

THE INFLUENCE OF DIGITAL LITERACY AND CYBERSECURITY AWARENESS ON EMPLOYEE PERFORMANCE AT PT. SOLUSI BANGUN ANDALAS IN THE DIGITAL ERA, MEDIATED BY ORGANIZATIONAL COMMITMENT

Amrullah^{1*}, Isthafan Najmi², Irwan Safwadi³

Faculty of Economics and Business, University of Abulyatama, Aceh, Indonesia

*Correspondence Email: amrullahbsc@gmail.com

Abstract: In the digital era, organizations must enhance employees' digital literacy and cybersecurity awareness to maintain performance and data security. This study examines the effect of digital literacy and cybersecurity awareness on employee performance, with organizational commitment as a mediating variable. The research was conducted at PT. Solusi Bangun Andalas, involving 117 permanent employees using a quantitative method and Structural Equation Modeling (SEM) with Smart PLS. Results show that both digital literacy and cybersecurity awareness significantly and positively affect employee performance. Moreover, organizational commitment plays a mediating role in strengthening these effects. These findings highlight the strategic importance of developing digital competencies and fostering a cybersecurity-aware culture to enhance employee performance and commitment. The study recommends that organizations invest in continuous digital skills development and structured cybersecurity training to support effective human resource management and digital transformation.

Keywords: Digital Literacy, Cybersecurity Awareness, Employee Performance, Organizational Commitment, Digital Transformation

1. Introduction

The ongoing digital revolution has fundamentally reshaped the global business landscape, compelling organizations to adapt to new paradigms of operation and competition. In this context, digital literacy and cybersecurity awareness have emerged as two indispensable pillars for organizational resilience and success. Digital literacy transcends basic technical skills, encompassing the ability to effectively find, evaluate, and utilize information using digital tools, which directly enhances employee productivity and performance (Ng, 2012; Van Laar et al., 2020). Simultaneously, the increasing sophistication and frequency of cyber threats have made cybersecurity awareness defined as the understanding of cyber risks and the adoption of secure behaviors a critical concern for safeguarding sensitive data and ensuring operational continuity (Torten, Reaiche, & Boyle, 2025). The World Economic Forum (2024) underscores this urgency, highlighting that organizations neglecting to invest in their workforce's digital capabilities can face a productivity loss of up to 30% and become significantly more vulnerable to devastating cyber incidents.

This global trend is acutely relevant within the Indonesian industrial sector. Companies are under pressure to digitally transform to remain competitive. PT. Solusi Bangun Andalas, as a forward-thinking manufacturing firm, has proactively launched several digital initiatives and training programs. However, a preliminary internal survey conducted among 50 employees revealed potential gaps in human resource readiness. The data indicated that only 62% of employees felt confident in using new digital applications, and participation in mandatory cybersecurity training stood at 68%. These figures suggest that while technological infrastructure may be advancing, the human element the proficiency and security consciousness of employees requires further development. This gap presents a compelling

research opportunity to investigate the interplay between digital competencies, security awareness, and crucial organizational outcomes like commitment.

Organizational commitment, characterized by an employee's emotional attachment, loyalty, and willingness to exert effort for the organization, is a well-established determinant of long-term stability and performance (Meyer & Allen, 1991). Contemporary research suggests that in the digital age, this commitment is increasingly influenced by factors such as an employee's ability to navigate technological demands and their perception of a secure work environment (Davis & Hulsheger, 2020). High digital literacy enables employees to work more efficiently and adapt to changes, thereby boosting their performance and self-efficacy (Cech & Rothwell, 2020). Similarly, a strong culture of cybersecurity awareness not only protects the organization but also fosters a climate of trust and safety, making employees feel more secure and, consequently, more committed to the organization (Ifinedo, 2014).

Within this framework, employee performance is theorized to play a pivotal mediating role. Performance, which reflects an individual's effectiveness in fulfilling their job duties, is positively influenced by both digital fluency and vigilant security practices (Sonnentag & Frese, 2002). When employees perform well, they are more likely to receive recognition and feel a greater sense of accomplishment, which in turn strengthens their emotional bond and commitment to the organization (Davis & Hulsheger, 2020). Thus, performance acts as a crucial mechanism through which digital and security competencies ultimately enhance organizational commitment.

