PERADABAN JOURNAL OF ECONOMIC AND BUSINESS
ISSN 2829-1441
Vol. 5, No. 2 (2026), Page 244–258
DOI: https://doi.org/10.59001/pjeb.v5i2.1305

Article

The Effects of Cybersecurity Awareness and Digital Platform Trust on Business Sustainability among Digital Entrepreneurs

Nurul Haeriyah Ridwan[1*], Muh. Irshan Sachrir[2], Dwiyanti[3]

[1] Universitas Negeri Makassar, Makassar, Indonesia;
email: nurul.haeriyah@unm.ac.id

[2] Universitas Negeri Makassar, Makassar, Indonesia;
email: irshan@unm.ac.id

[3] Universitas Negeri Makassar, Makassar, Indonesia;
email: dwiyanti@unm.ac.id

[*] Corresponding email: nurul.haeriyah@unm.ac.id

ABSTRACT

The rapid growth of digital entrepreneurship has expanded business opportunities while increasing exposure to cybersecurity threats and dependence on digital platforms. However, empirical evidence on how cybersecurity awareness and digital platform trust contribute to business sustainability remains limited. This study examines the effects of cybersecurity awareness and digital platform trust on the business sustainability of digital entrepreneurs in Indonesia by integrating the Resource-Based View (RBV), Protection Motivation Theory (PMT), and Trust Theory. A quantitative explanatory design was employed using survey data collected from digital entrepreneurs operating through e-commerce and social commerce platforms. Data were analyzed using Partial Least Squares–Structural Equation Modeling (PLS-SEM) with SmartPLS 4. The results show that cybersecurity awareness and digital platform trust have positive and statistically significant effects on business sustainability. Cybersecurity awareness strengthens entrepreneurs' ability to identify digital threats and implement protective practices, while digital platform trust supports secure transactions, reliable platform operations, and reduced operational risks. These findings indicate that sustainable digital entrepreneurship depends on both internal cybersecurity capabilities and confidence in external digital platform infrastructure. The study contributes to the

KEYWORDS

Business sustainability, cybersecurity awareness, digital entrepreneurship, digital platform trust, partial least squares–structural equation modeling (PLS-SEM)

digital entrepreneurship literature by integrating cybersecurity capability and platform trust into a unified framework and provides practical insights for entrepreneurs, platform providers, and policymakers to strengthen digital resilience and sustainable business growth.

ABSTRAK

Pesatnya pertumbuhan kewirausahaan digital telah memperluas peluang bisnis sekaligus meningkatkan paparan terhadap ancaman keamanan siber dan ketergantungan pada platform digital. Namun, bukti empiris mengenai bagaimana kesadaran keamanan siber dan kepercayaan platform digital berkontribusi terhadap keberlanjutan bisnis masih terbatas. Penelitian ini menguji pengaruh kesadaran keamanan siber dan kepercayaan platform digital terhadap keberlanjutan bisnis wirausahawan digital di Indonesia dengan mengintegrasikan Resource-Based View (RBV), Protection Motivation Theory (PMT), dan Trust Theory. Desain eksplanatori kuantitatif digunakan dengan memanfaatkan data survei yang dikumpulkan dari wirausahawan digital yang beroperasi melalui platform e-commerce dan social commerce. Data dianalisis menggunakan Partial Least Squares–Structural Equation Modeling (PLS-SEM) dengan SmartPLS 4. Hasil penelitian menunjukkan bahwa kesadaran keamanan siber dan kepercayaan platform digital berpengaruh positif dan signifikan secara statistik terhadap keberlanjutan bisnis. Kesadaran keamanan siber memperkuat kemampuan wirausahawan dalam mengidentifikasi ancaman digital dan menerapkan praktik perlindungan, sementara kepercayaan platform digital mendukung transaksi yang aman, operasional platform yang andal, dan pengurangan risiko operasional. Temuan ini mengindikasikan bahwa keberlanjutan kewirausahaan digital bergantung pada kemampuan keamanan siber internal sekaligus kepercayaan terhadap infrastruktur platform digital eksternal. Penelitian ini berkontribusi pada literatur kewirausahaan digital dengan mengintegrasikan kapabilitas keamanan siber dan kepercayaan platform ke dalam satu kerangka kerja yang terpadu, serta memberikan wawasan praktis bagi wirausahawan, penyedia platform, dan pembuat kebijakan untuk memperkuat ketahanan digital dan pertumbuhan bisnis yang berkelanjutan.

KATA KUNCI:
Keberlanjutan bisnis, kepercayaan platform digital, kesadaran keamanan siber, kewirausahaan digital, partial least squares–structural equation modeling (PLS-SEM)

INTRODUCTION

Digital entrepreneurship has become an increasingly important component of economic development as entrepreneurs integrate marketplaces, social media, digital payment systems, cloud services, and platform-based communication into their business operations. Digital platforms enable entrepreneurs to reach wider markets, reduce transaction costs, communicate directly with consumers, and conduct business without geographical limitations (Bellaaj, 2023; Etemad, 2023; Hokmabadi et al., 2024). In Indonesia, this transformation is reflected in the approximately 27 million micro, small, and medium enterprises that had adopted digital technology by August 2024, with the government targeting 30 million digitally connected enterprises by the end of that year. At the same time, Indonesia recorded approximately 221.56 million internet users in 2024, representing an internet penetration rate of 79.5%. These figures demonstrate that digital platforms have become an essential infrastructure for entrepreneurial activity and market participation in Indonesia.

