Cybersecurity decision-making in ethnic minority-owned small businesses: Refining a socio-cultural framework through qualitative evidence

International Journal of Economics, Business and Management Studies
Vol. 13, No. 1, 55-82, 2026
e-ISSN: 2226-4809/p-ISSN: 2304-6945

Ali Salehi[1]
Hamed Motaghi[2]

(Corresponding Author)

[1,2]*Département of Administrative Sciences, University of Quebec in Outaouais, Québec, Canada.*
[1]*Email:* Ali.salehi@uqo.ca
[2]*Email:* hamed.motaghi@uqo.ca

ABSTRACT

Small and medium-sized enterprises (SMEs) face growing cybersecurity threats, yet existing research often overlooks the socio-cultural dynamics shaping decision-making, particularly in ethnic minority-owned businesses. This study examines how individual capabilities, social relationships, and contextual or cultural factors interact to influence cybersecurity behavior in these SMEs. The study draws on 20 semi-structured interviews with minority SME owners in Québec and applies an inductive thematic analysis to explore how cybersecurity decisions emerge from everyday business practices and experiences. The findings identify three interrelated domains that shape cybersecurity behavior: individual factors, including prior experience, digital literacy, and perceived risk; social factors, such as trust, community networks, and peer influence; and contextual or cultural factors, including language barriers, cultural norms, and access to institutional support. Building on these insights, the study proposes a refined socio-cultural framework that highlights the iterative, experience-driven, and socially embedded nature of cybersecurity decision-making in minority-owned SMEs. The findings also reveal that informal community networks can simultaneously facilitate learning and unintentionally normalize cybersecurity risks. These results suggest that cybersecurity interventions should move beyond purely technical or resource-based approaches and instead incorporate culturally sensitive, socially grounded, and context-aware strategies. Policymakers and support organizations should therefore design outreach programs, training initiatives, and advisory services that leverage trusted community networks and improve institutional accessibility for diverse entrepreneurs navigating digital risks.

Keywords: *Behavioral decision-making, Community networks, Cybersecurity, Ethnic minority entrepreneurs, Qualitative research, SMEs, Socio-cultural factors.*

DOI: 10.55284/ijebms.v13i1.1779

Citation | Salehi, A., & Motaghi, H. (2026). Cybersecurity decision-making in ethnic minority-owned small businesses: Refining a socio-cultural framework through qualitative evidence. *International Journal of Economics, Business and Management Studies, 13*(1), 55–82.

Funding: This study received no specific financial support.

Institutional Review Board Statement: This study received ethical approval from the Research Ethics Committee of *University of Quebec in Outaouais*, on 2024-04-26 under protocol number "2024-2640". Informed verbal and written consent was obtained from all participants, and all data were anonymized to ensure participant confidentiality.

Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Data Availability Statement: The corresponding author may provide study data upon reasonable request.

Competing Interests: The authors declare that they have no competing interests.

Authors' Contributions: Both authors contributed equally to the conception and design of the study. Both authors have read and agreed to the published version of the manuscript.

History: Received: 14 January 2026/ Revised: 25 February 2026/ Accepted: 2 March 2026/ Published: 18 March 2026

Publisher: Online Science Publishing

Highlights of this paper

- This study explores how individual, social, and cultural factors shape cybersecurity decisions in ethnic minority-owned SMEs.
- Findings reveal that individual capabilities, social networks, and contextual factors interact to influence cybersecurity behavior.
- A socio-cultural framework is proposed to guide culturally sensitive interventions supporting SMEs in managing digital risks.

1. INTRODUCTION

As digital technologies become integral to daily business operations, small and medium-sized enterprises (SMEs) face growing exposure to cybersecurity threats. Despite their critical economic role, SMEs often lack sufficient financial resources, technical expertise, and formal organizational structures, making them disproportionately vulnerable to cyber incidents (Anderson & Moore, 2006; European Union Agency for Cybersecurity (ENISA), 2021). Existing research has largely approached SME cybersecurity as a technical or managerial challenge, emphasizing tools, standards, compliance mechanisms, and individual security behaviors (Herath & Rao, 2009; Puhakainen & Siponen, 2010). However, these approaches frequently overlook the social and cultural contexts that shape how small business owners perceive and respond to cyber risks.

This limitation is particularly evident in ethnic minority-owned SMEs. These entrepreneurs represent a significant and growing segment of the SME population but face distinctive constraints, including language barriers, limited access to mainstream institutional support, uneven digital literacy, and varying trust in public institutions and technology providers (Ram & Jones, 2008; Waldinger, Aldrich, & Ward, 1990). Many rely on family and community networks for information, advice, and resources, which can substitute for formal support but may also introduce informal norms influencing risk perception and managerial priorities (Kloosterman, Van der Leun, & Rath, 1998; Light & Gold, 2000). Dominant cybersecurity frameworks often assume rational, resource-driven decision-making, treating SMEs as a homogeneous group (Mmango & Gundu, 2024) which limits their ability to explain the substantial heterogeneity observed among ethnic minority-owned firms (Ifinedo, 2012).

Managerial decisions in SMEs are socially embedded, boundedly rational, and shaped by experience, trust, and social relationships rather than purely objective risk assessments (Brunetto & Farr-Wharton, 2007; Granovetter, 1985; Kahneman, 2003). Applied to cybersecurity, this perspective suggests that entrepreneurs' responses to threats are influenced by cultural norms, social ties, and contextual constraints beyond firm-level resources. Yet, socio-cultural perspectives in cybersecurity remain insufficiently specified, offering limited clarity on the internal structure, relative importance, and mechanisms through which these factors shape behavior across diverse SMEs. Existing frameworks also conceptualize socio-cultural factors as relatively static conditions, rather than as dynamic influences evolving through entrepreneurs' experiences and interactions with their social environment. These limits understanding of how cybersecurity awareness develops over time, how trust in technology providers is constructed or eroded, and how family and community networks simultaneously enable and constrain practices (Shepherd & Suddaby, 2017).

To address these gaps, the research refines socio-cultural perspectives on cybersecurity decision-making in SMEs through qualitative analysis of 20 semi-structured interviews with ethnic minority business owners. The analysis elaborates key constructs, clarifies their interrelationships, and provides deeper insight into how socio-cultural factors interact to shape decision-making across diverse contexts (Eisenhardt, 1989; Gioia, Corley, & Hamilton, 2013).

Building on these insights, the paper makes three contributions. First, it clarifies the boundaries and interrelationships of key constructs such as cybersecurity awareness, trust, community networks, and digital literacy, demonstrating how they co-evolve rather than operate independently. Second, it advances a process-oriented understanding of cybersecurity decision-making, emphasizing experience-driven, iterative, and socially embedded choices over linear adoption models (March, 1994). Third, it reveals the dual role of socio-cultural factors, showing how informal networks can facilitate learning and trust while also normalizing risk or delaying formal cybersecurity investments. Guided by these objectives, the study addresses the following research questions: 1) How do socio-cultural factors interact to shape cybersecurity decision-making in ethnic minority-owned SMEs? 2) In what ways do entrepreneurs' experiences and social contexts refine existing conceptualizations of cybersecurity awareness and practice? And 3) how does a refined socio-cultural framework enhance understanding of cybersecurity behavior beyond resource- and technology-centric models?

By refining a socio-cultural framework of cybersecurity decision-making, this study contributes to research at the intersection of cybersecurity, entrepreneurship, and SME studies, providing a foundation for future empirical testing and practical insights for culturally sensitive interventions.

2. LITERATURE REVIEW AND CONCEPTUAL BACKGROUND

2.1. Cybersecurity in Small Businesses

SMEs face disproportionate cybersecurity risks due to resource limitations and informal organizational structures (Anderson & Moore, 2006; Tetteh, 2024). Empirical studies show that SMEs often lack formal policies, rely on ad-hoc practices, and underinvest in security, despite exposure comparable to larger firms (Ponemon Institute, 2020; Renaud & Weir, 2016). Operational priorities, perceived complexity, and cost concerns strongly influence decision-making, suggesting that cybersecurity behavior is shaped as much by contextual and cognitive factors as by technical constraints (Herath & Rao, 2009; Ifinedo, 2012).

Behavioral research highlights the role of risk perception, prior experience, and trust. Compliance with security measures depends on owners' beliefs about threat severity, perceived ease of implementation, and confidence in technology solutions (Ifinedo, 2012; Puhakainen & Siponen, 2010). Yet, most studies assume a rational, resource-based model and overlook socio-cultural factors such as community networks, cultural norms, and prior experiences, which can enable or constrain protective behavior. This gap underscores the need for a framework that integrates behavioral, social, and contextual influences, particularly for culturally diverse and minority-owned SMEs.

2.2. Socio-Cultural Influences on Entrepreneurial Decision-Making

Decision-making in SMEs is influenced not only by technical or resource constraints but also by behavioral and socio-cultural factors. Behavioral decision theory posits that individuals make choices under bounded rationality, relying on heuristics and prior experience rather than fully optimizing outcomes (Kahneman, 2003; Simon, 1957). Economic sociology emphasizes that decisions are socially embedded, shaped by trust, networks, and cultural norms (Granovetter, 1985). These factors influence how entrepreneurs perceive risk, evaluate security measures, and prioritize protective actions.

Trust, peer influence, and social relationships are particularly critical. Entrepreneurs often rely on family, community, or professional networks to interpret risks and identify solutions, which can facilitate knowledge transfer but also reinforce existing norms (Kloosterman et al., 1998; Light & Gold, 2000). These socio-cultural factors interact with experience and prior exposure to threats, producing heterogeneous decision patterns even among SMEs with similar resources. Despite their importance, they are rarely integrated into cybersecurity models, creating a gap in understanding how social and cultural dynamics co-determine protective behavior, especially in minority-owned businesses.

