Global Journal of Computer Science and Technology: G
Interdisciplinary
Volume 25 Issue 1 Version 1.0 Year 2025
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Assessing Cybersecurity Response Readiness and Return on Security Investment Strategies among SMEs in Ecuador

By Franklin Orellana

Abstract- Cybersecurity remains a pressing concern for small and medium-sized enterprises (SMEs), particularly in developing nations where cultural, structural, and leadership barriers hinder proactive security adoption. This study investigates the unique organizational and national culture dynamics influencing cybersecurity behaviors in Ecuadorian SMEs, exploring how leadership traits, risk perception, and employee attitudes impact cybersecurity readiness through qualitative interviews with SME leaders across multiple sectors. Using analytical frameworks such as Hofstede's cultural dimensions, McClelland's motivation theory, and dialectical organizational theory, the research identifies five primary themes: symbolic implementation of cybersecurity policies, low formalization of risk response mechanisms, lack of return-on-investment frameworks, leadership styles that either support or hinder risk planning, and widespread resistance to behavioral change. Despite increasing exposure to cyber threats, many SMEs remain reactive rather than strategic, often lacking formal policies, employee training, or incident response plans. Leadership personality traits play a significant role in shaping organizational prioritization of cybersecurity, with achievement-oriented leaders driving more effective strategies.

Keywords: cybersecurity culture, ecuadorian smes, leadership behavior, organizational change, hofstede dimensions, risk management, mcclelland motivation theory, digital transformation.

GJCST-G Classification: LCC : HD2346.E2

ASSESSINGCYBERSECURITYRESPONSEREADINESSANDRETURNONSECURITYINVESTMENTSTRATEGIESAMONGSMESINECUADOR

Strictly as per the compliance and regulations of:

Open Association of Research Society, USA
Research | Diversity | Ethics

© 2025. Franklin Orellana. This research/review article is distributed under the terms of the Attribution-NonCommercial-No Derivatives 4.0 International (CC BYNCND 4.0). You must give appropriate credit to authors and reference this article if parts of the article are reproduced in any manner. Applicable licensing terms are at https://creativecommons.org/licenses/by-nc-nd/4.0/.

Assessing Cybersecurity Response Readiness and Return on Security Investment Strategies among SMEs in Ecuador

Franklin Orellana

Abstract- Cybersecurity remains a pressing concern for small and medium-sized enterprises (SMEs), particularly in developing nations where cultural, structural, and leadership barriers hinder proactive security adoption. This study investigates the unique organizational and national culture dynamics influencing cybersecurity behaviors in Ecuadorian SMEs, exploring how leadership traits, risk perception, and employee attitudes impact cybersecurity readiness through qualitative interviews with SME leaders across multiple sectors. Using analytical frameworks such as Hofstede's cultural dimensions, McClelland's motivation theory, and dialectical organizational theory, the research identifies five primary themes: symbolic implementation of cybersecurity policies, low formalization of risk response mechanisms, lack of return-on-investment frameworks, leadership styles that either support or hinder risk planning, and widespread resistance to behavioral change. Despite increasing exposure to cyber threats, many SMEs remain reactive rather than strategic, often lacking formal policies, employee training, or incident response plans. Leadership personality traits play a significant role in shaping organizational prioritization of cybersecurity, with achievement-oriented leaders driving more effective strategies. The study concludes that improving cybersecurity in Ecuadorian SMEs requires a multi-faceted approach involving cultural transformation, leadership development, and localized application of global standards. National campaigns, leadership training, stronger CSIRT partnerships, and practical tools like ROI calculators are essential to advancing digital resilience. This research provides an evidence-based framework for policymakers, educators, and business leaders aiming to enhance cybersecurity practices within the specific constraints of Latin American SMEs, recommending future exploration of industry-specific adaptations and scalable public-private partnerships to foster sustained cyber readiness.

Keywords: cybersecurity culture, ecuadorian smes, leadership behavior, organizational change, hofstede dimensions, risk management, mcclelland motivation theory, digital transformation.

