

“Assessment of cybersecurity investment and customer trust in SMEs of South Africa”

AUTHORS	Thabiso Sthembiso Msomi 
	 Nomfundo Kuhlekonke Minenhle Nxumalo 
ARTICLE INFO	Thabiso Sthembiso Msomi and Nomfundo Kuhlekonke Minenhle Nxumalo (2026). Assessment of cybersecurity investment and customer trust in SMEs of South Africa. <i>Problems and Perspectives in Management</i> , 24(3), 84-94. doi: 10.21511/ppm.24(3).2026.06
DOI	http://dx.doi.org/10.21511/ppm.24(3).2026.06
RELEASED ON	Tuesday, 21 July 2026
RECEIVED ON	Sunday, 21 December 2025
ACCEPTED ON	Wednesday, 13 May 2026
LICENSE	 This work is licensed under a Creative Commons Attribution 4.0 International License
JOURNAL	"Problems and Perspectives in Management"
ISSN PRINT	1727-7051
ISSN ONLINE	1810-5467
PUBLISHER	LLC “Consulting Publishing Company “Business Perspectives”
FOUNDER	LLC “Consulting Publishing Company “Business Perspectives”



NUMBER OF REFERENCES

41



NUMBER OF FIGURES

0



NUMBER OF TABLES

3

© The author(s) 2026. This publication is an open access article.



BUSINESS PERSPECTIVES



LLC "CPC "Business Perspectives"
Hryhorii Skovoroda lane, 10,
Sumy, 40022, Ukraine
www.businessperspectives.org

Type of the article: Research Article

Received on: 21st of December, 2025

Accepted on: 13th of May, 2026

Published on: 21st of July, 2026

© Thabiso Sthembiso Msomi,
Nomfundo Kuhlekonke Minenhle
Nxumalo, 2026

Thabiso Sthembiso Msomi, Ph.D.,
Lecturer, Department of Management
Accounting, Faculty of Accounting
and Informatics, Durban University of
Technology, South Africa.

Nomfundo Kuhlekonke Minenhle
Nxumalo, Master of Accounting,
Lecturer, Department of Auditing
and Taxation, Faculty of Accounting
and Informatics, Durban University
of Technology, South Africa.
(Corresponding author)



This is an Open Access article,
distributed under the terms of the
[Creative Commons Attribution 4.0
International license](https://creativecommons.org/licenses/by/4.0/), which permits
unrestricted re-use, distribution, and
reproduction in any medium, provided
the original work is properly cited.

Conflict of interest statement:

Author(s) reported no conflict of interest

Thabiso Sthembiso Msomi (South Africa),
Nomfundo Kuhlekonke Minenhle Nxumalo (South Africa)

ASSESSMENT OF CYBERSECURITY INVESTMENT AND CUSTOMER TRUST IN SMES OF SOUTH AFRICA

Abstract

Small and medium-sized enterprises (SMEs) are a key driver of employment and economic growth in South Africa, yet their increasing reliance on digital technologies has significantly increased exposure to cyber threats that can undermine customer trust and business sustainability. However, empirical evidence on how cybersecurity investment influences customer trust among SMEs in South Africa remains limited. This study aims to examine the relationship between cybersecurity investment and customer trust among SMEs operating in the retail, hospitality, e-commerce, professional services, and small-scale manufacturing sectors in KwaZulu-Natal, South Africa. These sectors were selected because of their high dependence on digital transactions and customer data processing. A quantitative research design was adopted using primary data collected through a structured questionnaire administered to SME owners and senior managers between 2024 and 2025. A total of 375 valid responses were analyzed using Pearson's correlation and linear regression techniques. The results reveal a statistically significant positive relationship between cybersecurity investment and customer trust ($r = 0.312, p < 0.001$). Regression analysis further indicates that cybersecurity investment explains 9.7% of the variance in customer trust ($R^2 = 0.097, p < 0.05$). SMEs that implemented secure digital payment systems, data protection measures, employee cyber-awareness training, and compliance with the Protection of Personal Information Act (POPIA) reported higher levels of customer confidence and perceived business credibility. These findings highlight that strategic investment in cybersecurity contributes to strengthening customer trust and improving the competitiveness and resilience of digitally enabled SMEs in South Africa.

Keywords

cybersecurity investment, customer trust, SMEs,
information security, technology adoption, digital risk
management, South Africa

JEL Classification

L26, K24

INTRODUCTION

Small and medium-sized enterprises (SMEs) play a vital role in South Africa's economic development, contributing approximately 42% of the country's gross domestic product and employing nearly 60% of the workforce. They also account for more than 90% of formal businesses in the country (Maharaj & Msomi, 2026). As SMEs increasingly adopt digital technologies to support online transactions, customer engagement, and operational efficiency, they are becoming more exposed to cybersecurity risks. Cyber incidents such as data breaches, phishing attacks, ransomware, and identity theft are becoming more frequent and pose significant operational and reputational threats to businesses operating in digital environments. In South Africa, the cybersecurity challenges faced by SMEs are intensified by structural constraints, including limited financial resources, a lack of specialized cybersecurity expertise, and relatively low levels of digital risk awareness. Although national regulatory frameworks, including the Protection of Personal Information Act (POPIA) and the Cybercrimes Act, aim to strengthen

data protection and improve cyber resilience, many SMEs still struggle to implement adequate security measures (Adelusi et al., 2022; Msomi & Ngcobo, 2023; Segotso et al., 2024). Consequently, SMEs often have weaker cybersecurity capabilities than large organizations, making them particularly vulnerable to cyber threats.