2.3. Ethnic Minority Entrepreneurship and Contextual Constraints

Ethnic minority entrepreneurs operate in distinctive social, cultural, and institutional environments that shape business practices, including cybersecurity. They often face language barriers, limited access to formal support, and reliance on informal networks, which influence decision-making and resource allocation (Kloosterman et al., 1998; Light & Gold, 2000; Ram & Jones, 2008). These constraints can both enable activity by providing informal guidance and constrain it by reinforcing risk normalization or delaying engagement with formal solutions.

Trust in institutions and technology providers is a key factor. Minority entrepreneurs may exhibit caution toward formal support due to perceived discrimination or prior exclusion, relying instead on social networks for advice (Kloosterman et al., 1998; Waldinger et al., 1990). This reliance can produce heterogeneous cybersecurity behaviors even among businesses with similar resources. Despite their importance, socio-cultural influences are rarely integrated into existing frameworks, limiting understanding of how contextual and cultural factors dynamically interact with behavioral and technical considerations. Addressing this gap is essential for developing culturally sensitive and empirically grounded frameworks.

2.4. Conceptual Framework for Socio-Cultural Decision-Making

Cybersecurity decision-making in SMEs can be understood as a complex interplay of individual, social, and contextual/cultural factors. Individual factors include prior experience, digital literacy, and exposure to cyber threats (Ifinedo, 2012; Puhakainen & Siponen, 2010). Social factors, such as trust in technology providers, peer influence, and reliance on networks, mediate risk interpretation and protective action selection (Granovetter, 1985; Light & Gold, 2000). Contextual and cultural factors, language proficiency, norms, and access to support, shape both awareness and perceived necessity of investments (Kloosterman et al., 1998; Ram & Jones, 2008; Waldinger et al., 1990).

These factors' interrelationships, relative importance, and influence mechanisms remain under-specified. Networks can accelerate learning yet normalize risk, and cultural norms can enable or constrain formal practices depending on prior experiences. These gaps indicate the need for a conceptual framework integrating individual, social, and contextual factors, emphasizing dynamic, experience-driven decision-making.

2.5. Gap and Justification for Framework Refinement

Prior research has identified individual, social, and contextual factors but frameworks remain fragmented and underdeveloped, often treating socio-cultural influences as static rather than dynamic (Shepherd & Suddaby, 2017). Interactions among these factors, their relative importance, and mechanisms remain poorly understood.

Existing models adopt a rational, resource-centric perspective, overlooking behavioral, experiential, and culturally grounded decision-making. Minority-owned SMEs face language barriers, informal networks, and variable trust, producing heterogeneous behaviors not captured in traditional frameworks (Kloosterman et al., 1998; Light & Gold, 2000; Waldinger et al., 1990).

These gaps justify a refined, process-oriented socio-cultural framework that accounts for dynamic interactions among behavioral, social, and contextual factors. This framework can explain variability in awareness and practices, provide theoretical clarity, and guide culturally sensitive interventions, forming the primary objective of the present study and setting the stage for the framework derived from findings.

3. METHODOLOGY

3.1. Research Design

This study adopts an exploratory qualitative approach to investigate cybersecurity decision-making in ethnic minority-owned SMEs in Québec. Qualitative research is particularly suited for examining complex, context-dependent phenomena, allowing for rich, detailed understanding of how social, cultural, and contextual factors shape managerial behavior (Eisenhardt, 1989; Gioia et al., 2013). The study builds on prior work by refining a socio-cultural framework, using empirical data to illuminate key constructs, relationships, and interactions that cannot be fully captured through quantitative methods.

3.2. Participants and Procedure

The study involved 20 ethnic entrepreneurs operating small businesses in Québec across sectors such as retail, food service, online commerce, and professional services (see Appendix 1). Potential participants were identified using lists of ethnic entrepreneurs provided by ethnic small business associations, consulting firms, and immigration advisory centers. Snowball sampling was also employed, whereby participants recommended other entrepreneurs in their networks. Inclusion criteria required participants to identify as belonging to an ethnic minority or immigrant group, currently own or partner in a business, and actively use digital technologies, including e-commerce, online marketing, financial tools, or social media. Data were collected through semi-structured interviews, which allowed participants to share their experiences in their own words while maintaining consistency across interviews. Each interview lasted 45–60 minutes and was conducted in person, online via secure video platforms, or over the phone, depending on participants' availability. With participants' consent, interviews were audio-recorded and transcribed verbatim, and brief field notes were taken to capture contextual observations. Ethical considerations, including informed consent, confidentiality, and voluntary participation, were strictly observed throughout the research process.

The sample was selected to ensure diversity in years of business experience, sector, and reliance on digital platforms. All interviews were conducted by one of the authors between January and September 2024, with ethical considerations and confidentiality fully explained at the outset of each interview. This sample size provided sufficient diversity while achieving data saturation, where no new themes emerged. The study's approach emphasizes depth over breadth, allowing for a rich understanding of the experiences and digital engagement of ethnic entrepreneurs.

3.3. Interview Guide

This study adopts a qualitative research design, with semi-structured interviews serving as the primary method of data collection. Qualitative inquiry is particularly well suited for exploring complex, socially embedded phenomena, as it prioritizes participants' perspectives and situates meaning within specific social and cultural contexts (Milne & Oberle, 2005). Semi-structured interviews enable the collection of rich, in-depth accounts while allowing flexibility to probe emergent themes and clarify participants' experiences and interpretations (Adeoye-Olatunde & Olenik, 2021).

The interview guide Appendix 2 was informed by the literature on cybersecurity in SMEs, entrepreneurial decision-making, and ethnic minority entrepreneurship, and was designed to support theory refinement rather than hypothesis testing. The guide was structured to elicit detailed narratives about participants' cybersecurity-related experiences, perceptions, and decision-making processes within their business contexts. The first part of the interview focused on participants' entrepreneurial background and business operations, including prior business experience, motivations for business ownership, familiarity with digital technologies, and current cybersecurity awareness and practices. Participants were asked to describe perceived cyber threats, experiences with cyber incidents or near-miss events, challenges in protecting digital assets, and the strategies adopted to manage or mitigate cyber risks.

The interview further explored participants' digital literacy, access to cybersecurity knowledge or training, perceived resource constraints, and the role of cybersecurity considerations in broader business decisions. These questions aimed to capture how individual-level factors, such as experience, capability, and perceived risk, shape cybersecurity awareness and behavior over time.

In addition, the interview guide collected demographic and contextual information relevant to understanding socio-cultural influences on decision-making, including age, ethnicity, mother tongue, language proficiency (English and French), level of education, entrepreneurial experience prior to migration, experience in other businesses, and residency status. The second part of the interview consisted of open-ended questions designed to examine the social, cultural, and contextual dimensions of cybersecurity decision-making. This section focused on how cultural background, family and community networks, trust in technology providers and institutions, and migration-related experiences influence perceptions of cyber risk and the adoption of protective measures.

Together, the interview questions were designed to generate rich empirical material that captures the dynamic interactions among individual, social, and contextual factors shaping cybersecurity decision-making in ethnic minority-owned small businesses. This approach enabled a deeper, process-oriented understanding of how cybersecurity practices emerge, evolve, and are negotiated within socially and culturally embedded entrepreneurial contexts.

3.4. Data Analysis

Data were analyzed using qualitative content analysis, following an inductive and exploratory logic (Hsieh & Shannon, 2005; Krippendorff, 2018). This approach was selected because the study seeks to examine cybersecurity decision-making in ethnic minority-owned small businesses in a context where existing theories insufficiently specify socio-cultural mechanisms. Qualitative content analysis allows patterns, categories, and relationships to emerge from participants' accounts while remaining sensitive to context, experience, and meaning-making processes, rather than imposing predefined theoretical structures.

The analytic process proceeded through four interrelated stages and was supported by NVivo 12 to facilitate systematic data management and transparency. First, initial inductive coding was conducted through a detailed, line-by-line reading of interview transcripts. Two researchers independently coded a subset of transcripts to identify meaningful units of text related to cybersecurity awareness, experiences, decision-making processes, and socio-cultural influences. Codes were intentionally descriptive and closely grounded in participants' language, reflecting lived experiences rather than abstract constructs. Also, the two researchers met regularly to compare, refine, and consolidate the evolving coding scheme. Discrepancies were resolved through iterative discussion and consensus-building, leading to the merging of overlapping codes and the organization of related codes into broader analytical categories. Throughout this process, analytic memos were maintained to document coding decisions, emerging interpretations, and reflexive considerations, thereby enhancing transparency and dependability.

In addition, theme integration involved examining relationships among categories to identify higher-order patterns that captured recurring logics of cybersecurity decision-making across participants. This stage focused on how individual experiences, social relationships, and contextual conditions interacted dynamically over time. To strengthen analytic rigor, the researchers engaged in peer debriefing and reflexive dialogue, critically examining alternative interpretations and challenging assumptions during the development of themes. Finally, an interpretive pattern-matching strategy was employed to refine the emerging conceptual framework. Once themes had fully emerged inductively, they were compared with existing constructs from the cybersecurity, entrepreneurship, and socio-cultural decision-making literatures. This comparison was used to assess conceptual alignment, extension, and refinement, rather than to test hypotheses or validate predefined models. Importantly, theoretical concepts informed interpretation only at this final stage and did not guide initial coding decisions.

Data saturation was used as both an analytic and sampling criterion. During the coding process, no substantively new themes or decision-making patterns emerged after approximately the twentieth interview, indicating sufficient conceptual depth and coverage. This analytic confirmation supported the decision to conclude data collection after 18 interviews. Together, these procedures constitute a transparent and auditable analytic pathway, ensuring that the findings are firmly grounded in participants' accounts while supporting the refinement of a socio-cultural framework of cybersecurity decision-making.