Therefore, this study is designed to empirically examine the influence of digital literacy and cybersecurity awareness on organizational commitment, with employee performance as a mediating variable, within the specific context of PT. Solusi Bangun Andalas. By elucidating these relationships, this research aims to contribute valuable insights into the human capital dimensions of digital transformation. The findings are expected to provide a strategic evidence base for the company to refine its HR development strategies, thereby strengthening its competitive edge in the modern digital economy.

2. Literature Review

2.1 Digital Literacy

Digital literacy refers to an individual's ability to effectively access, evaluate, and utilize information and communication technologies (ICT) for personal and professional purposes (Ng, 2012). In the modern workplace, it transcends basic technical skills to include a deeper understanding of how technology functions and its impact, enabling employees to enhance performance, adapt to new technologies, and make data-driven decisions (Abbas, 2019; Van Laar et al., 2020). Marsh (2021) further elaborates that digital literacy comprises technical, cognitive, and social dimensions, facilitating productive interaction and collaboration through digital platforms.

The adoption of digital tools by employees can be understood through models like the Technology Acceptance Model (TAM), which posits that perceived usefulness and ease of use are key determinants of technology adoption (Davis, 1989). From an organizational perspective, the Technology-Organization-Environment (TOE) framework suggests that technology adoption is influenced by the technology itself, organizational resources, and external environmental factors (Tornatzky & Fleischer, 1990). High levels of digital literacy allow employees to navigate complex information landscapes, work more efficiently, and adapt to rapid technological changes, directly impacting their productivity and effectiveness (Santosa, 2019).

These are the key indicators for measuring digital literacy include (Radovanović, 2020). Digital literacy is a multi-faceted competency, measured through several key indicators. First, Technical Ability refers to the fundamental proficiency in operating hardware and software. Second, Information Evaluation and Management involves the critical skill to find, assess, and organize digital information effectively. Third, Digital Communication and Collaboration denotes the capacity for effective interaction and teamwork using digital platforms. Fourth, Digital Security and Privacy encompasses the understanding and practices required to protect personal and organizational data. Fifth, Digital Problem-Solving is the ability to use technology innovatively to address challenges. Sixth, an Understanding of Digital Ethics and Social Impact includes awareness of copyright, responsible online behavior, and technology's broader societal effects. Finally, Adaptability to New Technology highlights the readiness and ability to learn and integrate emerging technological tools.

2.2 Cybersecurity Awareness

Cybersecurity awareness denotes an individual's understanding and attentiveness to the risks and responsibilities associated with using digital technology. It involves knowledge of safe online practices, such as using strong passwords and recognizing threats like phishing, to protect sensitive information (Arias, 2021; Muthuswamy, 2023). In an organizational context, it is crucial for mitigating risks of data breaches and cyber-attacks, which can cause significant operational and reputational damage (Al-Shaikh, 2020). A high level of cybersecurity awareness among employees fosters a secure work environment, builds trust, and minimizes errors that could jeopardize the organization (Bulgurcu, 2010).

These are primary indicators of cybersecurity awareness encompass (Halik, 2023). Cybersecurity awareness is defined by a set of critical behavioral and cognitive indicators. First, Digital Privacy Awareness is the understanding of the importance of protecting personal data and managing privacy settings. Second, Digital Security Awareness focuses on knowledge of digital threats and the implementation of preventive measures. Third, Digital Ethics Awareness pertains to adhering to ethical norms online, such as respecting intellectual property. Fourth, Social Impact Awareness involves an understanding of the broader effects of technology on society and interpersonal relationships. Fifth, Digital Divide Awareness reflects the recognition of inequalities in technology access. Sixth, Digital Time Management Awareness is the ability to regulate one's time spent on digital devices. Seventh, and lastly, the Positive Use of Technology indicates the application of digital tools for productive and beneficial purposes.

2.3 Organizational Commitment

Organizational commitment is defined as the psychological attachment an employee has to their organization, reflecting their loyalty and willingness to contribute to its goals. Bahri (2021) explained these indicators for organizational commitment. Organizational commitment is gauged through indicators that reflect the nature of an employee's bond with the organization. First, Affective Commitment represents the emotional attachment and identification with the organization. Second, Continuance Commitment is based on the perceived costs associated with leaving the organization. Third, Normative Commitment reflects a feeling of moral obligation to remain. Fourth, Job Involvement measures the degree of psychological immersion in one's work. Fifth, Participation in

Organizational Decisions assesses the level of involvement in the company's decision-making processes. Sixth, Job Satisfaction serves as a foundational indicator that influences and reflects the overall strength of commitment.

