (۰/۰۰)	۰/۲۷ (۰/۰۰)	۰/۲۷ (۰/۰۰)	۰/۲۷ (۰/۰۰)	۰/۲۷ (۰/۰۰)	۰/۲۷ (۰/۰۰)	۰/۲۷ (۰/۰۰)	۰/۲۷ (۰/۰۰)	۰/۲۷ (۰/۰۰)
TQ	۰/۲۶ (۰/۰۰)	۰/۲۶ (۰/۰۰)	۰/۲۶ (۰/۰۰)	۰/۲۶ (۰/۰۰)	۰/۲۶ (۰/۰۰)	۰/۲۶ (۰/۰۰)	۰/۲۶ (۰/۰۰)	۰/۲۶ (۰/۰۰)	۰/۲۶ (۰/۰۰)	۰/۲۶ (۰/۰۰)	۰/۲۶ (۰/۰۰)

منبع: یافته‌های پژوهشگر



جدول ۲

نتیجه شاخص هم خطی

متغیر مستقل	R^2 کمکی	شاخص VIF	تحمل تقریبی ^۱	وضعیت هم خطی
BIND (استقلال هیئت‌مدیره)	۰/۱۵۹	۱/۱۸۹	۰/۸۴۱	هم خطی در سطح قابل قبول
BSIZE (اندازه هیئت‌مدیره)	۰/۰۴۴	۱/۰۴۶	۰/۹۵۶	هم خطی در سطح قابل قبول
BFIN (تخصص مالی)	۰/۲۶۴	۱/۳۵۹	۰/۷۳۶	هم خطی در سطح قابل قبول
BIT (تخصص فناوری اطلاعات)	۰/۰۱۶	۱/۰۱۷	۰/۹۸۴	هم خطی در سطح قابل قبول
DUAL (دوگانگی مدیرعامل)	۰/۰۷۵	۱/۰۸۲	۰/۹۲۵	هم خطی در سطح قابل قبول
ITC (کمیت فناوری اطلاعات)	۰/۱۰۱	۱/۱۱۳	۰/۸۹۹	هم خطی در سطح قابل قبول
SIZE (اندازه شرکت)	۰/۱۴۸	۱/۱۷۳	۰/۸۵۲	هم خطی در سطح قابل قبول
LEV (اهرم مالی)	۰/۴۵۶	۱/۸۴۰	۰/۵۴۴	هم خطی در سطح قابل قبول
ROA (بازده دارایی‌ها)	۰/۴۴۳	۱/۷۹۶	۰/۵۵۷	هم خطی در سطح قابل قبول
TQ (کیوتوبین)	۰/۱۱۹	۱/۱۳۴	۰/۸۸۱	هم خطی در سطح قابل قبول

منبع: یافته‌های پژوهشگر

مطابق نتایج جدول ۷، مقدار VIF تمام متغیرهای توضیحی کمتر از ۲ و مقادیر شاخص تحمل تقریبی نیز بیشتر از ۰/۵۰ است؛ بنابراین، بر اساس معیارهای متعارف، شواهدی از هم خطی چندگانه شدید میان متغیرهای توضیحی مشاهده نمی‌شود.

تحلیل آزمون‌های تشخیصی و انتخاب مدل

برای انتخاب مناسب‌ترین روش برآورد از میان مدل‌های تلفیقی^۲ و تابلویی^۳ با اثرات ثابت یا تصادفی، از آزمون‌های استاندارد زیر استفاده شده است. تمام محاسبات با استفاده از نرم‌افزار EViews انجام گرفته است.

^۱ Tolerance^۲ Pooled^۳ Panel

بررسی اولیه

به منظور بررسی اولیه رابطه میان ویژگی‌های حاکمیت شرکتی و افشای ریسک فناوری اطلاعات و امنیت سایبری، ابتدا مدل پژوهش با استفاده از روش حداقل مربعات معمولی تلفیقی^۱ برآورد شد که نتایج در جدول ۸ قابل مشاهده است.

جدول ۸

نتایج برآورد مدل رگرسیون تجمعی اولیه

متغیر	نماد	ضریب	خطای معیار	آماره t	سطح معناداری (p-value)
عرض از مبدأ	C	-۶/۸۳۰	۱۲/۲۰۲	-۰/۵۶۰	۰/۵۷۵۹
استقلال هیئت مدیره	BIND	-۱۵/۳۸۱	۳/۲۵۷	-۴/۷۲۳	۰/۰۰۰۰
اندازه هیئت مدیره	BSIZE	۱۷/۳۶۷	۶/۴۰۸	۲/۷۱۰	۰/۰۰۶۹
تخصص مالی	BFIN	-۲/۰۴۴	۴/۰۳۸	-۰/۵۰۶	۰/۶۱۳۰
تخصص IT	BIT	۳۳/۶۶۱	۸/۷۲۳	۳/۸۵۹	۰/۰۰۰۱
دوگانگی مدیرعامل	DUAL	۰/۲۰۰	۱/۴۸۱	۰/۱۳۵	۰/۸۹۲۸
کمیت IT و ریسک	ITC	۱/۲۸۰	۲/۳۹۳	۰/۵۳۵	۰/۵۹۲۸
اندازه شرکت	SIZE	۰/۳۷۶	۰/۲۲۵	۱/۶۷۴	۰/۰۹۴۷
اهرم مالی	LEV	۰/۴۲۳	۱/۸۶۸	۰/۲۲۷	۰/۸۲۰۸
بازده دارایی‌ها	ROA	-۰/۰۰۱	۰/۰۲۷	-۰/۰۵۲	۰/۹۵۸۲
کیوتوبین	TQ	۲/۳۳۷	۰/۹۸۱	۲/۳۸۲	۰/۰۱۷۶
ضریب تعیین (R^2)		۰/۰۸۸	میانگین متغیر وابسته		۱۹/۲۰۹
ضریب تعیین تعدیل شده		۰/۰۷۲	انحراف معیار متغیر وابسته		۹/۲۳۳
آماره F		۵/۵۰۹	سطح معناداری آماره F		۰/۰۰۰۰
آماره دوربین - واتسون		۰/۶۶۳	تعداد کل مشاهدات		۵۸۵

منبع: یافته‌های پژوهشگر

نتایج ارائه شده در جدول ۸ نشان می‌دهد که ضریب تعیین R^2 مدل برابر با ۰/۰۸۸ است؛ به این معنا که حدود ۸/۸ درصد از تغییرات متغیر وابسته (افشای ریسک فناوری اطلاعات و امنیت سایبری) توسط مجموع متغیرهای توضیحی و کنترلی مدل تبیین می‌شود. همچنین ضریب تعیین تعدیل شده برابر با ۰/۰۷۲ برآورد شده است.