Despite providing significant opportunities, the rapid expansion of digital entrepreneurship has also increased business exposure to cyber risks (Chandna & Tiwari, 2023; Hokmabadi et al., 2024; Obitovich & Utkirovna, 2024; Saeed et al., 2023a). Digital entrepreneurs frequently store customer information, transaction histories, payment details, business documents, and marketing data through digital platforms (Gupta & Bose, 2022; Steininger et al., 2022). They are therefore vulnerable to phishing, credential theft, account takeover, malware, ransomware, fraudulent transactions, and data leakage. The Indonesian National Cyber and Crypto Agency reported approximately 330.53 million traffic anomalies during 2024 and detected 241 suspected data-leak incidents. These figures should not be interpreted as the number of successful cyberattacks or the number of affected enterprises; nevertheless, they illustrate the intensity of suspicious activities within Indonesia's digital ecosystem.

The vulnerability of digital entrepreneurs is increasingly concerning because micro and small businesses generally have limited financial, technological, and human resources to prevent and recover from cybersecurity incidents (Haj Mohammadi et al., 2026; Jamil et al., 2025; Vajjhala & Strang, 2023). The World Economic Forum reported that 35% of small organizations considered their cyber resilience inadequate in 2025, representing a sevenfold increase from the proportion recorded in 2022. The Verizon Data Breach Investigations Report further showed that ransomware was involved in 44% of the breaches examined in 2025. Its effect was disproportionately severe among small and medium-sized businesses, for which ransomware was associated with approximately 88% of the analyzed breaches. These findings indicate that cyber threats are no longer limited to large corporations with extensive databases, but have become a direct threat to the operational continuity of resource-constrained businesses.

The consequences of cybersecurity incidents extend beyond immediate financial losses. Cyberattacks can interrupt sales activities, prevent entrepreneurs from accessing digital accounts, compromise customer data, reduce consumer confidence, damage business reputation, and create substantial recovery costs (Bhakhri et al., 2024). IBM reported that the global average cost of a data breach reached USD4.44 million in 2025, although this figure represents organizations across different sizes and countries and should not be interpreted as the average loss experienced by Indonesian digital entrepreneurs. More specifically for small enterprises, the European Union Agency for Cybersecurity found that 90% of the surveyed SMEs expected cybersecurity problems to have serious negative consequences within one week, while 57% believed that a serious incident could lead to bankruptcy or business closure. This evidence positions cybersecurity as a strategic business sustainability issue rather than merely a technical information-system problem.

One internal capability that may reduce such vulnerability is cybersecurity awareness. Cybersecurity awareness refers to entrepreneurs' understanding of digital threats and their ability to recognize, prevent, and respond appropriately to cybersecurity risks (Akter et al., 2025; Dube & Mohanty, 2023; Oroni & Xianping, 2023; Taherdoost, 2024). It is reflected in practices such as creating strong and unique passwords, activating multifactor authentication, identifying fraudulent links, protecting customer information, updating software, controlling account access, conducting regular backups, and preparing incident-response procedures. A systematic review of SME cybersecurity literature concluded that insufficient awareness, limited cybersecurity literacy, and constrained financial resources are among the main obstacles preventing SMEs from developing effective cyber resilience. Therefore, entrepreneurs who possess greater cybersecurity awareness are expected to make safer digital decisions, reduce avoidable human errors, strengthen operational resilience, and maintain business activities when confronted with digital disruptions (Mmango & Gundu, 2024; Wilson & McDonald, 2025).

In addition to cybersecurity awareness, the sustainability of digital entrepreneurship is influenced by digital platform trust (Isa et al., 2026a; Krishna et al., 2023; Taherdoost, 2026). Digital platform trust represents entrepreneurs' confidence that a platform is secure, reliable, transparent, competent, and capable of protecting transactions and user information (Das, 2023). Such trust is particularly important because digital entrepreneurs commonly depend on external platforms for product promotion, customer communication, payment processing, order management, and market access. When entrepreneurs perceive that a platform provides adequate structural assurance, data protection, reliable services, transparent policies, and effective complaint resolution, they are more likely to maintain their participation and invest resources in platform-based activities (Abdalla et al., 2026; Estiri et al., 2026). Conversely, perceptions of insecurity, opaque algorithms, weak privacy protection, account restrictions, fraud, or recurring service disruptions may reduce platform dependence and threaten the continuity of digitally operated businesses.