4. FINDINGS

The analysis of the 20 semi-structured interviews generated in-depth insights into the socio-cultural dynamics shaping cybersecurity decision-making in ethnic minority-owned small and medium-sized enterprises (SMEs). Following an inductive thematic analysis, three overarching and interrelated themes emerged: (1) individual factors, (2) social factors, and (3) contextual and cultural factors. These themes capture recurrent patterns across participants' narratives while also reflecting variations in cybersecurity awareness, risk perception, and decision-making practices. Each theme is supported by verbatim quotations from participants (P1–P20) to preserve the richness and authenticity of the data and to illustrate how individual experiences, social relationships, and contextual conditions interact to shape cybersecurity practices.

4.1. Individual Factors

Individual factors emerged as critical determinants of cybersecurity awareness and behavior, shaping decision-making at the individual level through subjective interpretations of vulnerability, confidence, and responsibility rather than purely technical or objective assessments of cyber risk. These influences affected how entrepreneurs evaluated the relevance of cybersecurity to their businesses, their perceived ability to manage digital threats, and the priority assigned to protective actions amid competing operational demands. Importantly, individual-level influences were experience-based and situational, reflecting ongoing learning processes rather than fixed characteristics. Three interrelated sub-themes in clouding prior experience with cyber threats, digital literacy, and perceived risk, collectively form a dynamic set of factors that interact to shape cybersecurity decision-making. Their interplay produces uneven adoption patterns, highlighting that cybersecurity behavior in ethnic minority-owned SMEs is not solely resource-driven but deeply shaped by experience, perception, and capability. To illustrate this process, Table 1 presents a sample of the coding procedure, linking participants' quotes to initial codes, sub-themes, and the overarching theme of Individual Factors.

4.1.1. Prior Experience with Cyber Threats

Prior experience with cyber threats emerged as a powerful experiential trigger shaping how entrepreneurs interpreted cybersecurity risks and evaluated the necessity of protective measures. Participants' accounts indicate that direct encounters with cyber incidents, such as data breaches, phishing attempts, or system disruptions, often transformed cybersecurity from an abstract concern into an immediate and tangible business risk. These experiences heightened awareness, increased perceived vulnerability, and prompted more proactive engagement with security practices.

Entrepreneurs who had experienced cyber incidents described a shift toward greater vigilance and precautionary behavior, often accompanied by concrete changes in routines and systems:

> *"After our payment system was hacked last year, I immediately changed all passwords and started using a secure cloud service. Before that, I didn't think it was necessary" (P3).*
>
> *"We once received a phishing email that looked completely real. Since then, I'm very careful about opening attachments and checking where emails come from" (P8).*
>
> *"When it happened to us, even for a short time, I realized how fragile our systems were. It was a wake-up call" (P11).*

These narratives suggest that experience functioned as a learning mechanism, recalibrating risk perception and legitimizing cybersecurity investments that were previously viewed as optional or excessive. In several cases, participants emphasized that external advice or general warnings had limited impact until they encountered a threat firsthand:

> *"People always talk about cyber risks, but honestly, you don't take it seriously until it happens to you" (P6).*

In contrast, participants without direct experience of cyber incidents frequently expressed lower perceived urgency, relying on minimal or basic safeguards. For these entrepreneurs, the absence of negative events reinforced a sense of relative safety and contributed to delayed or incremental adoption of protective measures:

> *"I've never had a real problem, so I just rely on basic antivirus software. It seems enough for now" (P12).*
>
> *"Nothing bad has happened yet, so I don't feel pressure to invest more in security" (P19).*

Importantly, these accounts illustrate that the absence of experience did not necessarily reflect ignorance but rather a risk assessment grounded in past outcomes, where cybersecurity decisions were shaped by what had, or had not, occurred. This finding underscores that experience operates not only as a motivator for action but also as a boundary for concern, influencing how entrepreneurs balance cybersecurity against other operational priorities. Overall, prior experience with cyber threats played a central role in structuring individual decision-making, acting as a catalyst for heightened awareness and behavioral change. At the same time, the findings reveal that experience-driven learning can contribute to uneven adoption patterns, reinforcing proactive behavior among some entrepreneurs while sustaining complacency among others who have not yet encountered cyber incidents.

4.1.2. Digital Literacy

Digital literacy emerged as a key individual-level factor shaping entrepreneurs' ability to understand, evaluate, and implement cybersecurity measures. Participants' narratives indicate that digital literacy influenced not only the technical sophistication of protective practices but also confidence in decision-making and patterns of reliance on external support. Rather than functioning as a binary condition, digital literacy appeared as a continuum, producing distinct approaches to cybersecurity across participants.

Entrepreneurs with higher levels of digital literacy demonstrated a greater sense of control over cybersecurity decisions and were more likely to adopt layered or preventive measures. These participants described an ability to interpret technical guidance, compare available solutions, and independently implement security practices.

> *"I'm not an IT expert, but I understand enough to follow instructions and set things up properly, like two-factor authentication and secure backups" (P5).*
>
> *"Once you know what to look for, it's easier to decide which tools make sense and which ones are just marketing" (P9).*

For these participants, digital literacy reduced perceived complexity and lowered psychological barriers to action, enabling cybersecurity to be treated as a manageable operational task rather than an overwhelming technical challenge.

In contrast, participants with lower levels of digital literacy frequently expressed uncertainty, hesitation, and dependence on others when addressing cybersecurity issues. Limited understanding of technical concepts constrained their ability to assess risks or verify whether protective measures were correctly implemented:

"I don't really understand all the technical details, so I'm never sure if things are actually secure or not" (P17).

"I try to follow online instructions, but sometimes I don't know if I did it right" (P13).

As a result, many entrepreneurs relied on informal support networks, such as family members, friends, or community contacts, to manage cybersecurity-related tasks:

"If there is a problem, I usually ask my nephew or someone from the community who knows computers" (P14).

"I trust people I know more than companies I don't understand" (P18).

While this reliance on informal support often enabled basic protective actions, it also introduced inconsistencies and vulnerabilities, particularly when advice was fragmented or based on limited expertise. Several participants acknowledged that they implemented security measures selectively or partially, guided by what seemed understandable or feasible rather than by comprehensive risk assessments.

Importantly, digital literacy interacted closely with other individual and social factors. Participants with low digital literacy but high perceived risk often adopted reactive or minimal solutions, whereas those with higher literacy were more likely to engage in anticipatory and preventive practices. This interaction highlights that digital literacy does not operate in isolation but shapes how entrepreneurs interpret risk, evaluate trust in external providers, and navigate available support mechanisms.

Overall, digital literacy functioned as a capability-enabling mechanism in cybersecurity decision-making, influencing both the depth and consistency of protective behavior. The findings suggest that variations in digital literacy contribute to uneven cybersecurity practices among ethnic minority-owned SMEs, reinforcing the importance of addressing not only access to tools but also entrepreneurs' capacity to meaningfully engage with cybersecurity knowledge.

4.1.3. Perceived Risk

Perceived risk emerged as a central cognitive filter through which entrepreneurs evaluated the relevance and urgency of cybersecurity for their businesses. Participants' narratives indicate that cybersecurity decisions were guided less by objective assessments of threat likelihood and more by subjective interpretations of vulnerability, shaped by personal experience, information sources, and social comparison. As a result, perceived risk varied substantially across participants, producing divergent patterns of engagement with cybersecurity practices.

Entrepreneurs who perceived cyber threats as immediate and personally relevant tended to prioritize protective measures and expressed heightened awareness of potential consequences:

"I see cyber risks as something that could stop my business completely if it happens, so I try to be careful even if it costs time and money" (P1).

"When I hear about other small businesses getting hacked, I think it could easily be us next" (P10).

For these participants, perceived risk legitimized cybersecurity investments and justified allocating resources toward prevention, even when financial and operational constraints were present.

In contrast, participants who viewed cyber threats as distant, unlikely, or primarily affecting larger firms demonstrated lower levels of urgency and engagement. This perception often reduced the perceived necessity of investing in more advanced protections:

"I feel like hackers go after big companies, not small shops like mine" (P16).

"We don't have important data, so I don't think we are an attractive target" (P7).

These accounts suggest that perceived risk was closely tied to business size, industry type, and data sensitivity, rather than to broader threat awareness.

Importantly, perceived risk was not static but evolved over time through exposure to new information, peer experiences, or indirect encounters with cyber incidents. Some participants described shifts in perception triggered by media reports or stories within their community:

"When someone in our community had problems with ransomware, it made me rethink how safe we really are" (P4).

"I didn't worry much before, but after hearing about cases like ours, I started paying more attention" (P15).

Perceived risk also interacted with digital literacy and prior experience, shaping the form and intensity of responses. Participants with higher perceived risk but limited technical knowledge often adopted partial or reactive measures, while those with both high perceived risk and higher digital literacy were more likely to pursue comprehensive and preventive strategies. This interaction highlights that perceived risk alone was insufficient to drive effective action; its influence depended on complementary capabilities and resources.

Table 1. Coding process for individual factors.