¹ Pooled OLS



آماره F مدل برابر با $۵/۵۰۹$ و سطح معناداری آن برابر با $۰/۰۰۰$ است. از آنجاکه سطح معناداری آماره F کمتر از سطح خطای ۵ درصد است، فرضیه صفر مبنی بر عدم معناداری کلی مدل رد می‌شود؛ بنابراین مدل رگرسیون در مجموع از نظر آماری معنادار بوده و متغیرهای توضیحی به صورت هم‌زمان دارای توان تبیین‌کنندگی متغیر وابسته هستند.

در برآورد اولیه به روش تلفیقی، آماره دورین-واتسون برابر با $۰/۶۶۳$ به دست آمد که فاصله قابل توجهی از مقدار (۲) دارد و نشان‌دهنده وجود خودهمبستگی مثبت پسماندها و عدم لحاظ ناهمگنی‌های خاص هر شرکت در ساختار تلفیقی است. از این رو، برای تعیین دقیق ساختار داده‌ها و انتخاب میان روش داده‌های تلفیقی و داده‌های تابلویی و سپس گزینش نوع اثرات (ثابت یا تصادفی)، آزمون‌های تشخیصی چاو (F لیمر) و هاسمن اجرا گردید.

آزمون چاو (F لیمر)

به منظور بررسی وجود ناهمگنی‌های فردی میان شرکت‌های مورد مطالعه و انتخاب میان الگوی داده‌های تلفیقی و الگوی داده‌های تابلویی، آزمون چاو (F لیمر) اجرا گردید که در جدول ۹ قابل مشاهده است. فرضیه صفر H_0 در این آزمون بیانگر همگنی عرض از مبدأ بین مقاطع و ترجیح روش تلفیقی است، در حالی که فرضیه مقابل H_1 بر وجود ناهمگنی‌های مقطعی و برتری روش داده‌های تابلویی تأکید دارد.

جدول ۹

نتایج آزمون چاو

نوع آزمون	آماره آزمون	درجه آزادی	سطح معناداری (p -value)	نتیجه آزمون	مدل منتخب
آماره F مقطعی-Cross section (F)	$۵/۵۶۳$	(۴۵۸) (۱۱۶)	$۰/۰۰۰$	رد فرضیه H_0	داده‌های تابلویی
آماره کای‌دو مقطعی χ^2	$۵۱۴/۳۴۵$	۱۱۶	$۰/۰۰۰$	رد فرضیه H_0	داده‌های تابلویی

منبع: یافته‌های پژوهشگر



با توجه به نتایج حاصل از آزمون مطابق جدول ۹، مقدار آماره F مقطعی با درجه آزادی (۱۱۶، ۴۵۸) برابر با ۵/۵۶۳ و سطح معناداری آن برابر با ۰/۰۰۰ به دست آمده است. همچنین آماره کای دو مقطعی (X^2) با ۱۱۶ درجه آزادی برابر با ۵۱۴/۳۴۵ و با سطح معناداری ۰/۰۰۰ گزارش شده است. از آنجا که سطح معناداری هر دو آماره بسیار کمتر از سطح خطای ۵ درصد است، فرضیه صفر با اطمینان ۹۵ درصد رد می‌شود؛ بنابراین، تفاوت‌های مقطعی معناداری میان شرکت‌های تولیدی مورد بررسی وجود دارد و استفاده از الگوی داده‌های تابلویی (پانل) نسبت به روش تلفیقی ارجحیت دارد. در گام بعد، برای انتخاب بین مدل تلفیقی و مدل اثرات تصادفی، آزمون نسبت واریانس بروش - پاگان اجرا می‌شود.

آزمون بروش - پاگان (LM)

برای انتخاب بین مدل تلفیقی و مدل اثرات تصادفی^۱، از آزمون نسبت واریانس بروش - پاگان استفاده شد. فرضیات آزمون به صورت جدول ۱۰ است:

جدول ۱۰

نتایج آزمون LM بروش - پاگان

نوع اثر	آماره بروش - پاگان	سطح معناداری
مقطعی (Cross-section)	۲۲۸/۵۰۳	۰/۰۰۰۰
زمانی (Time)	۱۲/۹۰۴	۰/۰۰۰۳
هر دو / کل (Both)	۲۴۱/۴۰۷	۰/۰۰۰۰

منبع: یافته‌های پژوهشگر

با توجه به اینکه سطح معناداری آماره آزمون در تمام حالات (مقطعی، زمانی و کل) کمتر از سطح خطای ۱ درصد است ($p < 0.01$)، فرضیه صفر مبنی بر برابری واریانس اثرات مقطعی/زمانی با صفر رد می‌شود. این نتیجه بیانگر عدم کفایت مدل تلفیقی و وجود اثرات تصادفی (ناهمگنی‌های انفرادی و زمانی) در داده‌ها است؛ بنابراین، برآورد مدل با رگرسیون

¹ Random Effects



ساده/تلفیقی مجاز نبوده و جهت انتخاب نهایی میان مدل اثرات ثابت و مدل اثرات تصادفی، انجام آزمون هاسمن ضرورت می‌یابد.