Beyond operational disruptions, inadequate cybersecurity can directly affect customer perceptions and trust. In digital transactions, customers must rely on firms to safeguard personal and financial information. When businesses fail to demonstrate strong security practices, customers may become reluctant to share sensitive information or continue engaging with the firm (Karadağ et al., 2023). Customer trust has, therefore, become an increasingly important factor influencing the sustainability and competitiveness of SMEs operating in digitally mediated markets. While existing studies have examined cybersecurity practices and organizational security management, much of this research has focused on large corporations with well-established IT infrastructures (Hsu et al., 2012; Baskerville et al., 2014). There remains limited empirical evidence on how cybersecurity investment influences customer trust within SMEs, particularly in developing economy contexts such as South Africa. This gap is significant because SMEs often operate with constrained resources and must make strategic decisions about how to allocate limited investments in cybersecurity.

1. LITERATURE REVIEW

Cybersecurity has become a crucial component influencing customer trust, organizational credibility, and business sustainability in this changing environment. Due to their limited financial, technological, and human resources, SMEs in South Africa often struggle with cybersecurity readiness despite playing a critical role in job creation and economic growth. The South African Banking Risk Information Centre reported that digital banking fraud incidents almost doubled from 31,612 cases in 2023 to approximately 64,000 cases in 2024, with associated losses increasing from R1 billion to more than R1.4 billion (South African Banking Risk Information Centre [SABRIC], 2025). Similarly, a national cybersecurity survey found that 47% of South African organisations experienced between one and five cybersecurity incidents during the preceding year, while 88% reported experiencing at least one security breach. Malware and phishing were identified among the most prevalent threats (Council for Scientific and Industrial Research [CSIR], 2024). This threatening environment places SMEs at considerable risk of financial fraud, phishing, ransomware, malware and data breaches. Consequently, customers may become increasingly cautious about conducting business with companies that collect and process sensitive financial and personal information, particularly because perceived security significantly influences customer trust and loyalty in South African online transactions (Mofokeng, 2023).

The increasing amount of research emphasizes how crucial cybersecurity is to SMEs' long-term viability and competitiveness, especially as the number of digital transactions rises. Customers are more inclined to interact with businesses that exhibit robust cybersecurity procedures. For example, Rizomyliotis (2026) discovered that consumer trust in online SMEs is greatly increased by visible security features like encryption, secure payment gateways, and authentication mechanisms. According to Cao and Huang (2022), SMEs that are more prepared for cybersecurity are also more likely to keep clients because investing in security improves the company's reputation for professionalism and dependability. Data encryption, intrusion detection systems, and employee security awareness training are examples of cybersecurity tools that demonstrate a company's commitment to safeguarding customer information. These results are consistent with signaling theory, which holds that businesses can lessen information asymmetry and foster trust by giving stakeholders observable, credible assurances (Connelly et al., 2011). Thus, SME cybersecurity serves as a strategic signal that boosts customer confidence and encourages long-term digital engagement in addition to serving as a protective mechanism.

Research reveals significant differences in SMEs' awareness, investment, and organizational preparedness worldwide, despite compelling evidence of the importance of cybersecurity. Many

SMEs prioritize immediate operational needs over digital security, resulting in chronic underinvestment. According to Kshetri (2019), SMEs in developing nations frequently lack official cybersecurity policies and find it difficult to devote resources to security because of budgetary limitations and a lack of technical know-how. This conclusion is supported in the African context, where Bada et al. (2019) note that weak security postures among SMEs stem from low cybersecurity awareness, reliance on unofficial, trust-based business practices, and a lack of dedicated IT staff. In a similar vein, Kabanda et al. (2018) demonstrate that many African SMEs lack formal cybersecurity planning, making them susceptible to operational disruptions and data breaches. Meeting the requirements of POPIA in South Africa remains difficult, especially for SMEs without specialized personnel, as compliance requires implementing appropriate organizational and technical safeguards (Brodin, 2019). Similar difficulties can be seen in other developing nations: according to Flores et al. (2015), Latin American SMEs usually underinvest in cybersecurity because of financial constraints and low perceived vulnerability.

Numerous studies demonstrate how cybersecurity training and digital literacy improve organizational outcomes. Targeted cybersecurity training enhances employees' threat detection and compliance behaviors, which lowers the possibility of security breaches that could erode customer confidence, according to Parsons et al. (2017). Moreover, responsible and transparent communication regarding data handling procedures, in addition to technical protection, shapes digital trust (Cheng & Nasirov, 2025). In a similar vein, Alshaikh (2020) shows that increasing cybersecurity awareness within organizations through communication, training, and cultural development greatly increases stakeholder trust and lowers vulnerabilities. Cegarra-Navarro et al. (2014) demonstrate that knowledge-oriented training interventions improve both operational capability and customer confidence, despite being primarily focused on organizational performance more broadly. This supports the idea that developing human-centric cybersecurity skills is crucial for SMEs looking to create resilient and reliable digital environments.