Step	Data Example (Quote)	Initial Code	Sub-theme	Theme
1	"After our payment system was hacked last year, I immediately changed all passwords and started using a secure cloud service." (P3) "We once received a phishing email that looked completely real. Since then, I'm very careful about opening attachments and checking where emails come from." (P8) "When it happened to us, even for a short time, I realized how fragile our systems were. It was a wake-up call." (P11)	Direct experience with cyber incidents	Prior experience with cyber threats	Individual Factors
2	"People always talk about cyber risks, but honestly, you don't take it seriously until it happens to you." (P6) "I didn't think much about cybersecurity until a friend's business got hacked." (P4) "It was only after our own data was compromised that I realized the importance of protection." (P9)	Learning triggered by others' experiences		
3	"I've never had a real problem, so I just rely on basic antivirus software. It seems enough for now." (P12) "Nothing bad has happened yet, so I don't feel pressure to invest more in security." (P19) "I haven't experienced any hacking yet, so I just do minimal precautions for now." (P16)	No prior incidents / Low perceived urgency		
4	"I'm not an IT expert, but I understand enough to follow instructions and set things up properly, like two-factor authentication and secure backups." (P5) "Once you know what to look for, it's easier to decide which tools make sense and which ones are just marketing." (P9) "I can navigate security settings on my own and feel confident about my decisions." (P1)	Confident understanding of tech guidance	Digital literacy	

Continue Table 1. Coding Process for Individual Factors

Step	Data Example (Quote)	Initial Code	Sub-theme	Theme
5	"I try to follow online instructions, but sometimes I don't know if I did it right." (P13) "I don't really understand all the technical details, so I'm never sure if things are actually secure or not." (P17) "I need someone I trust to check whether I did things correctly." (P14)	Limited technical understanding	Digital literacy	Individual Factors
6	"I often rely on family or friends to set up security tools for me." (P18) "I can do the basics, but I ask my nephew to help with more complicated settings." (P2) "Without guidance from someone I trust, I wouldn't know how to configure certain protections." (P15)	Reliance on support networks		
7	"I see cyber risks as something that could stop my business completely if it happens, so I try to be careful even if it costs time and money." (P1) "When I hear about other small businesses getting hacked, I think it could easily be us next." (P10) "After hearing about a ransomware case in our community, I started reviewing our backups and security measures." (P15)	High perceived threat relevance	Perceived risk	
8	"I feel like hackers go after big companies, not small shops like mine." (P16) "We don't have important data, so I don't think we are an attractive target." (P7) "Nothing serious has ever happened, so I don't see the need to invest heavily in security." (P12)	Low perceived threat		
9	"Sometimes I know I should do more, but I weigh it against other priorities, and it feels optional." (P5) "I am aware of the risks, but limited time and resources make me focus on other business tasks." (P3) "I perceive some risk, but I adopt minimal measures until something serious happens." (P8)	Conditional or situational risk assessment		

Overall, perceived risk functioned as a decision-shaping mechanism, influencing when cybersecurity became a priority and how entrepreneurs justified their actions. The findings demonstrate that variations in perceived risk contribute to heterogeneous cybersecurity behaviors among ethnic minority-owned SMEs, reinforcing the need for frameworks that account for subjective, experience-driven interpretations of cyber threats rather than assuming uniform risk awareness.

4.2. Social Factors

Cybersecurity decision-making among ethnic minority-owned SMEs was strongly shaped by social relationships and collective influences rather than solely by individual judgment. Participants' accounts show that decisions related to cybersecurity were frequently negotiated through interactions with others, including technology providers, family members, and peers, and were embedded in ongoing processes of trust-building and informal knowledge exchange. These social interactions influenced how information was interpreted, which risks were taken seriously, and whether cybersecurity measures were perceived as necessary or legitimate. Three interconnected sub-themes emerged from the analysis: trust in technology providers and institutions, reliance on family and community networks, and peer influence and social comparison. Together, these elements constituted a socially grounded decision-making context in which cybersecurity choices were affirmed, postponed, or reconsidered through collective sense-making, highlighting the central role of social dynamics in shaping cybersecurity behavior beyond purely technical or individual considerations. In this regard, Table 2 provides a sample of the coding process for Social Factors, linking participants' statements to initial codes, sub-themes, and the overarching theme to illustrate the analysis procedure.

4.2.1. Trust in Technology Providers and Institutions

Trust emerged as a critical social determinant shaping whether entrepreneurs engaged with formal cybersecurity solutions and external support. Participants' accounts indicate that trust was not assumed but gradually constructed through prior interactions, reputational signals, and perceptions of alignment between providers' offerings and business needs. In the absence of trust, entrepreneurs often expressed hesitation, selective engagement, or outright avoidance of cybersecurity services, even when risks were acknowledged.

Several participants articulated skepticism toward technology vendors, particularly when services were perceived as overly complex, opaque, or driven by sales motives rather than genuine support. Limited technical understanding further intensified these concerns, undermining confidence in vendors' recommendations.

"Sometimes it feels like they just want to sell you something you don't really need, and I don't know enough to challenge them" (P18).

"They use too many technical terms. It's hard to trust something you don't fully understand" (P13).

This uncertainty frequently resulted in delayed decision-making or reliance on basic, low-commitment solutions perceived as less risky.

Trust in public institutions and formal support mechanisms was similarly uneven. Some participants reported limited engagement with government programs or institutional advisory services due to prior negative experiences, bureaucratic complexity, or a perceived mismatch between available support and the realities of small, minority-owned businesses:

"I don't feel those programs are really designed for businesses like mine" (P6).

"I tried asking for advice once, but it was complicated and not very helpful" (P11).

In contrast, entrepreneurs who had positive experiences with trusted consultants or advisors described greater willingness to invest in structured and proactive cybersecurity practices. Clear communication, transparency, and relational continuity appeared central to building confidence:

"We found a consultant who explained things clearly, and after that I felt more comfortable investing in proper security" (P2).

Taken together, these findings indicate that trust functions as a gatekeeping mechanism in cybersecurity decision-making, shaping whether formal resources are perceived as credible, accessible, and worthy of investment. Rather than being purely technical choices, engagements with cybersecurity providers and institutions were socially negotiated, reinforcing the central role of trust in mediating access to expertise and shaping protective behavior.

4.2.2. Reliance on Family and Community Networks

Family and community networks emerged as significant social resources shaping cybersecurity decision-making, particularly among participants with limited digital literacy or low levels of trust in formal institutions. These networks functioned as accessible and culturally familiar sources of advice, reassurance, and practical assistance, often substituting for professional cybersecurity services. Participants described turning to trusted individuals within their communities for guidance on technology-related issues, emphasizing shared experience and mutual support.

"If I have a question, I usually ask someone from my community who works with computers" (P14).

"We help each other. If someone learns something new, they share it with the rest of us" (P9).

Such networks played an enabling role by lowering perceived barriers to action, facilitating informal learning, and reinforcing cybersecurity awareness through shared experiences. Advice circulated within these networks was often trusted because it was embedded in existing social relationships and conveyed in familiar, non-technical language.

At the same time, participants recognized limitations associated with reliance on informal and non-expert advice. Guidance was sometimes perceived as inconsistent, subjective, or insufficiently grounded in technical expertise, generating uncertainty about appropriate cybersecurity practices.

"Sometimes the advice is based on personal opinion, not really on expert knowledge" (P17).

"Everyone does things differently, so it's hard to know what is actually correct" (P5).

In some cases, prevailing community norms contributed to the normalization of cyber risk, particularly when incidents were infrequent or not openly discussed. The absence of visible negative experiences reduced the perceived urgency of adopting protective measures.

"If no one around you has problems, you feel like it's probably not that serious" (P16).

Overall, these findings illustrate the dual role of family and community networks as both enabling and constraining influences on cybersecurity behavior. While such networks facilitated access to support and knowledge through collective sense-making, they also shaped norms and expectations that could limit engagement with formal standards or more robust protective practices.

4.2.3. Peer Influence and Social Comparison

Peer influence further shaped cybersecurity decision-making through processes of social comparison and observational learning. Participants frequently assessed their own cybersecurity practices in relation to those of similar businesses, using peers as informal reference points for determining what levels of protection were considered appropriate, sufficient, or excessive. In this context, peer behavior functioned as a practical benchmark, particularly in environments characterized by uncertainty and limited access to expert guidance:

"I look at what other shops like mine are doing. If they're fine with basic protection, I don't feel pressure to do more" (P12).

Peer experiences also operated as powerful signals of risk relevance, especially in the absence of direct personal exposure to cyber incidents. Several participants described heightened awareness and behavioral adjustment after observing or learning about cybersecurity breaches affecting comparable businesses.

"When I saw another business like ours get hacked, it made me rethink how prepared we really were" (P4).

"When it happened to someone in the same line of work, it suddenly felt much closer to home" (P10).

At the same time, peer influence could reinforce minimal or reactive approaches when prevailing informal norms emphasized cost avoidance or low-effort solutions. In such cases, social comparison contributed to the normalization of limited cybersecurity engagement rather than proactive investment. This dynamic suggests that peer influence operates as a contextual amplifier, capable of strengthening or dampening perceived urgency depending on dominant community narratives and shared interpretations of risk.

Table 2. Sample coding process for social factors.