آزمون هاسمن

به‌منظور انتخاب الگوی برتر میان مدل اثرات ثابت و مدل اثرات تصادفی، از آزمون هاسمن استفاده شد که نتایج آن در جدول ۱۱، قابل مشاهده است. فرضیه صفر این آزمون بر عدم وجود همبستگی میان خطاهای انفرادی مقاطع و متغیرهای توضیحی تأکید داشته و کارایی مدل اثرات تصادفی را تأیید می‌کند؛ در مقابل، فرضیه یک حاکی از وجود همبستگی میان این دو جزء بوده و لزوم به‌کارگیری مدل اثرات ثابت را نشان می‌دهد.

جدول ۱۱

نتایج آزمون هاسمن برای انتخاب بین اثرات ثابت و اثرات تصادفی

خلاصه آزمون	آماره کای‌دو	درجه آزادی	سطح معناداری	نتیجه آزمون
اثرات تصادفی مقطعی	۲۳/۲۳۴	۱۰	۰/۰۰۹۹	رد فرضیه صفر

منبع: یافته‌های پژوهشگر

باتوجه به نتایج ارائه‌شده در جدول شماره ۱۱ آماره کای‌دو با ۱۰ درجه آزادی برابر با ۲۳/۲۳۴ و سطح معناداری آن برابر با ۰/۰۰۹۹ برآورد گردیده است. از آنجاکه مقدار سطح معناداری کمتر از سطح خطای ۵ درصد است، فرضیه صفر با اطمینان ۹۹ درصد رد می‌شود؛ بنابراین، مدل داده‌های تابلویی با اثرات ثابت مقطعی به‌عنوان مدل مناسب و برتر جهت برآورد روابط رگرسیونی و آزمون فرضیه‌های پژوهش انتخاب می‌گردد.

جمع‌بندی مراحل انتخاب مدل

نتایج مراحل انتخاب مدل به‌صورت خلاصه در جدول ۱۲ ارائه شده است.



جدول ۱۲

جمع‌بندی فرآیند انتخاب مدل

مرحله	آزمون / روش	مقایسه انجام شده	مقدار آماره آزمون	مقدار احتمال	تصمیم و نتیجه گیری
۱	حداقل مربعات تلفیقی	برآورد اولیه داده‌ها	—	—	نیاز به اجرای آزمون‌های تشخیص ساختار
۲	آزمون چاو / لیمر	مدل تلفیقی در برابر اثرات ثابت	۵/۵۶۳	۰/۰۰۰۰	رد مدل تلفیقی و تأیید مدل تابلویی
۳	آزمون بروش - پاگان	مدل تلفیقی در برابر اثرات تصادفی	۲۴۱/۴۰۷	۰/۰۰۰۰	رد مدل تلفیقی و تأیید وجود اثرات تصادفی
۴	آزمون هاسمن	مدل اثرات ثابت در برابر اثرات تصادفی	۲۳/۲۳۴	۰/۰۰۹۹	رد مدل اثرات تصادفی و برتری اثرات ثابت
۵	الگوی نهایی منتخب	تعیین ساختار نهایی مدل رگرسیون	—	—	برآورد نهایی با روش ثابت مقطعی

منبع: یافته‌های پژوهشگر

آزمون بروش - پاگان نیز وجود اثرات تصادفی را نسبت به مدل تلفیقی تأیید می‌کند؛
 با این حال، انتخاب نهایی میان اثرات ثابت و تصادفی بر اساس آزمون هاسمن انجام شد.

انتخاب مدل نهایی پژوهش

در مرحله نخست، فرض شد که تفاوت معناداری میان شرکت‌ها وجود ندارد و برای همه آن‌ها یک عرض از مبدأ مشترک در نظر گرفته می‌شود. مدل اولیه پژوهش به صورت زیر برآورد شد:

$$CSRISK_{it} = \alpha + \beta_1 BIND_{it} + \beta_2 BSIZE_{it} + \beta_3 BFIN_{it} + \beta_4 BIT_{it} + \beta_5 DUAL_{it} + \beta_6 ITC_{it} + \beta_7 LEV_{it} + \beta_8 ROA_{it} + \beta_9 SIZE_{it} + \beta_{10} TQ_{it} + \varepsilon_{it}$$

سپس، با انجام مراحل ذکر شده در جدول ۱۲ و انتخاب مدل اثرات ثابت، مدل دوباره در نرم‌افزار EViews برآورد شد؛ اما این بار در بخش Cross Effects Specification گزینه section Fixed Effects انتخاب شد. در این مدل، برای هر شرکت یک اثر ثابت یا عرض از



مبدأ جداگانه در نظر گرفته می‌شود؛ بنابراین، تفاوت‌های ثابت و مشاهده‌نشده شرکت‌ها، مانند فرهنگ سازمانی، کیفیت مدیریت، ساختار داخلی و ویژگی‌های خاص شرکت، کنترل می‌شود. براین اساس، مدل نهایی پژوهش با در نظر گرفتن اثرات ثابت برای شرکت‌ها به صورت زیر برآورد شد:

$$CSRISK_{it} = \alpha_i + \beta_1 BIND_{it} + \beta_2 BSIZE_{it} + \beta_3 BFIN_{it} + \beta_4 BIT_{it} + \beta_5 DUAL_{it} + \beta_6 ITC_{it} + \beta_7 LEV_{it} + \beta_8 ROA_{it} + \beta_9 SIZE_{it} + \beta_{10} TQ_{it} + \varepsilon_{it}$$

در این مدل، α_i بیانگر اثرات ثابت مختص هر شرکت است و تفاوت‌های مشاهده‌نشده و پایدار میان شرکت‌ها را کنترل می‌کند. در نهایت، پس از انتخاب مدل اثرات ثابت مقطعی، رگرسیون نهایی پژوهش برآورد شد.