2.4 Employee Performance

Employee performance refers to the effectiveness and efficiency with which an individual fulfills their job responsibilities, measured by quality, quantity, and timeliness (Kuswati, 2020). It is influenced by a combination of factors, including individual ability and skills, motivation, job satisfaction, the work environment, and leadership support (Basheer, 2017). Performance can be assessed through self-assessment, supervisor ratings, 360-degree feedback, and achievement of Key Performance Indicators (KPIs) such as safety indices (OH&S), digital transformation progress, and innovation rates (Mulyani, 2020).

2.5 Relationships Between Variables and Hypothesis Development

The literature establishes clear connections between the core variables of this study. Research indicates that digital literacy has a positive influence on employee performance by enabling efficiency, faster adaptation, and higher-quality work (Ng, 2012; Van Laar et al., 2020; Cech & Rothwell, 2020). Similarly, cybersecurity awareness positively affects performance by reducing operational disruptions caused by security incidents and promoting safer work practices (Sullivan et al., 2021).

Furthermore, these competencies also impact organizational commitment. Digital literacy can strengthen commitment by increasing employees' self-efficacy and job satisfaction, making them feel more empowered and aligned with an innovative organization (Ng, 2012; Tondolo, 2021). Cybersecurity awareness fosters commitment by building trust; when employees feel the organization protects them, their emotional attachment and loyalty increase (Ifinedo, 2014; Hassan, 2020).

A strong reciprocal relationship exists between employee performance and organizational commitment. High performance leads to satisfaction and a sense of value, which strengthens commitment. Conversely, committed employees are more motivated to perform well (Meyer et al., 2004). This suggests that organizational commitment may act as a mechanism through which digital literacy and cybersecurity awareness ultimately enhance performance.

Based on this literature review, the following hypotheses are proposed:

1. H1: Cybersecurity Awareness has a positive and significant effect on Employee Performance.
2. H2: Cybersecurity Awareness has a positive and significant effect on Organizational Commitment.
3. H3: Digital Literacy has a positive and significant effect on Employee Performance.
4. H4: Digital Literacy has a positive and significant effect on Organizational Commitment.
5. H5: Organizational Commitment has a positive and significant effect on Employee Performance.
6. H6: Cybersecurity Awareness affects Employee Performance through Organizational Commitment as a mediator.
7. H7: Digital Literacy affects Employee Performance through Organizational Commitment as a mediator.

3. Method

This study was conducted at PT. Solusi Bangun Andalas. The research focuses on the relationship between employee performance, digital literacy, and cybersecurity awareness, with organizational commitment positioned as an intervening variable. The population for this study consisted of all 117 permanent employees of PT. Solusi Bangun Andalas in 2024. Non-permanent (outsourced) employees were excluded as they are contracted through external vendors. A census method was employed, meaning the entire population was taken as the sample. Primary data was collected using a questionnaire distributed to employees. The instrument contained statements related to the four variables: employee performance, organizational commitment, digital literacy, and cybersecurity awareness. Responses were measured using a 5-point Likert scale, ranging from 1 (Strongly Disagree) to 5 (Strongly Agree).

The variables were operationalized as follows: First is Exogenous Variables which are Digital Literacy (Abbas, 2019) and Cybersecurity Awareness (Muthuswamy, 2023). And second is Intervening Variable which is Organizational Commitment (Ridwan, 2020). And third is Endogenous Variable which is Employee Performance (Kuswati, 2020). Each variable was measured using multiple indicators on a 1-5 interval scale. Data analysis was performed using descriptive statistics and Structural Equation Modeling (SEM) with the SmartPLS software. Descriptive statistics were used to summarize the respondents' perceptions. The SEM analysis followed a two-step approach: evaluating the measurement model (outer model) and the structural model (inner model).