Step	Data Example (Quote)	Initial Code	Sub-theme	Theme
1	"Sometimes it feels like they just want to sell you something you don't really need, and I don't know enough to challenge them" (P18) "They use too many technical terms. It's hard to trust something you don't fully understand" (P13) "I often feel unsure about the advice from providers because it's too technical" (P7)	Skepticism toward providers	Trust in technology providers and institutions	Social Factors
2	"We found a consultant who explained things clearly, and after that I felt more comfortable investing in proper security" (P2) "Once the provider took time to explain step by step, I felt confident making decisions" (P5) "Good communication made me trust their recommendations" (P10)	Positive experience with trusted providers		
3	"I don't feel those programs are really designed for businesses like mine" (P6) "Some government programs just don't apply to us small shops" (P15) "I tried asking for advice once, but it was complicated and not very helpful" (P11)	Distrust in formal support		
4	"If I have a question, I usually ask someone from my community who works with computers" (P14) "We help each other. If someone learns something new, they share it with the rest of us" (P9) "I ask family or friends first before looking for professional help" (P17)	Informal advice and support	Reliance on family and community networks	
5	"Sometimes the advice is based on personal opinion, not really on expert knowledge" (P17) "Everyone does things differently, so it's hard to know what is actually correct" (P5) "I often get conflicting guidance from friends or family, which confuses me" (P12)	Limitations of informal guidance		
6	"I look at what other shops like mine are doing. If they're fine with basic protection, I don't feel pressure to do more" (P12) "When I saw another business like ours get hacked, it made me rethink how prepared we really were" (P4) "I try to keep up with what my peers are doing so I don't fall behind" (P8)	Social comparison and benchmarking	Peer influence and social comparison	
7	"When it happened to someone in the same line of work, it suddenly felt much closer to home" (P10) "Peer stories make you pay attention, or sometimes reassure you that nothing will happen" (P7) "Learning from other businesses' experiences helps me decide what to do next" (P3)	Peer experiences as risk signals		
8	"If no one around you has problems, you feel like it's probably not that serious" (P16) "Hearing that similar businesses have no issues sometimes makes me less cautious" (P12) "When peers are relaxed about security, I tend to relax too" (P5)	Social norms reducing urgency		
9	"Community discussions often guide what we think is important to do" (P9) "Seeing what others prioritize in the network shapes my own choices" (P14) "Peer experiences both warn and reassure me depending on the situation" (P8)	Contextual social cues		

4.3. Contextual and Cultural Factors

Contextual and cultural factors constituted the broader structural environment influencing cybersecurity decision-making, shaping how entrepreneurs interpreted risks, assessed the feasibility of protective measures, and interacted with formal support mechanisms. Participants' narratives indicate that decisions were deeply embedded within linguistic, cultural, and institutional contexts, which affected the accessibility of information, the perceived importance of cybersecurity, and the credibility of external guidance. From the analysis, three interconnected sub-themes emerged: language and communication barriers, cultural norms and values, and access to institutional support. These structural and cultural conditions interacted with individual capacities and social networks, producing cybersecurity practices that were highly context specific. To illustrate the analytic process, Table 3 presents a sample of how participants' quotes were coded, linking initial codes to sub-themes and the overarching theme of contextual and cultural factors.

4.3.1. Language and Communication Barriers

Language proficiency emerged as a critical structural factor shaping entrepreneurs' ability to access, interpret, and act upon cybersecurity information. Participants reported that technical documentation, vendor communications, and official guidance were often difficult to navigate due to complex terminology, specialized jargon, or limited availability of resources in their preferred language. These communication challenges affected how participants assessed risks, selected protective measures, and determined which cybersecurity actions were feasible for their businesses.

Several entrepreneurs described difficulties understanding formal guidance, which led them to focus on simpler or more familiar measures.

"Most of the information is very technical, and it's not in a language that's easy for me to fully understand" (P7).

"Even when there are guidelines, they use words that are hard to follow, so I'm not always sure what they really mean" (P13).

"Some instructions are only in English, and I struggle to translate them accurately" (P19).

To compensate, many participants relied on summaries, informal explanations, or trusted intermediaries, such as family, friends, or community members, to make cybersecurity information actionable.

"If someone explains it to me in simple terms, I feel more confident, but reading it myself is difficult" (P14).

"My nephew often translates technical guides for me, which makes it possible to follow some security steps" (P11).

"I usually ask someone I trust to explain what I don't understand in the emails from providers" (P9).

These narratives suggest that language barriers did not indicate a lack of concern or awareness about cybersecurity but instead functioned as a structural filter, shaping which practices were perceived as accessible, realistic, or worthwhile. Entrepreneurs with higher digital literacy or supportive social networks were better able to overcome these challenges, whereas those lacking such resources faced greater difficulty implementing comprehensive protections. At the same time, selective engagement with easier-to-understand measures sometimes led to uneven adoption patterns, with basic protections in place but more complex preventive strategies left unimplemented.

Overall, language and communication barriers played a central role in structuring how contextual and cultural factors influenced cybersecurity decision-making, interacting with individual capabilities and social networks to shape both access to information and the prioritization of protective actions.

4.3.2. Cultural Norms and Values

Cultural norms and values emerged as a key contextual factor influencing how entrepreneurs framed responsibility, assessed risk, and determined acceptable business practices. Participants frequently described prioritizing trust, relationship maintenance, and day-to-day operational survival, which shaped how cybersecurity was positioned relative to other business concerns. In many cases, cultural expectations encouraged risk normalization, especially when cyber incidents were rarely discussed or publicly acknowledged within the community.

"In our culture, we focus a lot on personal relationships and trust. You don't immediately think about digital threats" (P6).

"The priority is keeping the business running. Cybersecurity feels important, but not urgent compared to daily problems" (P19).

"People don't usually talk about these problems, so you assume it's not something common" (P16).

At the same time, cultural values emphasizing responsibility toward customers, employees, and family members often motivated entrepreneurs to adopt protective measures despite operational pressures.

"If something happened and customer data was lost, it would be shameful. That's why I try to be careful" (P1).

"I feel responsible for my staff and clients. Even small precautions matter" (P4).

"Maintaining trust with our community is important, so I follow the advice I get from trusted sources" (P9).

These narratives suggest that cultural norms do not simply constrain behavior but also provide a moral and relational framework through which cybersecurity is interpreted and prioritized. Entrepreneurs navigated tensions between operational survival, relational obligations, and ethical responsibility, leading to diverse adoption patterns. Overall, cultural norms and values played a central role in shaping both the perceived necessity and the ethical framing of cybersecurity actions, highlighting the importance of considering culturally embedded expectations when analyzing decision-making in minority-owned SMEs.

4.3.3. Access to Institutional Support

Access to institutional support, including government programs, training initiatives, and formal advisory services, emerged as a contextual factor influencing entrepreneurs' engagement with cybersecurity practices. Participants' accounts indicate that the availability, clarity, and perceived relevance of institutional resources shaped whether and how protective measures were adopted, with wide variation in awareness and utilization. Many entrepreneurs reported limited knowledge of programs, perceived complexity, or a sense that services were not tailored to small, minority-owned businesses.

"I know there are programs, but I don't really know how to access them or if they apply to my business" (P11).

"The process is complicated, and it doesn't feel designed for small businesses like ours" (P6).

"It feels like these services are made for bigger companies, not for people like us" (P18).

This limited accessibility often reinforced reliance on informal networks and selective, minimal engagement with cybersecurity measures. Entrepreneurs described seeking guidance from family, peers, or community contacts when formal mechanisms appeared opaque or misaligned:

"If I can't figure it out through the official channels, I ask someone I trust in my community" (P14).

"I often rely on advice from other shop owners rather than the government programs, which seem too complex" (P9).

Conversely, participants who successfully engaged with institutional support reported improved understanding, confidence, and adoption of cybersecurity practices:

"After attending a local workshop, I understood what steps I should take, and it made everything clearer" (P2).

"The advisor explained the procedures in a way I could follow, and I finally implemented proper backups" (P5).

"Having someone guide me through the official program made me take security more seriously" (P10).

These narratives indicate that institutional support functioned as a conditional enabler: when accessible, understandable, and aligned with business needs, it facilitated learning and practical action; when opaque, misaligned, or inaccessible, it reinforced selective adoption and reliance on informal guidance.

Table 3. Sample coding process for contextual and cultural factors.

Step	Data Example (Quote)	Initial Code	Sub-theme	Theme
1	"Most of the information is very technical, and it's not in a language that's easy for me fully understand" (P7) "Even when there are guidelines, they use words that are hard to follow, so I'm not always sure what they really mean" (P13) "Some instructions are only in English, and I struggle to translate them accurately" (P19)	Difficulty understanding technical materials	Language and Communication Barriers	Contextual and Cultural Factors
2	"If someone explains it to me in simple terms, I feel more confident, but reading it myself is difficult" (P14) "My nephew often translates technical guides for me, which makes it possible to follow some security steps" (P11) "I usually ask someone I trust to explain what I don't understand in the emails from providers" (P9)	Reliance on informal explanation		
3	"Instructions in official programs are confusing and not adapted to small businesses" (P6) "Language barriers make it hard to implement complex security measures" (P12) "I can do basic steps, but full guidelines are too complicated" (P8)	Limited independent engagement		
4	"In our culture, we focus a lot on personal relationships and trust. You don't immediately think about digital threats" (P6) "The priority is keeping the business running. Cybersecurity feels important, but not urgent compared to daily problems" (P19) "People don't usually talk about these problems, so you assume it's not something common" (P16)	Risk normalization	Cultural Norms and Values	
5	"If something happened and customer data was lost, it would be shameful. That's why I try to be careful" (P1) "I feel responsible for my staff and clients. Even small precautions matter" (P4) "Maintaining trust with our community is important, so I follow the advice I get from trusted sources" (P9)	Ethical/moral motivation		
6	"Cultural focus on daily survival sometimes reduces urgency for cybersecurity" (P12) "Cybersecurity is secondary to business operations in our community" (P8) "Trust and relationships often outweigh technical concerns" (P7)	Prioritization shaped by cultural norms		
7	"I know there are programs, but I don't really know how to access them or if they apply to my business" (P11) "The process is complicated, and it doesn't feel designed for small businesses like ours" (P6) "It feels like these services are made for bigger companies, not for people like us" (P18)	Limited awareness / perceived misalignment	Access to Institutional Support	
8	"After attending a local workshop, I understood what steps I should take, and it made everything clearer" (P2) "The advisor explained the procedures in a way I could follow, and I finally implemented proper backups" (P5) "Having someone guide me through the official program made me take security more seriously" (P10)	Successful engagement / confidence boost		
9	"When institutional resources are confusing, I rely on community or peers for guidance" (P14) "If official programs are opaque, I just follow what trusted people suggest" (P9) "Limited access to formal support reinforces minimal compliance" (P12)	Conditional adoption / reliance on informal networks		

Overall, access to institutional support shaped the structural context of cybersecurity decision-making, interacting with individual capabilities, social networks, and cultural expectations to produce diverse patterns of behavior among ethnic minority-owned SMEs.