جدول ۱۳

رگرسیون نهایی پژوهش

نام متغیر	نماد متغیر	ضریب β	خطای معیار	آماره t	سطح معناداری (p value)
عرض از مبدأ	C	۳۳/۹۵۳	۱۶/۰۷۰	۲/۱۱۳	۰/۰۳۵۲
استقلال هیئت‌مدیره	BIND	۱/۴۹۵	۵/۹۵۱	۰/۲۵۱	۰/۸۰۱۸
اندازه هیئت‌مدیره	BSIZE	-۱/۵۵۴	۷/۵۴۰	-۰/۲۰۶	۰/۸۳۶۸
تخصص مالی هیئت‌مدیره	BFIN	-۴/۱۹۴	۱۰/۶۶۱	-۰/۳۹۳	۰/۶۹۴۲
تخصص فناوری اطلاعات	BIT	۰/۶۲۲	۱۰/۵۴۰	۰/۰۵۹	۰/۹۵۳۰
دوگانگی وظیفه مدیرعامل	DUAL	-۲/۱۸۹	۲/۱۳۲	-۱/۰۲۶	۰/۳۰۵۲
کمیته فناوری اطلاعات/ریسک	ITC	-۸/۶۳۵	۳/۸۵۷	-۲/۲۳۹	۰/۰۲۵۷
اندازه شرکت	SIZE	-۰/۸۵۱	۰/۵۷۹	-۱/۴۶۹	۰/۱۴۲۶
اهرم مالی	LEV	-۱/۳۷۱	۲/۶۳۴	-۰/۵۲۰	۰/۶۰۳۱
بازده دارایی‌ها	ROA	۰/۰۴۱	۰/۰۳۷	۱/۱۱۰	۰/۲۶۷۷
کیوتوبین (ارزش بازار)	TQ	۳/۰۳۹	۲/۷۵۷	۱/۱۰۲	۰/۲۷۰۹

منبع: یافته‌های پژوهشگر



بر اساس نتایج مندرج در جدول ۱۳، از میان متغیرهای اصلی حاکمیت شرکتی و ویژگی‌های هیئت‌مدیره، تنها متغیر کمیته فناوری اطلاعات/ریسک دارای ضریب منفی ($-۸/۶۳۵$) و سطح معناداری کمتر از خطای ۵ درصد ($p = 0.0257$) است؛ این امر نشان می‌دهد وجود کمیته تخصصی ریسک یا فناوری اطلاعات بر سطح افشای ریسک‌های امنیت سایبری تأثیر معنادار دارد. در مقابل، سایر متغیرهای مرتبط با هیئت‌مدیره شامل استقلال ($p = 0.8018$)، اندازه ($p = 0.8368$)، تخصص مالی ($p = 0.6942$)، تخصص فناوری اطلاعات ($p = 0.9530$) و دوگانگی وظیفه مدیرعامل ($p = 0.3052$) سطوح معناداری بالاتر از ۰/۰۵ کسب کرده‌اند و بنابراین از نظر آماری تأثیر معناداری بر متغیر وابسته (CSRisk) نداشته‌اند. همچنین، متغیرهای کنترلی پژوهش (اندازه شرکت، اهرم مالی، بازده دارایی‌ها و ارزش بازار) نیز در سطح اطمینان ۹۵ درصد اثر معناداری بر افشای ریسک سایبری نشان ندادند. برای بررسی اعتبار مدل بر اساس جدول شماره ۱۴ شاخص‌های این مدل موارد زیر استخراج شد.

جدول ۱۴

شاخص‌های مدل

مقدار	شاخص آماری
۰/۶۲۱۲	ضریب تعیین (R^2)
۰/۵۱۷	ضریب تعیین تعدیل شده ($\text{Adjusted } R^2$)
۵/۹۶۲	آماره F مدل رگرسیون
$P < ۰/۰۰۱$	سطح معناداری آماره ($p\text{-value}$) F
۱/۴۸۷	آماره دوربین - واتسون ($D-W$)
۵۸۵ (۱۱۷ شرکت در ۵ سال)	تعداد کل مشاهدات
Panel Least Squares (Fixed Effects)	روش برآورد

منبع: یافته‌های پژوهشگر

بر اساس جدول ۱۴، ضریب تعیین مدل برابر با ۰/۶۲۱۲ (حدود ۶۲/۱ درصد از تغییرات متغیر وابسته در چارچوب مشخصات مدل و متغیرهای وارد شده به آن تبیین می‌شود) و ضریب تعیین تعدیل شده برابر با ۰/۵۱۷ است. همچنین، آماره F مدل برابر با ۵/۹۶۲ و سطح معناداری آن کمتر



از ۰/۰۰۱ گزارش شده است که نشان‌دهنده معناداری کلی مدل رگرسیون در سطح ۱ درصد است. مقدار آماره دوربین-واتسون برابر با ۱/۴۸۷ بوده و قرارگیری مقادیر عامل تورم واریانس (VIF) در دامنه مجاز، حاکی از عدم وجود هم‌خطی چندگانه شدید میان متغیرهای مستقل است.

جدول ۱۵

نتایج فرضیه‌ها

فرضیه	متغیر مستقل	ضریب	سطح معناداری	نتیجه فرضیه
H1	استقلال هیئت‌مدیره	۱/۴۹۵	۰/۸۰۱۸	عدم تأیید
H2	اندازه هیئت‌مدیره	-۱/۵۵۴	۰/۸۳۶۸	عدم تأیید
H3	تخصص مالی	-۴/۱۹۴	۰/۶۹۴۲	عدم تأیید
H4	تخصص IT	۰/۶۲۲	۰/۹۵۳۰	عدم تأیید
H5	دوگانگی مدیرعامل	-۲/۱۸۹	۰/۳۰۵۲	عدم تأیید
H6	کمیت IT/ریسک	-۸/۶۳۵	۰/۰۲۵۷	تأیید

منبع: یافته‌های پژوهشگر

تفسیر فرضیه‌ها

فرضیه اول: استقلال هیئت‌مدیره بر افزایش ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.