The Resource-Based View is employed as the grand theory of this study because it explains business sustainability through the possession and deployment of valuable organizational resources and capabilities (Kraaijenbrink et al., 2010). From this perspective, cybersecurity awareness constitutes an intangible, knowledge-based resource that enables digital entrepreneurs to identify risks, protect strategic information, and respond effectively to cyber incidents (Kraaijenbrink et al., 2010) . Digital platform trust can be understood as a relational and technological resource that facilitates continuous transactions, customer access, information exchange, and participation in the digital ecosystem. The Resource-Based View is complemented by Protection Motivation Theory, which explains cybersecurity behavior through perceived vulnerability, perceived severity, response efficacy, and self-efficacy. Trust Theory is also used to explain how platform security, reliability, integrity, competence, and structural assurance shape entrepreneurs' willingness to continue conducting business through digital platforms.

Previous studies have examined cybersecurity awareness, cybersecurity readiness, cyber resilience, digital transformation, platform trust, and sustainable business performance (Atance-Álvarez et al., 2026; Isa et al., 2026; Mohamed Noor et al., 2026; Saeed et al., 2023). However, these streams of research remain relatively fragmented. Cybersecurity studies involving SMEs primarily emphasize technical controls, employee behavior, risk management, security readiness, and incident prevention (Armenia et al., 2021; Hoppe et al., 2021; Ye, 2026) For instance, scholars such as (Scholapurapu & Deepa, 2025) and AL-Hawamleh (2024) highlight how internal cybersecurity capabilities and protective behavior serve as essential safeguards against operational vulnerabilities, yet these studies largely treat security as an isolated technical or defensive mechanism rather than a core strategic driver of firm continuity. Research on user adoption, transactional security, algorithmic assurance, or ecosystem participation (Elgendy et al., 2025; Gamboa-Cruzado et al., 2025; Mihale-Wilson & Carl, 2024). While these studies establish that trust mitigates transactional risk, they predominantly emphasize buyer-side perceptions or platform-level dynamics rather than positioning platform trust as a vital relational-technological resource for seller-side business viability. Meanwhile, studies of business sustainability more frequently investigate digital capabilities, innovation, entrepreneurial orientation, financial literacy, and digital market adaptation (Hidayat-ur-Rehman, 2025; Huang et al., 2026; Nuraisyiah et al., 2025). Recent research has begun to associate cybersecurity hygiene and digital adaptation with business resilience (AL-Hawamleh, 2024; Saeed et al., 2023), but limited empirical evidence simultaneously evaluates cybersecurity awareness as an internal entrepreneurial capability and digital platform trust as a relational-technological resource directly affecting long-term business sustainability.

This study addresses these limitations by investigating the effects of cybersecurity awareness and digital platform trust on business sustainability among digital entrepreneurs. Its novelty lies in developing an integrated resource-and-trust framework that combines an internal knowledge-based capability with entrepreneurs' confidence in external digital infrastructure, while positioning business sustainability as the principal outcome. The study also provides contextual novelty by examining digital entrepreneurs in Indonesia, an emerging economy characterized by high internet penetration, rapid digitalization of MSMEs, strong dependence on marketplace and social-commerce platforms, and substantial exposure to cyber risks. Using a quantitative survey and Partial Least Squares–Structural Equation Modeling, this study is expected to extend the Resource-Based View into the cybersecurity and platform-economy context, provide empirical evidence concerning the determinants of sustainable digital entrepreneurship, and assist entrepreneurs, platform providers, educators, and policymakers in designing cybersecurity education, platform-governance mechanisms, and digital resilience programs that support long-term business continuity.

Entrepreneurs with higher cybersecurity awareness are expected to be more capable of recognizing cyber threats, implementing preventive security practices, and safeguarding critical business and customer information throughout their digital operations. Likewise, entrepreneurs who develop stronger trust in digital platforms are more likely to continuously utilize platform-based services, maintain customer relationships, and sustain business activities within an increasingly competitive digital environment. Business sustainability, therefore, depends not only on entrepreneurs' ability to protect their digital assets from cybersecurity risks but also on their confidence in the reliability, security, and integrity of the digital platforms that support their entrepreneurial activities. The complementary interaction between cybersecurity awareness as an internal strategic capability and digital platform trust as a relational-technological resource is expected to strengthen organizational resilience and ensure the long-term sustainability of digital entrepreneurial ventures. Based on the theoretical arguments and empirical evidence presented above, this study proposes the following hypotheses:

H1: Cybersecurity awareness has a positive effect on the business sustainability of digital entrepreneurs in Indonesia.
H2: Digital platform trust has a positive effect on the business sustainability of digital entrepreneurs in Indonesia.

This study seeks to provide a more comprehensive understanding of how cybersecurity awareness and digital platform trust jointly contribute to the business sustainability of digital entrepreneurs in an emerging economy. By integrating the Resource-Based View, Protection Motivation Theory, and Trust Theory, this research offers a broader theoretical perspective on how internal cybersecurity capabilities and external platform-related trust interact to support long-term entrepreneurial resilience and sustainable business performance. The findings are expected to enrich the literature on digital entrepreneurship by extending existing knowledge beyond technological adoption toward strategic security capabilities and trust-based digital ecosystems. From a practical perspective, the results will provide valuable insights for digital entrepreneurs, platform providers, policymakers, and entrepreneurship support institutions in designing cybersecurity awareness programs, strengthening platform governance, and developing digital business policies that enhance organizational resilience, customer confidence, and sustainable entrepreneurial growth in the rapidly evolving digital economy.