5. REFINED SOCIO-CULTURAL FRAMEWORK FOR CYBERSECURITY DECISIONS

Building on the empirical findings presented in Section 4, this study proposes a refined socio-cultural framework for understanding cybersecurity decision-making in ethnic minority-owned SMEs. Unlike a prescriptive or fully validated model, the framework emerges inductively from participants lived experiences, integrating individual capabilities, social influences, and contextual/cultural conditions into a coherent explanatory structure. Its purpose is to clarify the mechanisms, interactions, and decision-making processes that shape cybersecurity behaviors, addressing gaps in prior research while remaining firmly grounded in qualitative evidence.

The findings demonstrate that cybersecurity decision-making is neither linear nor purely rational. Instead, it is an iterative, experience-driven process, shaped by subjective interpretations of risk, socially embedded knowledge, and structural constraints. The refined framework highlights three interrelated domains including individual, social, and contextual/cultural factors, and emphasizes how their interaction produces heterogeneous and context-specific cybersecurity behaviors across firms.

Figure 1 presents the refined socio-cultural framework for cybersecurity decision-making, integrating the insights from Sections 4.1–4.3. The diagram illustrates how individual factors (prior experience, digital literacy, perceived risk), social factors (trust, community networks, peer influence), and contextual/cultural factors (language barriers, cultural norms, institutional access) interact dynamically to shape cybersecurity behaviors. Arrows indicate iterative feedback loops, reflecting the evolving nature of decision-making as entrepreneurs encounter new information, experiences, and social or institutional influences. The figure provides a visual synthesis of the framework, clarifying relationships, mechanisms, and the context-specific nature of cybersecurity decision-making in ethnic minority-owned SMEs.

5.1. Individual Factors as Decision Catalysts

At the core of the framework, individual factors function as primary decision catalysts, shaping how entrepreneurs recognize, interpret, and respond to cybersecurity threats. As highlighted in Section 4.1, prior experience with cyber incidents recalibrates risk perception and legitimizes protective action, while digital literacy influences the capacity to evaluate and implement technical measures. Perceived risk acts as a cognitive filter, determining when cybersecurity becomes salient relative to other operational priorities.

Crucially, these individual-level influences are dynamic rather than static. Experience-driven learning processes continually reshape awareness, judgment, and behavior, producing uneven and evolving patterns of cybersecurity adoption. The framework conceptualizes individual factors as adaptive capabilities, sensitive to new information, direct encounters with threats, and feedback from social and cultural contexts.

5.2. Social Factors as Mediating Mechanisms

Social factors operate as mediators between individual cognition and concrete cybersecurity actions. Trust in technology providers and institutions determines whether formal solutions are perceived as credible, relevant, and accessible. Family and community networks provide informal guidance and reassurance, especially for entrepreneurs with limited digital literacy or low institutional trust. Peer influence and social comparison create normative benchmarks for what constitutes “adequate” cybersecurity practices.

The framework underscores the dual role of social factors. On one hand, they facilitate learning, build confidence, and encourage adoption; on the other, they can normalize minimal compliance or delay proactive measures. By amplifying or attenuating individual risk perceptions, social dynamics contribute to variability in cybersecurity behaviors, even among firms facing similar threats.

5.3. Contextual and Cultural Factors as Structural Conditions

Contextual and cultural factors define the structural environment in which decision-making unfolds. Language barriers constrain access to, comprehension of, and engagement with cybersecurity information. Cultural norms and values shape interpretations of responsibility, risk tolerance, and the ethical framing of protective measures. Access to institutional support affects whether entrepreneurs can leverage formal guidance, training, or advisory services.

The refined framework positions these influences as enabling or constraining conditions that interact with individual and social factors. For example, limited institutional access may increase reliance on trusted community networks, while cultural norms can determine whether cybersecurity is framed as an ethical responsibility or as a secondary operational concern. These structural factors do not dictate behavior directly but shape perceptions of feasibility, legitimacy, and necessity.

5.4. Dynamic Interactions and Iterative Decision-Making

A key contribution of the refined framework is its emphasis on dynamic, iterative interactions among individual, social, and contextual/cultural domains. Cybersecurity decisions evolve through feedback loops, where experiences with threats, advice from social networks, and encounters with institutional structures reshape subsequent perceptions, judgments, and actions. This iterative process explains why cybersecurity adoption is often reactive, uneven, and context-specific among ethnic minority-owned SMEs.

By foregrounding process and interaction, the framework moves beyond static lists of barriers or drivers. It offers a process-oriented explanation of decision-making that captures the complexity and lived realities of entrepreneurs navigating cyber risks in socially and culturally embedded contexts.

5.5. Framework Implications

The refined socio-cultural framework provides a conceptual foundation for future research, including empirical testing, comparative studies, and model validation. Practically, it suggests that effective cybersecurity interventions must go beyond technical guidance to include trust-building, culturally sensitive communication, and peer-supported learning mechanisms. Interventions should recognize that awareness, capability, and engagement are socially embedded and context-dependent, rather than uniform across SMEs.

By integrating individual capabilities, social dynamics, and contextual conditions into a unified structure, this framework explains heterogeneous cybersecurity behaviors among ethnic minority-owned SMEs, offering a nuanced lens for both theory development and practical application.

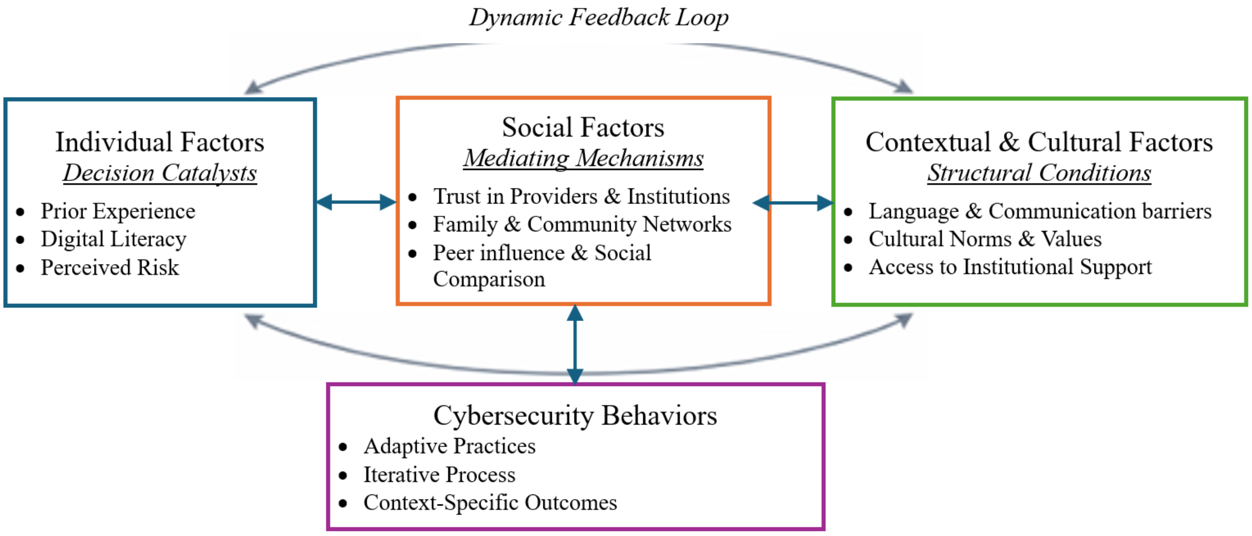
Dynamic Feedback Loop
Individual Factors
Decision Catalysts
• Prior Experience
• Digital Literacy
• Perceived Risk
Social Factors
Mediating Mechanisms
• Trust in Providers & Institutions
• Family & Community Networks
• Peer influence & Social Comparison
Contextual & Cultural Factors
Structural Conditions
• Language & Communication barriers
• Cultural Norms & Values
• Access to Institutional Support
Cybersecurity Behaviors
• Adaptive Practices
• Iterative Process
• Context-Specific Outcomes

Figure 1. Refined socio-cultural framework of cybersecurity decision-making in ethnic minority-owned SMEs.

6. DISCUSSION

6.1. Overview

This Discussion interprets the refined socio-cultural framework for cybersecurity decision-making in ethnic minority-owned SMEs, situating it within the qualitative evidence presented in Section 4 and the broader literature. The aim is to explain how individual capabilities, social influences, and contextual/cultural conditions interact to shape cybersecurity awareness, risk perception, and decision-making processes. By focusing on the mechanisms and dynamic interactions highlighted in the framework, this section considers both the experiential and socially embedded nature of entrepreneurial decision-making. The Discussion is structured to first interpret the framework's core components, then highlight theoretical contributions, and finally address practical implications and future research directions.

6.2. Interpreting the Refined Socio-Cultural Framework

The refined socio-cultural framework highlights that cybersecurity decision-making in ethnic minority-owned SMEs is a dynamic, iterative process shaped by the interaction of individual, social, and contextual/cultural factors. Unlike linear, resource-focused models, the framework emphasizes that entrepreneurial decisions are experience-driven and socially embedded, evolving through ongoing engagement with threats, social networks, and institutional structures. By interpreting the framework considering the qualitative findings, it becomes evident how mechanisms such as prior experience, trust, and cultural norms collectively shape perceptions of risk, priority-setting, and adoption of cybersecurity practices.

At the individual level, prior experience with cyber incidents functions as a critical trigger, recalibrating perceived risk and motivating protective action. Entrepreneurs with direct experience demonstrated proactive behaviors, such as implementing secure cloud services or routinely reviewing passwords, whereas those without exposure often relied on minimal safeguards, reflecting boundedly rational decision-making (Kahneman, 2003). Digital literacy further modulates the ability to interpret guidance, evaluate solutions, and implement preventive measures, while perceived risk acts as a cognitive filter, determining when cybersecurity becomes salient relative to competing operational demands. These findings align with prior research suggesting that SMEs' cyber behavior is strongly shaped by experiential learning and capability-driven interpretation of threats (Herath & Rao, 2009; Ifinedo, 2012).