Studies conducted outside of Africa support these conclusions. According to Renaud and Ophoff (2021), SMEs in the UK implemented strong cybersecurity controls, specifically encryption, authentication systems, and secure payment infrastructures, and reported noticeably higher customer confidence, particularly in industries that handled financial and personal data. In the Middle East, comparable trends have been noted. According to Alshaikh (2020), SMEs in Saudi Arabia experience quantifiable increases in customer trust when they exhibit adherence to international standards like ISO/IEC 27001 and national cybersecurity frameworks. Anukoonwattaka et al. (2021) demonstrate that cybersecurity investment has a significant impact on consumer confidence in digital services in the Asia-Pacific region, particularly in e-commerce and logistics SMEs, where customer willingness to transact is directly influenced by perceived data security. Taiwanese data support this worldwide trend; Adelusi et al. (2022) found that consumers' intention to interact with SME online platforms is significantly increased by cybersecurity readiness, as measured by incident response capability, secure infrastructure, and employee training. Together, these studies confirm that cybersecurity is a strategic driver of digital trust, customer retention, and long-term competitiveness for SMEs globally, rather than just a technical issue.

The literature also shows notable differences in cybersecurity awareness and investment, especially in developing nations, despite these established correlations. According to Kshetri (2019), SMEs in developing nations frequently underinvest in cybersecurity because they believe that operational or financial pressures are more pressing than digital risks. Due to financial constraints and a lack of technical know-how, Flores et al. (2015) found that many SMEs in Latin America deprioritize cybersecurity. Similar patterns are seen in African contexts. According to Bada et al. (2019), SMEs' capacity to put even the most basic security measures in place is hampered by low cybersecurity awareness and a lack of organized security planning. SMEs in South Africa that lack specialized IT or compliance staff find it particularly difficult to comply with POPIA, as they struggle to meet requirements related to data processing, security measures, and continuous risk management (Sema et al., 2025).

Numerous studies demonstrate that security training, cyber awareness, and digital literacy improve organizational outcomes. Bada and Nurse (2019) emphasize that by lowering the possibility of security breaches, cybersecurity education aids SMEs in better understanding digital threats, putting in place suitable controls, and preserving customer trust. This is consistent with research conducted in Brazil by Santos and Berssaneti (2024), who found that SMEs that took part in government-funded cybersecurity training programs had higher levels of customer trust and fewer security incidents. In a similar vein, Awad and Martín-Rojas (2024) show that training initiatives targeted at enhancing digital capability and risk awareness can improve organizational performance and customer trust.

When considered collectively, the reviewed literature emphasizes how crucial cybersecurity investment is for safeguarding private data, assisting with regulatory compliance, and fostering consumer confidence. However, issues like scarce resources, low levels of digital literacy, and disparities in cybersecurity adoption among South African SMEs continue to exist.

Therefore, this study aims to investigate the relationship between cybersecurity investment and customer trust among SMEs in KwaZulu-Natal, South Africa. The study also aims to offer insights that can support SME managers in prioritizing cybersecurity initiatives and inform policymakers seeking to strengthen digital resilience within the SME sector.

2. METHOD

This study employed a quantitative research design grounded in the positivist paradigm to examine the relationship between cybersecurity investment and customer trust among South African SMEs. A cross-sectional survey approach was selected because it enables the collection of standardized data from a relatively large number of firms and supports statistical testing of hypothesized relationships. As Creswell (2014) explains, quantitative survey designs are appropriate when the objective is to measure relationships among variables using statistical techniques. The quanti-

tative strategy was, therefore, considered suitable for assessing the strength and significance of associations between clearly defined constructs while enhancing objectivity and replicability.

The analysis was conducted in the province of KwaZulu-Natal, South Africa, which hosts a diverse and economically significant SME sector experiencing rapid digital adoption. The province was purposively selected due to its concentration of SMEs and increasing exposure to cyber risks associated with digital business operations. The enterprises included in the study primarily operated in retail, hospitality, e-commerce, professional services, and small-scale manufacturing sectors in which digital technologies are increasingly used for online payments, customer databases, digital marketing, and electronic business management systems. These sectors were considered particularly relevant because they routinely process customer data and financial transactions through digital platforms, making them more exposed to cybersecurity risks and trust-related challenges. Data collection was carried out between January and June 2025, ensuring that the information reflects recent cybersecurity practices within the current regulatory environment shaped by the implementation of the POPIA.

The target population consisted of formally registered SMEs operating within KwaZulu-Natal that actively use digital technologies in their business operations. In accordance with South African SME classification guidelines, eligible firms were those employing between 10 and 200 employees, thereby excluding microenterprises with minimal digital infrastructure and large corporations with substantially different cybersecurity capacities. The unit of analysis was the firm, while the unit of observation was the SME owner or senior managerial representative responsible for digital operations, information technology management, or cybersecurity oversight. These individuals were selected because they are directly involved in decision-making regarding cybersecurity investments and digital operational practices.