METHOD

The subjects of this study are digital entrepreneurs in Indonesia who actively conduct business through digital platforms, including e-commerce marketplaces, social commerce platforms, and digital business applications. Digital entrepreneurs were selected because they represent one of the fastest-growing segments of the digital economy while simultaneously facing increasing cybersecurity risks associated with online transactions, digital payment systems, customer data management, and platform dependency. Their business operations rely heavily on digital infrastructure, making cybersecurity awareness and digital platform trust essential capabilities for maintaining long-term business sustainability. The unit of analysis in this study is the business owner or manager, as these individuals are directly responsible for strategic decision-making, digital security practices, platform utilization, and the sustainability of business operations.

Given these characteristics of the study population and unit of analysis, this study adopts a quantitative approach using an explanatory research design to examine the causal relationships between cybersecurity awareness, digital platform trust, and business sustainability among digital entrepreneurs in Indonesia. The explanatory design is considered appropriate because the study aims to empirically test hypotheses developed from the Resource-Based View (RBV) as the grand theoretical foundation, supported by Protection Motivation Theory (PMT) and Trust Theory (Boer et.al, 1986; Kraaijenbrink et al., 2010) . These theoretical perspectives explain how cybersecurity awareness functions as an internal strategic capability and how trust in digital platforms contributes to sustaining entrepreneurial performance in an increasingly uncertain digital environment.

To obtain respondents who meet the specific requirements of the study, this study employs a non-probability sampling method using purposive sampling. This technique was selected because the research focuses on respondents who possess specific characteristics relevant to the objectives of the study rather than attempting to statistically generalize the findings to the entire population of digital entrepreneurs. The criteria for selecting respondents are as follows:

1. The respondent is the owner or manager of a digital business operating in Indonesia.
2. The business has been operating for at least one year.
3. The business actively utilizes at least one digital platform, such as Shopee, Tokopedia, TikTok Shop, Lazada, Instagram Shop, Facebook Marketplace, WhatsApp Business, or an independent e-commerce website, as its primary sales or business communication channel.
4. The respondent is directly responsible for managing digital business operations, customer data, platform accounts, and strategic business decisions.
5. The respondent has experience using digital payment systems and conducting online business transactions.

Based on these eligibility criteria, the sample size was then determined based on the methodological recommendations for Partial Least Squares–Structural Equation Modeling (PLS-SEM). The minimum sample size in PLS-SEM depends on the complexity of the structural model, the number of latent constructs, and the number of indicators used to measure each construct (Hair & Alamer, 2022). Since the proposed research model consists of two exogenous constructs (Cybersecurity Awareness and Digital Platform Trust) and one endogenous construct (Business Sustainability), all measured reflectively, a sample size ranging from 150 to 250 digital entrepreneurs is considered adequate to produce stable parameter estimates, sufficient statistical power, and reliable model evaluation. To improve the robustness and predictive capability of the structural model, this study targets approximately 200 respondents, which exceeds the recommended minimum sample size for variance-based structural equation modeling.

Having established the target population, sampling procedure, and sample size, the study subsequently operationalized the variables through three latent constructs: Cybersecurity Awareness, Digital Platform Trust, and Business Sustainability. All constructs were measured using a five-point Likert scale, ranging from 1 (strongly disagree) to 5 (strongly agree). The measurement indicators were adapted from previous empirical studies on cybersecurity awareness, digital trust, and business sustainability and were modified to fit the context of digital entrepreneurs in Indonesia. Prior to data collection, the questionnaire was reviewed by experts in digital entrepreneurship and information systems to ensure content validity and contextual relevance.

Table 1. Measurement of Research Variables

Variable	Code	Indicator	Measurement Scale
Cybersecurity Awareness	CA1	I understand the potential cybersecurity threats that may affect my digital business operations.	Likert 1–5
	CA2	I regularly implement cybersecurity practices such as strong passwords and multi-factor authentication.	Likert 1–5
	CA3	I am able to identify phishing attempts, fraudulent transactions, and other online security risks.	Likert 1–5

	CA4	I routinely protect customer and business data through backup and security management practices.	Likert 1–5
Digital Platform Trust	DT1	I believe that the digital platforms I use provide secure transaction systems.	Likert 1–5
	DT2	I trust that digital platforms adequately protect customer and business information.	Likert 1–5
	DT3	I believe that digital platforms operate transparently and reliably.	Likert 1–5
	DT4	I am confident that digital platforms effectively support the continuity of my business operations.	Likert 1–5
Business Sustainability	BS1	My business has maintained stable operational performance over time.	Likert 1–5
	BS2	My business is capable of adapting to technological and market changes.	Likert 1–5
	BS3	My business continues to maintain customer relationships and business growth.	Likert 1–5
	BS4	My business is able to sustain long-term competitiveness despite digital challenges.	

Source: Adapted from previous empirical studies on cybersecurity awareness, digital platform trust, and business sustainability, and modified for the context of digital entrepreneurs in Indonesia.