Social influences mediate the translation of individual cognition into concrete cybersecurity actions. Trust in technology providers and formal institutions determines the perceived credibility and accessibility of external support, whereas family and community networks offer culturally familiar guidance, particularly for entrepreneurs with limited digital literacy. Peer influence establishes normative benchmarks, reinforcing or attenuating perceived urgency. The dual role of social factors- enabling adoption while potentially normalizing minimal compliance- underscores the framework's emphasis on the socially embedded nature of decision-making, extending findings from Granovetter (1985) and Light and Gold (2000) by demonstrating these mechanisms in the cybersecurity domain.

Contextual and cultural factors operate as structural conditions, shaping both the feasibility and perceived legitimacy of cybersecurity actions. Language barriers constrain access to technical information, cultural norms influence the prioritization of cybersecurity relative to operational and relational obligations, and access to institutional support affects the ability to leverage formal guidance. These factors interact with individual and social domains, such that limited institutional access increases reliance on trusted community networks, while cultural values may frame cybersecurity as an ethical responsibility rather than a technical requirement. This interaction illustrates the importance of situating SME cybersecurity behavior within broader socio-cultural and structural contexts, complementing existing frameworks that often treat these influences as static barriers (Mmango & Gundu, 2024).

A key insight from the framework is that cybersecurity decisions are iterative and adaptive. Feedback loops between experiences, social interactions, and contextual conditions continuously reshape risk perception, trust, and behavioral choices. For example, exposure to a peer's cyber incident may increase perceived risk, prompting preventive action, which in turn can be reinforced or modified through guidance from community networks or institutional programs. These dynamics explain the heterogeneous and context-specific adoption patterns observed in the interviews, highlighting the co-evolution of awareness, capability, and behavior- a perspective that moves beyond static, one-size-fits-all approaches to SME cybersecurity.

The interpretation of the refined framework addresses the study's research questions by clarifying how socio-cultural factors interact to shape decision-making, revealing that entrepreneurs' experiences and social contexts refine traditional conceptualizations of cybersecurity awareness and practice. The framework demonstrates that cybersecurity behavior cannot be fully understood through resource availability or technology adoption alone, but requires attention to experiential learning, trust dynamics, social norms, and contextual constraints, providing a coherent explanation of the patterns identified in Section 4.

6.3. Theoretical Contributions

This study makes several contributions to the literature on cybersecurity decision-making in SMEs, particularly in the context of ethnic minority-owned businesses. First, it clarifies the role of socio-cultural factors in shaping cybersecurity behavior, moving beyond the traditional resource- and technology-centric models. By integrating individual capabilities, social dynamics, and contextual/cultural conditions into a coherent framework, the study demonstrates that decision-making is not solely determined by technical knowledge or financial resources, but also by experience-driven learning, trust relationships, community norms, and structural constraints. This provides a nuanced understanding of heterogeneity in cybersecurity adoption, complementing prior research that treats SMEs as a relatively homogeneous group (Ifinedo, 2012; Mmango & Gundu, 2024). Also, the study advances a process-oriented perspective on cybersecurity decision-making, emphasizing iterative and adaptive mechanisms rather than static compliance or adoption models. The framework illustrates how experiences with threats, social interactions, and contextual feedback loops co-evolve, shaping perceptions, priorities, and behaviors over time. This perspective extends prior work on bounded rationality and experiential learning in SMEs (Brunetto & Farr-Wharton, 2007; Granovetter, 1985; Kahneman, 2003) to the cybersecurity domain, showing that entrepreneurial decisions emerge from dynamic interplay between cognition, social influence, and environmental constraints.

In addition, the findings highlight the dual role of social and community networks, demonstrating that informal relationships can both enable and constrain cybersecurity practices. Family and community networks provide accessible guidance, reassurance, and culturally familiar explanations, facilitating learning and adoption. Simultaneously, reliance on these networks may normalize minimal compliance or delay engagement with formal solutions, illustrating the ambivalent impact of social embeddedness. This duality extends existing frameworks on social capital and SME risk behavior (Kloosterman et al., 1998; Light & Gold, 2000) offering new insights into how social structures influence technology-related decision-making in minority-owned enterprises. Finally, the study contributes to the conceptualization of context in cybersecurity research. By explicitly integrating language barriers, cultural norms, and access to institutional support, the framework situates decision-making within the broader structural and cultural environment. This addresses a key limitation in existing models, which often treat socio-cultural factors as static background conditions rather than dynamic, interacting influences that shape both perception and action (Ram & Jones, 2008; Shepherd & Suddaby, 2017).

Collectively, these contributions provide a richer theoretical lens for understanding SME cybersecurity, demonstrating that effective frameworks must account for the co-evolution of individual capabilities, social relationships, and contextual conditions. They offer a foundation for future empirical testing, comparative studies, and further refinement of socio-culturally sensitive models of cybersecurity decision-making.

6.4. Practical Implications

The refined socio-cultural framework offers actionable insights for practitioners seeking to enhance cybersecurity in ethnic minority-owned SMEs. First, the findings underscore the importance of experience-driven interventions. Entrepreneurs often respond more strongly to concrete experiences with cyber incidents than to abstract warnings or technical guidance. Accordingly, training programs and awareness campaigns should incorporate realistic scenarios, case studies, and simulations that illustrate the potential consequences of cyber threats, fostering tangible learning and motivating proactive measures. The study also highlights the central role of trust in technology providers and institutions. SMEs are more likely to adopt formal cybersecurity solutions when guidance is transparent, culturally sensitive, and delivered by trusted intermediaries. Practitioners should therefore prioritize relationship-building, clear communication, and consistent support, while ensuring that services are perceived as relevant and accessible to small, minority-owned businesses.

Furthermore, the dual role of family, community, and peer networks suggests that interventions can leverage existing social structures to promote adoption. Peer-led workshops, community mentors, and culturally familiar advisory networks can facilitate informal learning, reinforce normative expectations, and provide ongoing reassurance. At the same time, practitioners should be aware of potential pitfalls, such as the normalization of minimal compliance, and provide strategies to supplement informal advice with technically sound practices. The framework also highlights contextual and cultural considerations as critical determinants of engagement. Language barriers, cultural norms, and perceived misalignment with institutional programs can limit adoption of cybersecurity measures. Effective interventions should therefore offer multilingual resources, simplified instructions, and culturally adapted guidance that aligns with entrepreneurs' priorities and ethical frameworks.

Finally, the iterative nature of cybersecurity decision-making indicates that support should be continuous rather than one-off. SMEs benefit from ongoing access to updated guidance, feedback loops, and opportunities to learn from evolving threats and peer experiences. By addressing individual capabilities, social dynamics, and structural conditions simultaneously, interventions can enhance both the effectiveness and sustainability of cybersecurity practices in minority-owned SMEs.

Overall, these practical implications demonstrate that cybersecurity strategies for SMEs must go beyond technical solutions, adopting a holistic, socio-culturally informed approach that recognizes the interplay of experience, trust, social networks, and contextual constraints.

6.5. Limitations and Future Research

While this study provides novel insights into cybersecurity decision-making in ethnic minority-owned SMEs, several limitations should be acknowledged. First, the research is based on qualitative evidence from 20 semi-structured interviews, which, while rich and detailed, may limit generalizability. The findings reflect the specific experiences, social contexts, and cultural backgrounds of the participants, and patterns observed may differ in other regions, industries, or demographic groups. Future studies could adopt larger-scale quantitative or mixed-methods approaches to test the applicability of the refined socio-cultural framework across diverse SME populations. The study also focuses primarily on owner/manager perspectives, which provides valuable insight into decision-making but does not capture the experiences of other stakeholders, such as employees, IT consultants, or customers, who may also influence cybersecurity behavior. Future research could adopt multi-stakeholder approaches to examine how internal and external actors jointly shape cybersecurity practices in SMEs.

In addition, the research emphasizes self-reported experiences, perceptions, and behaviors, which are subject to recall bias and social desirability effects. While verbatim quotations and careful thematic analysis mitigate some of these limitations, future studies could incorporate behavioral or observational data, such as system audits, incident logs, or controlled experiments, to validate reported practices and risk perceptions. The study also captures a snapshot in time of cybersecurity decision-making. Given the dynamic and evolving nature of digital threats, trust relationships, and institutional support, longitudinal research would be valuable to explore how individual capabilities, social networks, and contextual conditions co-evolve over time, and how interventions may alter adoption patterns. Finally, while the refined framework provides a theoretical foundation for understanding socio-cultural influences on cybersecurity, empirical testing is needed to quantify relationships among constructs and evaluate the relative weight of individual, social, and contextual factors. Comparative studies across cultural and regulatory environments could further refine and validate the model, enhancing its generalizability and practical utility.

Despite these limitations, the study lays important groundwork by integrating individual, social, and contextual dimensions into a coherent framework and highlighting the mechanisms through which socio-cultural factors shape cybersecurity behavior in minority-owned SMEs. By addressing these gaps in future research, scholars can advance both theory and practice in SME cybersecurity, supporting more effective, culturally sensitive interventions.

7. CONCLUSION

As a concluding reflection, this study demonstrates that cybersecurity decision-making in ethnic minority-owned SMEs is not merely a technical or managerial task; it is a complex, socially embedded, and culturally influenced practice. Entrepreneurs navigate digital risks through a combination of lived experience, trust in personal and professional networks, and culturally shaped judgments about responsibility and feasibility. The findings highlight that protective behavior emerges from interactions among individual capabilities, social relationships, and contextual conditions, producing patterns that are adaptive, iterative, and context specific. Also, the refined socio-cultural framework shows that cybersecurity is best understood not as a linear process or a checklist of technical measures, but as a dynamic, relational, and human-centered activity. Effective interventions, therefore, must engage with entrepreneurs' social environments, leverage trust and community networks, and align with cultural values, rather than focusing solely on compliance or technology.