The measurement model was assessed for validity and reliability. Convergent Validity was confirmed by examining factor loadings (>0.70) and Average Variance Extracted (AVE >0.50). Discriminant Validity was established by ensuring indicators loaded higher on their respective constructs than on others. Reliability was assessed using Composite Reliability scores (>0.70). The structural model was evaluated to test the hypothesized relationships. First, R-Square (R^2) values were examined to assess the model's predictive power for the endogenous variables. Second, Path Coefficients and their significance levels ($p\text{-value} < 0.05$) were analyzed to determine the strength and significance of the relationships between variables. The seven hypotheses (H1-H7) proposing direct and indirect effects were tested by examining the p-values of the path coefficients in the PLS-SEM output. A p-value of less than 0.05 indicates a statistically significant relationship, leading to the acceptance of the alternative hypothesis.

4. Finding and Discussion

4.1 Descriptive Statistics

Descriptive analysis was conducted to summarize the respondents' perceptions of the four main variables: Digital Literacy (DL), Cybersecurity Awareness (CS), Organizational Commitment (OC), and Employee Performance (EP). The results, measured on a 5-point Likert scale, are categorized as follows: 1.00-1.90 (Low), 2.00-2.90 (Moderate), 3.00-3.90 (High), 4.00-5.00 (Very High). All variables scored within the "Very High" category. Digital Literacy (mean scores: 4.3 - 4.8) and Cybersecurity Awareness (mean scores: 4.5 - 4.8) indicate that employees are highly proficient and security-conscious. Organizational Commitment (mean scores: 4.1 - 4.6) shows strong employee loyalty, though items related to a sense of obligation ("normative commitment") scored slightly lower. Employee

Performance (mean scores: 4.3 - 4.5) was also perceived as very high, demonstrating employees' confidence in meeting targets and working effectively.

4.2 Measurement Model (Outer Model) Evaluation

The measurement model was assessed for reliability and validity to ensure the indicators accurately measured their constructs.

- a. Convergent Validity: The Average Variance Extracted (AVE) for all constructs exceeded the 0.50 threshold, confirming convergent validity. While some indicator loadings were below the ideal 0.70, they were all above the acceptable level of 0.50 (Haryono, 2016), so all items were retained.

Table 4.1 Outer Model

	CS	DL	EP	OC
CS1	0.649			
CS2	0.656			
CS3	0.679			
CS4	0.637			
CS5	0.703			
DL1		0.506		
DL2		0.655		
DL3		0.622		
DL4		0.674		
DL5		0.726		
DL6		0.558		
DL7		0.608		
EP1			0.682	
EP2			0.751	
EP3			0.719	
EP4			0.705	
EP5			0.606	
OC1				0.712
OC2				0.632
OC3				0.577
OC4				0.65
OC5				0.634

Source: Made by SmartPLS

- b. Discriminant Validity: The square root of the AVE for each construct was greater than its correlations with other constructs, establishing good discriminant validity.

Table 4.2 Discriminant Validity

	CS	DL	EP	OC
CS1	0.649	0.363	0.313	0.321
CS2	0.656	0.379	0.332	0.404
CS3	0.679	0.424	0.43	0.268
CS4	0.637	0.46	0.422	0.276
CS5	0.703	0.377	0.337	0.281
DL1	0.381	0.506	0.305	0.243
DL2	0.414	0.655	0.456	0.329
DL3	0.318	0.622	0.286	0.311
DL4	0.447	0.674	0.334	0.499
DL5	0.362	0.726	0.358	0.37
DL6	0.287	0.558	0.336	0.268
DL7	0.412	0.608	0.353	0.39
EP1	0.338	0.326	0.682	0.214
EP2	0.425	0.395	0.751	0.358
EP3	0.336	0.385	0.719	0.301
EP4	0.446	0.453	0.705	0.393

EP5	0.353	0.357	0.606	0.352
OC1	0.281	0.37	0.295	0.712
OC2	0.331	0.322	0.336	0.632
OC3	0.211	0.355	0.228	0.577
OC4	0.318	0.244	0.185	0.650
OC5	0.34	0.457	0.408	0.634

Source: Made by SmartPLS

- c. Reliability: Composite Reliability scores for all constructs (CS=0.799, DL=0.816, EP=0.822, OC=0.778) exceeded the 0.70 benchmark, confirming the instrument's high internal consistency.

