CICA Framework: Harnessing CSR, AI, and Blockchain for Sustainable Digital Culture

Danang Danang, Agustinus Budi Santoso, Maya Utami Dewi
Fakultas Studi Akademik, Universitas Sains dan Teknologi Komputer, Semarang, Indonesia

***Abstract*—Digital transformation has created new opportunities for organizations, but it has also intensified cybersecurity risk. In emerging economies, where institutional support and digital literacy remain limited, cybersecurity awareness plays a crucial role in strengthening digital resilience and fostering a sustainable digital culture. This study introduces the CSR-Integrated Cybersecurity Awareness (CICA) Framework, which conceptualizes Corporate Social Responsibility (CSR) as a key driver of cybersecurity awareness, reinforced by the adoption of artificial intelligence (AI) and blockchain technologies. Data were collected from companies in Central Java, Indonesia, that implement CSR-based digital initiatives, with responses gathered from managers, CSR officers, and IT staff. Using Structural Equation Modeling (SEM), the findings show that CSR significantly enhances cybersecurity awareness, AI adoption strengthens proactive security measures, and blockchain increases trust and transparency. The results also reveal that CSR mediates the relationship between digital technology adoption and sustainable digital culture. This study contributes by integrating CSR and cybersecurity through emerging technologies, offering theoretical insights and practical implications for organizations in developing regions.**

***Keywords*—Cybersecurity awareness; corporate social responsibility; artificial intelligence; blockchain; sustainable digital culture; emerging economies**

I. Introduction

The 21st century is marked by the phenomenon of digital transformation, which is fundamentally changing how organizations thrive and survive in the global marketplace. Digital transformation contributes greatly to business success and resilience. Digital transformation provides opportunities and challenges, so that organizations are encouraged to implement strategies to be more competitive and increase market share [1]. Success in the digital era requires more than adopting advanced technologies; it demands fundamental transformation in organizational operations, innovation, and value-creation strategies [2].

In terms of significant enhancements in efficiency, innovation, and business growth, digitization has a significant impact. However, on the other hand, it also causes the risk of cyber-attacks and digital vulnerabilities. The availability of artificial intelligence (AI), big data, cloud computing, and blockchain technologies accelerates the direction of digital transformation, but also brings cyber risks and threatens businesses [3] (Saeed et al., 2023). The World Economic Forum, through its Global Cybersecurity Outlook 2025 report, highlights the increasingly complex global cyber ecosystem, which has broad implications for countries and organizations. These driving factors include rapid technological developments, geopolitical uncertainty, evolving threats, complex regulations, supply chain vulnerabilities, and a shortage of cyber [4]. This has a sharp impact on widening the cyber gap. At a broader level, this could widen the gap between developing and developed countries, between sectors, and between large and small organizations. This has a significant impact on widening the cyber gap. At a broader level, this could widen the gap between developing and developed countries, between sectors, and between large and small organizations.

A study by Catal found that executive awareness of cyber risks is quite high, but their management varies across industries. Therefore, cybersecurity must be integrated into the entire digital transformation process [5]. Therefore, cybersecurity awareness is not solely the responsibility of IT professionals but is the responsibility of every individual. Both everyday internet users and professionals need to understand how to recognize and anticipate digital threats. Increasing cybersecurity literacy is a strategic step to protect personal data while maintaining a secure digital ecosystem for all.

In developing countries, the urgency of cybersecurity is increasingly apparent. Southeast Asia suffers an estimated USD 1.7 billion in losses annually due to cyberattacks [6], with Indonesia being a primary target. Despite the rapid adoption of digital developments across various sectors, Kaspersky reported the detection and interception of over 13 million web threats aimed at businesses in Southeast Asia (SEA) throughout 2023, with Indonesia reaching 4,968,729 threats in 2023 [7]. This paradox demonstrates that digitalization not only drives growth but also increases vulnerability to cyberthreats.

At the same time, Corporate Social Responsibility (CSR) has expanded beyond traditional domains such as environment, education, and health to include digital responsibility. Digital transformation impacts internal and external CSR, particularly on shareholder value and employee responsibility through business model innovation [8]. Forward-thinking companies are beginning to view CSR not only as philanthropy but also as a strategic path to increase stakeholder trust and digital resilience.

Visionary companies now view CSR not simply as a philanthropic activity, but as a strategy to build stakeholder trust and strengthen digital resilience [9]. Although the Corporate Social Responsibility (CSR) literature is replete with discussion on CSR as a standard element, there exists limited research that systematically links it to cybersecurity awareness in fostering maintenance of sustainable digital culture. Previous studies have explored different factors that influence CSR from the individual [10], organizational level to industry [11], and

institutional levels scale in a developing country context [12]. Corporate social responsibility is being demanded or required along with digital transformation to be increasingly considered in the light of ethical, sociopolitical, and security aspects that we see nowadays. There are several studies which also confirm that a CSR strategically aligned approach can increase the employees' understanding, organization learning, and promotion of other sustainable behavioral performance [13], [14], [15].

In [16], the authors state that CSR creates positive external legitimacy, while [17] and [18] found that CSR increases internal resilience by increasing safe internet behavior among employees. On the other hand, [19] states that issues related to corporate responsibility, such as data security, are interconnected and must be considered holistically within the framework of Corporate Digital Responsibility.

New prospects for enhancing digital security advancements are driven by the emergence of Artificial Intelligence (AI)-based blockchain technology. AI helps drive early threat detection with computerized responses, and blockchain is currently being used for transparency and immutability [20], [21], integrity, and trust within digital frameworks [22]. Integrating this technology with CSR-based awareness programs will result in the [Cybersecurity Integrated CSR Awareness] (CICA) model framework—an innovation for creating cybersecurity awareness among organizational members. For example, Yao's research shows a significant increase in social responsibility as innovative companies use AI in technology-based innovations [23].

This research is based on complementary theories: the Technology–Organization–Environment (TOE) framework and Institutional Theory. The Technology–Organization–Environment (TOE) framework examines how technological, organizational, and environmental factors shape the adoption of artificial intelligence (AI) and blockchain. Institutional Theory explains the pressures of norms, culture, and rules that drive CSR-based digital practices. Furthermore, the Resource-Based View (RBV) theory supports this study as a guideline for how CSR can be considered a strategic resource that strengthens resilience and competitive advantage.

The novelty of this study lies in the explicit integration of CSR with cybersecurity awareness, a relatively unexplored dimension within Corporate Digital Responsibility (CDR), and the conceptualization of AI and blockchain as not only enablers but also moderators that strengthen the relationship between CSR and cybersecurity. By focusing on emerging economies, particularly Indonesia, this research also addresses the geographic imbalance in CSR–cybersecurity research, which has been dominated by developed countries. The proposed CSR Integrated Cybersecurity Awareness (CICA) Framework further enriches the theoretical discourse by linking TOE, Institutional Theory, and RBV to explain how CSR can foster a sustainable digital culture.

II. Literature Review

A. Corporate Social Responsibility and Cybersecurity Awareness

Corporate Social Responsibility (CSR) describes how companies allocate available resources, both financial and human, in order to support long-term sustainable economic growth and appreciate the full scope of related social, cultural and environmental implications. The core principles of CSR show businesses must not merely seek short-term profit, but long-term sustainability. CSR embodies the need for a company to understand its role in society, and that it must balance its commercial activities with human and environmental interests.