I. Introduction

In today's digital economy, small and medium-sized enterprises (SMEs) represent both engines of economic growth and primary targets for cybercriminals. Globally, SMEs face considerable risks due to limited resources, outdated infrastructure, and a lack of cybersecurity awareness. According to the 2020 Verizon Data Breach Investigations Report, 28% of data breaches involved small businesses [1]. These organizations often perceive themselves as unlikely targets, a misconception that renders them especially vulnerable. Recent research confirms that SMEs in emerging markets are disproportionately affected by cyberattacks due to inadequate security postures [8].

Ecuador, a developing country in South America, has experienced significant technological transformation across its business sectors. As SMEs rapidly digitize, they increasingly depend on cloud computing, mobile platforms, and digital payment systems. However, this transition has not been matched with proportional cybersecurity investments or risk management practices. A 2018 study by the Inter-American Development Bank (IDB) and the Organization of American States (OAS) found that most Latin American countries lack robust cybersecurity strategies, and Ecuador scored below regional averages in policy implementation and public-private collaboration [2].This gap has been corroborated by more recent regional cybersecurity assessments highlighting persistent challenges in governance and resource allocation [15].

The importance of establishing a robust cybersecurity culture cannot be overstated. Numerous international studies have shown that organizational culture significantly influences the effectiveness of cybersecurity policies and practices [3, 4]. For SMEs in developing economies, cultivating a proactive security culture often depends on leadership engagement, employee behavior, and industry-specific awareness campaigns [11]. In Ecuador, however, SMEs often operate within informal structures and may lack dedicated IT departments or cybersecurity personnel, complicating the institutionalization of good practices.

As cybersecurity threats continue to evolve, the cost of neglect becomes increasingly detrimental. Reports from regional security organizations such as CSIRT Ecuador and the Latin American Federation of Information Security Professionals (FLISI) reveal that more than 60% of SME attacks go unreported or unresolved due to a lack of internal capacity [5]. With economic recovery post-pandemic relying heavily on digital operations, cyber resilience is no longer optional. Recent case studies in Latin America underscore the urgency of improving incident response readiness in SMEs to mitigate financial and reputational damage [13].

Author: e-mail: franklin_orellana@hotmail.com

© 2025 Global Journals

Beyond institutional weaknesses, cultural barriers also play a significant role. Drawing upon Hofstede's cultural dimensions, Ecuador scores high on power distance and uncertainty avoidance, which can lead to centralized decision-making and a fear of admitting vulnerabilities [6]. These factors make it more difficult to implement open cybersecurity training and transparent incident response systems. Furthermore, McClelland's achievement motivation theory [7] suggests that in environments where affiliation and security are prioritized over innovation and risk-taking, cybersecurity preparedness may take a backseat [12].

Dialectical organizational theory [8] adds further insight by describing how internal contradictions within SMEs* such as wanting digital transformation without associated security costs-can lead to ineffective or fragmented implementation strategies. Thus, to effectively address cybersecurity in Ecuadorian SMEs, one must examine not just the technical readiness but also the cultural ecosystem shaping those decisions.

This article investigates the state of cybersecurity culture and incident response readiness within Ecuadorian SMEs. Drawing from a qualitative study conducted for a doctoral dissertation, the paper analyzes cultural and organizational barriers using frameworks. These theories provide critical lenses to understand the behaviors, attitudes, and structural limitations influencing cybersecurity practices in the Ecuadorian context.

The Research is Guided by three Primary Objectives:

1. To explore how cultural norms affect incident response planning.
2. To evaluate the cybersecurity leadership styles present in Ecuadorian SMEs.
3. To recommend strategic actions for enhancing cybersecurity resilience.

Informed by 50 in-depth interviews with IT professionals, business owners, and cybersecurity consultants across Ecuador, this study identifies gaps in awareness, leadership, training, and policy alignment. Ultimately, it proposes a culturally adaptive framework for SME cybersecurity improvement. The findings underscore the importance of aligning global best practices with local cultural dynamics to promote a resilient cybersecurity posture across Ecuador's SME landscape.

The introduction of cybersecurity strategies that are not only technically proficient but also culturally awareness is critical in mitigating risks and building long-term resilience. By contextualizing these strategies within Ecuador's unique sociocultural and organizational fabric, stakeholders can foster meaningful engagement, sustainable training programs, and leadership structures that support a collective security mindset. As this article demonstrates, bridging the gap between global standards and local capabilities requires both empirical insight and theoretical grounding.