Based on the theoretical framework and previous empirical findings, this study proposes a conceptual model illustrating the relationships between Cybersecurity Awareness, Digital Platform Trust, and Business Sustainability, as presented in Figure 1.

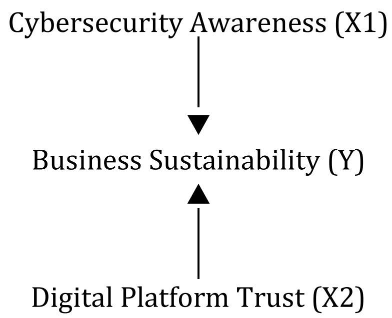

Figure 1. Conceptual Framework

Data were collected through an online self-administered questionnaire distributed to digital entrepreneurs across Indonesia through entrepreneurship associations, MSME communities, startup networks, digital business forums, and social media groups. The online survey approach was selected because digital entrepreneurs are geographically dispersed and predominantly conduct business activities through digital platforms. Respondents were instructed to answer each statement based on their actual experience in managing digital business operations, implementing cybersecurity practices, and utilizing digital platforms.

Prior to the main survey, a pilot test involving a small group of digital entrepreneurs was conducted to evaluate the clarity, readability, and reliability of the questionnaire. Feedback obtained during the pilot phase was used to refine the wording of several measurement items before large-scale data collection commenced. The collected data were analyzed using Partial Least Squares–Structural Equation Modeling (PLS-SEM) with the assistance of SmartPLS 4 software. PLS-SEM was selected because it is appropriate for analyzing predictive and explanatory research models involving latent constructs measured by multiple indicators. In addition, PLS-SEM is suitable for studies with moderate sample sizes, does not require multivariate normality, and effectively estimates complex causal relationships. The data analysis procedure consisted of two sequential stages:

1. Evaluation of the Measurement Model (Outer Model) by examining indicator reliability (outer loadings), internal consistency reliability (Cronbach's Alpha and Composite Reliability), convergent validity using the Average Variance Extracted (AVE), and discriminant validity using the Heterotrait-Monotrait Ratio (HTMT) and Fornell–Larcker Criterion.

2. Evaluation of the Structural Model (Inner Model) by assessing collinearity (Variance Inflation Factor/VIF), coefficient of determination (R^2), predictive relevance (Q^2), effect size (f^2), and hypothesis testing through path coefficients, t-statistics, and p-values generated using the bootstrapping procedure with 5,000 resamples.

To further evaluate the predictive capability of the proposed model, PLS Predict analysis was also conducted to compare prediction errors between the PLS model and a linear regression benchmark. The overall model quality was assessed using R^2, Adjusted R^2, Q^2 Predict, f^2, and Standardized Root Mean Square Residual (SRMR) to ensure that the structural model demonstrated acceptable explanatory and predictive performance. The significance level adopted in this study was 5% ($\alpha = 0.05$), whereby hypotheses were accepted when the t-statistic exceeded 1.96 and the p-value was less than 0.05.

RESULTS AND DISCUSSION

Descriptive Analysis

This study involved 200 digital entrepreneurs in Indonesia who actively operate their business ventures through e-commerce marketplaces, social commerce platforms, and digital applications. In alignment with the study's objective to provide robust estimations, demographic characteristics were recorded and utilized to ensure that the sample captures the real dynamics and diversity of Indonesia's digital entrepreneurial ecosystem. The detailed profile of the 200 respondents is presented in Table 2.

Table 2. Respondents' Characteristics

Characteristics	Category	Frequency	Percentage
Gender	Male	108	54.0%
	Female	92	46.0%
Age	< 30 years	68	34.0%
	30–39 years	86	43.0%
	> 40 years	46	23.0%
Business Duration	1–3 years	82	41.0%
	4–6 years	70	35.0%
	> 6 years	48	24.0%
Primary Platform Type	E-commerce Marketplaces	76	38.0%
	Social Commerce	68	34.0%
	Digital Services & Apps	36	18.0%
	Others	20	10.0%

Source: primary data (2026).

Overall, the respondents' profile reflects a wide diversity of entrepreneurial backgrounds in terms of age, business experience, and digital platform channel. The sample features a balanced gender distribution and is dominated by entrepreneurs in the productive age range of 30–39 years whose businesses have been operating between one and six years. Significant representation from e-commerce marketplaces and social commerce channels, coupled with contributions from service platforms and independent digital channels, ensures that the collected data captures the actual operational landscape of digital entrepreneurs in Indonesia. This inherent diversity strengthens the relevance and robustness of the analysis's findings in positioning cybersecurity awareness and digital platform trust as crucial determinants of business sustainability across various digital business contexts.

Measurement Model Evaluation (Outer Model)

The measurement model was evaluated to establish indicator reliability and convergent validity. Based on the criteria established by Hair et al. (2019), indicators with outer loadings above 0.70 are considered reliable. Additionally, all constructs met the requirements for Average Variance Extracted (AVE > 0.50) and Composite Reliability (CR > 0.70).