The concept of Corporate Social Responsibility (CSR) is evolving alongside the conversation about sustainability. Nowadays, organizations are expected to step up as drivers of social and environmental change [24]. Modern CSR is seen as a comprehensive approach to business, where companies are responsible not only for making profits but also for the well-being of people and the planet. Moreover, the rise of digitalization has brought new challenges to CSR, particularly in areas like data protection, privacy, digital skills, and access to technology. Companies are now tasked with not just fulfilling traditional social responsibilities but also creating a safe and inclusive digital landscape. When CSR initiatives align with business objectives, they can spark innovation, enhance competitive advantage, and ensure sustainable growth over time [25].

In today's digital age, Corporate Social Responsibility (CSR) has shifted towards digital accountability, encompassing aspects like technology inclusion, ethical practices, data protection, and cybersecurity awareness [26]. Empirical studies suggest that CSR has a positive influence on employees' awareness and responsible behaviors. For example, CSR programs were significantly associated with improved awareness and compliance in information security contexts [27], [28], [29]. Similarly, research on CDR highlights that when organizations publicly commit to digital responsibility, employees are more likely to internalize safe practices as part of their professional and ethical duties [30].

In addition, CSR contributes to the development of a sustainable digital environment that is in line with the idea of Corporate Digital Responsibility (CDR), which focuses on the ethical, safe, and sustainable management of data, artificial intelligence, and technology [31]. CSR is considered a component of strategic planning and managerial decision-making [32]. As a result, CSR can be seen as a key driver of digital trust. By integrating cybersecurity-focused initiatives into CSR efforts, organizations not only enhance their external credibility but also strengthen their internal resilience. As a foundation for building a secure, ethical, and resilient digital organization, the framework proposed in this study is:

H1: CSR initiatives positively affect cybersecurity awareness.

H2: CSR initiatives positively influence the development of a sustainable digital culture.

B. Sustainable Digital Culture

Rapid technological developments have transformed global society, with digital literacy rapidly increasing. These changes not only impact the use of digital devices and platforms but also our interactions, communications, and the expression of our cultural values. Digital culture is the starting point for the

sustainable development of businesses run by a company or organization. Consequently, digital culture has emerged as a crucial topic deserving attention.

Sustainable digital culture involves incorporating long-term digital ethics, accountability, and security into the practice of an organization [33], [34]. Awareness driven by corporate social responsibility (CSR) and the adoption of technology play vital roles in fostering this culture. The culture within an organization is marked by an ongoing necessity to adjust to an ever-evolving technological environment and to shift values in order to address or foresee future environmental needs [35].

Sustainable digital culture describes an organizational setting where digital technologies are woven into values, norms, and practices that emphasize both innovation and long-term security. Unlike digital practices that are reactionary or solely focused on compliance, a sustainable digital culture encompasses digital responsibility, ethical use of technology, and resilience as fundamental aspects of organizational behavior [36].

The significance of a sustainable digital culture has gained increasing acknowledgment in global discussions. According to the World Economic Forum, resilient organizations are those that integrate cybersecurity and digital responsibility into their corporate ethos, allowing them to endure challenges such as major data breaches or widespread cyberattacks [37]. Research indicates that organizations with robust digital cultures demonstrate greater flexibility during crises, such as the COVID-19 pandemic, by effectively utilizing digital tools in a secure and sustainable manner [38], [39].

Corporate Social Responsibility (CSR) is crucial in influencing sustainable digital culture. By incorporating cybersecurity awareness initiatives into CSR efforts, businesses foster values of accountability and shared responsibility. This supports the notion that CSR not only bolsters external legitimacy but also promotes internal resilience, thereby contributing to a secure and sustainable digital landscape.

C. Cybersecurity Awareness

Vulnerability to various threats is rapidly increasing due to our high dependence on technology for communication, financial transactions, and personal data management. As cyber threats become more sophisticated, organizations are responsible for equipping their employees with the knowledge and skills necessary to identify and prevent them. Human factors are often the weak link in cybersecurity [40], [41].. Cybersecurity awareness must be implemented with care [42]. Cybersecurity awareness is essential for reducing the risk of phishing, social engineering, and insider threats.

In fact, integrating cybersecurity awareness into CSR initiatives can be an ethical and socially responsible way to promote safe digital behavior. Cybersecurity awareness encompasses the ability of individuals within an organization to understand, recognize, and respond appropriately to cyber threats. It includes the knowledge, attitudes, and behaviors that contribute to the protection of digital assets and the reduction of vulnerabilities [43].

Increasing cybersecurity awareness does not only involve implementing training programs; it also involves fostering a deeper comprehension among individuals within the organization and providing them with the skills to respond to threats effectively [44]. A comprehensive strategy should incorporate organizational elements, operational processes, and human resources [45]. By deploying awareness and training initiatives, employees acquire insights into the organization's security needs, policies, and procedures for securing sensitive data, while also enhancing their capabilities in addressing cybersecurity threats [46].

Raising cybersecurity awareness goes beyond simply offering training programs; it also entails fostering a deeper understanding among individuals in the organization and providing them with the skills to effectively react to threats [44]. A holistic strategy must encompass organizational elements, operational processes, and human capital [45]. By implementing awareness and training initiatives, employees gain insight into the organization's security needs, policies, and procedures to safeguard sensitive data and enhance the handling of cybersecurity challenges [46].

The human aspect of information security has been designed to conceptualize cybersecurity awareness. The Human Aspects of Information Security Questionnaire (HAIS-Q) has identified several dimensions of awareness, including password management, email usage, social networking, information handling, and incident monitoring [47]. These dimensions reflect the idea that awareness is not only about mastering knowledge, but also about applying that knowledge into consistent and secure digital practices.

Scientific evidence confirms the importance of cybersecurity awareness. Training has been shown to reduce the risk of phishing and malware attacks [47], while a work culture that emphasizes accountability encourages compliance and follow-up on threats [48]. Therefore, awareness must be the foundation of an organization's cybersecurity strategy.

In the context of the CSR framework, cybersecurity awareness can be developed through digital literacy programs, training in the ethical use of technology, and community campaigns. This awareness plays a role in creating a sustainable digital culture, where CSR provides legitimacy and resources, while individuals apply these values to their daily practices, which can strengthen the organization's digital responsibility.

H3: Cybersecurity awareness positively contributes to the enhancement of a sustainable digital culture.

H4: Cybersecurity awareness mediates the relationship between Corporate Social Responsibility (CSR) and sustainable digital culture.

D. Artificial Intelligence Adoption

AI has revolutionized cybersecurity with its real-time threat detection and predictive analysis capabilities, increasing efficiency and resilience to attacks [49]. Unlike rule-based systems, AI can analyze big data, recognize abnormal patterns, and prevent risks before they develop.

Within the Technology–Organization–Environment (TOE) and Technology Acceptance Model (TAM) frameworks, AI adoption is influenced by technological factors, organizational readiness, and external pressures [50]. In developing countries, AI is adopted not only for operational efficiency but also to strengthen security and compliance [51].

In relation to CSR and cybersecurity, AI plays a role as an amplifier for awareness programs. Without technological support, CSR initiatives tend to be limited. AI tools such as intelligent firewalls, phishing detection, and behavioral analytics increase the effectiveness of training by reducing reliance on humans [52], [53].

Strategically, the integration of AI in CSR reflects a company's commitment to technological responsibility, not only for profit, but also to protect stakeholders and build public trust.

H5a: The adoption of Artificial Intelligence (AI) moderates the relationship between Corporate Social Responsibility (CSR) and cybersecurity awareness.

E. Blockchain Adoption

The adoption of blockchain is driven by technological, organizational, and environmental (TOE) factors, as well as perceived benefits, infrastructural readiness, and external pressures such as regulatory requirements and competition [54]. Blockchain offers secure, transparent, and immutable data management, making it relevant for cybersecurity governance and CSR reporting [55]. This technology is not only connected to cryptocurrency but also has vast promise for constructing reliable digital infrastructure through decentralization, transparency, and consensus mechanisms [21], [56]..In an organizational context, blockchain provides a verified and immutable transaction record, reducing the risk of fraud and increasing resilience to cyberattacks [57]. While adoption in emerging economies has likely been incremental, blockchain applications in supply chain, healthcare, and digital identity are steadily increasing [58].