A purposive sampling technique was employed to ensure that respondents possessed adequate knowledge of their organizations' cybersecurity practices and investment decisions, consis-

tent with guidance by Saunders et al. (2019) on information-rich sampling. Contact details of enterprises were obtained from publicly accessible business directories, including the Small Enterprise Development Agency (SEDA) database, regional SME associations, and official company websites, which provide listings of formally registered SMEs operating within the province.

The minimum required sample size was determined using the modified Cochran formula for finite populations, a widely accepted approach for survey research (Cochran, 1977). Based on an estimated sampling frame of approximately 850 eligible SMEs, the calculation yielded a required sample of 381 firms at a 95% confidence level and a 5% margin of error. A total of 380 questionnaires were returned, of which five were excluded following data screening for incompleteness and inconsistency, resulting in 375 valid responses for analysis. The participating enterprises varied in size, with the majority employing between 10 and 50 employees, while others employed 51–200 members, providing representation across the small and medium-sized spectrum.

Data were collected using a structured questionnaire comprising closed-ended items measured on a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). Likert-type scaling is widely used in behavioral and management research to measure attitudes and perceptions in a standardized manner, as noted by Likert (1932). The instrument was developed based on validated constructs from prior cybersecurity and trust literature and was adapted to the South African SME context to ensure contextual relevance.

The questionnaire captured firm demographics, cybersecurity investment practices, and customer trust perceptions. Cybersecurity investment items measured the presence of secure payment systems, data encryption mechanisms, employee cyber-awareness training programs, POPIA compliance practices, and other digital safeguards implemented within the enterprise. Customer trust items assessed perceived digital safety, confidence in sharing personal information, trust in online transactions, and overall perceived reliability of the firm's digital environment.

To enhance clarity and content validity, the instrument was pilot tested with 20 SME managers following recommendations by Saunders et al. (2019). Minor wording adjustments were made based on feedback, and pilot responses were excluded from the final dataset.

Data collection was conducted electronically using an online survey platform. Potential respondents received an invitation email outlining the purpose of the study, eligibility criteria, assurances of confidentiality, and a secure link to the questionnaire. Participation was voluntary, and two reminder emails were distributed at two-week intervals to improve response rates (Dillman et al., 2014). The survey remained open for approximately twelve weeks.

The study adhered to established ethical standards for research involving human participants. Prior to completing the questionnaire, respondents were presented with an informed consent statement explaining the purpose of the study, the voluntary nature of participation, and the intended use of the data. Consent was obtained electronically before access to the survey was granted. To ensure anonymity and impartiality, no personally identifying information was collected, and responses were analyzed in aggregated form only. The research protocol received approval from the relevant institutional research ethics committee.

The validated dataset comprising 375 responses was analyzed using the Statistical Package for the Social Sciences (SPSS). The analytical procedure followed a structured sequence beginning with data cleaning and screening, followed by descriptive statistics to profile respondents and participating firms. Pearson's correlation analysis was conducted to determine the strength and direction of the relationship between cybersecurity investment and customer trust, followed by linear regression analysis to evaluate the predictive effect of cybersecurity investment on customer trust. Statistical significance was assessed at the 5% level.

3. RESULTS

A total of 375 valid responses from SME owners and senior managers were retained for analysis after data screening. All items were measured on a

Table 1. Descriptive statistics of composite constructs

Construct	Indicators	Loadings	Mean	SD
Cybersecurity investment	SME invests adequately in data protection technologies	0.842	3.38	0.812
	Use of secure payment systems	0.861	3.52	0.785
	Employees receive cybersecurity awareness training	0.824	3.29	0.903
	Compliance with POPIA data protection requirements	0.879	3.47	0.768
	Regular updates of security software and firewalls	0.833	3.39	0.846
Customer trust	Customers perceive the business as secure	0.871	3.71	0.742
	Customers are confident sharing personal information	0.846	3.63	0.781
	Customers trust online transaction processes	0.888	3.69	0.736
	Cybersecurity practices enhance business credibility	0.854	3.74	0.705
	Customers are willing to continue transacting online	0.829	3.59	0.792

five-point Likert scale (1 = strongly disagree to 5 = strongly agree). Item scores were aggregated into composite indices for the two principal constructs.

Table 1 presents the descriptive statistics and factor loadings for the measurement items of cybersecurity investment and customer trust among South African SMEs. The results indicate that all indicators load strongly on their respective constructs, with standardized loadings ranging from 0.824 to 0.888, exceeding the commonly recommended threshold of 0.70. This confirms that the measurement items exhibit satisfactory indicator reliability and are appropriate representations of their underlying constructs. With respect to cybersecurity investment, the mean scores range from 3.29 to 3.52, indicating a moderate level of cybersecurity practice adoption among the sampled SMEs. The highest mean is observed for the use of secure payment systems ($M = 3.52$, $SD = 0.785$), indicating that transactional security measures are relatively more established. In contrast, employee cybersecurity awareness training ($M = 3.29$, $SD = 0.903$) records the lowest mean within this construct, reflecting comparatively weaker investment in human-centric cybersecurity capabilities. For customer trust, the mean values range from 3.59 to 3.74, indicating generally positive customer trust perceptions. The highest-rated item is cybersecurity practices enhance business credibility ($M = 3.74$, $SD = 0.705$), suggesting that visible security measures contribute to perceived organizational reliability. The relatively consistent standard deviations (approximately 0.70–0.90) across items indicate acceptable variability in responses without evidence of extreme dispersion.