Table 4.3 Nilai Composite Reliability

	Composite reliability (rho_c)
CS	0.799
DL	0.816
EP	0.822
OC	0.778

Source: Made by SmartPLS

4.3 Structural Model (Inner Model) and Hypothesis Testing

The structural model was evaluated to test the hypothesized relationships. The model's predictive power, shown by the R-square values, indicates that the independent variables explain 34.3% of the variance in Organizational Commitment and 40.7% of the variance in Employee Performance.

The hypotheses were tested by examining the path coefficients and their significance levels (p -values < 0.05). The results of the direct and indirect effect tests are summarized below.

Table 4.4 Direct Effects

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values
CS -> EP	0.306	0.307	0.093	3.281	0.001
CS -> OC	0.201	0.207	0.106	1.898	0.029
DL -> EP	0.273	0.281	0.101	2.708	0.003
DL -> OC	0.442	0.452	0.112	3.946	0.000
OC -> EP	0.179	0.180	0.099	1.804	0.036

Source: Made by SmartPLS

- a. H1: CS -> EP (Supported)

Cybersecurity Awareness has a significant positive effect on Employee Performance ($\beta = 0.306$, $p = 0.001$). Employees with high security awareness tend to work more diligently and responsibly, directly enhancing their effectiveness and efficiency (Permana et al., 2025).

- b. H2: CS -> OC (Supported)

Cybersecurity Awareness significantly increases Organizational Commitment ($\beta = 0.201$, $p = 0.029$). When employees act as guardians of company data, it fosters a stronger sense of responsibility and loyalty to the organization (Savitri, 2024).

- c. H3: DL -> EP (Supported)

Digital Literacy has a significant positive impact on Employee Performance ($\beta = 0.273$, $p = 0.003$). Proficiency with digital tools allows employees to work more productively, solve problems faster, and adapt to new systems, leading to higher output quality (Judijanto, 2024).

- d. H4: DL -> OC (Supported)

Digital Literacy significantly strengthens Organizational Commitment ($\beta = 0.442$, $p = 0.000$). This strong relationship can be explained by Social Exchange Theory; when a company invests in digital tools and training, employees reciprocate with increased loyalty and a stronger sense of belonging (Rachmad, 2024).

e. H5: OC $\rightarrow$ EP (Supported)

Organizational Commitment has a significant, though relatively smaller, positive effect on Employee Performance ($\beta = 0.179$, $p = 0.036$). Committed employees are more likely to be intrinsically motivated, disciplined, and go the extra mile to achieve organizational goals (Rifai, 2024).

Table 4.5 Indirect Effects (Mediation)

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values
CS $\rightarrow$ OC $\rightarrow$ EP	0.036	0.040	0.033	1.083	0.139
DL $\rightarrow$ OC $\rightarrow$ EP	0.079	0.078	0.046	1.714	0.043

Source: Made by SmartPLS

a. H6: CS $\rightarrow$ OC $\rightarrow$ EP (Not Supported)

Organizational Commitment does not mediate the relationship between Cybersecurity Awareness and Employee Performance ($\beta = 0.036$, $p = 0.139$). This suggests that while CS improves both OC and EP, its influence on performance is direct and not channelled through an increase in commitment. Cybersecurity practices may be viewed more as individual technical responsibilities rather than actions that deepen emotional bonds with the company.

b. H7: DL $\rightarrow$ OC $\rightarrow$ EP (Supported)

Organizational Commitment is a significant mediator between Digital Literacy and Employee Performance ($\beta = 0.079$, $p = 0.043$). This indicates that DL not only directly improves performance but also does so indirectly by fostering a stronger commitment to the organization. Employees who feel empowered by their digital skills are likely to feel more valued and connected to the company, which in turn motivates higher performance.

4.4 Discussion

The findings of this study confirm a robust and significant model where both Digital Literacy (DL) and Cybersecurity Awareness (CS) act as critical antecedents to improved Employee Performance (EP) and stronger Organizational Commitment (OC) at PT. Solusi Bangun Andalas. The strong support for hypotheses H1 through H5 underscores the indispensable role of investing in employees' digital capabilities and security mindset within the contemporary industrial landscape. This discussion delves deeper into the nuances of these relationships and situates the findings within the broader context of existing literature.