In the CSR-cybersecurity framework, blockchain has a role as a moderator by ensuring transparency and accountability. Through blockchain-based reporting systems, CSR initiatives regarding data security and digital literacy can be instated with more credibility, strengthening the effectiveness of cybersecurity awareness programs driven by CSR.

H5b: The adoption of Blockchain moderates the relationship between Corporate Social Responsibility (CSR) and cybersecurity awareness.

The reviewed literature shows that CSR and cybersecurity are often examined separately, with limited studies linking CSR to cybersecurity awareness. Existing models also tend to focus on individual behavior or technology adoption without considering CSR as a strategic driver of security practices. Additionally, the roles of AI and blockchain in supporting CSR-based security outcomes remain understudied, particularly in emerging economies.

To address these gaps, this study proposes the CICA Framework, which integrates CSR, cybersecurity awareness, and emerging technologies. By testing this framework empirically in an emerging-economy context, the study provides new evidence on how CSR, AI, and blockchain contribute to strengthen sustainable digital culture. Fig. 1 presents the research framework.

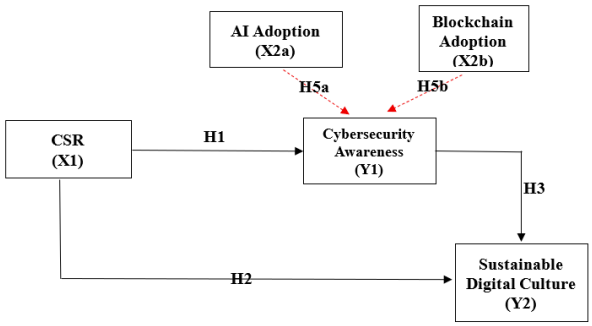

Fig. 1. Research framework.

III. METHODS

This research uses a quantitative design with a survey approach combined with Structural Equation Modelling (SEM) analysis. The research population includes companies and institutions in Central Java that have applied CSR programming and digital awareness practices or security-related programs. A purposive sampling technique was applied to select relevant respondents, including the CSR manager, IT or security personnel, academic officers involved in digital programs, and those actively involved in CSR-based awareness campaigns.

A total of 220 valid responses were collected, fulfilling the recommended minimum for SEM, which is 5 to 10 times the number of latent constructs or the maximum number of structural paths, rather than the number of indicators. The research questionnaire was structured and developed based on previous literature. The CSR indicators were modified from [59], cybersecurity awareness was adapted from [29], AI adoption was based on [49], blockchain adoption was derived from [55], and sustainable digital culture was adapted from [60]. All items were measured using a five-point Likert scale ranging from “strongly” to “strongly agree”. Data analysis consisted of assessing reliability and validity through Cronbach’s Alpha, Composite Reliability, and Confirmatory Factor Analysis (CFA). Structural relationships were examined using SEM–Partial Least Squares (SEM-PLS). Mediation analysis was further conducted to evaluate the role of cybersecurity awareness in mediating the influence of CSR on sustainable digital culture. Additionally, the correlation was tested using SEM-Partial Least Squares (SEM-PLS) [64]. Mediation analysis was also performed to examine the role of CSR in influencing sustainable digital culture through cybersecurity awareness.

IV. RESULTS

A. Respondent Characteristic

This research collected responses of 220 participants representing organizations in Central Java, Indonesia, that have implemented CSR and digital initiatives. The majority of respondents are female (61.4%), with the remaining 38.6%

male. In term of age distribution, the largest group are between 31 and 40 years old (38.6%), followed by over 40 years old (35.9%) and 21 – 30 years old (25%), with only 0.5% aged below 20.

In terms of educational qualification, 48.2% of respondents hold a diploma, 47.3% a bachelor's degree, and 4.5% a master's degree. Regarding professional occupation, 36.80% are IT/Security officers, 28.2% are CSR Managers, and then academic personal involved in digital programs are 13.6%. The respondent's work experience also varies, with 36.4% having worked for 4-6 years, and 30.9% for more than 6 years. 26.8% for 1-3 years, and only 5.9% for less than one year. The result of the respondent characteristic is displayed in Table I.

TABLE I. RESPONDENT CHARACTERISTIC

		Frequency	Per cent	Valid Per cent	Cumulative Per cent
Gender					
Valid	Male	85	38.6	38.6	38.6
	Female	135	61.4	61.4	100.0
	Total	220	100.0	100.0	
Age					
Valid	<20	1	.5	.5	.5
	21-30	55	25.0	25.0	25.5
	31-40	85	38.6	38.6	64.1
	>40	79	35.9	35.9	100.0
	Total	220	100.0	100.0	
Education					
Valid	Diploma	106	48.2	48.2	48.2
	Bachelor	104	47.3	47.3	95.5
	Master	10	4.5	4.5	100.0
	Total	220	100.0	100.0	
Occupation					
Valid	Employee	62	28.2	28.2	28.2
	Academic Staff	30	13.6	13.6	41.8
	Security Officer	81	36.8	36.8	78.6
	CSR Manager	47	21.4	21.4	100.0
	Total	220	100.0	100.0	
Years of Experience					
Valid	1	13	5.9	5.9	5.9
	1-3	59	26.8	26.8	32.7
	4-6	80	36.4	36.4	69.1
	>6	68	30.9	30.9	100.0
	Total	220	100.0	100.0	

Source: Data processing results, 2025

B. Measurement Model (Outer Model)

The outer loading analysis confirms that the majority of items load adequately onto their intended constructs, supporting the convergent validity of the measurement model.

1) Validity and reliability test: Table II shows the results of the reliability and validity test. Cronbach's alpha ranged from 0.686 to 0.814, which means that all were above the 0.70 threshold or close to acceptable levels for exploratory studies [61]. Composite Reliability (CR) values ranged between 0.784 and 0.877, exceeding the minimum requirement of 0.70. it confirms internal consistency reliability. Average Variance Extracted (AVE) values were above 0.50 for all constructs (0.529-0.641), demonstrating satisfactory convergent validity. These results confirm that all constructs meet the requirements for reliability and validity in the measurement model [62].

TABLE II. CONSTRUCT RELIABILITY AND VALIDITY

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
AI	0.712	0.727	0.817	0.529
BA	0.814	0.824	0.877	0.641
CA	0.686	0.686	0.784	0.613
CSR	0.737	0.737	0.820	0.532
SDC	0.794	0.805	0.847	0.582

Source: Data processing results, 2025

2) R-Square test (R^2): Table III explains the explanatory power of the structural model. The R^2 value for Cybersecurity Awareness (CA) is 0.616, indicating that CSR, AI, and Blockchain explain 61.6% of its variance. Meanwhile, Sustainable Digital Culture (SDC) shows an R^2 of 0.346, suggesting that CSR and CA togethers explain 34.6% of its variance. These values indicate substantial explanatory power for CA and moderate explanatory power of SDC.

TABLE III. R-SQUARE

	R-Square	R-Square Adjusted
CA	0.616	0.611
SDC	0.346	0.340

Source: Data processing results, 2025

3) Model fit test: The goodness-of-fit indices for the measurement and structural model are presented in Table IV. The Standardized Root Mean Square Residual (SRMR) values of 0.085 (saturated model) and 0.089 (estimated model) fall below the recommended threshold of 0.10, indicating an acceptable model fit. The d_ULS and d_G values also fall within acceptable ranges for PLS-SEM exploratory models. The Chi-square values for both models (803.085 and 816.569) show consistency between the saturated and estimated structures. Additionally, the Normed Fit Index (NFI) values of 0.912 and 0.905 exceed the recommended cut-off of 0.90, demonstrating strong model fit and confirming the adequacy of the proposed structural relationships. Then, the model fit statistics confirm that the measurement and structural models are appropriate.