II. Materials and Methods

a) Research Design

A qualitative, phenomenological research approach was employed to capture the lived experiences of cybersecurity professionals and SME leaders in Ecuador. The study was interpretive in nature, allowing for deep exploration of cultural and organizational phenomena related to cybersecurity. This method was selected due to its capacity to extract nuanced insights into the social constructs that influence incident response behaviors [1]. Phenomenology provides a framework for under-standing subjective perspectives, which are essential when evaluating how cultural norms influence professional decision-making.

This design also aligns with Creswell and Poth's recommendations for research involving complex social behaviors in culturally distinct environments [9]. The focus was not just on gathering descriptive data but on interpreting how participants assign meaning to their cybersecurity-related practices. This approach was particularly valuable in understanding how deeply embedded cultural values manifest in everyday IT operations and decision-making processes.

Additionally, interpretive design enabled the researcher to interact with multiple layers of context, considering not just participant responses but also underlying motivations and systemic constraints. The methodology allowed for iterative reflection and the generation of emergent themes that would be inaccessible through a purely quantitative approach. The choice of this design underscores the study's emphasis on contextual understanding rather than generalizability.

b) Participants

Fifty participants were recruited via purposive sampling from professional LinkedIn networks and cybersecurity forums in Ecuador. Criteria included being a cybersecurity officer, IT manager, business owner, or consultant affiliated with an SME (defined as having fewer than 250 employees). These individuals represented diverse sectors, including healthcare, logistics, retail, and manufacturing. The demographic distribution included 36 males and 14 females, aged between 28 and 60. Most participants held at least a bachelor's degree, and 38% had formal training in IT or cybersecurity.

To increase representativeness, stratified purposive sampling was used to ensure coverage of both coastal and highland regions in Ecuador, acknowledging regional differences in business culture.

This helped reduce location bias and revealed interesting contrasts in cybersecurity preparedness

© 2025 Global Journals

between urban and rural businesses. The stratification ensured that the findings reflect a broad spectrum of organizational experiences, from relatively advanced SMEs in Quito to more resource-constrained enterprises in rural provinces.

Participants also differed in organizational roles, with some holding strategic decision-making power while others were responsible for daily IT operations. This range enabled the study to explore how cybersecurity culture is experienced differently across hierarchical levels, adding richness to the data set.

c) *Data Collection Tools*

Data was gathered through semi-structured electronic questionnaires and follow-up interviews via Zoom. Questions focused on cybersecurity policies, incident response planning, cultural practices, leadership attitudes, and ROI perceptions related to cybersecurity investments. The semi-structured format ensured that core topics were addressed while allowing flexibility to probe deeper into emergent issues. Interviews were conducted in Spanish and translated into English for analysis, ensuring fidelity to cultural nuance.

The questionnaire consisted of 20 main items, categorized under five themes: organizational culture, incident response capabilities, leadership, employee engagement, and perceived risks. Probing questions allowed researchers to explore individual perspectives more deeply, especially in cases of conflicting or unclear responses.

Participants were encouraged to share anecdotes and real-life incidents, enriching the data with contextually grounded examples. The dual-stage data collection-questionnaire followed by interview-allowed for initial thematic mapping and subsequent deep dives, enhancing both reliability and interpretive depth.

d) *Analytical Method*

Thematic coding was conducted using Maxqda software. Codes were derived from both theory and emergent data. The themes were categorized under cultural, technical, and strategic domains. Coding reliability was ensured through inter-coder agreement and iterative refinement [1]. The thematic analysis involved open coding, axial coding, and selective coding, with peer debriefing sessions held to verify interpretations. Member checking and triangulation with secondary data sources improved internal validity, while researcher reflexivity reduced bias.

Coding was guided by a codebook developed in alignment with the research questions and theoretical frameworks. Examples of key codes included "risk normalization," "top-down decision-making," "training gaps," and "cost avoidance." Patterns were compared across sectors to identify variations in cybersecurity readiness and culture.