The significant direct effect of Digital Literacy on Employee Performance (H3) aligns seamlessly with Human Capital Theory (Becker, 1993), which posits that investments in employee skills enhance their productivity. In today's digital economy, DL is a fundamental component of human capital. Employees proficient in using digital tools can process information faster, collaborate more efficiently, and solve problems more effectively, leading directly to higher quality and quantity of work output. This finding is strongly supported by previous research. For instance, a study by Judijanto (2024) in the Indonesian context found that digital literacy was a primary driver of work effectiveness in technology-dependent organizations. Similarly, Kurniawan (2022) demonstrated that

employees with high digital literacy were more innovative and adaptive, leading to superior task performance. The very high descriptive scores for DL indicators in this study, particularly in using daily applications and managing digital information, further corroborate that these competencies are directly translating into perceived performance gains.

Furthermore, the finding that Digital Literacy significantly strengthens Organizational Commitment (H4) is a powerful insight. This relationship can be effectively explained by the Social Exchange Theory (Blau, 1964). When an organization provides the resources, training, and technological infrastructure that enhance an employee's digital competence, it is perceived as an investment in their personal and professional development. In return, employees feel a sense of obligation, gratitude, and loyalty, strengthening their affective and normative commitment to the organization. This result resonates with the work of Rachmad (2024), who found that digital empowerment initiatives led to significantly higher employee engagement and loyalty. Likewise, Andrie (2025) argued that in the era of digital transformation, a company's support for digital skill development is a key factor in fostering a strong sense of belonging among employees. The high mean scores on OC items related to pride and investment in the company suggest that employees at PT. Solusi Bangun Andalas do view their digital competencies as being intertwined with their identity within the organization.

Similarly, the direct positive impact of Cybersecurity Awareness on Employee Performance (H1) highlights a crucial dimension of modern work ethics. This goes beyond mere technical compliance and touches upon the concept of *Human Factors in Cybersecurity*. An employee who is vigilant against phishing attempts, conscientious about password hygiene, and understands data privacy protocols is inherently a more careful, disciplined, and responsible worker. This heightened sense of caution and responsibility naturally reduces errors and security breaches, thereby enhancing overall work efficiency and quality. This finding is consistent with Permana et al. (2025), who established a direct correlation between cybersecurity training and improved individual performance metrics. The very high scores on CS items, especially regarding understanding the importance of protecting company data, indicate that employees recognize this link between security-conscious behavior and professional conduct.

The significant relationship between Cybersecurity Awareness and Organizational Commitment (H2) suggests that employees who act as guardians of company data develop a deeper stake in the organization's well-being. By protecting digital assets, they are directly contributing to the organization's stability and reputation, which fosters a stronger sense of ownership and moral responsibility (Meyer & Allen, 1991). This aligns with findings by Wartono (2025), who reported that employees with high cybersecurity awareness exhibited more responsible work behavior and a stronger emotional connection to their organization. Savitri (2024) also noted that involvement in security protocols made employees feel more integral to the organization's defense, thereby increasing their loyalty.

However, the most insightful findings emerge from the mediation analysis. The fact that Organizational Commitment does **not** mediate the relationship between Cybersecurity Awareness and Employee Performance (H6 not supported) indicates that the influence of CS on EP is primarily direct and practical. Cybersecurity practices may be perceived more as individual, technical responsibilities mandated by policy rather than

actions that fundamentally deepen one's emotional bond with the company. The effect is on immediate work behavior rather than on long-term affective commitment.

In stark contrast, the significant mediation effect of OC on the relationship between DL and EP (H7 supported) reveals a more complex, dual pathway for Digital Literacy. This means that DL not only provides the *practical tools* for better performance (direct effect) but also enhances the *psychological and emotional attachment* to the company (indirect effect), which in turn motivates even higher performance. This finding is critical for strategic human resource management. It suggests that investments in digital literacy training yield a compound return: they build capability and simultaneously foster loyalty.

For managers at PT. Solusi Bangun Andalas and similar organizations, this study offers clear implications. First, fostering Digital Literacy should be a top priority, as it simultaneously boosts performance and commitment. Training programs should be framed not just as skill-building but as an investment in the employee's future within the company. Second, while Cybersecurity Awareness is crucial for risk mitigation and direct performance gains, efforts should be made to integrate it more deeply into the organizational culture. This could involve linking security protocols to corporate values, recognizing employees who exemplify good security practices, and leadership communication that emphasizes how every employee's vigilance protects the collective future of the organization. By doing so, the company can potentially activate the motivational pathway of organizational commitment for cybersecurity as well, creating a more resilient and highly performing workforce.