TABLE IV. MODEL FIT

	Saturated Model	Estimated Model
SRMR	0.085	0.089
d_ULS	2.915	3.213
d_G	0.688	0.700
Chi-Square	803.085	816.569
NFI	0.912	0.905

Source: Data processing results, 2025

4) Model selection criteria: The result of the model selection criteria is displayed in Table V. Based on the table, all indices (AIC, BIC, and HQ) values provide additional robustness checks for comparing alternatives model specifications. Negative AIC and BIC values for CA and SDC suggest good model parsimony. Corrected criteria (AICc, HQCc) [63] also support the stability of the estimated model. While all these values are supplementary, they reinforce the appropriateness of the selected framework.

TABLE V. MODEL SELECTION CRITERIA

	AIC (Akaike's Information Criterion)	AICu (Unbiased Akaike's Information Criterion	AICc (Corrected Akaike's Information Criterion)	BIC (Bayesian Information Criteria)	HQ (Hannan Quinn Criterion)	HQc (Corrected Hannan-Quinn Criterion)
CA	-203.498	-199.462	18.782	-189.924	-198.017	-197.639
SDC	-88.396	-85.375	133.790	-78.215	-84.285	-84.050

Source: Data processing results, 2025

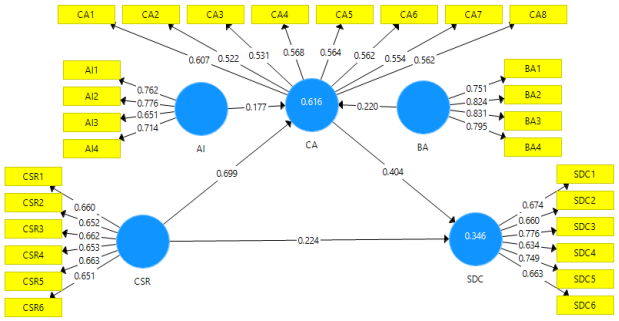

Fig. 2. Outer model or measurement model.

Source: Data processing results, 2025

Annotation:

AI: AI Adoption

BA: Blockchain Adoption

CA: Cybersecurity Awareness

CSR: Corporate Social Responsibility

SDC: Sustainable Digital Culture

Fig. 2 illustrates the outer model and the standardized factor loadings for all constructs. The measurement model demonstrates that each indicator loads strongly on its intended latent construct. All loading values exceed the recommended threshold of 0.60, indicating acceptable convergent validity. The CSR construct shows loading values ranging from 0.640 to 0.683, while AI adoption indicators load between 0.714 and 0.762. Blockchain adoption indicators demonstrate strong loadings ranging from 0.775 to 0.841.

Cybersecurity awareness (CA) indicators also perform satisfactorily, with loadings between 0.528 and 0.582, which are acceptable for exploratory PLS-SEM studies. The sustainable digital culture (SDC) construct shows consistently high indicator loadings between 0.674 and 0.749, demonstrating strong reflective measurement reliability.

Furthermore, the coefficient of determination (R^2) indicates that the model has good explanatory power. CSR, AI, and blockchain collectively explain 61.6% of the variance in cybersecurity awareness (CA), while CSR and CA explain 34.6% of the variance in sustainable digital culture (SDC). These values demonstrate that the model has meaningful predictive capability.

Overall, the outer model satisfies the key reliability and validity criteria, confirming that each construct is measured accurately and consistently. The indicators are therefore suitable for inclusion in the structural model assessment.

C. Structural Inner Model and Hypothesis Test

Table VI reveals the results of the path coefficients used to test the hypothesized relationships in the structural model. The results indicate several significant relationships. CSR → Cybersecurity Awareness (CSA). CSR has a strong and positive influence on CSA ($\beta = 0.699$, $t = 17.363$, $p < 0.001$). This indicates that CSR initiatives significantly increase cybersecurity awareness among organizational members. CSR → Sustainable Digital Culture (CSA). CSR also directly influences CSA ($\beta = 0.224$, $t = 2.462$, $p = 0.014$). Although the effect is smaller than CSA, these results indicate that CSR contributes to building a sustainable digital culture. Cybersecurity Awareness (CSA) → Sustainable Digital Culture (CSA). CSA exhibits a significant positive impact on CSA ($\beta = 0.404$, $t = 4.338$, $p < 0.001$). This suggests that increased awareness of cybersecurity practices fosters stronger digital sustainability within organizations. AI → CA. AI adoption significantly increases CA ($\beta = 0.177$, $t = 3.850$, $p < 0.001$). This confirms AI's role in increasing awareness by enabling predictive threat detection and intelligent digital monitoring. Blockchain Adoption (BA) → CA. Blockchain adoption positively impacts CA ($\beta = 0.220$, $t = 3.515$, $p < 0.001$). This suggests that blockchain's transparency and security features contribute to increased cybersecurity awareness within organizations.

TABLE VI. PATH COEFFICIENT

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDE)	P Values
AI -> CA	0.177	0.185	0.046	3.850	0.000
BA -> CA	0.220	0.217	0.063	3.515	0.000
CA -> SDC	0.404	0.408	0.093	4.338	0.000
CSR -> CA	0.699	0.697	0.040	17.363	0.000
CSR -> SDC	0.224	0.231	0.091	2.462	0.014

Source: Data processing results, 2025

These results provide strong empirical support for the CSR-Integrated Cybersecurity Awareness Framework (CICA). CSR has both direct and indirect impacts on sustainable digital culture, with cybersecurity awareness as a key mediating construct. Furthermore, the adoption of AI and blockchain technologies strengthens cybersecurity awareness, in line with their theoretical role as moderators in the conceptual framework.

▲

D. Mediation Analysis

1) Indirect effects: Table VII reports the results of the indirect effect analysis to probe the mediating role of Cybersecurity Awareness (CSA) in the relationship between CSR, AI, blockchain adoption, and Sustainable Digital Culture (SDC). Based on the analysis results, it was revealed that AI → CSA through CSA: AI has a significant indirect effect on CSA through CSA (β = 0.071, t = 2.742, p = 0.006). This indicates that AI contributes to sustainable digital culture, primarily by strengthening cybersecurity awareness. Additionally, Blockchain Adoption (AP) → CSA through CSA: AP also has a significant indirect effect on CSA through CSA (β = 0.089, t = 2.454, p = 0.014), indicating that blockchain adoption promotes digital sustainability when combined with increased cybersecurity awareness. Finally, CSR → SDC through CA: CSR has strong and significant indirect effects on SDC mediated by CA (β = 0.283, t = 4.289, p < 0.001). This underlines the essential role of cybersecurity awareness as an intervention mechanism through which CSR initiatives improve sustainable digital culture.

TABLE VII. INDIRECT EFFECTS

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
AI -> CA					
AI -> SDC	0.071	0.075	0.026	2.742	0.006
BA -> CA					
BA -> SDC	0.089	0.090	0.036	2.454	0.014
CA -> SDC					
CSR -> CA					
CSR -> SDC	0.283	0.284	0.066	4.289	0.000

Source: Data processing results, 2025

These results simultaneously support H4, establishing CA as a key mediator that directs the influence of CSR, AI, and blockchain adoption into the development of a sustainable digital culture. These findings strengthened the theoretical proposition of the CSR Integrated Cybersecurity Awareness Framework (CICA), in which cybersecurity awareness serves as a foundation that connects organizational responsibility and technology adoption with long-term digital sustainability.