Pearson's correlation coefficient was employed to assess the strength and direction of the association, and the outcomes are presented in Table 2.

Table 2. Correlation between cybersecurity investment and customer trust in South African SMEs

Construct A	Construct B	Pearson's correlation (r)	p-value
Cybersecurity Investment	Customer Trust	.312**	< .0005

Note: Correlation is significant at the 0.01 level (2-tailed).

Table 2 shows that among South African SMEs, cybersecurity investment and customer trust are positively and statistically significantly correlated ($r = 0.312$, $p < .0005$). This indicates that SMEs that devote more financial and strategic resources to cyber-safe security, such as data encryption systems, intrusion detection software, secure payment gateways, employee cyber-awareness training, and adherence to the POPIA, tend to foster greater levels of customer trust. In essence, cybersecurity turns into an obvious indicator of an organization's dependability and dedication to protecting client information.

In South Africa, where cybercrime has increased dramatically over the past ten years, this relationship is especially significant. According to reports from the South African Banking Risk Information Centre (2025), SMEs are increasingly being targeted because of their relatively weak cybersecurity defenses, making South Africa one of the nations with the highest number of cyberattacks in Africa. Customers are now more sensitive to concerns about identity theft, online fraud, and privacy as a result. Nowadays, customers are more wary when doing business with small companies, particularly internet merchants, SMEs involved in fintech, and service-oriented businesses that handle personal data. As a result, better cybersecurity procedures not only increase perceived safety but

Table 3. Linear regression – Cybersecurity investment and customer trust

Variables in the Equation	B	Beta	T	p-value	R ²	F	df
Constant	9.214		5.031	< .0005	0.097	12.441	1; 148
Cybersecurity Investment	.528	.312	3.528	< .05			

Note: DV – Customer Trust. Predictor – Cybersecurity Investment.

also strengthen professionalism, legitimacy, and organizational credibility, all of which are essential for fostering trust in cutthroat markets.

To determine how much cybersecurity investment predicts customer trust, a regression analysis was carried out after the correlation analysis.

According to the regression analysis (Table 3), cybersecurity investment accounts for 9.7% of the variation in customer trust levels among South African SMEs, with an R^2 value of 0.097. Although this may seem insignificant at first, it has significance in behavioral and social science research, where a variety of factors, including service quality, pricing, reputation, brand engagement, and customer experience, influence customer trust. In South Africa's increasingly digitalized market environment, cybersecurity investment is becoming increasingly important, as it accounts for nearly 10% of customers' trust decisions. $F(1,148) = 12.441$, $p < .05$, which supports the model's overall significance, indicates that cybersecurity investment is a statistically and practically significant predictor of customer trust rather than an incidental or peripheral factor.

Additionally, the positive regression coefficient ($B = 0.528$, $p < .05$) indicates that each small increase in cybersecurity spending, technological advancements, or enhancements to digital security procedures results in a measurable increase in customer trust. This implies that consumers actively interpret visible cybersecurity features as signs of a company's dependability, such as encrypted communication, secure payment badges, POPIA compliance statements, and verified website security certificates. To put it another way, cybersecurity influences consumer perceptions in ways that go beyond conventional elements like service effectiveness or product quality. South African consumers' expectations of digital security become entwined with their willingness to transact with SMEs as they become more conscious of data breaches, SIM-swap fraud, phishing scams, and financial cybercrime.

4. DISCUSSION

This study examined whether cybersecurity investment contributes to customer trust among South African SMEs. The empirical results reveal a positive and statistically significant relationship between cybersecurity investment and customer trust ($r = 0.312$, $p < 0.001$). The regression analysis further indicates that cybersecurity investment significantly predicts customer trust ($B = 0.528$, $p < 0.05$) and explains 9.7% of the variance in customer trust ($R^2 = 0.097$). These findings indicate that SMEs allocating greater resources to cybersecurity tend to experience higher levels of customer trust. In practical terms, investments in secure payment systems, encryption technologies, compliance with the Protection of Personal Information Act (POPIA), and cybersecurity awareness practices appear to strengthen customer confidence in digital transactions with SMEs.

This finding is consistent with signaling theory, which suggests that visible organizational commitments reduce information asymmetry and enhance stakeholder confidence (Connelly et al., 2011; Msomi & Olarewaju, 2021). In digital markets where customers cannot directly observe internal security practices, cybersecurity measures serve as signals that firms are capable of protecting sensitive data and maintaining safe digital environments. The results, therefore, suggest that cybersecurity investments function not only as protective mechanisms but also as trust-building signals that influence customer perceptions of reliability and professionalism.