Ultimately, by foregrounding these socio-cultural dimensions, this research shifts the perspective on SME cybersecurity toward a more nuanced, lived understanding of risk, decision-making, and protection. It provides a conceptual lens for scholars and practical guidance for policymakers and advisors, emphasizing that meaningful cybersecurity adoption depends as much on relationships, learning, and social context as it does on tools and resources. In this way, the study lays the groundwork for interventions that are both culturally sensitive and practically effective, while inviting further exploration of how socio-cultural mechanisms shape digital resilience in diverse small business settings.

REFERENCES

Adeoye-Olatunde, O. A., & Olenik, N. L. (2021). Research and scholarly methods: Semi-structured interviews. *Journal of the American College of Clinical Pharmacy, 4*(10), 1358-1367.

Anderson, R., & Moore, T. (2006). The economics of information security. *Science, 314*(5799), 610-613.

Brunetto, Y., & Farr-Wharton, R. (2007). The moderating role of trust in SME owner/managers' decision-making about collaboration. *Journal of Small Business Management, 45*(3), 362-387. https://doi.org/10.1111/j.1540-627X.2007.00218.x

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review, 14*(4), 532-550. https://doi.org/10.5465/amr.1989.4308385

European Union Agency for Cybersecurity (ENISA). (2021). *Cybersecurity for SMEs: Challenges and recommendations*. Retrieved from Publications Office of the European Union:

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational Research Methods, 16*(1), 15-31. https://doi.org/10.1177/1094428112452151

Granovetter, M. (1985). Economic action and social structure: The problem of embeddedness. *American Journal of Sociology, 91*(3), 481-510. https://doi.org/10.1086/228311

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165. https://doi.org/10.1016/j.dss.2009.02.005

Hsieh, H.-F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research, 15*(9), 1277-1288.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007

Kahneman, D. (2003). A perspective on judgment and choice: Mapping bounded rationality. *American Psychologist, 58*(9), 697–720. https://doi.org/10.1037/0003-066X.58.9.697

Kloosterman, R., Van der Leun, J., & Rath, J. (1998). Across the border: Immigrants' economic opportunities, social capital and informal business activities. *Journal of Ethnic and Migration Studies, 24*(2), 249-268. https://doi.org/10.1080/1369183X.1998.9976632

Krippendorff, K. (2018). *Content analysis: An introduction to its methodology* (4th ed.). Thousand Oaks, CA: SAGE Publications.

Light, I., & Gold, S. J. (2000). *Ethnic economies*. San Diego, CA: Academic Press.

March, J. G. (1994). *A primer on decision making: How decisions happen*. New York: Free Press.

Milne, J., & Oberle, K. (2005). Enhancing rigor in qualitative description: A case study. *Journal of Wound, Ostomy and Continence Nursing*, *32*(6), 413–420. https://doi.org/10.1097/00152192-200511000-00014

Mmango, N., & Gundu, T. (2024). *Cultivating collective armor: Towards a collaborative cybersecurity resilience framework for SMEs*. Paper presented at the European Conference on Innovation and Entrepreneurship (pp. 523-531). Academic Conferences International Limited.

Ponemon Institute. (2020). *Cost of a data breach report 2020. IBM Security*. Retrieved from https://www.ibm.com/security/data-breach

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 757-778. https://doi.org/10.2307/25750704

Ram, M., & Jones, T. (2008). Ethnic-minority businesses in the UK: A review of research and policy developments. *Environment and Planning C: Government and Policy*, *26*(2), 352-374. https://doi.org/10.1068/c0722

Renaud, K., & Weir, G. R. S. (2016). *Cybersecurity and cyberwar: What everyone needs to know*. New York: Oxford University Press.

Shepherd, D. A., & Suddaby, R. (2017). Theory building: A review and integration. *Journal of Management*, *43*(1), 59-86. https://doi.org/10.1177/0149206316647102

Simon, H. A. (1957). Background of decision making. *Naval War College Review*, *10*(3), 1-24.

Tetteh, A. K. (2024). Cybersecurity needs for SMEs. *Issues in Information Systems*, *25*(1), 235–246. https://doi.org/10.48009/1_iis_2024_120

Waldinger, R., Aldrich, H., & Ward, R. (1990). *Ethnic entrepreneurs: Immigrant business in industrial societies*. Newbury Park, CA: SAGE Publications.

Appendix 1. Characteristics of cited participants.

…	Business history	Type of business	Age	Gender	Nationality	Education	Canadian experience	Previous job	# of employees	City
1	2	Consultancy Owner	68	Male	Persian	Bachelor's degree	No	Lawyer	1	Longueuil
2	5	Grocery store	45	Female	Chinese	College certificate	Yes	Seeler and Cashier	3	Longueuil
3	4	Bakery	43	Male	Afghani	Secondary school	No	Construction	5	Longueuil
4	2	Electronics Shop Owner	32	Male	Pakistani	University certificate	No	Student	2	Longueuil
5	3	Pastry	44	Male	Lebanese	College certificate	No	Pastry maker	6	Montreal
6	8	Small Retail Shop Owner	50	Male	Chinese	Secondary school	Yes	Grocery	5	Montreal
7	11	Beauty Salon Owner	51	Male	Moroccan	University certificate	Yes	Construction	3	Longueuil
8	13	Exchange office	54	Female	Romanian	Bachelor's degree	No	Money changer	5	Sain-Laurant
9	12	Exchange office	52	Male	Iranian	Bachelor's degree	No	Bank clerk	3	Montreal
10	9	Restaurant	47	Male	Arab	College certificate	Yes	Employee	8	Sain-Laurant
11	17	Online Retailer	54	Male	Taivan	Secondary school	No	General worker	6	Montreal
12	7	Clothsing retailer	51	Female	Moroccan	College certificate	No	General worker	2	Montreal
13	15	Cleaning Services Owner	63	Female	Haitian	College certificate	Yes	General worker	7	Montreal
14	18	Food supplier	63	Female	Jamaican	University certificate	Yes	Immigrant services	9	Montreal
15	4	Café Owner	38	Male	Algerian	Bachelor's degree	No	Computer technician	3	Montreal
16	8	Fashion Business	45	Female	Marconian	Bachelor's degree	Yes	Designer	2	Montreal
17	16	Import/Export Business	57	Male	Iranian	College certificate	No	Employee	6	Montreal
18	7	Electrician	54	Male	Egyptian	College certificate	Yes	Electrical technician	3	Longueuil
19	3	Hair Salon Owner	37	Female	Tunisian	College certificate	Yes	Beauty technician	5	Sherbrooke
20	5	Online Craft Seller	50	Female	Iranian	Bachelor's degree	No	Employee	1	Montreal

Appendix 2. Interview guide.

Introduction and Purpose

This interview explores how ethnic minority entrepreneurs make decisions about cybersecurity in their businesses, including how they perceive risks, manage digital tools, and respond to cyber threats. The goal is to understand participants' experiences, strategies, and the factors that influence their decisions.

Participation is completely voluntary, and participants may choose not to answer any question or stop the interview at any time without any consequence. All information provided will be kept strictly confidential, and any reporting of results will ensure that participants cannot be personally identified. Participants are encouraged to share their perspectives openly; there are no right or wrong answers.

Section 1: Entrepreneurial and Business Background

(Objective: understand personal and business context)

1. Can you tell me about your background and how you started your business?
2. What motivated you to become an entrepreneur?
3. Can you describe your previous work or business experience, including before or after migration?
4. How would you describe your familiarity with digital tools and technologies used in your business?
5. What type of business do you operate (sector, size, number of employees, years in operation)?
6. Demographic/contextual details:

- Age, ethnicity, country of origin, mother tongue.
- Proficiency in English or French.
- Level of education.
- Residency or migration status.
- Previous entrepreneurial experience.

Section 2: Experiences and Practices Related to Cybersecurity

(Objective: explore knowledge, behaviors, and challenges)

1. How would you describe your understanding of cybersecurity?
2. Have you ever experienced or heard of cyber incidents (e.g., hacking, phishing, data breaches)?
3. How do you perceive cyber risks to your business?
4. What actions or strategies do you take to protect your digital assets?
5. What challenges or barriers do you face in managing cybersecurity?
6. How do you decide which cybersecurity practices to adopt?

Section 3: Interactions and Support

(Objective: examine the role of others and social influence)

1. Do you discuss cybersecurity issues with family, friends, peers, or business contacts?
2. How does advice or guidance from others affect your choices?
3. Are there examples where discussions with others influenced your actions or decisions?
4. How do observations of others' practices influence your own decisions?

Section 4: Environmental and Contextual Considerations

(Objective: explore broader conditions influencing decisions)

1. Are there aspects of your cultural or community environment that influence how you manage cybersecurity?
2. Do language or communication challenges affect your ability to access or understand cybersecurity information?

3. How does access (or lack of access) to training, guidance, or institutional support influence your decisions?
4. How do your experiences as a migrant or member of an ethnic minority affect how you view and respond to cyber risks?
5. Are there community-based resources or programs that support your cybersecurity practices?

Section 5: Reflections and Closing

(Objective: Provide opportunity for participants to summarize or add insights)

1. In your view, what does "good cybersecurity" mean for a small business like yours?
2. What advice would you give to other entrepreneurs from your community regarding cybersecurity?
3. Is there anything else you would like to add about your experiences or decision-making regarding cybersecurity?

Notes for Interviewer:

- Interviews should last approximately 45–60 minutes.
- Questions are open-ended and flexible, with follow-up prompts as needed.
- The interviewer may adapt the sequence or wording to maintain a conversational flow.