Table 3. Measurement Model Results

Variable	Indicator	Outer Loading	Cronbach's Alpha	CR	AVE
Cybersecurity Awareness	CA1	0.82	0.83	0.89	0.66
	CA2	0.78			
	CA3	0.84			
	CA4	0.81			
Digital Platform Trust	DT1	0.85	0.84	0.89	0.66
	DT2	0.80			
	DT3	0.83			
	DT4	0.79			
Business Sustainability	BS1	0.87	0.85	0.90	0.69
	BS2	0.83			
	BS3	0.82			
	BS4	0.80			

Source: SmartPLS output (2026).

The empirical assessment of the measurement model confirms that all item loadings exceed the conservative threshold of 0.70, which signifies high indicator reliability. Moreover, the internal consistency of the constructs is well-established, as both Cronbach's Alpha and Composite Reliability (CR) values are significantly above the recommended 0.70 level. Convergent validity is further substantiated by Average Variance Extracted (AVE) values that consistently surpass the 0.50 requirement. Collectively, these statistical results demonstrate that the measurement model adheres to the rigorous criteria for both reliability and convergent validity.

1. Discriminant Validity

a) Fornell–Larcker Criterion

Table 4. Fornell–Larcker Criterion

Construct	Cybersecurity Awareness	Digital Platform Trust	Business Sustainability
Cybersecurity Awareness	0.81		
Digital Platform Trust	0.62	0.81	
Business Sustainability	0.68	0.71	0.83

Source: SmartPLS output (2026).

The assessment of discriminant validity, as evidenced by the Fornell–Larcker criterion, indicates that the square root of the AVE for each latent variable (the diagonal elements in bold) is consistently superior to the correlation coefficients between that construct and others in the model. This statistical alignment confirms that the constructs are sufficiently distinct and that the measurement model possesses satisfactory discriminant validity.

b) HTMT Criterion

Table 5. HTMT Results

Construct Pair	HTMT Value
Cybersecurity Awareness – Digital Platform Trust	0.72
Cybersecurity Awareness – Business Sustainability	0.79
Digital Platform Trust – Business Sustainability	0.83

Source: SmartPLS output (2026).

All HTMT values are strictly below the recommended threshold of 0.90, further confirming discriminant validity between the research constructs.

Structural Model Evaluation (Inner Model)

1. Coefficient of Determination (R^2)

Table 6. R-square (R^2)

Endogenous Variable	R-square (R2)	R-square Adjusted
Business Sustainability	0.62	0.61

Source: SmartPLS output (2026).

The R^2value of 0.62 indicates that Cybersecurity Awareness and Digital Platform Trust together explain 62% of the variance in Business Sustainability among digital entrepreneurs in Indonesia. Based on the criteria of Hair & Alamer (2022), these results indicate that the model possesses moderate-to-substantial explanatory power, while the remaining 38% is influenced by other organizational or environmental factors outside the scope of this study.

2. Effect Size (f^2)

Table 7. Effect Size (f^2)

Relationship	f-square (f^2)
Cybersecurity Awareness →Business Sustainability	0.25
Digital Platform Trust →Business Sustainability	0.38

Source: SmartPLS output (2026).

The effect size results suggest that Digital Platform Trust has a large effect (f^2= 0.38) on Business Sustainability, while Cybersecurity Awareness exerts a moderate-to-medium effect (f^2= 0.25).

Hypothesis Testing

Hypothesis testing was conducted using a bootstrapping procedure with 5,000 subsamples at a 5% significance level. The statistical results are presented in Table 8.

Table 8. Hypothesis Testing Results

Hypothesis	Relationship	β	T-statistic	P-value	Decision
H1	Cybersecurity Awareness → Business Sustainability	0.35	3.82	0.000	**Supported**
H2	Digital Platform Trust → Business Sustainability	0.48	5.64	0.000	**Supported**

Source: SmartPLS output (2026).

The results indicate that both Cybersecurity Awareness and Digital Platform Trust have positive and statistically significant effects on the Business Sustainability of digital entrepreneurs in Indonesia.

Theoretical Interpretation of the Effects on Business Sustainability

This study provides empirical evidence that cybersecurity awareness and digital platform trust are key determinants of business sustainability among digital entrepreneurs in Indonesia. The findings demonstrate that both variables exert positive and statistically significant effects on long-term business sustainability, indicating that entrepreneurial performance in a digital economy context is shaped by the interaction between internal security capabilities and external trust in digital platform infrastructure.

The positive effect of cybersecurity awareness confirms that digital entrepreneurs who possess a strong understanding of cyber threats and regularly implement preventive security measures are better equipped to safeguard operational data, maintain business continuity, and adapt to digital disruptions. From a Resource-Based View (RBV) perspective, this result supports the argument that cybersecurity awareness functions as an intangible, knowledge-based capability that protects strategic business assets from severe online risks. In digital environments where formal IT security departments are often absent, cybersecurity awareness substitutes for sophisticated security infrastructure by reducing human vulnerabilities, preventing credential theft, and mitigating ransomware or phishing risks(Aslan et al., 2023; Hossain et al., 2024; Masmoudi, 2025). Furthermore, alignment with Protection Motivation Theory indicates that heightened risk perception and self-efficacy directly translate into proactive protective behaviors that preserve enterprise performance during unexpected digital incidents.