نتایج برآورد مدل نشان می‌دهد ضریب مربوط به استقلال هیئت‌مدیره برابر با ۱/۴۹۵ بوده، اما سطح معناداری آن برابر با ۰/۸۰۱۸ است؛ بنابراین، با توجه به بالاتر بودن سطح معناداری از سطح خطای ۵ درصد، شواهد آماری کافی برای تأیید اثر معنادار استقلال هیئت‌مدیره بر افزایش ریسک فناوری اطلاعات و امنیت سایبری مشاهده نشد. از این رو، فرضیه اول پژوهش تأیید نمی‌شود. این نتیجه به معنای اثبات نبود هرگونه رابطه میان دو متغیر نیست، بلکه بیانگر آن است که در نمونه و دوره مورد بررسی، اثر آماری معناداری مشاهده نشده است.

فرضیه دوم: اندازه هیئت‌مدیره بر افزایش ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.



ضریب اندازه هیئت‌مدیره برابر با $1/554$ - و سطح معناداری آن برابر با $0/8368$ به دست آمده است. با توجه به عدم معناداری آماری این ضریب در سطح ۵ درصد، شواهد کافی برای تأیید اثر معنادار اندازه هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری وجود ندارد؛ بنابراین، فرضیه دوم پژوهش تأیید نمی‌شود.

فرضیه سوم: تخصص مالی اعضای هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.

نتایج نشان می‌دهد ضریب تخصص مالی اعضای هیئت‌مدیره برابر با $4/194$ - و سطح معناداری آن برابر با $0/6942$ است؛ بنابراین، رابطه مشاهده‌شده از نظر آماری معنادار نیست و شواهد کافی برای تأیید اثر تخصص مالی هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری به دست نیامد. براین اساس، فرضیه سوم پژوهش تأیید نمی‌شود.

فرضیه چهارم: تخصص فناوری اطلاعات اعضای هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.

ضریب تخصص فناوری اطلاعات اعضای هیئت‌مدیره برابر با $0/622$ و سطح معناداری آن برابر با $0/9530$ است. اگرچه جهت ضریب برآوردشده مثبت است، مقدار سطح معناداری نشان می‌دهد این رابطه از نظر آماری معنادار نیست؛ بنابراین، در نمونه و دوره مورد بررسی، شواهد کافی برای تأیید اثر تخصص فناوری اطلاعات اعضای هیئت‌مدیره بر افشای ریسک فناوری اطلاعات و امنیت سایبری مشاهده نشد و فرضیه چهارم تأیید نمی‌شود.

فرضیه پنجم: دوگانگی مدیرعامل بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.

ضریب دوگانگی مدیرعامل برابر با $2/189$ - و سطح معناداری آن برابر با $0/3052$ است؛ بنابراین، اثر دوگانگی مدیرعامل بر افشای ریسک فناوری اطلاعات و امنیت سایبری در سطح ۵ درصد معنادار نیست. در نتیجه، شواهد آماری کافی برای تأیید فرضیه پنجم پژوهش وجود ندارد.

فرضیه ششم: وجود کمیته ریسک یا کمیته فناوری اطلاعات بر افشای ریسک فناوری اطلاعات و امنیت سایبری تأثیر دارد.



ضریب مربوط به وجود کمیته تخصصی فناوری اطلاعات/ریسک برابر با $۸/۶۳۵$ - و سطح معناداری آن برابر با $۰/۰۲۵۷$ است. باتوجه به اینکه سطح معناداری کمتر از ۵ درصد می‌باشد، این رابطه از نظر آماری معنادار است. اگرچه علامت منفی ضریب نشان می‌دهد شرکت‌های دارای این کمیته‌ها، میزان افشای ریسک سایبری کمتری در گزارش‌های عمومی خود دارند، اما این یافته از منظر نظری قابل تبیین است؛ به این معنا که این کمیته‌ها با درک عمق تهدیدات و بر اساس «نظریه هزینه‌های مالکانه»، جهت جلوگیری از افزایش احتمال حملات هکری و حفظ موقعیت رقابتی، افشای عمومی آسیب‌پذیری‌ها را محدود می‌کنند. همچنین، مهار ریسک‌های سایبری در سطوح درون‌سازمانی توسط این کمیته‌ها، نیاز به افشای گسترده ریسک‌های باقیمانده را کاهش می‌دهد. از این رو، فرضیه ششم پژوهش با جهت اثر منفی تأیید می‌گردد.

در میان متغیرهای توضیحی مدل، هیچ یک از متغیرها رابطه معناداری با افشای ریسک فناوری اطلاعات و امنیت سایبری نشان ندادند. به عنوان نمونه، ضریب مربوط به اهرم مالی برای برابر با $۱/۳۷۰$ - با سطح معناداری $۰/۶۰۳۱$ برآورد شده است که نشان می‌دهد باتوجه به بالاتر بودن سطح معناداری از سطح خطای بالای ۵ درصد، اهرم مالی تأثیر معناداری بر میزان افشای ریسک‌های سایبری در شرکت‌های مورد بررسی ندارد.

بحث و نتیجه‌گیری

پژوهش حاضر با هدف بررسی تجربی رابطه سازوکارهای حاکمیت شرکتی و ویژگی‌های ساختاری هیئت‌مدیره با سطح افشای ریسک‌های فناوری اطلاعات و امنیت سایبری در شرکت‌های تولیدی پذیرفته‌شده در بورس اوراق بهادار تهران انجام گرفت. با گسترش تحول دیجیتال و تشدید تهدیدات امنیتی، نیاز مبرم بازار سرمایه و ذی‌نفعان به شفافیت اطلاعاتی، تبیین نقش نظارتی ارکان حاکمیتی را ضروری ساخته است. در ادامه، نتایج حاصل از آزمون فرضیه‌های پژوهش به تفکیک مورد بحث، تبیین نظری و مقایسه با ادبیات پیشین قرار می‌گیرد:

بحث پیرامون فرضیه اول: استقلال هیئت‌مدیره و افشای ریسک فناوری

اطلاعات و امنیت سایبری

یافته‌های پژوهش نشان داد که استقلال هیئت‌مدیره تأثیر معناداری بر سطح افشای ریسک‌های فناوری اطلاعات و امنیت سایبری در شرکت‌های نمونه ندارد و این فرضیه تأیید