2) Specific indirect effects: Table VIII presents specific indirect effects confirming that KSI significantly mediates the relationship between CSR, AI, blockchain adoption, and sustainable digital culture (SDC). AI → KSI → SDC: The indirect effect is significant (β = 0.071, t = 2.742, p = 0.006), indicating that AI adoption enhances sustainable digital culture primarily through its positive influence on cybersecurity awareness. BA → KSI → SDC: The indirect path is also significant (β = 0.089, t = 2.454, p = 0.014), indicating that blockchain adoption enhances digital sustainability when it increases cybersecurity awareness. CSR → CA → SDC: The strongest mediation effect occurs in the CSR path (β = 0.283, t = 4.289, p < 0.001), indicating that CSR initiatives significantly strengthen sustainable digital culture by first increasing cybersecurity awareness.

These results provide strong support for H4, which confirms CA as a central mediating mechanism. This means that CSR and emerging technologies do not directly transform digital culture separately; their effects are significantly strengthened when both first increase cybersecurity awareness within the organization.

TABLE VIII. SPECIFIC INDIRECT EFFECTS

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDE|)	P Values
AI -> CA -> SDC	0.071	0.075	0.026	2.742	0.006
BA -> CA -> SDC	0.089	0.090	0.036	2.454	0.014
CSR -> CA -> SDC	0.283	0.284	0.066	4.289	0.000

Source: Data processing results, 2025

TABLE IX. TOTAL EFFECTS

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
AI -> CA	0.177	0.185	0.046	3.850	0.000
AI -> SDC	0.071	0.075	0.026	2.742	0.006
BA -> CA	0.220	0.217	0.063	3.515	0.000
BA -> SDC	0.089	0.090	0.036	2.454	0.014
CA -> SDC	0.404	0.408	0.093	4.338	0.000
CSR -> CA	0.699	0.697	0.040	17.363	0.000
CSR -> SDC	0.507	0.515	0.044	11.527	0.000

Source: Data processing results, 2025

Table IX provides a comprehensive understanding of the direct and indirect relationships between variables. CSR → SDC: CSR shows the strongest total effect on SDC (β = 0.507, t = 11.527, p < 0.001), which illustrates that CSR initiatives play an important role in shaping a sustainable digital culture. This total effect combines the direct path (CSR → SDC) and the indirect path mediated by CA (CSR → CA → SDC). CA → SDC: Cybersecurity awareness significantly influences sustainable digital culture (β = 0.404, t = 4.338, p < 0.001), reaffirming its important role in achieving digital sustainability outcomes. AI and BA → SDC: Both AI (β = 0.071, p = 0.006) and blockchain adoption (β = 0.089, p = 0.014) have a significant total effect on SDC, although their main influence occurs indirectly through CA.

These findings confirm the central role of CSR as a key driver of cybersecurity awareness and digital sustainability. Furthermore, the integration of new technologies—AI and

blockchain—further strengthens this relationship by enhancing cybersecurity readiness, which in turn fosters a resilient and sustainable digital culture.

3) Bootstrapping results: Fig. 3 demonstrates the bootstrapping results for the internal model of the CSR Integrated Cybersecurity Awareness Framework (CICA). Bootstrapping analysis with 5,000 subsamples validates the stability and significance of the path coefficients obtained in the structural model.

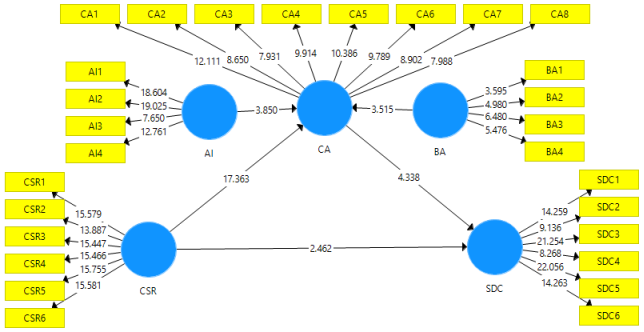

Fig. 3. Inner model (bootstrapping).

Source: Data processing results, 2025

The results show that all hypothesized relationships are statistically significant, as indicated by T-statistic values above the minimum threshold of 1.96: CSR → CA ($t = 17.363$, $p < 0.001$), confirming the strong role of CSR in enhancing cybersecurity awareness. CSR → SDC ($t = 2.462$, $p = 0.014$), indicating that CSR directly supports a sustainable digital culture. CA → SDC ($t = 4.338$, $p < 0.001$), indicating that cybersecurity awareness significantly contributes to digital sustainability. AI → CA ($t = 3.850$, $p < 0.001$) and BA → CA ($t = 3.515$, $p < 0.001$), confirming that new technologies strengthen cybersecurity awareness. In addition, the external loadings also exhibited strong significance, with most indicators indicating t values above 7.0, supporting the reliability of the measurement model. Overall, the bootstrapping results validate all direct hypotheses (H1–H3, H5a, H5b) and reinforce the mediating role of CA in the influence of CSR on sustainable digital culture (H4).

E. Moderating Effect

Fig. 4 describes the moderating effect of Artificial Intelligence (AI) and Blockchain (BA) adoption on the relationship between Corporate Social Responsibility (CSR) and Cybersecurity Awareness (CA). Bootstrapping analysis confirms that Blockchain (BA) adoption significantly moderates the CSR–CA relationship ($t = 2.426$, $p < 0.05$). This indicates that CSR initiatives are more effective in enhancing cybersecurity awareness when accompanied by blockchain adoption, which strengthens digital transparency and trust. On the other hand, the moderating effect of AI adoption is not significant ($t = 0.132$, $p > 0.05$). This indicates that although AI directly strengthens CA (as shown in Fig. 2), its role as a moderator in the CSR–CA path is not supported in this study. Overall, these findings partially support H5a and H5b. Specifically, H5b (Blockchain adoption as a moderator) is supported, while H5a (AI as a moderator) is not supported.

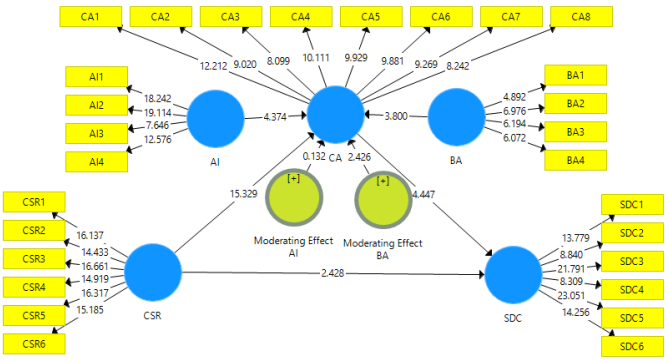

Fig. 4. Moderating effect analysis of AI and BA on the relationship between CSR and CA.

Source: Data processing results, 2025

F. Path Analysis

Table X displays the results of the final path analysis, with the following findings:

TABLE X. PATH ANALYSIS

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
AI -> CA	0.195	0.200	0.045	4.374	0.000
BA -> CA	0.232	0.233	0.061	3.800	0.000
CA -> SDC	0.404	0.410	0.091	4.447	0.000
CSR -> CA	0.681	0.679	0.044	15.329	0.000
CSR -> SDC	0.224	0.229	0.092	2.428	0.016
Moderating Effect AI -> CA	0.006	0.006	0.045	0.132	0.895
Moderating Effect BA -> CA	0.126	0.124	0.052	2.426	0.016

Source: Data processing results, 2025

H1: (CSR → CA): Supported. CSR has a strong and significant effect on cybersecurity awareness ($\beta = 0.681$, $t = 15.329$, $p < 0.001$).