Several previous studies have indicated that digital platform trust exhibits a comparatively stronger effect on business sustainability, highlighting the critical role of platform governance and infrastructure confidence in supporting digital ventures (Hadizadeh et al., 2024; Kluiters et al., 2023; Liu et al., 2024; Ochinanwata et al., 2024; Salgado-Criado et al., 2024). This result suggests that trusting a digital platform enhances business sustainability not only through smooth daily transactions, but also by providing structural assurance, operational reliability, and transaction security. When entrepreneurs perceive that platform providers maintain secure payment gateways, safeguard account integrity, and enforce transparent dispute resolution policies, they are more willing to invest strategic resources and commit long-term operations to those digital ecosystems. As digital entrepreneurs depend heavily on external platforms for customer reach, market access, and payment processing, high platform trust directly reduces perceived transactional risk and stabilizes continuous revenue streams.

Importantly, the findings imply that cybersecurity awareness and digital platform trust serve complementary roles in shaping business sustainability. Cybersecurity awareness provides entrepreneurs with the internal capability to identify risks and execute safe digital choices, whereas digital platform trust offers a secure relational and technological environment that facilitates platform reliance and operational expansion. When combined, an internal security capability and confidence in external digital infrastructure reinforce organizational resilience, allowing entrepreneurs to navigate volatile digital markets effectively.

In the Indonesian context, where rapid digital expansion among MSMEs coexists with an increasing incidence of data breaches and online fraud, these findings carry significant strategic implications (Lukiyanto, 2025; Saiful et al., 2025). The results demonstrate that promoting digital transformation alone is insufficient without simultaneously strengthening security awareness and platform reliability. Theoretical integration of the Resource-Based View, Protection Motivation Theory, and Trust Theory within a single explanatory framework extends current entrepreneurship literature by demonstrating that long-term digital business viability depends on both internal strategic capabilities and external ecosystem trust.

CONCLUSION

This study investigates the effects of cybersecurity awareness and digital platform trust on the business sustainability of digital entrepreneurs in Indonesia. The empirical results confirm that both cybersecurity awareness and digital platform trust exert positive and statistically significant influences on business sustainability. These findings indicate that sustainable digital entrepreneurship in an emerging economy depends on both internal security capabilities and confidence in external digital platform infrastructure. Cybersecurity awareness strengthens entrepreneurs' ability to identify threats and maintain operational continuity, while digital platform trust reduces risks and supports continuous platform engagement. Together, these factors contribute to digital resilience and long-term business viability. The findings offer practical insights for digital entrepreneurs, platform providers, and policymakers. Entrepreneurs are encouraged to strengthen cybersecurity hygiene and carefully select trustworthy platforms, while platform providers should enhance security measures and operational transparency. Policymakers and business associations may also integrate cybersecurity literacy into digital inclusion programs. Nevertheless, this study has several limitations, including its cross-sectional design, reliance on perceptual measures of sustainability, and focus on micro and small digital ventures in Indonesia. Future research is recommended to employ longitudinal designs, incorporate objective financial indicators, and examine potential moderating factors such as platform dependency or regulatory environment.

REFERENCES

Adelia, R., Suryani, Y., & Habibie, A. (2024). Pengaruh leverage, ukuran perusahaan dan struktur modal terhadap nilai perusahaan dengan profitabilitas sebagai variabel intervening pada perusahaan manufaktur yang terdaftar di bursa efek indonesia periode 2017-2022. *Jurnal Ekonomi Bisnis, Manajemen dan Akuntansi (JEBMA), 4*(3), 2131–2140. https://doi.org/10.47709/jebma.v4i3.4426

Adisty, F. P., Mardi, & Ulupui, I. G. K. A. (2024). Revealing the role of profitability in mediating leverage, liquidity, and company size on firm value in health sector. *Jurnal Pendidikan Ekonomi, Perkantoran, dan Akuntansi, 5*(3), 643–662. https://doi.org/10.21009/jpepa.0503.10

Aditya, I., Hasanah, N., Mardi, & Armeliza, D. (2021). Pengaruh leverage dan ukuran perusahaan terhadap nilai perusahaan dengan profitabilitas sebagai variabel intervening pada perusahaan industri dasar dan kimia. *Jurnal Wahana Akuntansi, 16*(2), 124–152. https://doi.org/10.21009/wahana.16.021

Ajiani, I. P. F., & Mubaraq, M. R. (2023). Nilai perusahaan manufaktur ditinjau dari rasio leverage. *Riset, Ekonomi, Akuntansi dan Perpajakan (Rekan), 4*(1), 87–96. https://doi.org/10.30812/rekan.v4i1.2883

Annisya, F., Nurdiwaty, D., & Solikah, M. (2025). Pengaruh likuiditas, profitabilitas dan ukuran perusahaan terhadap nilai perusahaan dengan kinerja keuangan sebagai intervening. *Maslahah: Jurnal Manajemen dan Ekonomi Syariah, 3*(4), 31–47. https://doi.org/10.59059/maslahah.v3i4.2695