نشد. این نتیجه با یافته‌های الودات و همکاران (۲۰۲۵) و ماتمانه و همکاران (۲۰۲۴) که بر اساس نظریه نمایندگی، اعضای مستقل را محرک اصلی ارتقای شفافیت و افشای داوطلبانه ریسک‌ها می‌دانند، غیرهمسو است؛ اما با نتایج هروکس و فورتین (۲۰۲۳) تطابق دارد. در تبیین این ناهمسویی می‌توان بیان نمود که در شرکت‌های فعال در بازار سرمایه ایران، اعضای مستقل و غیرموظف هیئت‌مدیره عمدتاً فاقد سواد و تخصص فنی لازم در حوزه سامانه‌های اطلاعاتی و پدافند سایبری هستند. افزون بر این، در بسیاری از ساختارهای شرکتی داخلی، حضور اعضای مستقل جنبه انطباق‌سازی با الزامات دستورالعمل‌های حاکمیت شرکتی را داشته و این اعضا به دلیل محدودیت دسترسی به داده‌های عملیاتی و عمق رویدادهای فنی، نقش فعالی در سیاست‌گذاری افشای ریسک‌های پیچیده فناوری ایفا نمی‌کنند.

بحث پیرامون فرضیه دوم: اندازه هیئت‌مدیره و افشای ریسک فناوری اطلاعات و امنیت سایبری

بر اساس یافته‌ها، اندازه هیئت‌مدیره اثر معناداری بر افشای ریسک‌های فناوری اطلاعات و امنیت سایبری بر جای نگذاشت و فرضیه دوم مورد تأیید قرار نگرفت. این یافته با نتیجه الشیراح (۲۰۲۴) که هیئت‌مدیره‌های بزرگ‌تر را به دلیل تنوع مهارت‌ها عاملی برای ارتقای سطح افشا دانسته بود، ناهمخوان است؛ لیکن با نتایج فصیحی و برشد (۱۴۰۲) و گائو و کالدرون (۲۰۲۵) همسویی دارد. تبیین نظری این وضعیت بیانگر آن است که اگرچه افزایش تعداد اعضای هیئت‌مدیره می‌تواند منابع و دیدگاه‌های متنوع‌تری فراهم آورد، اما هم‌زمان چالش‌های هماهنگی، کندی فرایند تصمیم‌گیری، تعارضات درون‌گروهی و پدیده سواری رایگان را در نظارت راهبردی تشدید می‌کند؛ بنابراین صرفاً تعدد اعضا بدون داشتن درک تخصصی از تهدیدات دیجیتال، پیامد مثبت معناداری بر شفافیت سایبری در پی نداشته است.

بحث پیرامون فرضیه سوم: تخصص مالی اعضای هیئت‌مدیره و افشای ریسک فناوری اطلاعات و امنیت سایبری

نتایج آزمون حاکی از عدم وجود رابطه معنادار میان تخصص مالی اعضای هیئت‌مدیره و سطح افشای ریسک‌های فناوری اطلاعات و امنیت سایبری است؛ ازاین‌رو فرضیه سوم رد شد. این نتیجه با یافته‌های اسماعیلی و همکاران (۲۰۲۳) و امانی و همکاران (۲۰۲۵) که تخصص مالی را پیش‌ران ارتقای شفافیت افشای ریسک در گزارشگری می‌دانند مغایر بوده، اما با



یافته‌های هروکس و فورتین (۲۰۲۳) سازگار است. دلیل این ناهمبستگی را می‌توان به تمرکز سنتی مدیران دارای پیشینه مالی و حسابداری در ایران بر شاخص‌های عملکرد مالی، مدیریت سود، مباحث مالیاتی و ساختار تأمین مالی نسبت داد. از منظر این مدیران، مباحث امنیت داده و ریسک زیرساخت‌های فناوری اطلاعات همچنان مقوله‌ای صرفاً فنی تلقی شده و ارزیابی پیامدهای مالی یا تعهدات ناشی از حملات سایبری در اولویت تصمیمات گزارشگری آنان قرار نگرفته است.

بحث پیرامون فرضیه چهارم: تخصص فناوری اطلاعات اعضای هیئت‌مدیره و افشای ریسک فناوری اطلاعات و امنیت سایبری

یافته‌های این مطالعه نشان داد که تخصص فناوری اطلاعات اعضای هیئت‌مدیره رابطه معناداری با افشای ریسک‌های سایبری برقرار نمی‌کند و فرضیه چهارم تأیید نگردید. این یافته با نتایج گائو و کالدرون (۲۰۲۵) و حسینی و همکاران (۱۴۰۱) که حضور مدیران مسلط به فناوری را عاملی کلیدی در جهت‌دهی شرکت به افشای دقیق ریسک‌های دیجیتال معرفی کرده‌اند، غیرهمسو است. دلیل اصلی این نتیجه را باید در بافتار ترکیب هیئت‌مدیره شرکت‌های تولیدی بورس تهران جست‌وجو کرد؛ جایی که تعداد اعضای دارای مدارک یا تجارب مدیریتی مرتبط با فناوری اطلاعات بسیار اندک بوده و این اقلیت محدود توانایی اثرگذاری غالب بر مصوبات جمعی هیئت‌مدیره در خصوص سیاست‌های گزارشگری بیرونی را ندارند.