Further analysis included comparison matrices and conceptual mapping to identify key patterns and contradictions in the data. These techniques illuminated how organizational behaviors are shaped not only by policies but also by deeply rooted cultural assumptions and economic constraints.

e) *Ethical Considerations*

IRB approval was obtained from Northcentral University. Participants provided informed consent. Data was anonymized to protect confidentiality. Ethical considerations also included safeguarding digital files through encrypted storage and limiting access to research personnel. Participants were informed of their right to withdraw at any point without consequence. No financial incentives were offered to maintain voluntary participation.

Confidentiality agreements were explained verbally and in writing before interviews. Participants were given the opportunity to review their transcripts before inclusion in the final analysis, in accordance with best practices in qualitative ethics [1].

The ethical safeguards applied were consistent with the Belmont Report principles of respect for persons, beneficence, and justice. The dual-language process of interview transcription and translation was conducted with special care to preserve intent, tone, and cultural context. Data will be retained in encrypted storage for a period of five years before permanent deletion.

III. Results

a) *Organizational Culture*

Participants frequently described informal workplace environments where cybersecurity policies were either lacking or symbolic. In many cases, leadership decisions were guided more by interpersonal dynamics than by formal procedures or evidence-based protocols. The lack of structure resulted in inconsistencies in how security measures were communicated and implemented. Several respondents mentioned that cybersecurity was perceived as a peripheral concern rather than a core business function. A high degree of hierarchical deference was observed, consistent with Hofstede's high power distance index for Ecuador [5]. This often translated into unquestioned top-down decision-making, where employees did not feel empowered to raise concerns about digital security or suggest improvements. Despite some organizations having documented policies, many reported that these policies were rarely enforced, seldom updated, and not understood by the broader employee base. Interviews revealed that while some SMEs attempted to implement cybersecurity policies to meet basic compliance standards, the lack of internal awareness and training rendered these efforts largely ineffective [10].

b) *Risk Perception and Response Readiness*

Despite the rise in cyberattacks targeting Latin America, including high-profile cases of ransomware and phishing attacks, only 14% of participants reported having a documented incident response plan. The remainder relied on informal, ad hoc responses to incidents, often driven by panic or improvisation rather than strategic planning. This lack of preparedness was linked to multiple factors, including a general underestimation of risk, resource limitations, and a cultural inclination toward short-term crisis management rather than long-term planning. Many SMEs lacked even basic cybersecurity hygiene measures, such as multi-factor authentication, access control logs, or password rotation protocols. Several participants admitted that cybersecurity only became a priority after a significant breach or financial loss. This reactive posture placed companies at continuous risk and further delayed the institutionalization of preventive practices. In addition, the absence of formal threat modeling or vulnerability assessments limited the organizations' capacity to respond to new and emerging threats [13].

c) *ROI on Cybersecurity Investments*

Discussions around Return on Security Investment (ROSI) were largely absent among participants. Most indicated that cybersecurity was not seen by senior leadership as a value-adding activity or a competitive differentiator, but rather as a cost to be minimized. Budget allocation for cybersecurity was often limited, and funding was typically redirected toward revenue-generating functions. This sentiment was especially strong in family-owned SMEs, where financial decisions were centralized and conservative. Only those who had previously suffered a cybersecurity breach showed a noticeable shift toward proactive investment. A recurring theme in the interviews was the difficulty of articulating the financial value of preventive cybersecurity to non-technical leadership. Without clear metrics or risk quantification models, it was challenging to justify ongoing investments. As a result, many SMEs fell into a cycle of reactive spending-addressing breaches as they occurred rather than preparing for them in advance [13].

d) *Leadership Styles*

Drawing from McClelland's Human Motivation Theory, many leaders were characterized by high levels of "power motivation." These individuals exhibited a preference for control and centralization, often resisting the delegation of cybersecurity responsibilities. This leadership style correlated with minimal investment in training and limited adoption of decentralized cybersecurity protocols. Conversely, leaders who demonstrated "achievement motivation" were more open to adopting structured cybersecurity programs, implementing audits, and engaging external experts [6]. However, such leadership was less common. A significant challenge identified was leadership turnover, which disrupted the continuity of cybersecurity initiatives. Furthermore, many SME leaders lacked formal managerial or IT training, limiting their ability to understand or prioritize complex cybersecurity issues. This leadership gap contributed to inconsistent security practices and low organizational commitment to resilience-building strategies [12].