The findings are consistent with previous empirical research demonstrating that security assurance mechanisms positively influence customer trust in digital environments. For example, Bélanger et al. (2002) found that visible e-commerce security features significantly enhance consumer trust and purchase intentions. Similarly, Sassi et al. (2022) reported that perceived structural assurances and

security mechanisms are critical determinants of online trust formation. The present study confirms these relationships within the context of South African SMEs, thereby extending prior research that has largely focused on large organizations or developed economies.

The results also align with regional studies examining cybersecurity practices in African SMEs. Sang (2023) observed that South African e-commerce SMEs implementing security controls such as SSL certification and transparent privacy policies reported higher levels of customer trust. Likewise, Khoza and Hoeyi (2025) found that cybersecurity readiness among African SMEs is positively associated with customer retention and willingness to share personal information. The current findings, therefore, reinforce existing evidence that cybersecurity capabilities contribute to trust-building within digitally enabled business environments.

However, the magnitude of the relationship observed in this study differs somewhat from that reported by Noutchie (2025), who found a weaker association between cybersecurity investment and customer trust in informal township-based SMEs. One possible explanation for this difference is the level of digital integration. In highly digitized SMEs, customers interact primarily through online systems, making security assurances more salient for trust formation. In contrast, in less digitized or informal business environments, trust may be shaped more strongly by interpersonal relationships, price sensitivity, or convenience rather than digital security mechanisms.

The regression results also indicate that cybersecurity investment explains 9.7% of the variance in customer trust, suggesting that while cybersecurity plays a meaningful role in shaping trust, it is not the sole determinant. This finding is consistent with prior research indicating that trust is a multi-dimensional construct influenced by sev-

eral factors beyond security. For instance, Zhang et al. (2023) report that perceived security significantly contributes to online trust but interacts with factors such as service quality and user experience. Similarly, Jones (2026) found that cybersecurity readiness influences consumer trust among SMEs in Asia-Pacific contexts but operates alongside other relational and experiential drivers. The present results, therefore, support the interpretation that cybersecurity investment represents one important component of a broader trust-building framework.

An additional insight emerging from the descriptive results concerns the comparatively lower adoption of employee cybersecurity training among SMEs. While many firms appear to prioritize technical safeguards such as secure payment systems and encryption, behavioral cybersecurity practices receive comparatively less emphasis. This observation is consistent with Parsons et al. (2017), who highlight that human error remains a major contributor to cybersecurity incidents in small organizations. Limited investment in employee awareness programs may, therefore, constrain the full trust-enhancing potential of cybersecurity strategies. Strengthening human-centered security practices could enhance both the protective and perceptual benefits of cybersecurity investment.

In the South African context, the importance of cybersecurity investment may also be influenced by an increasingly regulatory and risk-laden environment. The implementation of the POPIA has increased organizational responsibility for safeguarding personal data. SMEs that visibly comply with these regulatory requirements may, therefore, differentiate themselves as trustworthy custodians of customer information. As digital commerce continues to expand across South Africa, cybersecurity investment is likely to become an increasingly important determinant of SME competitiveness and customer trust.

CONCLUSION

The purpose of this study was to examine the relationship between cybersecurity investment and customer trust among SMEs in South Africa. The empirical results demonstrate a positive and statistically significant relationship between cybersecurity investment and customer trust. Regression analysis further indicates that cybersecurity investment significantly predicts customer trust, suggesting that SMEs

investing more in cybersecurity tend to experience higher levels of customer confidence. Specifically, practices such as data encryption, secure payment systems, POPIA compliance, and employee cyber-awareness initiatives were associated with stronger perceptions of trust and digital reliability among customers. Several conclusions follow from these findings. First, cybersecurity investment should be viewed not only as a technical safeguard but also as a strategic trust-building mechanism that signals reliability and responsible data protection to customers. Second, SMEs that demonstrate a visible commitment to cybersecurity may strengthen their competitive position in digital markets by reducing perceived transaction risks and enhancing brand credibility. Third, while cybersecurity investment contributes significantly to customer trust, it explains only part of the overall trust formation process, indicating that SMEs should complement cybersecurity initiatives with broader strategies related to service quality, customer experience, and reputation management. Finally, the comparatively lower emphasis on employee cybersecurity training suggests that strengthening human-centered security practices could further enhance the protective and reputational benefits of cybersecurity investment within SMEs.

AUTHOR CONTRIBUTIONS

Conceptualization: Thabiso Sthembiso Msomi, Nomfundo Kuhlekonke Minenhle Nxumalo.
 Data curation: Thabiso Sthembiso Msomi.
 Formal analysis: Thabiso Sthembiso Msomi, Nomfundo Kuhlekonke Minenhle Nxumalo.
 Funding acquisition: Thabiso Sthembiso Msomi.
 Investigation: Thabiso Sthembiso Msomi, Nomfundo Kuhlekonke Minenhle Nxumalo.
 Methodology: Thabiso Sthembiso Msomi, Nomfundo Kuhlekonke Minenhle Nxumalo.
 Project administration: Thabiso Sthembiso Msomi, Nomfundo Kuhlekonke Minenhle Nxumalo.
 Resources: Thabiso Sthembiso Msomi.
 Software: Thabiso Sthembiso Msomi.
 Supervision: Thabiso Sthembiso Msomi.
 Validation: Thabiso Sthembiso Msomi, Nomfundo Kuhlekonke Minenhle Nxumalo.
 Visualization: Thabiso Sthembiso Msomi, Nomfundo Kuhlekonke Minenhle Nxumalo.
 Writing – original draft: Thabiso Sthembiso Msomi, Nomfundo Kuhlekonke Minenhle Nxumalo.
 Writing – review & editing: Thabiso Sthembiso Msomi, Nomfundo Kuhlekonke Minenhle Nxumalo.