بحث پیرامون فرضیه پنجم: دوگانگی وظیفه مدیرعامل و افشای ریسک فناوری اطلاعات و امنیت سایبری

نتایج حاصل از آزمون مدل نشان داد که تمرکز قدرت ناشی از دوگانگی مدیرعامل اثر آماری معناداری بر سطح افشای ریسک امنیت سایبری ندارد و فرضیه پنجم تأیید نشد. این یافته با پژوهش‌های الشاعر و همکاران (۲۰۲۵) و ترین و همکاران (۲۰۲۵) که رابطه منفی و کاهنده معناداری میان تمرکز نقش‌ها و افشای داوطلبانه مستند کرده بودند ناهمسو، ولی با یافته‌های نمازی و ابراهیمی میمند (۱۳۹۵) در بازار سرمایه ایران همسو است. تبیین این یافته بر این مبنا استوار است که به‌موجب قوانین و دستورالعمل‌های حاکمیت شرکتی سازمان بورس و اوراق بهادار، تفکیک پست مدیرعامل از ریاست هیئت‌مدیره به‌طور گسترده پیاده‌سازی شده و وقوع

دوگانگی در شرکت‌های نمونه به حداقل رسیده است؛ در نتیجه نوسانات این متغیر نمی‌تواند تعیین‌کننده اصلی در نوسان سطح افشای سایبری در سطح بازار باشد.

بحث پیرامون فرضیه ششم: وجود کمیته تخصصی فناوری اطلاعات/ریسک و افشای ریسک فناوری اطلاعات و امنیت سایبری

تنها یافته معنادار حاصل از متغیرهای حاکمیتی پژوهش، تأیید رابطه معکوس (منفی) و معنادار میان وجود کمیته تخصصی فناوری اطلاعات/ریسک با سطح افشای ریسک فناوری اطلاعات و امنیت سایبری است؛ بدین ترتیب فرضیه ششم با جهت اثر منفی تأیید شد. اگرچه بر پایه فرضیه کلاسیک نمایندگی و یافته‌های ماتمانه و همکاران (۲۰۲۴)، انتظار می‌رفت ایجاد کمیته‌های تخصصی به شفافیت بیشتر بینجامد، اما یافته معکوس این پژوهش با مبانی «نظریه هزینه‌های مالکانه» و نتایج فیروزی و محسنی (۲۰۲۳) و لینگ و همکاران (۲۰۲۵) انطباق کامل دارد. در چارچوب هزینه‌های مالکانه، اعضای این کمیته‌ها با درک عمیق از آسیب‌پذیری‌های امنیتی و حساسیت داده‌های صنعتی، افشای عمومی و پر جزئیات رخدادهای موجب تضعیف موقعیت رقابتی و راهنمایی مهاجمان سایبری می‌دانند. از این رو، وجود این کمیته‌ها بیشتر به جای تحریک گزارشگری عمومی، نقش سازوکاری تدافعی را ایفا نموده که به مهار درون‌سازمانی، اصلاح آسیب‌پذیری‌ها و اتخاذ تدابیر احتیاطی بدون افشای بیرونی می‌انجامد.

پیشنهادهای کاربردی

یافته‌های این پژوهش حامل دلالت‌های مهمی برای ارکان حاکمیتی و سیاست‌گذاران بازار سرمایه است:

- **به هیئت‌مدیره شرکت‌ها** پیشنهاد می‌شود سازوکار نظارت سایبری را از سطح یک اقدام تدافعی صرف به یک مزیت راهبردی تبدیل کنند. همچنین ارتقای سواد سایبری اعضای غیرموظف و مستقل و استفاده از مشاوران تخصصی در کمیته‌های حسابرسی و ریسک می‌تواند تصمیم‌گیری در خصوص میزان افشای متوازن را تسهیل نماید.
- **به سازمان بورس و اوراق بهادار** پیشنهاد می‌گردد نسبت به تدوین راهنماها و چارچوب‌های استاندارد افشای حوادث و ریسک‌های امنیت سایبری اقدام کند تا ضمن



حفظ محرمانگی راهبردی شرکت‌ها (کاهش هزینه‌های مالکانه)، کف شفافیت لازم برای تصمیم‌گیری سرمایه‌گذاران تأمین شود.

محدودیت‌های پژوهش

تفسیر نتایج حاضر باید با در نظر داشتن این محدودیت‌ها صورت پذیرد. نخست، انحصار جامعه آماری به شرکت‌های بخش تولیدی، تعمیم‌پذیری مستقیم یافته‌ها به نهادهای مالی دارای حساسیت شدید داده‌ای (نظیر بانک‌ها و بیمه‌ها) را با احتیاط مواجه می‌سازد. دوم، تکیه بر تحلیل محتوای گزارش‌های سالانه و تفسیری مدیریت که بازتاب‌دهنده افشای عمومی است و ممکن است با وضعیت واقعی و زیرساخت‌های پنهان امنیتی شرکت‌ها انطباق کامل نداشته باشد. محدودیت سوم، محرمانگی رخدادهای امنیتی در ایران و عدم دسترسی به داده‌های هزینه‌ای مربوط به نقض داده‌ها یا خسارات سایبری، می‌باشد.

پیشنهاد برای پژوهش‌های آتی

- ارزیابی این الگو در شرکت‌های خدمات مالی، بانکی و فین‌تک‌ها که مواجهه مستقیم‌تری با حملات سایبری دارند.
- بررسی متغیرهای واسطه‌ای نظیر اثربخشی حسابرسی داخلی و سامانه‌های کنترل داخلی بر رابطه حاکمیت شرکتی و افشای سایبری.
- استفاده از مصاحبه‌های نیمه‌ساختاریافته با مدیران ارشد امنیت اطلاعات (CISO) و اعضای کمیته‌های ریسک به منظور واکاوی دلایل رفتاری در مهار درون‌سازمانی و احتراز از افشای عمومی.

ملاحظات اخلاقی

حامی مالی: مقاله حامی مالی ندارد.

مشارکت نویسندگان: تمام نویسندگان در آماده‌سازی مقاله مشارکت داشته‌اند.

تعارض منافع: بنابر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافی وجود ندارد.

تعهد کپی رایت: طبق تعهد نویسندگان حق کپی رایت رعایت شده‌است.