H2: (CSR → SDC): Supported. CSR has a positive effect on sustainable digital culture ($\beta = 0.224$, $t = 2.428$, $p = 0.016$).

H3: (CA → SDC): Supported. Cybersecurity awareness contributes strongly to sustainable digital culture ($\beta = 0.404$, $t = 4.447$, $p < 0.001$).

H5a: (AI → CA): Supported as a direct effect. AI adoption significantly increases CA ($\beta = 0.195$, $t = 4.374$, $p < 0.001$). However, the moderating effect of AI was not significant ($\beta = 0.006$, $t = 0.132$, $p = 0.895$), indicating that AI does not strengthen the CSR–CA relationship.

H5b: (BA → CA): Supported. Blockchain adoption has a direct positive impact on CA ($\beta = 0.232$, $t = 3.800$, $p < 0.001$). Furthermore, the moderating effect was significant ($\beta = 0.126$, $t = 2.426$, $p = 0.016$), confirming that blockchain adoption strengthens the influence of CSR on cybersecurity awareness.

Overall, these results suggest that CSR plays a central role in shaping cybersecurity awareness and a sustainable digital culture, with CA acting as a key mediator (H4). AI and blockchain adoption directly strengthen cybersecurity awareness, but only blockchain shows a significant moderating effect on the CSR–CA pathway.

V. Discussion

This study aims to design and test the CSR-Integrated Cybersecurity Awareness Framework (CICA), which links corporate social responsibility (CSR) initiatives, cybersecurity awareness, a sustainable digital culture, and the moderating role of artificial intelligence (AI) and blockchain adoption. The findings provide strong empirical support for theoretical propositions and contribute to the growing discussion on CSR and digital sustainability.

The results of this study indicate that CSR has a significant influence on cybersecurity awareness (H1) and also has a direct effect on sustainable digital culture (H2). This finding aligns with previous research, which revealed that CSR initiatives not only focus on external legitimacy but also strengthen internal organizational resilience [30].

By integrating cybersecurity-related programs into their corporate social responsibility (CSR) initiatives, organizations help employees understand digital threats, ethical data management, and safe internet browsing. The dual function of CSR—both for the external community and within the organization—demonstrates that CSR continues to adapt to meet the challenges of digital change.

Raising cybersecurity awareness significantly contributes to the formation of a sustainable digital culture, and further analysis indicates that this awareness serves as a key mediator in the relationship between CSR and a sustainable digital culture. This suggests that CSR initiatives indirectly support digital sustainability by increasing employee understanding of cybersecurity threats and practices. These results align with organizational culture theory, which emphasizes the importance of awareness and shared values as determinants of long-term resilience [65]. The mediating role of CA emphasizes the importance for organizations to incorporate cybersecurity education into CSR programs to ensure innovative and secure digital transformation.

The adoption of emerging technologies has a significant impact on improving the understanding of cybersecurity. Both artificial intelligence (direct effect H5a) and blockchain (direct effect H5b) substantially improve CA. Artificial intelligence assists through predictive analytics and intelligent monitoring [49], while blockchain adds transparency, integrity, and trust to online transactions [56].

The findings of this study, based on moderation analysis, show mixed results. Blockchain used significantly strengthens the relationship between CSR and CA, confirming H5b, while AI used does not show a significant moderating effect (H5a). This suggests that blockchain provides structural support to CSR programs by building trust and accountability in digital practices, while AI's role is more focused on technical and operational aspects. This finding reiterates the argument that blockchain implementation is often linked to governance and compliance frameworks, making it more directly relevant to CSR initiatives, while the impact of AI depends on its maturity and alignment with organizational strategy.

VI. Conclusion

This study develops and empirically validates the CSR-Integrated Cybersecurity Awareness (CICA) Framework, highlighting how CSR initiatives, supported by AI and blockchain adoption, contribute to increased cybersecurity awareness and a sustainable digital culture.

CSR as a key enabler – CSR significantly increases cybersecurity awareness and directly drives a sustainable digital culture, underscoring its dual role in external legitimacy and internal resilience. Cybersecurity awareness as a mediator – CSR mediates the relationship between CSR and SDC, affirming its central position in translating CSR initiatives into sustainable digital practices. Emerging technologies as enablers – Both AI and blockchain adoption directly strengthen cybersecurity awareness, with blockchain further moderating the CSR–CICA relationship. However, AI does not exhibit a significant moderating effect, indicating differences in the maturity and integration of these technologies. Overall, these results validate the CICA framework as a novel theoretical contribution, extending the CSR discourse into digital transformation and resilience.

A. Implications

Theoretically, the study advances the CSR literature by linking it to digital resilience and sustainability. It extends CSR discourse beyond environmental and social domains into the realm of cybersecurity and digital ethics, areas that are increasingly critical in the Fourth Industrial Revolution. The CICA framework offers a novel lens to understand how CSR can be operationalized in digital contexts.

Practically, the findings suggest that organizations—particularly universities and enterprises in emerging markets—should:

- Integrate cybersecurity education and training into CSR programs.
- Leverage blockchain technologies as strategic tools to enhance trust and amplify the effectiveness of CSR initiatives.
- Consider AI adoption as a direct enabler of awareness but ensure strategic alignment for it to play a stronger organizational role.

B. Future Research

The CICA Framework demonstrates that integrating CSR, cybersecurity awareness, and emerging technologies can strengthen digital resilience. Future studies should examine this model across different industries and regions to enhance generalizability. Additional moderating factors—such as organizational culture or leadership style—may also offer deeper insights into the CSR–cybersecurity relationship. Longitudinal approaches are recommended to capture changes in CSR, cybersecurity behavior, and technology adoption over time.

This study has several limitations. Its cross-sectional design restricts causal interpretation, and reliance on self-reported data may introduce bias. The sample is limited to organizations in Central Java, which may affect broader applicability. Furthermore, the model focuses on AI and blockchain, while other emerging technologies, such as IoT-based security or edge computing, were not examined. Future research should consider wider samples, mixed-method approaches, multi-level analyses, and additional technological or organizational factors to further refine and extend the CICA Framework.

REFERENCES

[1] S. Kraus, P. Jones, N. Kailer, A. Weinmann, N. Chaparro-Banegas, and N. Roig-Tierno, "Digital Transformation: An Overview of the Current State of the Art of Research," Sage Open, vol. 11, no. 3, Jul. 2021, doi: 10.1177/21582440211047576.

[2] A. A. Vărzaru and C. G. Bocean, "Digital Transformation and Innovation: The Influence of Digital Technologies on Turnover from Innovation Activities and Types of Innovation," Systems, vol. 12, no. 9, p. 359, Sep. 2024, doi: 10.3390/systems12090359.

[3] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations," Sensors, vol. 23, no. 15, p. 6666, Jul. 2023, doi: 10.3390/s23156666.

[4] World Economic Forum, "Global Cybersecurity Outlook 2025 – Navigating Through Rising Cyber Complexities," World Economic Forum. Accessed: Jul. 25, 2025. [Online]. Available: https://www.weforum.org/press/2025/01/global-cybersecurity-outlook-2025-navigating-through-rising-cyber-complexities/

[5] C. Catal, G. Kar, and M. Zarali, "Strategic technological innovation investment: enhancing resilience in the age of digital transformation," J. Innov. Digit. Transform., vol. 2, no. 1, pp. 50–72, Mar. 2025, doi: 10.1108/JIDT-05-2024-0010.