5. Conclusion and Recommendation

This study concludes that Cybersecurity Awareness (CS) and Digital Literacy (DL) have a significant positive direct influence on both Employee Performance (EP) and Organizational Commitment (OC) at PT. Solusi Bangun Andalas. Furthermore, Organizational Commitment itself significantly enhances Employee Performance. A key finding is that Digital Literacy improves Employee Performance not only directly but also indirectly by strengthening Organizational Commitment. However, the mediating role of Organizational Commitment in the relationship between Cybersecurity Awareness and Employee Performance was not found to be significant, indicating that while CS is crucial, its impact on performance is direct and not channeled through employee loyalty.

Theoretically, these findings reinforce Human Capital and Social Exchange theories, emphasizing that digital competencies and a reciprocal relationship of trust are vital for modern organizational success. They provide empirical evidence that Digital Literacy is a pivotal variable that can strengthen the emotional bond employees have with their organization. Practically, for management, this underscores the necessity of making continuous digital literacy development a core human resource strategy. It is recommended that the company integrate cybersecurity values into the organizational culture beyond mere technical compliance and develop a reward system that recognizes both digital proficiency and security compliance. For the HR department, specific actions include designing a curriculum focused on digital skills and cybersecurity, conducting regular digital competency assessments, and implementing employee engagement programs like digital innovation contests to foster commitment. For future research, it is advisable to incorporate additional variables such as work motivation or transformational leadership, employ a mixed-methods approach for deeper insights, and replicate the study in different industrial sectors to enhance the generalizability of the findings. Considering external factors like government regulations or

Industry 4.0/5.0 technological shifts as potential moderators could also provide a more comprehensive understanding of these dynamics.

Reference

- [1] Abbas, M. K. M., Yahaya, R. A., & Din, M. S. F. (2019). Digital Literacy and its Relationship with Employee Performance in the 4IR. *Journal of International Business, Economics and Entrepreneurship*, 4(2), 29-29.
- [2] Al-Shaikh, M. (2020). The role of cybersecurity awareness in mitigating cybercrime. *Journal of Information Security and Cybercrime*, 15(3), 210-225.
- [3] Allen, N.J. dan J.P. Meyer. (1991). The Measurement and Antecedents of Affective, Continuance and Normative Commitment to the Organizational. *Journal of Occupational Psychology*, 1, 1-18.
- [4] Andrie Firmansyah, S. E., Ichsan Milang, S. E., & Sri Mulyaningsih Kamaru, S. (2025). HR 5.0: Transformasi Sumber Daya Manusia di Era AI. Takaza Innovatix Labs.
- [5] Arias, L. (2021). Digital awareness and online behavior: A study of social media users. *Journal of Digital Media Studies*, 10(2), 85-101.
- [6] Bahri, S., Ramly, M., & Gani, A. (2021). Organizational commitment and civil servants performance: The contribution of intelligence, local wisdom and organizational culture. *European Journal of Business and Management Research*, 6(1), 128-134.
- [7] Basheer, A. and Singh, S. (2017). Determinants of organizational performance: a proposed framework *International Journal of Productivity and Performance Management Article information. International Journal of Productivity and Performance Management*, 65(December), 844-859.
- [8] Becker, Gary Stanley. (1993). *Human Capital: a theoretical and empirical analysis, with special reference to education* (3rd edition). London: The University of Chicago Press, Ltd.
- [9] Blau, P. M. (1964). Justice in Social Exchange. *Sociological Inquiry*, 34(2), 193-206.
- [10] Bulgurcu, H. (2010). The impact of cybersecurity on organizational performance. *Journal of Business and Information Technology*, 5(4), 301-315.
- [11] Cech, A., & Rothwell, S. (2020). The relationship between digital literacy, organizational commitment, and job performance. *Journal of Workplace Learning*, 32(5), 320-335.
- [12] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319-340.
- [13] Halik, A. (2023). Indicators of cybersecurity maturity in organizations. *Journal of Information Security*, 18(1), 45-60.
- [14] Ifinedo, P. (2014). Cybersecurity awareness and its impact on employee behavior: A conceptual framework and research agenda. *Journal of Information Technology Management*, 25(2), 120-135.
- [15] Judijanto, L., Setiawan, Z., Wiliyanti, V., Gunawan, P. W., Suryawan, I. G. T., Mardiana, S., ... & Joni, I. D. M. A. B. (2024). *Literasi Digital di Era Society 5.0: Panduan Cerdas Menghadapi Transformasi Digital*. PT. Sonpedia Publishing Indonesia.
- [16] Kurniawan, S. (2025). *Literasi Digital untuk Abad Ke-21*. Pustaka Aksara.
- [17] Kuswati, Y. (2020). The effect of motivation on employee performance. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)*, 3(2), 995-1002.
- [18] Marsh, E. (2021). Understanding the effect of digital literacy on employees' digital workplace continuance intentions and individual performance. In