منابع

- کریمی، صیفی (۱۴۰۳). حاکمیت شرکتی، افشای ریسک و بازده سهام در شرکت‌های مالی ایران. پژوهش‌های تجربی حسابداری، ۱۴(۵۳)، ۲۱۵-۲۳۸. <https://doi.org/10.22051/jera.2025.51375.3593>
- فصیحی، ستاره و برشد، رضوان (۱۴۰۲). افشای ریسک شرکت‌ها: تأثیر ویژگی‌های کمیته حسابرسی. پژوهش‌های تجربی حسابداری، ۱۳(۱)، ۱۴۱-۱۶۰. <https://doi.org/10.22051/jera.2022.37494.2924>
- نمازی، محمد و ابراهیمی میمند، مهدی (۱۳۹۵). بررسی تأثیر سازوکارهای راهبری شرکتی بر افشای ریسک در شرکت‌های پذیرفته شده در بورس اوراق بهادار تهران. فصلنامه حسابداری مالی، ۸(۳۰)، ۱-۲۷.
- <http://qfaj.mobarakeh.iau.ir/article-1-813-fa.html>
- هیئت وزیران (۱۴۰۴). سند ستاد توسعه علوم و فناوری افتا (امنیت سایبری) (تصویب‌نامه شماره ۳۶۶۰۸ مورخ ۱۴۰۴/۰۲/۳۱). پایگاه ملی اطلاع‌رسانی قوانین و مقررات کشور. <https://qavanin.ir>

References

- Alodat, A. Y., Hao, Y., Nobanee, H., Ali, H., Mansour, M., & Al Amosh, H. (2025). Board characteristics and cybersecurity disclosure: evidence from the UK. *Electronic Commerce Research*, 25(6), 1–32. <https://doi.org/10.1007/s10660-024-09867-w>
- Al-Shaer, H., Albitar, K., Derouiche, I., & Hussainey, K. (2025). The role of CEO power and audit committees in cybersecurity risk management. *The International Journal of Accounting*, Advance online publication.
- Alshira'h, A. F. (2024). Board of directors' characteristics, political connection and risk disclosure: Evidence from an emerging market context. *Risks*, 12(3), 54–73.
- Amani, F., Magnan, M., & Moldovan, R. (2025). Cybersecurity risks and incidents disclosure: A literature review. *Accounting Perspectives*, Advance online publication. <https://doi.org/10.1111/1911-3838.12411>
- Council of Ministers. (2025). *Document of the High Council for Cyberspace and Cyber Security Development (AFTA)* (Resolution No. 36608 dated 2025/05/21). National Database of Laws and Regulations of the Islamic Republic of Iran. <https://qavanin.ir> (in Persian)
- Fasihi, S., & Borshed, R. (2023). Corporate risk disclosure: The impact of audit committee characteristics. *Journal of Empirical Research in Accounting*, 13(1), 141–160. <https://doi.org/10.22051/jera.2022.37494.2924> (in Persian)
- Firoozi, M., & Mohsni, S. (2023). Cybersecurity disclosure in the banking industry: A comparative study. *Journal of Banking Regulation*, 25(2), 173–192. <https://doi.org/10.1057/s41310-023-00190-8>
- Gao, L., & Calderon, T. G. (2025). Cybersecurity risk governance and companies' cybersecurity risk disclosures in their 10-K filings. *Journal of Accounting and Public Policy*, 54(5), Article 107376. <https://doi.org/10.1016/j.jaccpubpol.2025.107376>
- Héroux, S., & Fortin, A. (2024). Board of directors' attributes and aspects of cybersecurity disclosure. *Journal of Management and Governance*, 28(2), 527–562. DOI: 10.1007/s10997-022-09660-7
- ISACA. (2019). *COBIT 2019 Framework: Governance and Management Objectives*. Information Systems Audit and Control Association (ISACA).
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360. [https://doi.org/10.1016/0304-405X\(76\)90026-X](https://doi.org/10.1016/0304-405X(76)90026-X)



- Karami, M., & Seyfi, A. (2024). Corporate governance, risk disclosure and stock returns in Iranian financial firms. *Journal of Empirical Research in Accounting*, 14(53), 215–238. <https://doi.org/10.22051/jera.2025.51375.3593> (in Persian)
- Ling, S., Liu, Z. F., & Xia, H. (2025). Code, control and cybersecurity: How board IT expertise shapes corporate risk management. *Journal of Accounting Literature*, 1–23. <https://doi.org/10.1108/JAL-06-2025-0320>
- Elgammal, M. M., Hussainey, K., & Ahmed, F. (2018). Corporate governance and voluntary risk and forward-looking disclosures. *Journal of Applied Accounting Research*, 19(4), 592–607. <https://doi.org/10.1108/JAAR-01-2017-0014>
- Matemane, R., Denhere, V., Mokabane, M., & Ojeyinka, T. A. (2024). Cybersecurity risk disclosure, board characteristics, and firm performance in the Fourth Industrial Revolution era: Evidence from an emerging economy. *African Finance Journal*, 26(1), 34–53. https://journals.co.za/doi/abs/10.10520/ejc-finj_v26_n1_a2
- Namazi, M., & Ebrahimi Meimand, M. (2016). Investigating the effect of corporate governance mechanisms on risk disclosure in companies listed on Tehran Stock Exchange. *Financial Accounting Quarterly*, 8(30), 1–27. <https://sid.ir/paper/517517/fa> (in Persian)
- Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.1299>
- Pfeffer, J., & Salancik, G. R. (2003). *The External Control of Organizations: A Resource Dependence Perspective*. Stanford University Press. <https://www.sup.org/books/business/external-control-organizations>
- Trinh, V. Q., Elnahass, M., & Pasiouras, F. (2025). Personal traits of CEOs and cybersecurity-related disclosure. *Journal of International Accounting, Auditing and Taxation*, 58, Article 100680 <https://doi.org/10.1016/j.intaccaudtax.2025.100680>
- Smaili, N., Radu, C., & Khalili, A. (2023). Board effectiveness and cybersecurity disclosure. *Journal of Management and Governance*, 27(4), 1049–1071. <https://doi.org/10.1007/s10997-022-09637-6>

COPYRIGHT



This license allows others to download the works and share them with others as long as they credit them, but they can't change them in any way or use them commercially.