[6] Microsoft and Frost & Sullivan, "Cybersecurity threats to cost organizations in Asia Pacific US$1.75 trillion in economic losses," Microsoft Asia News Center. Accessed: Jul. 25, 2025. [Online]. Available: https://news.microsoft.com/apac/2018/05/18/cybersecurity-threats-to-cost-organizations-in-asia-pacific-us1-75-trillion-in-economic-losses/?utm_source=chatgpt.com

[7] C. Knowles, "Cyber threats surge in SEA: Kaspersky detects 13 million attacks," IT Brief Asia. Accessed: Sep. 25, 2025. [Online]. Available: https://itbrief.asia/story/cyber-threats-surge-in-sea-kaspersky-detects-13-million-attacks

[8] C. Na, X. Chen, X. Li, Y. Li, and X. Wang, "Digital Transformation of Value Chains and CSR Performance," Sustainability, vol. 14, no. 16, p. 10245, Aug. 2022, doi: 10.3390/su141610245.

[9] G. Pfajfar, A. Shoham, A. Małecka, and M. Zalaznik, "Value of corporate social responsibility for multiple stakeholders and social impact – Relationship marketing perspective," J. Bus. Res., vol. 143, pp. 46–61, Apr. 2022, doi: 10.1016/j.jbusres.2022.01.051.

[10] T. Fatima and S. Elbanna, "Corporate Social Responsibility (CSR) Implementation: A Review and a Research Agenda Towards an Integrative Framework," J. Bus. Ethics, vol. 183, no. 1, pp. 105–121, Feb. 2023, doi: 10.1007/s10551-022-05047-8.

[11] Y. Zhao, M. Abbas, M. Samma, T. Ozkut, M. Munir, and S. F. Rasool, "Exploring the Relationship Between Corporate Social Responsibility, Trust, Corporate Reputation, and Brand Equity," Front. Psychol., vol. 12, Nov. 2021, doi: 10.3389/fpsyg.2021.766422.

[12] J. del Brío and E. L. Bolaños, "Effects of CSR and CR on Business Confidence in an Emerging Country," Sustainability, vol. 12, no. 12, p. 5221, Jun. 2020, doi: 10.3390/su12125221.

[13] T. K. Vuong and H. M. Bui, "The role of corporate social responsibility activities in employees' perception of brand reputation and brand equity," Case Stud. Chem. Environ. Eng., vol. 7, p. 100313, Jun. 2023, doi: 10.1016/j.cscee.2023.100313.

[14] Ms. S. Shireesha, Dr. T. Varalaxmi, and C. Architha, "Corporate Social Responsibility: Integrating Sustainable Practices into Business Operations," Int. Res. J. Adv. Eng. Manag., vol. 2, no. 05, pp. 1717–1722, May 2024, doi: 10.47392/IRJAEM.2024.0250.

[15] J. Etikan, "Corporate Social Responsibility (CSR) and its Influence on Organizational Reputation," J. Public Relations, vol. 2, no. 1, pp. 1–12, Feb. 2024, doi: 10.47941/jpr.1694.

[16] D. Amani, "Internal corporate social responsibility and university brand legitimacy: an employee perspective in the higher education sector in Tanzania," Soc. Responsib. J., vol. 19, no. 4, pp. 611–625, Mar. 2023, doi: 10.1108/SRJ-12-2021-0540.

[17] M. Bedoya et al., "The impacts of corporate social responsibility on internal organizational processes to create shared value," Cogent Bus. Manag., vol. 12, no. 1, Dec. 2025, doi: 10.1080/23311975.2024.2418420.

[18] L. Wolf et al., "The role of internal CSR in guiding the digitalisation of work," Int. J. Corp. Soc. Responsib., vol. 9, no. 1, p. 6, Dec. 2024, doi: 10.1186/s40991-024-00089-9.

[19] K. V. Carl, "Data Privacy and Security in the Context of Corporate Digital Responsibility:A Scoping Review," in Conference: INFORMATIK 2023:Designing Futures: Zukünfte gestalten, Bonn: Gesellschaft für Informatik e.V, 2023.

[20] O. Kuznetsov, P. Sernani, L. Romeo, E. Frontoni, and A. Mancini, "On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security," IEEE Access, vol. 12, pp. 3881–3897, 2024, doi: 10.1109/ACCESS.2023.3349019.

[21] Z. Li and Z. Xu, "Digital technology and innovation:The impact of blockchain application on enterprise innovation," Technovation, vol. 139, p. 103136, Jan. 2025, doi: 10.1016/j.technovation.2024.103136.

[22] J. J. Xu, "Are blockchains immune to all malicious attacks?," Financ. Innov., vol. 2, no. 1, p. 25, Dec. 2016, doi: 10.1186/s40854-016-0046-5.

[23] M. Yao and M. Xu, "Exploring the Roles of Corporate Social Responsibility and Artificial Intelligence Adoption in the Impact of Political Connections on Innovation Performance," Sustainability, vol. 17, no. 17, p. 7883, Sep. 2025, doi: 10.3390/su17177883.

[24] H. M. Aslaksen, C. Hildebrandt, and H. C. G. Johnsen, "The long-term transformation of the concept of CSR: towards a more comprehensive emphasis on sustainability," Int. J. Corp. Soc. Responsib., vol. 6, no. 1, p. 11, Dec. 2021, doi: 10.1186/s40991-021-00063-9.

[25] M. Muslim and M. F. A. Pelu, "Corporate Social Responsibility: Best Practices and Industry Comparisons," J. Bus. Manag. Res., vol. 6, no. 1, pp. 27–42, Jan. 2023, doi: 10.55098/tjbmr.v6i1.578.

[26] Jinyoung Hwang, "Corporate Social Responsibility (CSR) in the Digital Age: Investigating the challenges and future insights," GSC Adv. Res. Rev., vol. 21, no. 1, pp. 503–518, Oct. 2024, doi: 10.30574/gscarr.2024.21.1.0383.

[27] B.-J. Kim and J. Lee, "The impact of corporate social responsibility on cybersecurity behavior: The crucial role of organizationally-prescribed perfectionism," Humanit. Soc. Sci. Commun., vol. 12, no. 1, p. 172, Feb. 2025, doi: 10.1057/s41599-025-04511-w.

[28] Temitayo Oluwaseun Abrahams, Oluwatoyin Ajoke Farayola, Simon Kaggwa, Prisca Ugomma Uwaoma, Azeez Olanipekun Hassan, and Samuel Onimisi Dawodu, "CYBERSECURITY AWARENESS AND EDUCATION PROGRAMS: A REVIEW OF EMPLOYEE ENGAGEMENT AND ACCOUNTABILITY," Comput. Sci. IT Res. J., vol. 5, no. 1, pp. 100–119, Jan. 2024, doi: 10.51594/csitrj.v5i1.708.

[29] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," Comput. Secur., vol. 98, p. 102003, Nov. 2020, doi: 10.1016/j.cose.2020.102003.

[30] L. Lobschat et al., "Corporate digital responsibility," J. Bus. Res., vol. 122, pp. 875–888, Jan. 2021, doi: 10.1016/j.jbusres.2019.10.006.

[31] C. Cheng and M. Zhang, "Conceptualizing Corporate Digital Responsibility: A Digital Technology Development Perspective," Sustainability, vol. 15, no. 3, p. 2319, Jan. 2023, doi: 10.3390/su15032319.

[32] S. S. Hishan, S. Ramakrishnan, L. B. Keong, and A. Umar, "The Concept of Corporate Social Responsibility (CSR)—A Review of Literature," Adv. Sci. Lett., vol. 23, no. 9, pp. 9287–9290, Sep. 2017, doi: 10.1166/asl.2017.10072.