REFERENCES

- Adelusi, B. S., Ojika, F. U., & Uzoka, A. C. (2022). Advances in cybersecurity strategy and cloud infrastructure protection for SMEs in emerging markets. *Journal of Frontiers in Multidisciplinary Research*, 3(1), 467-482. <https://doi.org/10.54660/JFMR.2022.3.1.467-482>
- Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98, Article 102003. <https://doi.org/10.1016/j.cose.2020.102003>
- Anukoonwattaka, W., Romao, P., Bhogal, P., Bentze, T., & Lobo, R. S. (2021). *Digital economy integration in Asia and the Pacific: Insights from DigiSRII 1.0* (ARTNeT Working Paper Series No. 208). Asia-Pacific Research and Training Network on Trade. Retrieved from <https://artnet.unescap.org/index.php/publications/working-papers/digital-economy-integration-asia-and-pacific-insights-digisrii-10>
- Awad, J. A., & Martín-Rojas, R. (2024). Digital transformation influences organisational resilience through organisational learning and innovation. *Journal of Innovation and Entrepreneurship*, 13(1), Article 69. <https://doi.org/10.1186/s13731-024-00405-4>
- Bada, A., Sasse, M. A., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *Cryptography and Security*. <https://doi.org/10.48550/arXiv.1901.02672>
- Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security*, 27(3), 393-410. <https://doi.org/10.1108/ICS-07-2018-0080>
- Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management*, 51(1), 138-151. <https://doi.org/10.1016/j.im.2013.11.004>
- Bélanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in

- electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, 11(3-4), 245-270. [https://doi.org/10.1016/S0963-8687\(02\)00018-5](https://doi.org/10.1016/S0963-8687(02)00018-5)
9. Brodin, M. (2019). A framework for GDPR compliance for small- and medium-sized enterprises. *European Journal for Security Research*, 4(2), 243-264. <https://doi.org/10.1007/s41125-019-00042-z>
 10. Cao, C., & Huang, S. (2022). How can SMEs boost trust through third-party means? Tracing the multidimensional institutional basis of online trust. *IEEE Access*, 10, 127149-127167. <https://doi.org/10.1109/ACCESS.2022.3226889>
 11. Cegarra-Navarro, J. G., Soto-Acosta, P., & Wensley, A. (2014). Structured knowledge processes and firm performance: The role of organizational agility. *Journal of Business Research*, 69(5), 1544-1549. <https://doi.org/10.1016/j.jbusres.2015.10.014>
 12. Cheng, L., & Nasirov, J. (2025). Promoting trust and security in the digital domain: A discourse analysis of legal constructs. *International Journal of Legal Discourse*, 10(1), 13-34. <https://doi.org/10.1515/ijld-2025-2003>
 13. Cochran, W. G. (1977). *Sampling techniques* (3rd ed.). John Wiley & Sons. Retrieved from <https://www.wiley.com/en-us/Sampling%2BTechniques%2C%2B3rd%2BEdition-p-9780471162407>
 14. Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R. (2011). Signaling theory: A review and assessment. *Journal of Management*, 37(1), 39-67. <https://doi.org/10.1177/0149206310388419>
 15. Council for Scientific and Industrial Research. (2024, October 8). *CSIR issues national survey results on the state of cybersecurity in South Africa*. Retrieved from <https://www.csir.co.za/csir-issues-national-survey-results-on-state-cybersecurity-south-africa>
 16. Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications. Retrieved from https://www.ucg.ac.me/skladiste/blog_609332/objava_105202/fajlovi/Creswell.pdf
 17. Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). *Internet, phone, mail, and mixed-mode surveys: The tailored design method* (4th ed.). John Wiley & Sons. <https://doi.org/10.1002/9781394260645>
 18. Flores, W. R., Holm, H., Nohlberg, M., & Ekstedt, M. (2015). Investigating personal determinants of phishing and the effect of national culture. *Information & Computer Security*, 23(2), 178-199. <https://doi.org/10.1108/ICS-05-2014-0029>
 19. Hsu, C., Lee, J. N., & Straub, D. W. (2012). Institutional influences on information systems security innovations. *Information Systems Research*, 23(3), 918-939. Retrieved from <https://www.jstor.org/stable/23274653>
 20. Jones, C. A. M. (2026). The foundation of digital trust. In *Advancing IT interoperability and trade facilitation in Southeast Asia* (pp. 295-324). Singapore: Palgrave Macmillan. https://doi.org/10.1007/978-981-95-3660-3_8
 21. Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, 28(3), 269-282. <https://doi.org/10.1080/10919392.2018.1484598>
 22. Karadağ, H., Sahin, F., & Matemane, R. (2023). Disentangling the innovation orientation, intellectual capital, and dynamic innovation capability relationships in emerging economy start-ups. *International Journal of Innovation Management*, 27(7-8), Article 2350039. <https://doi.org/10.1142/S1363919623500391>
 23. Khoza, N. G., & Hoeyi, P. (2025). Cyber security preparedness among SMMEs in the digital economy. *African Journal of Innovation & Entrepreneurship*, 4(3), 71-96. <https://doi.org/10.31920/2753-314X/2025/v4n3a4>
 24. Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2), 77-81. <https://doi.org/10.1080/1097198X.2019.1603527>
 25. Likert, R. (1932). A technique for the measurement of attitudes. *Archives of Psychology*, 22(140), 1-55. Retrieved from https://legacy.vote-view.com/pdf/Likert_1932.pdf
 26. Maharaj, A., & Msomi, T. S. (2026). The effect of strategic planning on operational efficiency in South African SMEs. *Problems and Perspectives in Management*, 24(1), 578-588. [https://doi.org/10.21511/ppm.24\(1\).2026.38](https://doi.org/10.21511/ppm.24(1).2026.38)
 27. Mofokeng, T. E. (2023). Antecedents of trust and customer loyalty in online shopping: The moderating effects of online shopping experience and e-shopping spending. *Heliyon*, 9(5), Article e16182. <https://doi.org/10.1016/j.heliyon.2023.e16182>
 28. Msomi, T. S., & Ngcobo, N. G. (2023). Monetary access and survival of small and medium-sized enterprises in South Africa post-COVID-19 era. *Problems and Perspectives in Management*, 21(3), 351-360. [https://doi.org/10.21511/ppm.21\(3\).2023.28](https://doi.org/10.21511/ppm.21(3).2023.28)
 29. Msomi, T. S., & Olarewaju, O. M. (2021). Does financial literacy and access to finance impact the viability of small- and medium-sized enterprises in South Africa? In *Proceedings of the 6th International Conference on Governance and Accountability (ICGA 2021)* (pp. 9-13). Retrieved from <https://ir.unimas.my/id/eprint/35194/1/Kit%20Yeng.pdf>
 30. Noutchie, S. C. O. (2025). Unlocking SME potential through digital platforms: Insights from three African digital economies. *International Journal of Business Ecosystem & Strategy*, 7(4), 106-112. <https://doi.org/10.36096/ijbes.v7i4.859>
 31. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-