e) *Cultural Resistance to Change*

Employees frequently resisted changes to established workflows, particularly when new security measures were perceived as inconvenient. For example, several SMEs struggled to implement two-factor authentication or enforce VPN usage due to push back from staff. The preference for convenience over security was a recurring pattern, which some participants attributed to Ecuador's relatively low score in uncertainty avoidance [5]. This cultural trait may foster adaptability in some contexts but can undermine efforts to implement strict security protocols. Training programs, where available, were often limited in scope, lacked follow-up assessments, and failed to engage employees meaningfully. Informal work environments reinforced this complacency, often trivializing cybersecurity threats as exaggerated or unlikely. Peer influence played a strong role, with some employees adopting lax security behaviors modeled by their colleagues or supervisors [15].

f) *External Collaboration*

Only five SMEs in the sample had active partnerships with national or regional Computer Security Incident Response Teams (CSIRTs). The vast majority were either unaware of such resources or expressed skepticism regarding the effectiveness of public sector initiatives. This disconnect represents a significant missed opportunity for knowledge sharing, threat intelligence, and incident support. Interviews revealed a general mistrust in government-led cybersecurity programs, often citing bureaucracy, slow response times, and lack of confidentiality as barriers to collaboration. Some participants also mentioned the absence of clear incentives for engaging with CSIRTs, such as subsidized training or compliance benefits. Those who had established partnerships reported more structured incident response capabilities and access to valuable threat intelligence. Strengthening public-private collaboration emerged as a critical area for improvement, requiring both policy reform and trust-building campaigns to encourage greater SME participation in national cybersecurity efforts [15].

IV. Discussion

The findings reflect a pattern of cultural inertia and leadership disconnect that impedes cybersecurity progress in Ecuadorian SMEs. The application of

Hofstede's dimensions elucidates key challenges: high power distance discourages bottom-up innovation, while low uncertainty avoidance normalizes security complacency[5]. These cultural patterns hinder the development of proactive risk management frameworks and instead perpetuate reactive behaviors across organizational levels. In environments where employees hesitate to question authority or raise concerns, vital cybersecurity gaps may remain unaddressed until a breach occurs.

McClelland's motivation framework reveals that cybersecurity effectiveness is tied not just to technical capacity but to the personality traits of organizational leaders [6]. Leaders driven by a need for power tend to centralize decision-making and neglect collaborative security planning, while those motivated by achievement promote innovation and strategic risk mitigation. These dynamic underscores the importance of leadership development as a key cybersecurity enabler. Leadership traits influence not only policy formation but also the allocation of resources, the pace of digital transformation, and the establishment of a security-conscious culture [11].

Dialectical organizational theory sheds light on the contradictory pressures SMEs face: rapid digital adoption vs. rigid traditional structures [7]. Many SMEs are trapped between the push for modernization and adherence to legacy workflows. This tension often results in superficial digital transformations that do not include robust cybersecurity planning. While SMEs may invest in new customer-facing technologies, backend infrastructure and staff training are often neglected. This imbalance creates a vulnerable surface for cyber threats.

While international standards like ISO 27001 offer robust guidelines, they often fail in Ecuador due to misalignment with local capabilities and values. Contextualized approaches that blend global best practices with culturally sensitive implementation are needed [1]. Training programs should be rooted in local languages, examples, and economic realities. For instance, cybersecurity literacy efforts must address the economic constraints of SMEs and present cybersecurity as a strategic necessity rather than a compliance checkbox. Locally adapted tools, such as simplified risk assessments and budget calculators, could facilitate broader adoption of effective security practices [14].

V. Conclusions

This research demonstrates that improving cybersecurity in Ecuadorian SMEs requires more than technical tools. A comprehensive approach must include cultural transformation, leadership development, and policy alignment. It is evident from the findings that SMEs are most vulnerable when they lack structured risk management plans, leadership buy-in, and sustained education on digital threats. Moreover, existing national and international support systems remain underutilized, reflecting a gap in outreach and trust-building.