[33] J. Famularo, "Corporate social responsibility communication in the ICT sector: digital issues, greenwashing, and materiality," Int. J. Corp. Soc.

Responsib., vol. 8, no. 1, p. 8, Dec. 2023, doi: 10.1186/s40991-023-00082-8.

[34] I. O. Pappas, P. Mikalef, Y. K. Dwivedi, L. Jaccheri, and J. Krogstie, "Responsible Digital Transformation for a Sustainable Society," Inf. Syst. Front., vol. 25, no. 3, pp. 945–953, Jun. 2023, doi: 10.1007/s10796-023-10406-5.

[35] A. L. Leal-Rodríguez, C. Sanchís-Pedregosa, A. M. Moreno-Moreno, and A. G. Leal-Millán, "Digitalization beyond technology: Proposing an explanatory and predictive model for digital culture in organizations," J. Innov. Knowl., vol. 8, no. 3, p. 100409, Jul. 2023, doi: 10.1016/j.jik.2023.100409.

[36] A. Bharadwaj, O. A. El Sawy, P. A. Pavlou, and N. Venkatraman, "Digital Business Strategy: Toward a Next Generation of Insights," MIS Q., vol. 37, no. 2, pp. 471–482, Jun. 2013, doi: 10.25300/MISQ/2013/37:2.3.

[37] World Economic Forum, "Global Cybersecurity Outlook 2022 INSIGHT REPORT," Jan. 2022.

[38] N. Abidi, S. Sakha, and M. El Herradi, "Digitalization and Resilience: Firm-level Evidence During the COVID-19 Pandemic," IMF Work. Pap., vol. 2022, no. 034, p. 1, Feb. 2022, doi: 10.5089/9798400201073.001.

[39] A. Khalil, H. el W. Bousselmi, M. El Amine Abdelli, I. Baccouche, L. Caridad y López del Río, and H. E. Nasr, "The Impact of Digital Technologies on SMEs' Resilience During the COVID-19 Pandemic," 2022, pp. 111–126. doi: 10.1108/S1877-636120220000029008.

[40] E. Kadena and M. Gupi, "Human Factors in Cybersecurity," Secur. Sci. J., vol. 2, no. 2, pp. 51–64, Dec. 2021, doi: 10.37458/ssj.2.2.3.

[41] W. J. Triplett, "Addressing Human Factors in Cybersecurity Leadership," J. Cybersecurity Priv., vol. 2, no. 3, pp. 573–586, Jul. 2022, doi: 10.3390/jcp2030029.

[42] S. Akter, M. R. Uddin, S. Sajib, W. J. T. Lee, K. Michael, and M. A. Hossain, "Reconceptualizing cybersecurity awareness capability in the data-driven digital economy," Ann. Oper. Res., vol. 350, no. 2, pp. 673–698, Jul. 2025, doi: 10.1007/s10479-022-04844-8.

[43] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," J. Comput. Inf. Syst., vol. 62, no. 1, pp. 82–97, Jan. 2022, doi: 10.1080/08874417.2020.1712269.

[44] K. Renaud and J. Ophoff, "A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs," Organ. Cybersecurity J. Pract. Process People, vol. 1, no. 1, pp. 24–46, Oct. 2021, doi: 10.1108/OCJ-03-2021-0004.

[45] S. Chaudhary, V. Gkioulos, and S. Katsikas, "A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises," Comput. Sci. Rev., vol. 50, p. 100592, Nov. 2023, doi: 10.1016/j.cosrev.2023.100592.

[46] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, "Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review," Comput. Ind., vol. 137, p. 103614, May 2022, doi: 10.1016/j.compind.2022.103614.

[47] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," Comput. Secur., vol. 42, pp. 165–176, May 2014, doi: 10.1016/j.cose.2013.12.003.

[48] R. Torten, C. Reaiche, and S. Boyle, "The impact of security Awareness on information technology professionals' behavior," Comput. Secur., vol. 79, pp. 68–79, Nov. 2018, doi: 10.1016/j.cose.2018.08.007.

[49] Y. K. Dwivedi et al., "Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy," Int. J. Inf. Manage., vol. 57, p. 101994, Apr. 2021, doi: 10.1016/j.ijinfomgt.2019.08.002.

[50] E. Sánchez, R. Calderón, and F. Herrera, "Artificial Intelligence Adoption in SMEs: Survey Based on TOE–DOI Framework, Primary Methodology and Challenges," Appl. Sci., vol. 15, no. 12, p. 6465, Jun. 2025, doi: 10.3390/app15126465.

[51] M. M. Rana, M. S. Siddiqee, M. N. Sakib, and M. R. Ahamed, "Assessing AI adoption in developing country academia: A trust and privacy-augmented UTAUT framework," Heliyon, vol. 10, no. 18, p. e37569, Sep. 2024, doi: 10.1016/j.heliyon.2024.e37569.

[52] Onuh Matthew Ijiga, Idoko Peter Idoko, Godslove Isenyo Ebiega, Frederick Itunu Olajide, Timilehin Isaiah Olatunde, and Chukwunonso Ukaegbu, "Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention," Open Access Res. J. Sci. Technol., vol. 11, no. 1, pp. 001–004, May 2024, doi: 10.53022/oarjst.2024.11.1.0060.

[53] N. Mohamed, "Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms," Knowl. Inf. Syst., vol. 67, no. 8, pp. 6969–7055, Aug. 2025, doi: 10.1007/s10115-025-02429-y.

[54] M. M. Queiroz and S. Fosso Wamba, "Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA," Int. J. Inf. Manage., vol. 46, pp. 70–82, Jun. 2019, doi: 10.1016/j.ijinfomgt.2018.11.021.

[55] D. Tapscott and A. Tapscott, lockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World. New York: Penguin, 2016.

[56] M. Crosby, Nachiappan, P. Pattanayak, S. Verma, and V. Kalyanaraman, "BlockChain Technology: Beyond Bitcoin ," Appl. Innov. Rev. , no. 8, Jun. 2018.

[57] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," Telemat. Informatics, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.

[58] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," Int. J. Prod. Res., vol. 57, no. 7, pp. 2117–2135, Apr. 2019, doi: 10.1080/00207543.2018.1533261.

[59] A. B. Carroll and K. M. Shabana, "The Business Case for Corporate Social Responsibility: A Review of Concepts, Research and Practice," Int. J. Manag. Rev., vol. 12, no. 1, pp. 85–105, Mar. 2010, doi: 10.1111/j.1468-2370.2009.00275.x.

[60] T. M. Wut, D. Lee, W. M. Ip, and S. W. Lee, "Digital Sustainability in the Organization: Scale Development and Validation," Sustainability, vol. 13, no. 6, p. 3530, Mar. 2021, doi: 10.3390/su13063530.

[61] J. C. Nunnally and I. H. Bernstein, Psychometric Theory, 3rd ed. New York: McGraw-Hill., 1994.

[62] J. F. Hair, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, . A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), 3rd ed. Sage Publication: Thousand Oaks, CA, 2012.

[63] L. Hu and P. M. Bentler, "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives," Struct. Equ. Model. A Multidiscip. J., vol. 6, no. 1, pp. 1–55, Jan. 1999, doi: 10.1080/10705519909540118.

[64] W. W. Chin, "he partial least squares approach to structural equation modeling. In G. A. Marcoulides (Ed.)," in Modern methods for business research, Mahwah, NJ: Lawrence Erlbaum Associates Publishers, 1998, pp. 295–336.

[65] M. Pradana, A. Silvianita, S. Syarifuddin, and R. Renaldi, "The Implication of Digital Organisational Culture on Firm Performance," Front. Psychol., vol. 13, May 2022, doi: 10.3389/fpsyg.2022.840699.