Astawinetu, E. D., Istiono, I., Rachmawati, T., & Penangsang, P. (2023). Can profitability intervene in the effects of liquidity, activity, and leverage on company value? *Journal of Economics, Finance and Management Studies, 6*(7). https://doi.org/10.47191/jefms/v6-i7-37

Dewi, N. P. I. K., & Abundanti, N. (2019). Pengaruh leverage dan ukuran perusahaan terhadap nilai perusahaan dengan profitabilitas sebagai variabel mediasi. *E-Jurnal Manajemen Universitas Udayana, 8*(5), 3028. https://doi.org/10.24843/EJMUNUD.2019.v08.i05.p16

Fadhillah, N., Syukri, A., Mubyarto, N., & Nasrullah, M. (2024). The effect of profitability, leverage and company size on company value in Sharia National Pension Savings Bank for the period 2014-2023. *The Asian Journal of Professional & Business Studies, 5*(2). https://doi.org/10.61688/ajpbs.v5i2.362

Fajri, S., Wahyuni, I., & Subaida, I. (2023). Leverage dan ukuran perusahaan terhadap nilai perusahaan pada perusahaan pertambangan yang terdaftar di bursa efek indonesia dengan profitabilitas sebagai variabel intervening. *Jurnal Mahasiswa Entrepreneurship (JME), 2*(4), 666. https://doi.org/10.36841/jme.v2i4.3440

Ghazali, M. H., Azhar, S. S., & Ihsani, M. M. (2018). Factor analysis of a novel scoring-based instrument on forecasting Malaysian travelers' behavioral preparedness for travel-related infectious diseases. *International Journal of Travel Medicine and Global Health, 6*(2), 54–63. https://doi.org/10.15171/ijtmgh.2018.11

Gultom, D. K., & Tartila, M. (2022). Pengaruh debt to equity ratio terhadap price to book value dengan return on equity sebagai variabel intervening pada perusahaan sub sektor otomotif dan komponen yang terdaftar di bei periode 2016-2020. *Prosiding Seminar Nasional Multidisiplin Ilmu, 3*(1).

Helfin, C., & Trisnawati, E. (2020). Pengaruh related party transaction terhadap tax avoidance dengan variabel moderasi pengungkapan tata kelola perusahaan pada perusahaan manufaktur yang terdaftar di bursa efek indonesia (BEI) periode 2013-2017. *Jurnal Paradigma Akuntansi, 2*(2), 818–825.

Nanang, A. P., & Hendang, T. (2019). Pengaruh corporate governance (CG) terhadap kualitas laba dengan manajemen laba sebagai variabel intervening pada perusahaan manufaktur yang terdaftar di bei periode 2015-2017. *Jurnal Muara Ilmu Ekonomi dan Bisnis, 3*(2), 267–288.

Nazariah, N., Indriani, Y., & Kasymir, E. (2021). Pola konsumsi dan sikap mahasiswa universitas lampung terhadap kopi robusta. *Jurnal Ilmu-Ilmu Agribisnis: Journal of Agribusiness Science, 9*(3), 477–484.

Puri, R. M., Yuliani, Y., & Thamrin, K. M. H. (2024). The effect of company size and capital structure on firm value with profitability as an intervening variable. *Eduvest - Journal of Universal Studies, 4*(4), 2274–2292. https://doi.org/10.59188/eduvest.v4i4.1359

Putri, M. R. S., Hermuningsih, S., & Wiyono, G. (2024). Pengaruh profitabilitas, leverage, ukuran perusahaan, dan pertumbuhan aset terhadap nilai perusahaan. *Owner, 8*(2), 1823–1838. https://doi.org/10.33395/owner.v8i2.1997

Radja, A. I., Pramitasari, T. D., & Subaida, I. (2025). Ukuran perusahaan modal kerja dan leverage terhadap nilai perusahaan dengan profitabilitas sebagai variabel intervening pada perusahaan sub sektor makanan dan minuman yang terdaftar di bei periode 2022-2023. *Jurnal Mahasiswa Entrepreneurship (JME), 4*(4), 731. https://doi.org/10.36841/jme.v4i4.6720

Trading Economics. (2026). *Indonesia GDP from mining*. Retrieved from https://id.tradingeconomics.com/indonesia/gdp-from-mining

Wulandari, T., & Mujiyati. (2024). Company value: Within the scope of company size, leverage, profitability, and capital structure. *Dinasti International Journal of Economics, Finance & Accounting, 5*(3), 1785–1797. https://doi.org/10.38035/dijefa.v5i3.3029

Zakaria, R., Pamungkas, G., Adelya, D., Khoirunnisa, L., & Cahyani, G. (2024). Pengaruh profitabilitas, leverage, dan ukuran perusahaan terhadap nilai perusahaan. *Jurnal Riset Manajemen dan Ekonomi (JRIME), 3*(1), 158–170. https://doi.org/10.54066/jrime-itb.v3i1.2838