- Q). *Computers & Security*, 42, 165-176. <https://doi.org/10.1016/j.cose.2013.12.003>
32. Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organizational Cybersecurity Journal: Practice, Process and People*, 1(1), 24-46. <https://doi.org/10.1108/O CJ-03-2021-0004>
33. Rizomyliotis, I. (2026). Consumer trust and online purchase intention for sustainable products. *American Behavioral Scientist*, 70(5), 706-724. <https://doi.org/10.1177/00027642241236174>
34. Sang, K. (2023). *Cybersecurity assessment model for small and medium enterprises (SMEs) e-commerce in Kenya* (Master's Thesis). KCA University. Retrieved from <https://repository.kcau.ac.ke/handle/123456789/1527>
35. Santos, M. P., & Berssaneti, F. T. (2024). Impacts of technological innovation on product and service quality and sustainable financial, environmental and social results in the aeronautics sector: A Brazilian case study. *Sustainability*, 16(8), Article 3476. <https://doi.org/10.3390/su16083476>
36. Sassi, Sahli A., Hammami, H., & Ben Lallouna Hafsia, H. (2022). Perceived risk, structural assurance and trust in mobile payments. *Journal of Telecommunications and the Digital Economy*, 10(4), 41-56. <https://doi.org/10.18080/jtde.v10n4.619>
37. Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed.). Pearson Education. Retrieved from <https://www.pearson.com/en-gb/subject-catalog/p/research-methods-for-business-students/P200000003197>
38. Segotso, T., Mvunabandi, J. D., & Phesa, M. (2024). A systematic literature review of the challenges of adopting and implementing IFRS for SMEs in South Africa. *International Journal of Economics and Financial Issues*, 14(5), 131-147. <https://doi.org/10.32479/ijefi.16133>
39. Sema, G. G., Owolawi, P. A., & Olugbara, O. O. (2025). Protection of Personal Information Act in practice: A systematic synthesis of research trends, sectoral applications, and implementation barriers in South Africa. *Sustainability*, 17(19), Article 8529. <https://doi.org/10.3390/su17198529>
40. South African Banking Risk Information Centre. (2025, August 28). *Media statement: SABRIC annual crime statistics 2024*. Retrieved from <https://www.sabric.co.za/media-statement-sabric-annual-crime-statistics-2024/>
41. Zhang, R., Jun, M., & Palacios, S. (2023). M-shopping service quality dimensions and their effects on customer trust and loyalty: An empirical study. *International Journal of Quality & Reliability Management*, 40(1), 169-191. <https://doi.org/10.1108/IJQRM-11-2020-0374>