The Study Recommends the Following actions:

- Launching nationwide cybersecurity literacy campaigns tailored to SME contexts
- Promoting leadership training that incorporates cybersecurity planning
- Enhancing CSIRT outreach and collaboration with SMEs through incentives and localized programs
- Developing localized ROI/ROSI calculators to justify and monitor cybersecurity spending

The findings emphasize the interplay between national culture, organizational behavior, and technological adaptation. Future studies should assess the longitudinal impact of these interventions and explore sector-specific adaptations in industries such as finance, education, and manufacturing. Furthermore, research should examine how policy changes and public-private partnerships can accelerate the diffusion of cybersecurity best practices. By fostering alignment between global standards and local needs, Ecuadorian SMEs can better prepare for the evolving threat landscape while sustaining operational growth.

Abbreviations

SME: Small and Medium-sized Enterprise

CSIRT: Computer Security Incident Response Team

ROI: Return on Investment

ROSI: Return on Security Investment

NIST: National Institute of Standards and Technology

IATF: Information Assurance Technical Framework

FISMA: Federal Information Security Management Act

IDB: Inter-American Development Bank

OAS: Organization of American States

FLISI: Latin American Federation of Information Security Professionals

VPN: Virtual Private Network

ISO: International Organization for Standardization

References Références Referencias

1. Verizon. 2020 Data Breach Investigations Report. Available from: https://enterprise.verizon.com/resources/reports/dbir/ (accessed 1 July 2024)
2. Inter-American Development Bank & Organization of American States. Cybersecurity: Risks, Progress, and the Way Forward in Latin America and the Caribbean. 2018. Available from: https://publications. iadb.org/en/cybersecurity-risks-progress-and-way-forward-latin-america-and-caribbean.
3. Gordon, L. A., Loeb, M. P., & Zhou, L. (2015). The impact of information security breaches: Has there been a downward shift in costs? Journal of Computer Security, 23(1), 1-23. https://doi.org/10.3233/JCS-140530

4. AlHogail, A. (2015). Improving information security culture through employee participation. International Journal of Information Management, 35(3), 345-351. https://doi.org/10.1016/j.ijinfomgt.2015.02.002
5. Hofstede, G. Dimensionalizing Cultures: The Hofstede Model in Context. Online Readings in Psychology and Culture, 2(1), 2011, 1-26.
6. McClelland, D. The Achieving Society. Princeton, NJ: Van Nostrand; 1961.
7. Montgomery, B., & Baxter, L. Dialectical Approaches to Studying Personal Relationships. In Handbook of Personal Relationships, Routledge, 1998.
8. Smith, J., & Kumar, R. (2022). Cybersecurity challenges and responses in small businesses: Evidence from developing countries. Computers & Security, 109, 102392.
9. Creswell, J., & Poth, C. (2018). Qualitative Inquiry and Research Design: Choosing Among Five Approaches (4th ed.). Sage.
10. Ahmed, S., & Lee, J. (2022). Quantifying cybersecurity investments: Bridging the gap for SME decision-makers. Journal of Cybersecurity Research, 8(1), 45-62.
11. Garcia, M., Santos, R., & Perez, L. (2021). Leadership styles and cybersecurity resilience in Latin American SMEs. International Journal of Information Security, 20(3), 289-303.
12. Liu, Y., & Fernandez, V. (2022). Transformational leadership as a catalyst for cybersecurity culture change in SMEs. Leadership Quarterly, 33(6), 101594.
13. Ocampo, D., Torres, M., & Lopez, C. (2023). Return on security investment models adapted for Latin American SMEs. Journal of Risk and Financial Management, 16(2), 87.
14. Patel, N., & Gomez, R. (2021). Localizing ISO 27001 for emerging economies: A cultural adaptation framework. Information Systems Frontiers, 23(5), 1211-1225.
15. Rodriguez, J., & Silva, T. (2023). Enhancing cybersecurity readiness in SMEs through collaborative governance: Lessons from Brazil and Mexico. Journal of Cyber Policy, 8(2), 180-196.

© 2025 Global Journals