- Research anthology on digital transformation, organizational change, and the impact of remote work (pp. 1638-1659). IGI Global.
- [19] Meyer, J. P., & Allen, N. J. (1991). A three-component conceptualization of organizational commitment. *Human Resource Management Review*, 1(1), 61-89.
 - [20] Mulyani, M. (2020). Pengaruh Penilaian Prestasi Kerja 360 Derajat Terhadap Keadilan Prosedural Dengan Persepsi Karyawan Sebagai Variabel Intervening (Studi Kasus Pada PT. Bank BNI Syariah Cabang Medan) (Doctoral dissertation, Universitas Islam Negeri Sumatera Utara).
 - [21] Muthuswamy, R. (2023). The importance of digital awareness in enhancing cybersecurity. *Journal of Cybersecurity Education, Research and Practice*, 8(1), 1-15.
 - [22] Ng, W. (2012). Digital literacy skills and a changing workforce. In D. A. J. Van Deursen (Ed.), *Handbook of Research on Digital Media and Technology* (pp. 45-60). Hershey, PA: IGI Global.
 - [23] Permana, R. A., Anindita, R., Zainol, Z., & Quinn, A. (2025). Analisis Metode dan Teknologi untuk Perlindungan Data dan Informasi dari Ancaman Siber: Analysis of Methods and Technologies for Data and Information Protection Against Cyber Threats. *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, 3(2), 137-146.
 - [24] Rachmad, Y. E., Indrayani, N., Harto, B., Judijanto, L., Rukmana, A. Y., Rahmawati, N. F., ... & Saktisya Putra, S. (2024). *Digital Technology Management: Mengelola Daya Saing melalui Teknologi Digital*. PT. Sonpedia Publishing Indonesia.
 - [25] Radovanović, D. (2020). Digital literacy and its indicators: A systematic review. *Journal of Information Technology*, 12(4), 310-325.
 - [26] Ridwan, M., Mulyani, S. R., & Ali, H. (2020). Improving employee performance through perceived organizational support, organizational commitment and organizational citizenship behavior. *Systematic Reviews in Pharmacy*, 11(12).
 - [27] Rifai, M. A., Wibowo, A., & Sosidah, S. (2024). Pengaruh Kepuasan Kerja, Employee Engagement dan Budaya Organisasi terhadap Kinerja Pegawai. *Co-Value Jurnal EOCnomic Operasi dan kewirausahaan*, 15(3).
 - [28] Savitri, P. (2024). *Transformasi digital dalam industri perbankan: Implikasi terhadap akuntansi dan teknologi informasi*. Penerbit NEM.
 - [29] Sonnentag, S., & Frese, M. (2002). Performance at work: A review of the literature. *Journal of Managerial Psychology*, 17(2), 101-118.
 - [30] Sullivan, J., Chen, H., & Kim, S. (2021). Cybersecurity Awareness and Its Impact on Employee Performance. *Journal of Information Systems Security*, 16(2), 130-145.
 - [31] Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington, MA: Lexington Books.
 - [32] Torton, A., Reaiche, C., & Boyle, E. (2025). A framework for cybersecurity awareness in the digital era.
 - [33] Van Laar, E., Van Deursen, A. J., & Van Dijk, J. A. (2020). The effect of digital skills and digital literacy on employee performance: A systematic review and meta-analysis. *Computers in Human Behavior*, 107, 106296.
 - [34] Wartono, T., Darmun, D., Judijanto, L., Tadius, T., Sucianti, R., Bari, A., ... & Puspitasari, K. A. (2025). *Pengantar Ilmu Manajemen*. PT. Sonpedia Publishing Indonesia.